МВС України
Харківський національний університет внутрішніх справ
Громадська спілка «Глобальний центр взаємодії в кіберпросторі»

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

Збірник матеріалів
Міжнародної науково-практичної конференції
(м. Харків, 18 травня 2021 року)

Харків
2021

УДК [351.74:004](477)(08)
П83

Друкується згідно з рішенням оргкомітету
за дорученням Харківського національного університету внутрішніх справ
від 17.03.2021 № 46

Протидія кіберзлочинності та торгівлі людьми : зб. матеріалів міжнарод. П83 наук.-практ. конф. (м. Харків, 18 травня 2021 р.) / МВС України, Харків. нац. ун-т внутр. справ ; ГС «Глобальний центр взаємодії в кіберпросторі». – Харків : ХНУВС, 2021. – 92 с.

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

УДК [351.74:004](477)(08)

Матеріали викладені в авторській редакції з незначними коректорськими правками.
Відповідальність за точність поданих фактів, цитат, цифр і прізвищ несуть автори.

Електронна копія збірника безоплатно розміщується у відкритому доступі на сайті Харківського національного університету внутрішніх справ (http://www.univd.edu.ua) у розділі «Наука», сторінка «Конференції, семінари, та круглі столи»), а також у репозитарії ХНУВС (http://dspace.univd.edu.ua/xmlui/).

ЗМІСТ

Вітальне слово 7

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

Сокуренко В. В.

Практична складова фахової професійної підготовки кадрів для підрозділів кіберполіції Національної поліції України 8

Швець Д. В.

Побудова інформаційної моделі формування соціального портрета особистості за допомогою технології OSINT 9

Бандурка О. М.

Доінтернетний період розвитку комп'ютерних технологій У підрозділах МВС 11

Гусаров С. М.

Профілактична робота щодо недопущення порушень під час проведення навчальних занять з використанням інтернет-платформи відеоконференцзв'язку Zoom 12

Бортник С. М.

Аналіз сучасних тенденцій консолідації інформації в групах користувачів для Національної поліції України 14

Бурдін М. Ю.

Використання технологій IoT в охоронних системах технічного захисту 15

Могілевський Л. В.

Кіберзлочинність у проєкті Європолу SOCTA 16

Вінцук В. В.

Торгівля людьми та транснаціональна злочинність 18

Заворіна М. А.

Проблемні питання правового регулювання та запровадження обігу криптовалюти 20

Іващенко В. А.

Реалізація основних напрямів державної політики у сфері протидії торгівлі людьми 22

Козар А. В.

Соціальна інженерія як спосіб шахрайства 24

Коростельова Л. А.

Штучний інтелект у протидії кібератакам
в умовах глобальної пандемії 25

Коршенко В. А.

Законодавче врегулювання обігу криптовалюти в Україні 26

Maftea S., Vrabie C.

Использование даркнета в преступных целях 28

Пампура І. І., Остапович І. П.

Деякі загрози негативного впливу соціальних мереж
на особистість дитини 30

Тимченко Л. Л.

Ransomware: хакерські «пустощі» чи елемент гібридної війни?
Погляд GC3 32

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

Бурак М. В., Шевчук О. Ю.

Використання комп'ютерно-технічної експертизи
в розкритті кіберзлочинів 35

Єрмоленко Б. С., Клімушин П. С.

Кібербулінг в соціальних мережах: виховна робота з дітьми
та підлітками 36

Ковтун В. О., Рвачов О. М.

Щодо проблеми оцінки вартості інформації 38

Лизогубенко Є. В.

Детермінанти кіберзлочинності 40

Можаєв М. О.

Підвищення показників ефективності інформаційної системи судової
експертизи за рахунок застосування вейвлет-перетворень 42

Olber P.

The role and importance of computer forensics in combating cybercrime 44

Орлов Р. Р., Онищенко Ю. М.

Виявлення підозрілих фінансових операцій, які можуть бути пов'язані з
відмиванням доходів, отриманих у сфері кіберзлочинності 46

Перець О.В., Онищенко Ю. М.

Використання віртуальних банківських карток,
як захід протидії шахрайським діям 47

Політова А. С.

Стаття 149 Кримінального кодексу України: чи нагальна потреба удосконалення? 48

Саєнко Д. Л., Онищенко Ю. М.

Види кіберзлочинів та способи захисту від них 50

Фіалка М. І.

Сутність поняття «інформації» в Розділі XVI Кримінального кодексу України та її вплив на кваліфікацію суспільно небезпечного діяння 52

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

Водяницький К.Ю.

Технологія блокчейн в роботі правоохоронних органів 54

Гнусов Ю. В., Калякін С. В.

Про деякі проблеми виявлення шкідливого програмного забезпечення 55

Горелов Ю. П., Амельницька А. М.

Моделі та структура штучних нейронних мереж 57

Liqiang Zh., Weiling C., Semenov S.

Analysis and comparative research of the main approaches to the mathematical formalization of the penetration testing process 58

Демидов З. Г.

Найвідоміші хакери світу 59

Загорецька Э. Л., Світличний В. А.

Деякі аспекти протидії кіберзлочинам в Україні 60

Клімушин П. С., Спасібов Д. В.

Технології для забезпечення безпеки інтернет-речей 61

Колісник Т. П., Ющенко Я. В.

Актуальні проблеми кібербезпеки: небезпека соціальної інженерії в кіберпросторі 63

Манжай О. В., Манжай І. А.

Що таке кібергігієна? 65

Можаєв О. О., Звірянський Г. В.

Використання нечітких критеріїв під час побудови соціального профілю 67

Можаєв О. О., Пересічанський В. М., Рог В. Є.

Аналіз використання ґрід-мереж для потреб Національної поліції України 69

Мордвинцев М. В., Хлєстков О. В., Ницюк С. П.

Тенденції світового розвитку систем відеоспостереження задля забезпечення публічної безпеки 71

Носов В. В., Манжай О. В.

Зміст та методологія практичного навчання з питань кібергігієни 72

Орлов Р. Р., Грищенко Д. О.

Основні тренди у сфері кібербезпеки з захисту банківських платежів 74

Тулупов В. В.

Використання методів соціальної інженерії для отримання інформації шахрайським шляхом 75

Semenov S., Liqiang Zh., Weiling C.

The software security testing first stage mathematical model 77

Соляник Т. М., Большов Р. С.

Технологія blockchain як один з сучасних методів захисту інформації 78

Струков В. М., Гуділін В. В.

Захист від атак підвищення привілеїв в корпоративних інформаційних системах 79

Чугай А. М., Шеховцов С. Б., Яськов Г. М.

Застосування паралельних обчислень в задачах оптимізації інформаційних систем 83

РОЗДІЛ 4.
МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

Войціховський А. А.

Діяльність Ради Європи у протидії торгівлі людськими органами 85

Макаренко В. С., Макаренко П. В.

Торгівля людьми як суспільно-небезпечне соціальне явище в Південно-Африканській Республіці 87

Мовчан А. В.

Діяльність міжнародних правоохоронних і безпекових організацій щодо координації зусиль у сфері протидії торгівлі людьми 88

Оставчук Д., Руснак К.

Политика Республики Молдова в области предотвращения торговли людьми 90

ВІТАЛЬНЕ СЛОВО

ректора Харківського національного університету внутрішніх справ,
доктора юридичних наук, професора, члена-кореспондента
Національної академії правових наук України, заслуженого юриста України,
генерала поліції третього рангу
Валерія Васильовича Сокуренка

Шановні учасники конференції!

Від імені ректорату та Вченої ради Харківського національного університету внутрішніх справ вітаю вас із початком Міжнародної науково-практичної конференції «Протидія кіберзлочинності та торгівлі людьми».

Керівництво держави, МВС України та Національної поліції приділяє велику увагу проблемам протидії кіберзлочинності і торгівлі людьми.

Тематика наукового заходу є надзвичайно актуальною для нашого суспільства.

На сьогодні кібербезпека є одним із пріоритетів у системі національної безпеки України. Для забезпечення кібербезпеки нашої держави необхідно створити умови безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, своєчасно попереджувати можливі кібератаки на об'єкти критичної інфраструктури держави тощо.

14 травня 2021 р. Рада національної безпеки та оборони України затвердила Стратегію кібербезпеки України на 2021–2025 роки, яка дозволяє фінансувати і здійснювати заходи в цьому напрямі, покращувати ту ситуацію, в якій перебуває Україна.

Із розвитком інтернет-простору набирає обертів кіберзлочинність. Особливо чітко це відчувалося під час карантину, коли в «онлайн» масштабно перейшли робота, покупки, зустрічі та навчання.

За 2020 р. в Україні було зареєстровано понад 5 тисяч кіберзлочинів, у процесі розслідування яких правоохоронцям вдалося оперативно затримати більше 100 фігурантів кримінальних проваджень, серед яких – 13 педофілів. Матеріальні збитки від дій кібершахраїв становлять 241 мільйон гривень.

Говорячи про протидію торгівлі людьми, необхідно зазначити, що в 2020 р. МВС України було розроблено Концепцію посилення системи протидії торгівлі людьми, відповідно до якої в Національній поліції України Департамент протидії торгівлі людьми було переформатовано в Департамент міграційної поліції і призначено нового його керівника, а також відбулася зміна ключових напрямів роботи департаменту.

Отже, висвітлені під час конференції проблемні питання та спільне їх вирішення є перспективними для покращення рівня протидії кіберзлочинності та торгівлі людьми в умовах сьогодення.

Науково-теоретичне та практичне значення конференції зумовлюється передусім проблематикою питань, винесених на обговорення, що представлено в чотирьох основних напрямах роботи конференції.

До організаційного комітету для включення до збірника конференції було надіслано 50 тез наукових доповідей 72 авторів, серед яких представники Молдови, Польщі та Китайської народної республіки, а також вітчизняні учені, практики, курсанти і студенти.

Сподіваюся, що конференція стане міцною платформою для висловлення учасниками власного бачення напрямів розвитку процесу підготовки правоохоронців у нашій державі, обміну досвідом між науковцями, практичними працівниками та їх колегами з інших країн, а потужний науковий потенціал учасників сприятиме досягненню поставленої мети.

Бажаю всім плідної роботи, творчого натхнення, здоров'я, миру та добра.

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

УДК 342:343.346.8
СОКУРЕНКО Валерій Васильович,
доктор юридичних наук, професор,
член-кореспондент Національної академії правових наук України,
заслужений юрист України,
ректор Харківського національного університету внутрішніх справ
https://orcid.org/0000-0001-8923-5639

ПРАКТИЧНА СКЛАДОВА ФАХОВОЇ ПРОФЕСІЙНОЇ ПІДГОТОВКИ КАДРІВ ДЛЯ ПІДРОЗДІЛІВ КІБЕРПОЛІЦІЇ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

На сьогодні незмінною залишається тенденція останніх років у напрямі збільшення кількості та масштабності правопорушень у кіберсфері. За даними експертів, щорічні збитки від кіберзлочинів також стрімко зростають. Так, дослідники американської компанії McAfee, яка спеціалізується на комп'ютерній безпеці, та Центру стратегічних і міжнародних досліджень (CSIS) установили, що у 2020 році хакери завдали світовій економіці збитки у розмірі понад трильйон доларів, або 820 мільярдів євро, що становить понад один відсоток світового ВВП. Завдані цьогоріч хакерами збитки є на 50 відсотків вищими, ніж у 2018 році.

Ураховуючи той факт, що цифровізація світового суспільства також швидко набирає обертів, у найближчому майбутньому не слід очікувати стабілізації або зменшення темпів росту кіберзлочинності. Із цього випливає актуальність застосування всіх можливих факторів підвищення якості підготовки майбутніх кіберполіцейських.

Найважливішим чинником підготовки кіберполіцейських є практична складова навчання. Компонентами цієї складової у їх підготовці є такі: а) фахова практична спрямованість навчальних практичних і лабораторних занять, яка полягає у вирішенні практичних завдань професійної діяльності кіберполіцейських; б) рішення фахових завдань практичного спрямування в процесі написання курсових робіт, а також випускної кваліфікаційної роботи; в) отримання професійних практичних навичок під час навчальної практики.

Крім перелічених обов'язкових компонентів, які передбачено навчальними планами підготовки, важливу роль відіграють інші, нерегламентовані форми неформального залучення курсантів та викладачів до співробітництва з практичними органами у сфері протидії кіберзлочинності. У ХНУВС були запроваджені й результативно застосовуються такі форми залучення курсантів та викладачів:

– моніторинг кіберпростору з метою сприяння діяльності Департаменту кіберполіції та Департаменту кримінального аналізу НПУ в межах функціонування Центру боротьби з кіберзлочинністю та моніторингу кіберпростору ХНУВС;

– відпрацювання практичних навичок виявлення кібератак і реагування на них на тренінгових платформах Центру боротьби з кіберзлочинністю та моніторингу кіберпростору ХНУВС;

– співробітництво з громадською спілкою «Глобальний центр взаємодії кіберпростору» з метою сприяння вирішенню завдань з профілактики і запобігання онлайн-шахрайству, встановлення осіб кіберзлочинців та їх місцезнаходження;

– участь у проведенні тренінгів під егідою КМЕС та ОБСЄ для фахівців у сфері кібербезпеки та протидії торгівлі людьми як т'юторів;

– участь курсантів і викладачів у міжнародних тренінгових онлайн-платформах для фахівців у сфері кібербезпеки.

До особливостей застосування перелічених вище форм практичної підготовки можна віднести такі.

1. Високі вимоги до параметрів технічного забезпечення використовуваної комп'ютерної і комунікаційної техніки і, відповідно, її висока вартість.

2. Обмежені функціональні можливості безкоштовних тренінгових платформ і висока вартість розвинутих багатофункціональних тренінгових платформ.

3. Необхідність урахування вітчизняних і особливо міжнародних нормативних актів у галузі захисту персональної інформації під час моніторингу кіберпростору (здійснення заходів OSINT) для запобігання їх порушенням.

4. Відсутність (наразі) можливості практичного знайомства із сучасними платформами автоматичного моніторингу кіберпростору в режимі 24/7 для виявлення і прогнозування злочинної активності на основі «слабких сигналів».

Одержано 07.04.2021

УДК 004.04:004.67:004.77

ШВЕЦЬ Дмитро Володимирович,
доктор юридичних наук, доцент, заслужений працівник освіти України,
перший проректор Харківського національного університету
внутрішніх справ
https://orcid.org/0000-0002-1999-9956

ПОБУДОВА ІНФОРМАЦІЙНОЇ МОДЕЛІ ФОРМУВАННЯ СОЦІАЛЬНОГО ПОРТРЕТА ОСОБИСТОСТІ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ OSINT

Зараз з урахуванням бурхливого розвитку інформаційних технологій і соціальних процесів гостро стоїть проблема ефективного виконання управлінських завдань та ухвалення рішень під час роботи з великими неструктурованими гетерогенними масивами даних на основі соціального портрета особистості. Це пов'язано зі значним ускладненням як первинних даних, так і структури керуючих інформаційних систем. Аналогічні проблеми є і в структурах кримінального аналізу Національній поліції України. Тому пошук шляхів їх вирішення є досить актуальним завданням.

Для моделювання та дослідження таких систем наразі широке застосування отримала OSINT (англ. – Open Source INTelligence) – концепція, методологія і технологія легального отримання і використання інформації з відкритих джерел.

Пошук за відкритими джерелами (OSINT) – процес, під час якого здійснюються виявлення, вибір, збір та аналіз інформації, що перебуває у вільному доступі, та може дозволити істотно підвищити ефективність систем ухвалення управлінських рішень.

Методика роботи за принципами OSINT вже тривалий час активно використовується в бізнес-колах провідних країн світу для пошуку й отримання законними шляхами інформації про партнерів або конкурентів. Одним із базових «золотих правил» такої концепції є те, що близько 90 % інформації, необхідної для аналізу й ухвалення відповідних рішень, розміщено у відкритих джерелах.

На тлі стрімкого розвитку сучасних інформаційних технологій цьому виду пошукової діяльності приділяється дедалі більше уваги. Різниця між новачком, який шукає в інтернеті інформацію, та OSINT-продажем є досить помітною: там, де початківець побачить фото, репости, групи і сторінки, на які підписані людина або організація в соціальній мережі, фахівець побачить активність, дати публікацій, тло на фотографіях, можливі причини підписки на певні групи та кола спілкування. Найчастіше людина використовує один або кілька псевдонімів у мережі, а значить, за знайденим нікнеймом через запит можна знайти й іншу її

активність в інтернеті, наприклад у соціальній мережі або на форумах, які вона відвідує. І це лише кілька прикладів. При цьому зібрана інформація служить основою для подальшої обробки, очищення (шляхом оцінювання надійності джерел отримання та достовірності відомостей), аналітичного узагальнення та інтерпретації кінцевих результатів.

Отже, базова ідея OSINT – це цілеспрямований збір інформації (Harvesting) про об'єкт зацікавленості з метою подальшої обробки та різновекторного контент-аналізу отриманих даних (створення «портрета» особистості, виявлення неочевидних фактів або зв'язків, прогноз її поведінки тощо).

OSINT зручний тим, що:

– передбачає набагато менше ризиків: не порушуються чиясь приватність і закони;

– ця технологія є дешевшою – не потрібні якесь додаткове обладнання і дорогий софт;

– до такої інформації легко отримати доступ (зайти в мережі Інтернет), і частіше за все вона є завжди актуальною.

Існує два основні методи збору інформації.

1. Пасивний. У цьому разі шукачу інформації неможливо видати себе і те, що він шукає. Пошук обмежується контентом на сайті об'єкта дослідження, архівною або кеш інформацією, незахищеними файлами.

2. Активний. Цей метод використовується для інтернет-розвідки набагато рідше. Для отримання інформації досліджується IT-інфраструктура компанії, здійснюється активна взаємодія з комп'ютерами і машинами. Використовуються просунуті техніки для отримання доступу до відкритих портів, сканування уразливостей і серверних вебдодатків. У цьому разі інформаційну розвідку можна легко розпізнати. Соціальна інженерія теж належить до цього.

Тому використання технології OSINT для побудови соціальних портретів різного ступеню диференціації є досить актуальним завданням, вирішенню якого присвячено ці дослідження.

Соціальний портрет являє собою інформаційну структуру, що описує соціальні властивості окремої людини чи спільноти, причому ця інформація має властивість ясності для людиномашинного сприйняття, що забезпечує можливість її автоматизованої обробки в різних прикладних завданнях.

Виходячи з визначення, соціальний портрет являє собою неоднорідну семантичну мережу, що складається з персоналізованих даних. На інформаційній моделі соціального портрету ґрунтуються модель соціального середовища і методика рішення завдання побудови соціальних портретів.

Описи соціальних явищ є важливими для цілісного уявлення про соціальне середовище й окремі соціальні портрети: найчастіше в соціальних дослідженнях вони можуть виявитися в безлічі центральних об'єктів. Соціальні явища мають низку властивостей:

– час і місце виникнення;

– список учасників визначення характеристик явища;

– посилання на джерела інформації, що підтверджують факт здійснення явища;

– пов'язані інші соціальні об'єкти і явища.

У завданнях управління соціальні явища представлено громадськими подіями і заходами, інноваційними впровадженнями, законодавчими ініціативами тощо. Відповідно до теорії елементи соціального портрета, виражені характеристиками, поняттями, подіями та явищами, являють собою актанти, а соціальні зв'язки між елементами – предикати.

Результати побудови соціального портрета є структурованими даними, виділеними з динамічного контенту і пов'язаними з інформаційної картою в процесі аналізу. Вони являють собою безмасштабну мережу, яка для подання і подальшого використання аналітиками має зберігатися в базах даних, здатних зберігати графи і слабо структуровані відомості. Тому їх використання дозволить покращити результати моніторингу кримінальної обстановки в Україні.

Одержано 22.04.2021

УДК 343.43+004
БАНДУРКА Олександр Маркович,
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
https://orcid.org/0000-0002-0240-5517

ДОІНТЕРНЕТНИЙ ПЕРІОД РОЗВИТКУ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ У ПІДРОЗДІЛАХ МВС

У 1970-ті рр. більшість правоохоронців розглядали комп'ютери більше як забаганку керівництва, але найбільш далекоглядні працівники вже бачили суттєвий потенціал у впровадженні технологій. У цей період за підтримки тодішнього керівництва союзного Міністерства внутрішніх справ у міністерствах республік було створено декілька обчислювальних центрів, які назвали зональними. Велику роботу в напрямку інформатизації органів внутрішніх справ тоді виконав Український інститут кібернетики. Спочатку було створено 11 відповідних центрів у великих містах, серед них три в Україні (мм. Київ, Луганськ (тоді Ворошиловград) та Дніпропетровськ (нині Дніпро)). Їх обладнали машинами Мінськ-32, які записували інформацію на магнітні стрічки (у подальшому ЕС-1020 із магнітними дисками на 3 Мегабайти).

У м. Київ обладнали центр, оскільки це була столиця, у Дніпропетровську (нині Дніпро) – як на батьківщині тодішнього генсека, а от у Луганську цим процесом був дуже зацікавлений тодішній начальник главку, який побачив перспективу в нових технологіях та серйозно підтримував цей процес, безпосередньо взаємодіючи з Інститутом кібернетики.

Для оперативно-розшукових потреб в центрах було передбачено використання розрахунково-аналітичних машин. Для господарчих потреб використовувались машино-розрахункові станції. Координувалася вся ця діяльність штабом Міністерства та Головним інформаційно-обчислювальним центром МВС. Основними завданнями центрів були довідково-інформаційні, спрямовані на вирішення оперативних та штабних завдань. При цьому стрічки, на які записувалася інформація, були дуже довгі – більше кілометра, відтак для того, щоб дістатися, якихось конкретних даних доводилося чекати, доки цю стрічку перемотають.

Складністю запровадження програмного забезпечення саме в МВС було те, що не можна було адаптувати відповідні програми з інших міністерств, як це робили для інших відомств. Наприклад, в машинобудівних міністерствах розв'язувались переважно обчислювальні задачі, а в МВС була зовсім інша специфіка. Тому доводилось розробляти програми для потреб правоохоронних органів з нуля. В обчислювальних центрах МВС України першою запровадили інформаційну систему «Розшук», яка дозволила суттєво скоротити час пошуку інформації про розшукуваних осіб за непрямими ознаками. Також згодом запрацювала кадрова система, контролю доручень тощо. Вже тоді почали організовувати зв'язок між обласними та центральними банками даних. Щоправда важливі короткі повідомлення передавалися телетайпом, а великими об'ємами даних обмінювалися на перфострічках за допомогою поштового зв'язку.

У Харківській міліції Інформаційний центр вперше відкрили у 1976 році та укомплектували його електронно-обчислювальними машинами ЄС-1033. До 1979 року працівники центру здійснювали первинне накопичення даних, передусім для системи «Розшук». Спочатку основним носієм інформації в центрі були перфострічки, згодом їх замінили перфокарти, а вже у 1990-ті роки перейшли на дискети та ZIP-диски. Поступово ближче до середини 1990-х років в міліції вже почали застосовувати мережні технології. У якості лінії зв'язку всередині області переважно використовувалися телефонні лінії, а між Главком та обласним управлінням було прокладено окрему виділену лінію. Процес передачі файлів забезпечувався за допомогою модемів та вже нових серверних і персональних комп'ютерів. Уже тоді була цілком очевидною перспектива, яку надаватиме обмін цифровою інформацією на великі відстані в режимі реального часу.

Одержано 06.04.2021

УДК 378.147+37.018.4:343.592
ГУСАРОВ Сергій Миколайович,
заслужений юрист України, доктор юридичних наук, професор,
професор кафедри адміністративного права та процесу факультету № 1
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0002-8136-0694

ПРОФІЛАКТИЧНА РОБОТА ЩОДО НЕДОПУЩЕННЯ ПОРУШЕНЬ ПІД ЧАС ПРОВЕДЕННЯ НАВЧАЛЬНИХ ЗАНЯТЬ З ВИКОРИСТАННЯМ ІНТЕРНЕТ-ПЛАТФОРМИ ВІДЕОКОНФЕРЕНЦЗВ'ЯЗКУ ZOOM

Використання дітьми та дорослими сучасних інформаційних технологій і засобів комунікації несе не тільки поліпшення і полегшення, але і створює певні ризики і загрози, через те, що різного роду зловмисники теж використовують інформаційні технології для вчинення протиправної діяльності [1, с. 151].

На початку 2020 року у всьому світі через глобальну пандемію масово почали проводити дистанційні заняття з використанням спеціальних інтернет-платформ відеоконференцзв'язку, у тому числі «Zoom» (https://zoom.us/).

Під час проведення дистанційних занять деякі з їх учасників почали зривати проведення цих заходів. Такі дії було названо зумбомбінг (англ. zoombombing), або зум-тролінг – атака на онлайн-захід з метою зірвати його або хоча б збентежити його учасників [2].

Проблема стосується не тільки платформи «Zoom», але й інших платформ, які використовують інтернет-користувачі для відеоконференцій.

До переліку негативних дій, які можуть скоювати учасники онлайн-заходу можна віднести:

1) вигукування нецензурних слів, образ на адресу учасників заходу або його організатора (наприклад, вчителя);

2) відтворення звукових файлів, у тому числі із нецензурними словами;

3) демонстрація відеофрагментів, у тому числі порнографічних;

4) надсилання у публічний та приватні чати образливих повідомлень;

5) малювання на екрані демонстрації написів, у тому числі із нецензурними словами та зображеннями;

6) зміна віртуального фону на своїх відеотрансляціях;

7) «одягання віртуальних костюмів» на себе;

8) підписування у відеоконференції чужими іменами, в тому числі іменами «легальних учасників заходу».

Такі дії зумбомберів (кібертролів) можна кваліфікувати як:

– дрібне хуліганство;

– булінг;

– поширення порнографії.

Доволі часто зумбомбер фіксує свої дії за допомогою програмного забезпечення для захоплення екрану та потім або розсилає цей відеозапис серед своїх знайомих, або публікує його у соціальних комп'ютерних мережах.

На сьогодні в інтернеті існують інтернет-ресурси, що присвячені саме зумбомбінгу.

Під час проведення онлайн-заходів вчиняють хуліганські дії:

1) «легітимні» учасники онлайн-заходу;

2) сторонні особи, які отримають дані (посилання) для підключення до онлайн-заходу:

– від «легітимних» учасників заходу;

– самостійно знаходять на публічних ресурсах установ (вебсайті або сторінці у соціальних комп'ютерних мережах), у тому числі за допомогою пошукових інтернет-сервісів (наприклад, Google);

– підбирають самостійно.

На початку квітня 2021 року до поліції звернувся педагогічний колектив однієї із загальноосвітніх шкіл, розташованої на території Основ'янського району м. Харків, з проханням

провести перевірку щодо неодноразового зриву дистанційних занять через інтернет-платформу для проведення відеоконференцій.

Під час перевірки правоохоронці ГУНП в Харківській області встановили особу школяра, який надавав доступ до навчання іншим особам, які заважали проводити відеоконференції.

З порушником та його батьками провели профілактичну бесіду. Відносно батьків хлопця складено адміністративний протокол за ст. 184 (невиконання батьками, або особами, що їх замінюють, обов'язків щодо виховання дітей) Кодексу України про адміністративні правопорушення [3].

Пропонується дотримуватися наступних рекомендації для забезпечення безпеки відеоконференції у Zoom:

1. Не ділитися у соціальних мережах гіперпосиланням на захід у Zoom або ID заходу.
2. Створювати унікальний ідентифікатор для кожного онлайн-заходу.
3. Зробити захід приватним, призначити ко-модератора.
4. Встановити пароль для зустрічі.
5. Використовувати функцію «зал очікування».
6. Зробити всі можливі функції неактивними для учасників заходів.
7. Відключити можливість залишати коментарії учасниками заходу.
8. Відключити чат.

З метою недопущення та зменшення випадків порушень під час проведення навчальних занять з використанням інтернет-платформ відеоконференцзв’язку учасникам освітнього процесу рекомендується:

1) організаторам відеоконференції (вчителям) навчитися налаштовувати параметри відеоконференції у відповідності до наданих вище рекомендації [4];

2) періодично доводити до відома учасників освітнього процесу про передбачену відповідальність за вчинення протиправних дій під час участі у відеоконференціях.

Список використаних джерел

1. Зуб Л. В., Рвачов О. М. Сучасні загрози сімейній онлайн безпеці: класифікація та профілактика виникнення // Актуальні питання протидії кіберзлочинності та торгівлі людьми : збірник матеріалів Всеукр. наук.-практ. конф. (23 листоп. 2018 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2018. С. 149-154. URL: http://univd.edu.ua/general/publishing/konf/23_11_2018/pdf/45.pdf (дата звернення: 01.05.2021).

2. Коен О. Що таке «зумбомбінг» та як безпечно використовувати Zoom? // Explainer : вебсайт. 21.04.2020. URL: https://explainer.ua/shho-take-zumbombing-ta-yak-bezpechno-vikoristovuvati-zoom/ (дата звернення: 01.05.2021).

3. Левченко Д. У Харкові школяр зривав дистанційні уроки та опинився у поліції // Gromada Group | Група місцевих ЗМІ Харківщини : вебсайт. 15.04.2021. URL: https://gromada.group/news/news/-7682-u-harkovi-shkolyar-zrivav-distancijni-uroki-ta-opinivsya-u-policiyi (дата звернення: 01.05.2021).

4. У Чугуєві шукали протиотруту «зумбомбінгу» // Громадський простір : вебсайт. 14.04.2021. URL: https://www.prostir.ua/?news=u-chuhujevi-shukaly-protyotrutu-zumbombinhu (дата звернення: 01.05.2021).

5. «Зумбомбінг» або зривання онлайн уроків: що це таке і як уникнути даної проблеми // YouTube : вебсайт. 26.11.2020. URL: https://www.youtube.com/watch?v=j838DpHwOc8 (дата звернення: 01.05.2021).

Одержано 01.05.2021

УДК 004.04:004.67:004.77
БОРТНИК Сергій Миколайович,
доктор юридичних наук, доцент,
проректор Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-5281-6007

АНАЛІЗ СУЧАСНИХ ТЕНДЕНЦІЙ КОНСОЛІДАЦІЇ ІНФОРМАЦІЇ В ГРУПАХ КОРИСТУВАЧІВ ДЛЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Для попередження і запобігання злочинів необхідно мати знання про настрої, наявні у злочинному співтоваристві, а також інформацію про плани, які виношують злочинці. Отримання цієї інформації є дуже складним та багатогранним завданням. Для його вирішення використовуються різноманітні методи побудови соціальних профілів суспільства. При цьому слід зазначити, що недостатньо дослідженими залишаються проблеми застосування комунікативних моделей у межах функціонування соціальних груп, зокрема віртуальних співтовариств, залежно від їх особливостей. Але, на жаль, вони не зовсім задовольняють вимоги, які висуваються до інформації, що аналізується в інформаційній системі Національної поліції. Тому метою досліджень, результати яких надаються у цій доповіді, є аналіз консолідації інформації для побудови соціальних профілів.

Соціальною групою вважається сукупність людей, якій притаманна відносна стійкість. При цьому необхідно зазначити, що люди, які входять до складу соціальної групи, мають спільні інтереси, цінності та поведінкові норми, що формуються в межах історичного розвитку суспільства. У межах кожної із соціальних груп втілено певні взаємозв'язки індивідів як між собою, так і із суспільством в цілому. При цьому необхідно зазначити, що ці взаємозв'язки можуть піддаватися регулюючому впливу як формальних, так і неформальних соціальних інститутів. Залежно від особливостей взаємозв'язків у соціальних групах формуються внутрішньогрупові норми поведінки.

Зокрема, консолідація інформації щодо психологічних характеристик, стратегій поведінки, ролі та статусу користувачів соціальних мереж надає можливість суттєво вдосконалити комерційну діяльність компанії. Зокрема, доцільним є створення системи управління взаємовідносинами з клієнтами CRM (англ. − Customer Relationship Management). Використання такої системи уможливить отримання інформації про клієнтів з різнохарактерних джерел з паралельним усуненням дублювання даних, уніфікацію структури інформації щодо клієнтів до єдиного вигляду та формування вітрин даних про них.

У загальному випадку про соціальні мережі можна говорити в різних аспектах: як про соціальне явище (установлення соціальних зв'язків між людьми), як про універсальний інструмент соціологічного аналізу і, нарешті, як про інтернет-послугу або інтернет-сервіс стосовно побудови соціальної мережі у Всесвітній павутині для одержання соціального капіталу.

Багато сервісів інтернет, що дозволяють людям установлювати зв'язки, автоматично формують соціальні мережі. Відповідно, на певному етапі було створено сервіс, головною метою якого було накопичення соціального капіталу, тобто особистих ділових зв'язків у вигляді соціальної мережі. У результаті з'явився інтернет-сервіс стосовно побудови соціальних мереж.

Аналіз соціальних груп у мережі Інтернет дозволяє одержати інформацію, яка згодом може бути корисною для правоохоронних органів з урахуванням особливостей членів соціальної групи. Однак на сучасному етапі відсутній універсальний метод систематизації такої інформації.

Зв'язок членів соціальної групи в мережі Інтернет можна математично моделювати за допомогою графу, в якому вершини є учасниками соціальної групи, а ребра – відносинами між ними. Математичний апарат аналізу графів дозволяє розрахувати цілу низку параметрів і дати кількісні відповіді на багато питань.

В аналізі соціальних груп у мережі Інтернет на базі теорії графів виділяють:

– розрахунок індексів для соціальної групи в цілому та для окремих членів такої групи;

– виділення підструктур у соціальній групі.

Проте аналіз соціальних груп у мережі Інтернет за допомогою графів можна здійснювати винятково з математичного погляду, без урахування якісних параметрів, що характеризують учасників соціальної групи. Для всебічного аналізу соціальних груп у мережі Інтернет доцільно використовувати системи консолідації інформації.

Системи консолідації даних у соціальних групах у мережі Інтернет дозволять:

– підвищити швидкість доступу до даних соціальних груп;

– забезпечити компактність зберігання інформації щодо учасників соціальних груп;

– автоматично підтримувати цілісність структури даних про членів соціальних груп;

– здійснювати контроль несуперечності даних щодо соціальних груп.

Отже, використання систем консолідації даних для аналізу соціальних груп у мережі Інтернет є оптимальним з погляду їх обробки на конкретній аналітичній платформі та ухвалення відповідних управлінських рішень, орієнтованих на позитивний економічний ефект від комерційної діяльності.

Одержано 16.04.2021

УДК 342:343.346.8

БУРДІН Михайло Юрійович,
доктор юридичних наук, професор,
проректор Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-6748-3321

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ IOT В ОХОРОННИХ СИСТЕМАХ ТЕХНІЧНОГО ЗАХИСТУ

Стрімкий розвиток технологій інтернету речей (Internet of Things – IoT), «розумних міст» (Smart City) і «розумних домів» (Smart House) відкриває принципово нові можливості для правоохоронних структур, зокрема у сфері охоронної безпеки й технічного захисту об'єктів. За даними експертів всесвітнього економічного форуму в Давосі, у наступні десять років понад 80 млрд підключених пристроїв у всьому світі постійно обмінюватимуться даними з людьми й один з одним. Ця величезна мережа взаємодіючих пристроїв докорінно змінить способи виробництва об'єктів, передбачатиме наші потреби і забезпечить нові погляди на світ. Водночас розподілені системи поставлять під сумнів звичні нам способи створення, оцінювання та розподілу даних і цінностей. Повсюдне поширення різних датчиків змінить світ і в інших відносинах. Наприклад, із супермаркетів зникне контрольне обладнання, а в ресторанах швидкого харчування кількість персоналу скоротиться більше ніж наполовину. Потоки даних досягнуть колосальних обсягів, а загрози кібербезпеці стануть предметом повсякденних обговорень.

Використання IoT відкриває найбільші можливості для поліції за всю історію існування інформаційних технологій.

Поєднання технологій IoT з можливостями систем штучного інтелекту обумовлює революційні зміни, зокрема в охоронних системах. І ці зміни вже відбуваються в наш час. Наступні приклади ілюструють реальність цих змін.

У межах науково-технологічних досліджень, які фінансуються Поліцейським науковим фондом Великобританії, компанія LM і лабораторія робототехніки Даремського університету розробили програмно-апаратну систему «Пастка». Система підключається до розумного будинку. У розумному будинку встановлено спеціальні допоміжні штори і передбачено особливий режим функціонування вхідних дверей. Систему програмно підключено до всіх компонентів розумних речей у будинку і, крім того, до прихованих камер, розташованих у кімнатах. Установлено, що режим використання розумних речей господарями є більш-менш стабільним. Також він описується приблизно тими ж само параметрами, коли в будинку опиняються гості. Відповідно, система діє, спостерігаючи за відхиленнями. Якщо в використанні розумних речей помічено відхилення, то вмикаються таємні камери відеоспостереження. Якщо камери фіксують нові обличчя

або людей без облич (в капюшонах тощо), то процесор камери дає команду на ввімкнення надзвичайного режиму роботи штор і вхідних дверей. Одночасно йде сигнал до найближчої поліцейської дільниці. Буквально через хвилину будинок або квартира перетворюються для злочинця на герметично закриту ємність, до якої спрямовується найближчий поліцейський патруль. За ціни комплексу трохи більше 600 фунтів стерлінгів, компанія виробник отримала замовлення тільки по Великобританії більш ніж на 100 тис. подібного роду охоронних систем.

У 2018 році фонд у співпраці з концерном «Мерседес» та Імперським коледжем в Лондоні за участю компанії «Тесла» почав випуск перших в історії захищених від крадіжки автомобілів. Суть винаходу полягає в такому. Фізико хімічному центру Імперського коледжу вдалося створити прозору наноплівку товщиною 0,02 мм, яка виконує роль однофункційного процесора. Зазначена плівка наноситься на будь-яку внутрішню частину автомобіля або будь-якого іншого технічно складного пристрою. Плівка без зарядки дозволяє протягом семи діб передавати точну інформацію про пересування транспортного засобу. Більш того, процесор здатен передавати групу команд, пов'язаних з роботою вузлів і комплексів транспортного засобу. Перші випробування, проведено влітку 2017 р. з п'ятьма автомобілями «Мерседес S» показали, що нанопроцесор, розміщений на внутрішній стороні корпусу, дозволяє не лише відстежити рух транспортного засобу, а й фіксувати різницю в манері водіння. Кожен водій має свій власний почерк. На думку начальника транспортної поліції Лондона, поєднання такої системи з підрозділами, відповідальними за попередження автомобільних крадіжок, по суті, ставить хрест на крадіжці автомобілів у Великобританії.

Керівництво Імперського коледжу на спільній з Ілоном Маском прес-конференції повідомило, що такі нанопроцесори, які сигналізують про небезпеку і переміщення того чи іншого об'єкта, можуть бути нанесені на тильну сторону картин в музеї, на ювелірні вироби тощо, без жодної шкоди для їх зовнішнього виду і колекційної цінності. У цьому разі стають непотрібними величезні витрати на системи сигналізації в музеях, складні сейфи у власників ювелірних прикрас тощо. На прес-конференції було також повідомлено, що І. Маск профінансує установку тривожних нанопроцесорів на картинах і експонатах всесвітньо відомого Британського королівського національного музею. Він стане першим музеєм, звідки просто неможливо буде вкрасти будь-яке твір мистецтва.

Наведені приклади наочно ілюструють факт реального переходу сфер охоронної безпеки й технічного захисту об'єктів в іншу сучасну площину, де провідну роль відіграватимуть новітні системи та засоби технічної охорони, що ґрунтуються на використанні технологій IoT та штучного інтелекту. Поліцейські підрозділи Великобританії, США демонструють напрям, в якому необхідно рухатися правоохоронним структурам інших країн.

Одержано 19.03.2021

УДК [351.74(100):004.9](075.8)

МОГІЛЕВСЬКИЙ Леонід Володимирович,
доктор юридичних наук, професор, заслужений юрист України,
проректор Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-6994-6086

КІБЕРЗЛОЧИННІСТЬ У ПРОЄКТІ ЄВРОПОЛУ SOCTA

Постійний моніторинг та аналіз стану і трендів у сфері організованої злочинності, особливо кіберзлочинності, є невід'ємною частиною у плануванні діяльності правоохоронних структур. Надважливим кроком у розвитку цього напряму діяльності й інтеграції зусиль правоохоронних органів країн Європейського Союзу є проєкт SOCTA.

SOCTA (англ. SOCTA – Serious and Organized Crime Threat Assessment) розробляється і публікується Європолом у співпраці з консультативною групою SOCTA, до складу якої входять

держави члени ЄС, агентства ЄС, Європейська комісія та Генеральний секретаріат Ради за підтримки європейських країн партнерів та організацій Європолу. Методологію схвалено Радою міністрів юстиції та внутрішніх справ ЄС.

Проєкт Європолу SOCTA охоплює:

– підготовку та затвердження детальних вимог одержувача даних;

– підготовку та схвалення методології;

– визначення вимог до збору оперативних даних;

– збір даних;

– аналіз даних (у т. ч. і Великих Даних);

– складання звіту SOCTA, включно зі списком основних загроз і ризиків;

– презентація результатів і рекомендованих пріоритетів.

У процесі аналізу особлива увага приділяється чотирьом такими елементам:

1) галузі / види тяжкої та організованої злочинної діяльності;

2) організовані злочинні групи / мережі та поодинокі правопорушники, причетні до тяжких злочинів;

3) середовище: уразливості, можливості та інфраструктура;

4) наслідки і шкода.

SOCTA розвиває Національну модель організації розвідувальної діяльності Управління Організації Об'єднаних Націй з наркотиків і злочинності, яка ґрунтується на дев'яти аналітичних методах і продуктах:

1) системний аналіз злочинної практики – це загальний термін для декількох видів аналізу, включно з виявленням тенденцій та аналізом «гарячих точок»;

2) аналіз демографічних / соціальних тенденцій, що оцінює вплив соціально-економічних і демографічних змін на злочинність, а також демографічні зрушення і ситуацію з безпритульністю;

3) мережевий аналіз, що оцінює напрямок, частоту і силу зв'язків між спільниками у злочинній мережі;

4) аналіз потенційного ринку збуту, що оцінює кримінальний ринок щодо певного товару, такого як наркотики або проституція;

5) аналіз сфери злочинного бізнесу, визначає бізнес модель і методи, використовувані окремими злочинцями або ОЗУ;

6) аналіз ризиків, що оцінює масштаб ризиків або загроз, створюваних правопорушниками або організаціями для окремих потенційних жертв, поліції і громадськості;

7) аналіз цільового профілю, що описує злочинця, його сильні та слабкі сторони, спосіб життя, зв'язки, злочинну діяльність і точки можливого заходу у життя цільового злочинця;

8) оцінка оперативної розвідувальної діяльності, що розглядає відповідність збору інформації раніше узгодженим завданням і виявляє прогалини в зусиллях із проведення розвідувальних дій (у великомасштабних проєктах та операціях);

9) аналіз результатів, що оцінює ефективність діяльності правоохоронних органів і контролює перебіг виконання планів.

У межах підготовки доповіді Європол в 2015–2017 рр. здійснив найбільший в історії аналіз Великих Даних щодо серйозної та організованої злочинності в ЄС. Європол використовував тисячі доповідей, інформаційних довідок та файлів держав-членів, оперативних і стратегічних партнерів. У доповіді в повному обсязі відображено дані оперативної розвідки, що зберігаються в базах даних Європолу. У результаті цього в межах підготовки доповіді вдалося надати найбільш докладну оцінку характеру і масштабів загроз злочинності, що стоять перед ЄС і його державами-членами.

У доповіді Європолу зазначено, зокрема, що «злочинці швидко впроваджують і інтегрують нові технології в свій modus operandi або створюють абсолютно нові бізнес моделі навколо них. Використання нових технологій ОЗУ впливає на злочинну діяльність по всьому спектру серйозної та організованої злочинності. В першу чергу, це відноситься до цифрового криміналу, який широко використовує масштабування онлайн торгівлі і повсюдне поширення зашифрованих каналів зв'язку».

У 2013 р. Європол повідомив про наявність у ЄС не менш ніж 3600 міжнародних груп організованої злочинності (ОЗУ). У SOCTA в 2017 р. ідентифіковано близько 5 тис. міжнародних ОЗУ, які на початок 2018 р. перебували в розробці або під слідством у державах ЄС. Збільшення кількості ОЗГ порівняно з попередньою доповіддю пов'язується насамперед зі значним підвищенням ефективності кримінальної розвідки. Воно також свідчить про нові процеси у сфері злочинності, серед іншого про появу невеликих груп та індивідуальних злочинців, що діють переважно в кіберпросторі.

Ці та інші висновки експертів Європолу в доповіді SOCTA свідчать, зокрема, про те, що:

– організована злочинність дедалі більше використовує кіберпростір для підготовки і здійснення масштабних злочинів;

– підготовка масштабних злочинів, особливо у кіберсфері, супроводжується дедалі серйознішими заходами і засобами приховування і маскування;

– виявлення і прогнозування на етапі підготовки з метою попередження кіберзлочинів потребує застосування високотехнологічних інструментів аналізу кіберпростору на кшталт Palantir, ePOOLICE;

– ефективна протидія організованій кіберзлочинності в сучасних умовах є можливою, як правило, лише за умови тісної консолідації зусиль національних правоохоронних структур із міжнародними правоохоронними структурами та правоохоронними органами інших країн.

Одержано 29.04.2021

УДК 343

ВІНЦУК Вікторія Володимирівна,
кандидат юридичних наук,
доцент кафедри кримінального процесу, криміналістики
та експертології факультету № 6 Харківського національного університету
внутрішніх справ

ТОРГІВЛЯ ЛЮДЬМИ ТА ТРАНСНАЦІОНАЛЬНА ЗЛОЧИННІСТЬ

В державі на сьогодні склалася принципово нова ситуація в ідеологічній, політичній, економічній, соціальній та правовій сфері життєдіяльності українського суспільства. Не дивлячись на тяжку епідеміологічну ситуацію, пандемію, локдауни та карантинні заходи, пов'язані з COVID-19, які вимагають від громадян дотримуватись деяких обмежень та незручностей, злочинність не зважає на ці неподобства і торгівля людьми не зупиняється навіть за цих умов.

Суспільна небезпека торгівлі людьми полягає у тому, що завдається шкода суспільним відносинам, які забезпечують право людини на свободу. Явище торгівлі людьми, яке існує з давніх часів, пов'язане з товарно-грошовими відносинами. В римському праві цей вид злочину мав назву plagium (лат., букв. – викрадення), – викрадення вільної людини та продаж її у рабство.

Так історично склалося, що певному етапу розвитку суспільства була притаманна торгівля людьми, хоч це рабовласницький устрій, хоч певний період капіталістичного устрою, і тільки розквіт демократії дав позитивні поштовхи для її викорінювання. Але у сучасному світі торгівля людьми досі є одним із найбільш масових порушень прав і свобод людини.

«Руська Правда» встановлювала відповідальність за крадіжку і подальший продаж челядина (ст. 38). У Литовському статуті (редакція 1588) існувала норма, що забороняла представникам нехрист, народів, які перебували на території Великого князівства Литовського, купувати, поневолювати і закладати християн (ст. 9). За такі дії винний втрачав гроші, які заплатив, купуючи християнина, а останнього треба було звільнити. У слов'ян Соборним уложенням 1649 передбачалася кримінальна відповідальність за викрадення людей. Уложенням про покарання кримінальні й виправні 1885 встановлювалася відповідальність за повне позбавлення

волі: продаж у рабство, в т. ч. будь-яку передачу підданих під різними приводами, зокрема продаж жінок за кордон для поміщення там у будинки розпусти, торгівля неграми, викрадення дітей, що могли виявлятися у таких трьох гол. формах, як викрадення у вузькому розумінні, підміна, самовільне утримання у себе (покарання посилювалося, якщо дитина була викрадена або прихована для жебрацтва чи ін. аморального заняття або з корисливою метою), викрадення жінок. Згідно з Уложенням 1903 каралися викрадення дітей віком до 14 років, їх самовільне утримання, викрадення неповнолітніх віком від 14 до 16 років, продаж або передання людей у рабство чи неволю, торгівля неграми [1].

Отже, змінюються епохи, часи, державотворення, але торгівля людьми існує і до цього часу, змінюються тільки форми скоєння кримінальних правопорушень, пов'язаних з цим злочинним явищем. Торгівля людьми має різні види, серед яких примусова праця, рабство, звичаї подібні до рабства, сексуальна експлуатація, використання у порнобізнесі, примусова вагітність, вилучення органів, проведення дослідів над людиною, використання у жебрацтві, втягнення в злочинну діяльність, використання у збройних конфліктах, усиновлення (удочеріння) з метою наживи, продаж дитини.

15 листопада 2000 року прийнято 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 [2].

Враховуючи небезпеку торгівлі людьми за сучасних умов, Україна вживає заходів щодо протидії цьому протиправному явищу, оскільки чинним законодавством торгівлю людьми визначено як суспільно небезпечне діяння, за яке встановлено кримінальну відповідальність. Тобто, масштаби розповсюдження негативних проявів призвели до прийняття в Україні у відповідності до міжнародних нормативно-правових актів Закону України «Про протидію торгівлі людьми».

У ст. 1 Закону України «Про протидію торгівлі людьми» надані визначення та їх тлумачення. Розглянемо деякі: боротьба з торгівлею людьми – система заходів, що здійснюються в рамках протидії торгівлі людьми, спрямованих на виявлення злочину торгівлі людьми, у тому числі незакінченого, осіб, які від цього постраждали, встановлення фізичних/юридичних осіб – торгівців людьми та притягнення їх до відповідальності; попередження торгівлі людьми – система заходів, спрямованих на виявлення та усунення причин і умов, що призводять до торгівлі людьми; протидія торгівлі людьми – система заходів, спрямованих на подолання торгівлі людьми шляхом її попередження і боротьби з нею та надання допомоги і захисту особам, які постраждали від торгівлі людьми; торгівля людьми – 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 КК України визнаються злочином та інші [3].

Пріоритети держави направленні на превентивні заходи, але латентність деяких різновидів торгівлі людьми не дає змоги дієво вплинути на них, тому наступний шаг це боротьба з різними її проявами. А науковці М.П. Бліщенко, В.Є. Ємінова, Г.О. Зоріна, І.І. Карпець, В.П. Панов, Ю.І. Римаренко, О.С. Овчинський, В.С. Овчинський, О.В. Святун, В.Д. Скулиш; П.П. Яблоков та інші, вивчаючи торгівлю людьми як злочин транснаціонального характеру надавали не лише їх визначення, форми й алгоритм протидії їй, але ж минають роки й злочинці винаходять нові форми торгівлі людьми, використовуючи мережу Інтернет.

Список використаних джерел

1. Торгівля людьми чи інша незаконна угода про передачу людини // Юридична енциклопедія: В 6 т. / Редкол.: Ю. С. Шемшученко (голова редкол.) та ін. URL: https://leksika.com.ua/10320617/-legal/torgivlya_lyudmi_chi_insha_ nezakonna_ugoda_pro_peredachu_lyudini (дата звернення: 17.03.2021).

2. 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 : резолюція 55/25 Генеральної Асамблеї від 15 листопада 2000 року // БД «Законодавство України» / ВР України : офіційний вебпортал. URL: https://zakon.rada.gov.ua/laws/show/995_791 (дата звернення: 17.03.2021).

3. Торгівля людьми // Вікіпедія : вільна енциклопедія. URL: https://uk.wikipedia.org/-wiki/%D0%A2%D0%BE%D1%80%D0%B3%D1%96%D0%B2%D0%BB%D1%8F_%D0%BB%D1%8E%D0%B4%D1%8C%D0%BC%D0%B8 (дата звернення: 17.03.2021).

Одержано 04.04.2021

УДК 343.21

ЗАВОРІНА Марія Артемівна,
студентка групи ІТШІ-20-2
факультету комп'ютерних наук
Харківського національного університету радіоелектроніки

ПРОБЛЕМНІ ПИТАННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ТА ЗАПРОВАДЖЕННЯ ОБІГУ КРИПТОВАЛЮТИ

У наш час нікого не здивуєш механізмом запровадження і використання віртуального обігу грошей: оплатою за товари та послуги карткою, телефоном, транзакцією он-лайн, які давно стали буденною звичкою, яка переростає у повсякденне зручне застосування. Але технології нашого сьогодення вийшли на новий рівень, зокрема стрімко набуває популярності використання криптовалюти, майнінг якої буквально перевернув сучасне уявлення про обіг грошових одиниць та отримання як форми заробітку у всьому світі.

Що ж являє собою криптовалюта? Визначення такого терміну надала В.Б. Родичева: «криптовалюта є різновидом електронних грошей (перш за все, цифрових/віртуальних). Віртуальною одиницею валюти є монета, яка захищена від підробки. Вона являє собою зашифровану інформацію, розповсюджену через мережу Інтернет та інші види віртуального зв'язку, скопіювати яку неможливо. Криптовалюта імітується в такій мережі і не пов'язана зі звичайною валютою або державною валютною системою» [1, с. 355].

За дослідженням встановлено, що існує багато різновидів криптовалюти, але найвідомішою і більш поширеними вважаються Bitcoin, Ethereum, Ripple (XRP), Monero (XMR), Litecoin, Namecoin, Binance Coin (BNB) тощо. З цього приводу В.В. Скрипник зазначив, що «сьогодні загальна кількість різновидів криптовалюти сягнула вже близько двох тисяч, хоча найпоширеніший її різновид це біткоїн, який створено лише в 2008 році» [2, с. 38]. Україна входить в ТОП-10 країн світу за кількістю користувачів Bitcoin (одного з виду криптовалют), тому питання її правового регулювання є не лише доцільним, а й необхідним. Зважаючи на стрімкий розвиток майнінгу, в Україні існує нагальна необхідність створення законопроєктів, які сприятимуть правовому підґрунтю обігу криптовалюти, використання якої, станом на сьогодні, є повністю анонімним, що, в свою чергу, призводить до зловживання нею, зокрема до відмивання коштів, ухиляння від сплати податків, фінансуванню тероризму та інших зловживань.

Слід констатувати, що правове врегулювання обігу криптовалюти в Україні відсутнє. В той же час, проєкт Закону України № 7183 від 06.10.2017 «Про обіг криптовалюти в Україні», зареєстрований у Верховній Раді України, є першим кроком щодо розв'язання цього питання. Так, вказаний законопроєкт визначає криптовалюту програмним кодом (набором символів, цифр та букв), що виступає як об'єкт права власності, який може бути придбаний і застосовуватись засобом міни та відомості про який вносяться і зберігаються у системі блокчейн в якості облікових одиниць поточної системи блокчейн у вигляді даних (програмного коду) [3]. Окрім визначеного, проєкт Закону України № 7183-1 від 10.10.2017 «Про стимулювання ринку криптовалют та їх похідних в Україні» доповнює зазначене визначення криптовалюти ще й наступним елементом як децентралізований цифровий вимір вартості, що може бути виражений в цифровому вигляді та функціонує як засіб обміну, збереження вартості або одиниця обліку, що заснований на математичних обчисленнях, є їх результатом та має криптографічний захист обліку. Криптовалюта для мети правничого унормування визнається фінансовим активом [4], що ми підтримуємо.

Навколо цієї дефініції точаться дискусії. Зокрема, як зазначають О.О. Лов'як та Т.О. Лозова: «узагальненим завданням цих Законопроєктів є створення умов для стимулювання розвитку діяльності криптовалют в Україні та їх добування, використання криптовалют у повсякденному житті під час здійснення товарообмінних операцій суб'єктами господарювання, захист прав, законних інтересів професійних учасників ринку та кваліфікованих інвесторів. Узагальненою метою є встановлення основних правових та організаційних засад здійснення діяльності у сфері криптовалютних відносин в України, стимулювання розвитку платіжної й цифрової інфраструктур, що забезпечують добування та обіг криптовалют, забезпечення прав і законних інтересів осіб, що здійснюють добування криптовалют, та інвесторів» [5, с. 105]. Проте легалізація криптовалюти на законодавчому рівні допоможе обмежити її головну перевагу – анонімність.

Правове регулювання криптовалюти є нагальним та необхідним, про що свідчить досвід зарубіжних країн. Неврегульованість процесів майнінгу призводить до втрати додаткових надходжень до бюджету й невикористання можливостей інвестиційних майданчиків. Слід наголосити, що 22 жовтня 2015 року за наслідками розгляду звернення Європейським судом щодо справедливості прийнято рішення по справі С-264/14, яке містить такі висновки, які не беруть до уваги згадані законопроекти: 1) «… не існує єдиного емітента віртуальної валюти. Натомість вона створюється мережею за допомогою спеціального алгоритму. Система дозволяє забезпечити анонімність власників і переказів між ними. «Біткоін адреси» виступають аналогами банківських рахунків» (п. 11 Рішення); 2) «… на відміну від електронних грошей, віртуальним валютам притаманні власні одиниці обліку, як, наприклад, «1 біткоін» (п. 12 Рішення); 3) «… не може вважатись «матеріальним майном» у розумінні ст. 14 ПДВ Директиви ЄС, оскільки віртуальна валюта може виступати лише платіжним засобом» (п. 24 Рішення); 4) «… перекази віртуальних валют можуть бути здійснені без залучення банків чи фінансових установ» (п. 37 Рішення); 5) «… віртуальна валюта «біткоін» не може вважатись поточним банківським рахунком, депозитним рахунком, платежем чи грошовим переказом. На відміну від грошових чеків, боргових зобов'язань, інструментів кредитування біткоін виступає прямим платіжним засобом між суб'єктами розрахунків» (п. 42 Рішення); 6) «… єдиним призначенням віртуальної валюти «біткоін» є здійснення розрахунків між суб'єктами відносин» (п. 52 Рішення); 7) «… віртуальна валюта «біткоін» не може вважатись цінним папером або інструментом, що посвідчує право на майно» (п. 55 Рішення) [6].

Неоднозначний досвід і законодавчій підхід світової спільноти в галузі правового регулювання обігу віртуальної валюти ставить під сумнів питання можливості запровадження в Україні дієвих механізмів такого рівня, хоча в нашій країні вже запровадженні перші ініціативи та кроки по вирішенню цього проблемного питання, яке слід вирішити насамперед з урахуванням необхідності визначення правового статусу власника криптовалюти та впровадження правових механізмів оподаткування. Таким чином, слід зробити висновок, що правове врегулювання обігу криптовалюти залишається в дискусійному полі, незважаючи на наявні законодавчі ініціативи щодо фінансового моніторингу криптовалют, які спрямовані на впровадження кращих міжнародних правових стандартів та практик щодо протидії відмиванню коштів і фінансуванню тероризму. Одним із наступних кроків повинна бути реформа у податковому законодавстві, що передбачено у проєкті Закону України № 2461 від 15.11.2019 «Про внесення змін до Податкового кодексу України та деяких інших законів України щодо оподаткування операцій з криптовактивами». Крім того, подальшого законодавчого врегулювання потребує визначення самого поняття «криптовалюта» в Кримінальному кодексі України та у Цивільному кодексі України.

Втім, підняті питання не є остаточними та потребують додаткового і окремого дослідження або наукового вивчення.

Список використаних джерел

1. Родичева В.Б. Криптовалюта: история происхождения и развитие. Екатеринбург, 2018. 355 с.

2. Скрипник В.В.. Місце криптовалюти в системі об'єктів цивільних прав. Кременчуг, 2018. 38 с.

3. Про обіг криптовалюти в Україні : проект Закону України № 7183 від 06.10.2017 // ВР України : офіційний вебпортал. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62684 - (дата звернення: 30.04.2021).

4. Про стимулювання ринку криптовалют та їх похідних в Україні : проект Закону України № 7183-1 від 10.10.2017 // ВР України : офіційний вебпортал. URL: http://w1.c1.rada.gov.ua/pls/zweb2/-webproc4_1?pf3511=62710 (дата звернення: 30.04.2021).

5. Лов'як О.О., Лозова Т.О. Окремі аспекти обігу криптовалюти в Україні (цивільно-правовий аспект). *Національний юридичний журнал: теорія та практика.* 2018. С. 104-108.

6. Верланов С. Правова природа криптовалют у судовій практиці європейського суду справедливості. URL: http://advisortax.org/wp-content/uploads/2017/11/Legal-natureof-cryptocurrencies-Verlanov.pdf (дата звернення: 30.04.2021).

Одержано 01.05.2021

УДК 351:343.431

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

РЕАЛІЗАЦІЯ ОСНОВНИХ НАПРЯМІВ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ПРОТИДІЇ ТОРГІВЛІ ЛЮДЬМИ

У сучасному світі гострою проблемою залишається протидія торгівлі людьми. Зростання масштабів цього правопорушення наприкінці XX століття обумовило необхідність в Україні встановлення кримінальної відповідальності за торгівлю людьми та прийняття спеціальної нормативно-правової бази щодо її протидії.

Закон України від 20 вересня 2011 року «Про протидію торгівлі людьми» [1] визначив організаційно-правові засади протидії торгівлі людьми, гарантуючи гендерну рівність, основні напрями державної політики та засади міжнародного співробітництва у цій сфері, повноваження органів виконавчої влади, порядок встановлення статусу осіб, які постраждали від торгівлі людьми, та порядок надання допомоги таким особам.

Розглянемо основні напрями державної політики у цій сфері, до яких згідно зі ст. 4 зазначеного Закону віднесено:

– по-перше, попередження торгівлі людьми шляхом підвищення рівня обізнаності населення, превентивної роботи, зниження рівня вразливості населення, подолання попиту;

– по-друге, боротьба зі злочинністю, пов'язаною з торгівлею людьми, шляхом виявлення злочинів торгівлі людьми, осіб, причетних до скоєння злочину, притягнення їх до відповідальності;

– по-третє, надання допомоги та захисту особам, які постраждали від торгівлі людьми, шляхом удосконалення системи відновлення їхніх прав, надання комплексу послуг, впровадження механізму взаємодії суб'єктів у сфері протидії торгівлі людьми.

Отже, попередження торгівлі людьми здійснюється за такими напрямами як вивчення ситуації, стану, причин і передумов поширення торгівлі людьми, підвищення рівня обізнаності населення про зазначене кримінальне правопорушення, зниження рівня вразливості населення, подолання попиту шляхом реалізації організаційних, дослідницьких, інформаційних, освітніх, правових, соціально-економічних та інших заходів.

Як зазначено в щорічній доповіді Державного департаменту США про торгівлю людьми [2], органи влади спільно з міжнародними організаціями та місцевими партнерами провели низку інформаційних кампаній по всій країні, зокрема за допомогою телевізійних і кінопрограм, вуличної реклами, публічних заходів та роботи в громадах.

Відповідно до ст. 11 Закону України «Про протидію торгівлі людьми» боротьба з торгівлею людьми є невід'ємною складовою частиною діяльності органів Національної поліції по боротьбі зі злочинністю, які, зокрема, здійснюють заходи щодо виявлення злочинів торгівлі людьми, осіб, які постраждали від торгівлі людьми, встановлення осіб – торгівців людьми та притягнення їх до відповідальності. Так, у згаданій вище щорічній доповіді Державного

департаменту США [2] зазначено, що у 2019 році правоохоронні органи розслідували 297 злочинів, пов'язаних із торгівлею людьми, порівняно з 275 злочинами у 2018 році. Серед цих злочинів було 135 випадків торгівлі людьми з метою трудової експлуатації, 112 випадків сексуальної експлуатації, 47 – для примусової участі в злочинній діяльності і три для примусового жебракування.

З метою надання ефективної допомоги та захисту особам, які постраждали від торгівлі людьми, створюється Національний механізм взаємодії суб'єктів, які здійснюють заходи у сфері протидії торгівлі людьми.

Особа має право звернутися до місцевої державної адміністрації із заявою про встановлення статусу особи, яка постраждала від торгівлі людьми. При цьому у неї з'являється право на забезпечення особистої безпеки, інформування про свої права та можливості, медичну, психологічну та іншу допомогу, тимчасове розміщення у закладах допомоги для осіб, які постраждали від торгівлі людьми. Причому надання допомоги особі, яка постраждала від торгівлі людьми, не залежить від її звернення до правоохоронних органів та її участі у кримінальному процесі. Так, за даними Міністерства соціальної політики України [3], наприклад, у 2020 році 132 особам встановлено статус постраждалих від торгівлі людьми, з яких 97 – чоловіки, 33 – жінки, 2 – діти (хлопчики). Більшість постраждалих використовувались у сфері трудової експлуатації та в збройних конфліктах.

Підсумовуючи викладене, можна зробити висновок, що в Україні поступово реалізуються основні напрями державної політики у сфері протидії торгівлі людьми. Проте зазначене кримінальне правопорушення залишається латентним, винні особи не завжди реально відбувають призначені покарання, а звільняються від їх відбування з випробуванням. Тому спеціальна правова база з протидії торгівлі людьми, стандарти надання соціальних послуг особам, які постраждали від неї, і в подальшому мають вдосконалюватися. Захист та допомога жертвам торгівлі людьми мають здійснюватися при повній повазі їхніх прав і свобод.

Список використаних джерел

1. Про протидію торгівлі людьми : Закон України від 20.09.2011№ 3739-VI // БД «Законодавство України» // ВР України : офіційний вебпортал. URL: https://zakon.rada.gov.ua/laws/show/3739-17 (дата звернення: 17.03.2021).

2. Доповідь про торгівлю людьми // Офіційні доповіді та звіти / Посольство США в Україні : офіційний вебсайт. URL: https://ua.usembassy.gov/wp-content/uploads/sites/151/TIP_Report_20_Ukr.pdf (дата звернення: 17.03.2021).

3. Кількість осіб, яким Мінсоцполітики встановлено статус особи, яка постраждала від торгівлі людьми у 2020 році (інфографіка) // Міністерство соціальної політики України : офіційний вебсайт. 08.12.2020. URL: https://www.msp.gov.ua/news/19413.html (дата звернення: 17.03.2021).

Одержано 27.04.2021

УДК 004.7
КОЗАР Анатолій Володимирович,
начальник 2-го відділу
Управління протидії кіберзлочинам в Харківській області
Департаменту кіберполіції Національної поліції України,
полковник поліції

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК СПОСІБ ШАХРАЙСТВА

На сьогоднішній день існує безліч варіантів, якими користуються зловмисники для з'ясування конфіденційних даних особи, необхідних для розкрадання безготівкових грошових коштів, починаючи від програм з вмістом спеціального коду до передачі таких даних самим потерпілим. До найбільш поширених способів скоєння шахрайських дій з використанням соціальної інженерії належать: створення сайтів, що містять неправдиву інформацію, дозволяють ввести потерпілого в оману (і отримати особисті дані); розсилка листів на електронну пошту з вмістом шкідливого коду, посилання; незаконне отримання реєстраційних даних жертви; розкрадання безготівкових грошових коштів шляхом злому даних, призначених для входу в електронні гаманці; отримання грошових коштів через віртуальні інтернет-магазини.

Техніки соціальних інженерів різноманітні, але їх об'єднує одне – в основі лежать когнітивні спотворення (тобто людська дурість і неуважність). Крім цього останнім часом почастішали випадки шахрайства за допомогою соціальної інженерії – метод незаконного отримання доступу до певної інформації, не використовуючи технічні обладнання та засоби. Головним чином використовуються слабкості людського фактора, і полягає в маніпулюванні поведінкою людини. Шахраї за допомогою соціальних і психологічних навичок змушують особу зробити будь-які дії, достатні для розкрадання його коштів або «заволодіння особистими даними».

До способів здійснення шахрайства за допомогою соціальної інженерії належать: фальшиві SMS-розсилки (зазвичай в такому повідомленні міститься інформація про блокування банківської карти із зазначенням номера менеджера банку, з яким необхідно зв'язатися. При дзвінку на вказаний номер, шахраї представляються співробітниками банку і повідомляють особу про те, що з його рахунку була здійснена підозріла спроба переказу грошових коштів); злом даних для входу на популярний соціальний інтернет-ресурс (шахраї, вивчаючи листування з певними контактами, роблять їм розсилку від імені власника з проханням зайняти певну суму грошей); фішинг (даний спосіб полягає в розсилці повідомлень, підроблених під офіційний лист банку або платіжної системи, і містить посилання на фальшиву вебсторінку, така сторінка містить логотип організації і спеціальну форму з введенням персональних даних від адреси проживання до пін-коду банківської картки); квіпрокво (шахраї дзвонять за випадковим номером телефону компанії і представляються співробітниками технічної підтримки, метою є введення певних команд самим потерпілим, що дозволяють запустити шкідливе програмне забезпечення) і т.д.

Особу потерпілого можна характеризувати як особу довірливу, цікаву, найчастіше експлуатується люб'язність, лінь і навіть ентузіазм. До основних рис також можна віднести прагнення особи заощадити. Шахрайство по відношенню до фізичних осіб можна розділити на три групи. Відносно найменш захищених верств населення, що мають низький рівень фінансового достатку і кіберграмотності (пенсіонери, жителі невеликих міст). Для економічно активної частини населення, яка користується інтернетом, шахраї вибирають спам-розсилки листів, що містять інформацію про уявні знижки, отримання пільг, компенсацій, соціальних виплат. Такі повідомлення містять шкідливі програми або посилання на фішингові сайти, в результаті використання яких відбувається зараження пристрою і компрометація платежів його власника. До останньої групи можна віднести осіб, які активно користуються сучасними мобільними пристроями з операційними системами Android та IOS. Використовуючи шкідливе програмне забезпечення, зловмисники отримують доступ і контроль до встановлених на пристрої додаткам, які містять конфіденційні дані, що дозволяє їм здійснювати фінансові операції включаючи перекази грошових коштів з карт жертви.

Таким чином, варіанти шахрайства з використанням соціальної інженерії вельми різноманітні. Такий метод маніпуляції діями людини полягає в використанні слабкостей людського фактора. Висока поширеність даного виду шахрайства підтверджує, що своєчасне інформування про загрози – це ключовий захисний механізм, який необхідний для користувачів засобів сучасної комунікації. Соціальна інженерія нематеріальна, її неможливо усунути фізично. Найдієвіший спосіб не стати жертвою шахрайства – це не втрачати пильності і не дозволяти шахраєві себе провести. Крім цього, захистити конфіденційну інформацію допомагає використання сучасного та актуального антивірусного програмного забезпечення. Глибоке і ретельне вивчення сучасних видів шахрайства сприяє виявленню його особливостей, які сприяють подальшому розслідуванню і правильному вибору проведених уповноваженою особою заходів з розслідування і запобігання злочину.

Одержано 01.05.2021

УДК 343.85

КОРОСТЕЛЬОВА Лілія Анатоліївна,
ад'юнкт Луганського державного університету внутрішніх справ імені Е. О. Дідоренка

ШТУЧНИЙ ІНТЕЛЕКТ У ПРОТИДІЇ КІБЕРАТАКАМ В УМОВАХ ГЛОБАЛЬНОЇ ПАНДЕМІЇ

За останні десятиліття питання боротьби з кіберзлочинністю стає не тільки відомим пересічному громадянину, а й нагально потребує обговорення в рамках не лише науковими та практичними ресурсами окремої держави, а і міжнародного співтовариства [1, с. 155].

Кількість атак на інформаційні системи збільшується кожний рік. При цьому атаки стають все більш вразливими, а збитки від атак – збільшуються [2]. Під час глобальної пандемії COVID-19 стався помітний сплеск злочинів в сфері кібербезпеки, це пов'язано з тим, що значно побільшала кількість людей в мережі, і тим самим зросла кількість атак.

Професор Джейсон Нерс із Інституту кібербезпеки суспільства (iCSS) Кентського університету стверджує, що Covid-19 значно вплинув на суспільство, і помітне зростання кіберзлочинності у всьому світі. Дослідники з WMG, Університету Уоріка, Університету Абертей, Університету Кента, Оксфордського університету та Університету Стратклайда у своєму спільному дослідженні «Кібербезпека у вік COVID-19: хронологія та аналіз кіберзлочинності та кібернетики», класифікували кібератаки за категоріями, і виявили, що: 86% були пов'язані з фішингом, 65% пов'язані з шкідливим ПЗ, 34% були пов'язані з фінансовим шахрайством, 15% – вимагання, 13% це фармінг, 5% це зломом, 5% пов'язані з відмовою в обслуговуванні [3].

Дана статистика свідчить, про те, що «класичні» засоби антивірусної боротьби вже не спроможні подолати сучасні кібератаки, 90% спеціалістів із кібербезпеки в США і Японії стверджують, що кіберзлочинці почнуть використовувати штучний інтелект для проведення атак. І цей сценарій, по суті вже реальність сучасності [6]. Використання технологій штучного інтелекту здатне не тільки значно збільшити масштаби традиційної злочинності, можливою є поява принципово нових видів кримінальних правопорушень. Ідеться про так звані «змагальні» атаки (adversarial attacks) та «отруєння» штучного інтелекту. Перші полягають у відшукуванні недосконалостей створених систем розпізнавання образів або мовлення (звуку) та подальшому їх використанні для приведення пристроїв зі штучним інтелектом у некоректний режим роботи. «Отруєння» штучного інтелекту полягає у втручанні в процес розробки пристроїв шляхом внесення змін до так званих «навчальних» наборів даних. У результаті подібних дій пристрій зі штучним інтелектом у певних ситуаціях функціонує у спосіб, який значно відрізняється від запланованого розробниками [5, с. 36].

Без сумніву, існує велика необхідність правоохоронним органам запроваджувати технології штучного інтелекту для протидії сучасними кібератаками. Інструменти безпеки штучного

інтелекту працюють над виявленням, прогнозуванням, обґрунтуванням, діянням та вивченням потенційних загроз кібербезпеки, які не потребують особливого втручання людини [4, с. 191].

Запровадження в правоохоронну діяльність технологій штучного інтелекту дозволить вдосконалити методику протидії кіберзлочинності та ефективно боротись із кібератаками.

Список використаних джерел

1. Таволжанський О. В. Особливості забезпечення кібербезпеки у сучасному світі: огляд суб'єктів запобігання кіберзлочинності. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького*: Серія Право. 2018. Вип. 6 (18). С. 154-163.

2. Почему искусственный интеллект все чаще принимают на кибервооружение? // CNews Безопасность : вебсайт. 01.06.2020. URL: https://safe.cnews.ru/articles/2020-06-01_pochemu_iskusstvennyj_-intellekt_vse (дата звернення: 25.04.2021).

3. Sait zhurnalu «EurekAlert! Science News» // EurekAlert! Science News : Site of journal. URL: https://www.eurekalert.org/pub_releases/2021-03/uow-crc032221.php (дата звернення: 25.04.2021).

4. Федоренко О. А. Використання технологій штучного інтелекту для виявлення та припинення кіберзагроз // Збірник Матеріалів міжвідомчого наукового столу (м. Київ, 25 лютого 2021 р.). Київ : НАВС, 2021. С. 190-192.

5. Карчевський М. В. Штучний інтелект та протидія злочинності // Використання технологій штучного інтелекту у протидії злочинності : матеріали наук.-практ. онлайн-семінару (м. Харків, 5 листоп. 2020 р.). Харків : Право, 2020. С. 32-43.

6. Защищаемся от ИИ с помощью ИИ: решения с поддержкой искусственного интеллекта для киберугроз нового поколения // SecurityLab.ru : офіційний сайт. 16.04.2021. URL: https:// /www.securitylab.ru/analytics/518993.php (дата звернення: 25.04.2021).

Одержано 01.05.2021

УДК 340:004

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

ЗАКОНОДАВЧЕ ВРЕГУЛЮВАННЯ ОБІГУ КРИПТОВАЛЮТИ В УКРАЇНІ

02 грудня 2020 року на 3 сесії IX скликання Верховної Ради України в першому читанні було прийнято за основу законопроєкт № 3637 «Про віртуальні активи» [1]. Зважаючи на те, що по теперішній час Національний банк України офіційно розглядає криптовалюту як грошовий сурогат, який не має забезпечення реальною вартістю, це великий крок до легалізації обігу криптовалюти в Україні. Станом на сьогодні прямої законодавчої заборони використання криптовалюти в Україні немає і попри законодавчої неврегульованості питання обігу криптовалюти її фактичний обіг в усьому світі в цілому і в Україні зокрема постійно збільшується.

Слід зазначити що це не перша спроба навести лад у сфері обігу віртуальних активів в нашій державі. До цього були законопроєкти: № 7183-1 «Про стимулювання ринку криптовалют та їх похідних в Україні» [2], № 4328 «Про токенізовані активи та криптоактиви» [3], що були подані до парламенту, але так і не були розглянуті, та декілька законопроєктів які навіть не були подані до парламенту, наприклад законопроєкт анонсований депутатом України Олексієм Мушаком оприлюднений лише в вигляді презентації [4].

На основі експрес-аналізу законопроєкту № 3637 «Про віртуальні активи» було виявлено наступні суттєві нововведення.

1. В цивільний кодекс України додається стаття 190-1, в якій визначається що віртуальні активи є різновидом майна, розпорядження якими здійснюється відповідно до норм Закону України «Про віртуальні активи», а також вносяться зміни до статті 190, шляхом внесення віртуальних активів в перелік майна.

2. Визначаються учасники ринку віртуальних активів, їх права та обов'язки.

3. Законодавчо визначається поняття постачальників послуг, пов'язаних з обігом віртуальних активів як суб'єктів підприємницької діяльності, які здійснюють в інтересах третіх осіб один або декілька з наступних видів діяльності:

– зберігання або адміністрування віртуальних активів або інструментів, що дають змогу контролювати віртуальні активи;

– обмін віртуальних активів;

– переказ віртуальних активів;

– надання посередницьких послуг, пов'язаних з продажем чи пропозицією продажу віртуальних активів.

4. Започатковується здійснення державного регулювання обігу віртуальних активів шляхом державної реєстрації постачальників послуг, пов'язаних з обігом віртуальних активів.

5. Контроль за виконанням законодавства у сфері обігу віртуальних активів покладається на Мінцифри.

Очікуємо від Верховної Ради України остаточного прийняття закону «Про віртуальні активи» та вважаємо це дуже актуальною подією, адже в Україні вже давно виникла необхідність якомога швидше врегулювати на законодавчому рівні питання, пов'язані з використанням криптовалюти, впровадити процедуру оподаткування операцій з видобутку, купівлі та продажу криптовалюти, а також визначити відповідні правила функціонування криптовалютних бірж і пунктів обміну криптовалюти.

В більшості держав світу операції з криптовалютою знаходяться в правовому полі і або повністю легалізовані, або з певними обмеженнями, такими як національна заборона на окремі види угод, тощо. Україна також не може залишитись осторонь процесів легалізації криптовалюти, адже відсутність прямої вказівки держави на закон, який потрібно застосовувати до операцій з криптовалютою створює правовий вакуум і як наслідок дуже високі ризики її використання.

Список використаних джерел

1. Про віртуальні активи : проєкт Закону України № 3637 від 11.06.2020 // ВР України : офіційний вебпортал. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69110 (дата звернення: 13.03.2021).

2. Про стимулювання ринку криптовалют та їх похідних в Україні : проєкт Закону України № 7183-1 від 10.10.2017 // ВР України : офіційний вебпортал. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=62710&pf35401 =436015 (дата звернення: 13.03.2021).

3. Про токенізовані активи та криптоактиви : проєкт Закону України № 4328 від 05.11.2020 // ВР України : офіційний вебпортал. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70353 (дата звернення: 13.03.2021).

4. Реальные деньги | Пора делиться. В Украине хотят ввести налог на криптовалюту // Інформаційне агентство ЛІГАБізнесІнформ : вебсайт. 06.08.2018. URL: https://biz.liga.net/all/it/article/pora-delitsya-v-ukraine-hotyat-vvesti-nalog-na-kriptu (дата звернення: 13.03.2021).

Одержано 27.04.2021

УДК 004.7+343.3
MAFTEA Serghei,
доктор физико-математических наук,
Академия «Штефан чел Маре» МВД Республика Молдова;
VRABIE Corneliu
Академия «Штефан чел Маре» МВД Республика Молдова

ИСПОЛЬЗОВАНИЕ ДАРКНЕТА В ПРЕСТУПНЫХ ЦЕЛЯХ

Скрытый Интернет или даркнет – это совокупность веб-сайтов, доступных только через специализированное программное обеспечение, например через браузер Tor (The Onion Router) [1]. Технология, используемая в даркнете, направлена на обеспечение анонимности и конфиденциальности онлайн-активности, последняя может быть как законной, так и незаконной. В то время как некоторые пользователи используют это средство связи и взаимодействия для защиты своих личных данных при просмотре открытого Интернета для доступа к новостным веб-сайтам, электронной коммерции, социальным сетям [2], другие – для доступа к ресурсам, заблокированным правительством, а другая категория пользователей, под прикрытием анонимности участвовать в различных преступных действиях, которые обычно связаны с товарами и услугами, например, сексуальной эксплуатацией детей, наркотиками, оружием, краденными товарами, контрафактными товарами, хакерскими инструментами. Оплата этих товаров и услуг обычно производится с помощью виртуальной валюты, такой как биткойн, которая также является анонимной [3, с. 55].

Использование даркнета в преступных целях – это быстро развивающееся явление, которое показывает изменение парадигмы в том, как совершаются преступления сегодня, что требует упреждающего и скоординированного ответа со стороны всех государств [4]. Мы считаем, что ключевую роль в этой ситуации играет помощь правительств со стороны различных международных организаций и органов в целях укрепления потенциала национальных систем уголовного правосудия по реализации положений международно-правовых инструментов по борьбе с использованием даркнета в преступных целях.

Учитывая международную осведомленность и признание, в последние годы, угрозы создаваемой использованием даркнета в уголовных деяниях и технологической инфраструктуры поддерживающей сеть даркнет, вероятно, будет довольно сложно, а может быть, даже невозможно определить универсальный специализированный инструмент для исследованиях в этой области. Кроме того, на данный момент возможности специализированного обучения персонала правовым и практическим аспектам расследования преступной деятельности, связанной с сетью даркнет, весьма ограничены.

Даркнет (темная сторона Интернета) – это среда, в которой размещается множество различных ресурсов, через / с помощью которых совершаются незаконные действия. Таким образом, даркнет – это термин, который не только относится к веб-сайтам, доступным через браузер Tor, но и представляет собой нечто большее, чем расширения .onion, поскольку существуют также альтернативные протоколы, такие как I2P (Invisible Internet Project), FreeNet, GNUnet или Riffle [5]. Ресурсы, оказывающие пагубное влияние на граждан и общество, включают криминальные рынки [6], хакерские сообщества и форумы, а также новостные ресурсы о сайтах даркнета, такие как Deep Dot Webcare который присутствовал как в даркнете, так и в открытой сети [7].

Учитывая все это, правоохранительные органы сталкиваются с рядом вопросов, один из которых можно сформулировать так: «можно ли управлять даркнетом?». Это довольно сложный вопрос, поскольку он необходим для изучения как части относящейся к технологии поддерживающей этот тип сети, так и части связанной с национальными и международными правовыми положениями, которые способствуют расследованию преступлений, совершенных через / с помощью даркнета. Таким образом, дать четкий и исчерпывающий ответ на этот вопрос довольно сложно. В качестве примера, подтверждающего этот порядок идей,

можно привести международные операции, направленные на расследование и уничтожение различных криминальных «проектов», осуществляемых и поддерживаемых в даркнете. Таким образом, против только одного «проекта» в даркнете используются операции, организованные ФБР, и скоординированные усилия 20 стран и нескольких международных организаций и органов (Европол, ФБР, Евроюст) [8].

Следственная деятельность должна предусматривать в качестве направления деятельности выявление и задержание администраторов даркнет-сайтов, продвигающих нелегальный контент. Также важно, чтобы соответствующие следственные действия также были нацелены на поиск и размещение серверов, на которых размещены эти сайты. В результате может быть достигнута цель направленные на их закрытие (ликвидация, деструктуризация) и в то же время возможность выявления, возможно, других незаконных ресурсов, размещенных на них, для идентификации операторов, клиентов этих ресурсов.

Географический спектр расположения серверов, участвующих в поддержке нелегальных ресурсов даркнета, разнообразен. Они размещаются в государствах, чьи позиции в списке стран по индексу человеческого развития чрезвычайно разнообразны, так в случае с рынком DarkMarket были задействованы такие страны, как Германия, США (рынок Уолл-стрит), которые входят в первую десятку с очень высокий уровень экономического развития, и такие страны как Украина и Молдова (DarkMarket) которые имеют высокий уровень экономического развития и средний уровень экономического развития, соответственно [8, 9].

Что касается клиентов нелегальных сайтов в даркнете, то можно с сожалением отметить, что в некоторых случаях их количество может быть огромным. Таким образом, пользовательская база даркнета Wall Street Market насчитывала около 1,15 млн человек, из которых 5400 относились к категории продавцов наркотиков, украденных данных, поддельных документов и вредоносного ПО. Для оплаты покупатели на этих онлайн-рынках использовали криптовалюты Биткойн и Монеро [10].

Следует отметить, что усилия, предпринятые для ликвидации даркнета с незаконными ресурсами, заслуживают похвалы, но они не исключают полностью преступную деятельность, поскольку появляются новые такие сайты, что доказывает, что преступный аспект даркнета не так просто остановить. Вероятно, только риски, связанных с судебным преследованием, недостаточно для сдерживания киберпреступников, что доказывает, что пользователи нелегальной среды даркнета каким-то образом привыкли к нестабильности в этой среде и не так боятся, как вначале.

На уровне координации уголовных расследований в даркнете можно выделить Европол, который выполняет роль координации действий европейских стран. В этом контексте мы хотели бы выделить комментарий исполнительного директора Европола Катрин Де Болле: «Эти расследования подчеркивают важность международного сотрудничества между правоохранительными органами и показывают, что незаконная деятельность в даркнете не так анонимна, как могут думать преступники» [11].

Даркнете – это среда, которая напрямую подчеркивает тот факт, что преступники могут действовать при поддержке транснациональной платформы, поэтому в ответ государства должны разработать технические и процедурные механизмы, чтобы действовать таким же образом на транснациональных платформах. Необходимо также подчеркнуть важность развития комплексного опыта, необходимого для удовлетворения потребностей государств в технической помощи в борьбе с этой растущей глобальной угрозой.

Преступность во всех ее формах затрагивает как отдельного человека, так и общество в целом, тем самым разрабатывая и внедряются различные тактики и процедуры для предотвращения и борьбы, однако с развитием даркнета методы расследования устаревают и и становятся неактуальными всех, в результате потенциальное воздействие на жертв не только имеет тенденцию к увеличению, но и становится устойчивым. Одна из поддержек необходимых для разработки эффективного инструмента уголовного правосудия для борьбы с этой транснациональной угрозой заключается в выделении конкретных преступных дел, связанных с даркнетом, и продвижении передовых методов расследования, ситуация, которая

должна основываться на понимании того, как коммуникационные технологии могут быть неправомерно использованы для содействия преступной деятельности и конечно, о постоянном сотрудничестве между государствами, организациями и международными структурами с соответствующим спектром деятельности.

Список використаних джерел

1. Tor project. URL: https://www.torproject.org/download (дата звернення: 12.03.2021).

2. Facebook Core. URL: https://en-gb.facebookcorewwwi.onion/ (дата звернення: 12.03.2021).

3. Maftea Serghei, Dodica Serghei, Gherman Marian. Atacuri de tip Ransomware. Chișinău, 2018, 120 p.

4. Justice. URL: https://search.justice.gov/search?query=darkweb&op=Search& affiliate=justice (дата звернення: 12.03.2021).

5. Dark Web Monitoring Service // Network Box : вебсайт. URL: https://www.network-box.com/nb5-darkWeb_monitoring (дата звернення: 12.03.2021).

6. Darkmarket: world's largest illegal dark web marketplace taken down // Europol : офіційний сайт. 12.01.2021. URL: https://www.europol.europa.eu/ newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down (дата звернення: 12.03.2021).

7. Deepdotweb shut down: administrators suspected of receiving millions of kickbacks from illegal dark web proceeds // Europol : офіційний сайт. 08.05.2019. URL: https://www.europol.europa.eu/newsroom/news/deepdotweb-shut-down-administrators-suspected-of-receiving-millions-of-kickbacks-illegal-dark-web-proceeds (дата звернення: 12.03.2021).

8. Darkmarket: world's largest illegal dark web marketplace taken down // Europol : офіційний сайт. 12.01.2021. URL: https://www.europol.europa.eu/ newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down (дата звернення: 12.03.2021).

9. Lista țărilor după indi cele dezvoltării umane // Wikipedia : вебсайт. URL: https://ro.wikipedia.org/wiki/Lista_%C8%9B%C4%83rilor_dup%C4%83_indi cele_dezvolt%C4%83rii_umane (дата звернення: 12.03.2021).

10. Double blow to dark web marketplaces // Europol : офіційний сайт. 03.05.2019. URL: https://www.europol.europa.eu/newsroom/news/double-blow-to-dark-web-marketplaces (дата звернення: 12.03.2021).

Одержано 23.04.2021

УДК 343.9.01:316.62

ПАМПУРА Ігор Іванович,
старший науковий співробітник
науково-дослідної лабораторії психологічного забезпечення
Державного науково-дослідного інституту МВС України;
ОСТАПОВИЧ Інна Петрівна,
начальник сектору ювенальної превенції
УПД ГУНП у Волинській області
майор поліції

ДЕЯКІ ЗАГРОЗИ НЕГАТИВНОГО ВПЛИВУ СОЦІАЛЬНИХ МЕРЕЖ НА ОСОБИСТІСТЬ ДИТИНИ

Сьогодні всесвітня комп’ютерна мережа стала невід’ємною частиною нашого життя. Проте слід зазначити, що вона надає можливість не тільки для розвитку здібностей, покращення знань та розширення кола інтересів, але й містить у собі реальні загрози як для дорослих, так і для дітей.

Одним із сучасних інструментів комунікації, який займає важливе місце та активно застосовується для впливу на масову свідомість є соціальні мережі, адже сьогодні діти (особи віком до 18 років) проводить все більше часу саме в них. Соціальна мережа – це інтернет-сервіс, призначений одночасно для комунікації користувачів і для розміщення і поширення ними інформації [1].

Важливо пам'ятати, що сьогодні соціальні мережі досить сильно впливають на будь-яку особистість та на процес формування її поведінки, особливо це стосується особистості дитини. Аналіз існуючого стану справ свідчить, що інформація в інтернет-мережі є недостатньо організованою та керованою тому особливого впливу (часто негативного) відчувають на собі комунікаційний, ціннісний, пізнавальний та поведінковий особистісні компоненти людини.

Неконтрольований час перебування дитини біля комп'ютера, захоплення спілкуванням у чатах та на форумах обумовлюють дезадаптацію та особистісні порушення у дитини, які проявляються у зміщеннях «Я-реального» та «Я-віртуального». Шукаючи способи втечі від реальних проблем повсякденного життя, діти потрапляють у вир інших проблем, які ведуть їх до соціальної ізоляції. Не маючи сформованих психологічних механізмів захисту вони наражають себе на ризик розвитку нав'язливих станів, втрату контролю над віртуальною реальністю, яка починає контролювати їх. Усе це відбувається на фоні зростаючих труднощів у взаємодії дітей з батьками, педагогами, а надалі – із суспільством в цілому.

Серед основних загроз негативного впливу соціальних мереж на особистість дитини вважаємо за необхідне виділити такі [2, 3]:

– загроза ознайомлення (у тому числі ненавмисного) з негативною інформацією (що несе загрозу фізичному та психологічному розвитку (зокрема, суїцидального характеру), а також інформацією, що пропагує який-небудь вид кримінальної субкультури або заборонена до поширення);

– загроза кібербулінгу (переслідування з використанням інформаційних комунікаційних технологій, в більшості випадків систематичне, інколи поєднане з реальними або уявними загрозами, що викликають у жертви почуття небезпеки або тривоги) щодо дітей, а також використання особистої інформації, розміщеної у соціальних мережах, в кримінальних цілях. До форм кібербулінгу належать і сексуальні домагання;

– загроза цілеспрямованого залучення дітей до злочинну діяльність, формування у неповнолітнього криміногенних установок, віктимної поведінки;

– загроза впливу на психічне здоров'я дитини. Для людей, особливо для неповнолітніх, інтернет-середовище іноді видається навіть більш адекватним, ніж реальний світ. Великий обсяг негативної інформації, з якою користувач стикається в соціальній мережі, здатний призвести до негативних наслідків, пов'язаних з інформаційними перевантаженнями, з протиріччями між величезними обсягами інформації та обмеженими можливостями її сприйняття і переробки, з інтернет-залежністю, а також до різних психічних розладів аж до неконтрольованої агресії;

– загроза інформаційного управління в соціальних мережах, яке здатне призвести до змін у масовій, груповій та індивідуальній свідомості, нав'язування своєї волі і перепрограмування поведінки (через подачу «спеціально створених семантичних повідомлень у вигляді текстів, відео – і аудіорядів, розрахованих на сприйняття свідомістю, осмислення і емоційний відгук» з боку об'єкта управління з метою обрання бажаної для суб'єкта управління лінії поведінки).

Сьогодні соціальні мережі швидко набувають популярності та збільшують кількість користувачів. Нажаль при значній кількості позитивних моментів функціонування соціальних мереж, вимушені констатувати, що існують і негативні фактори впливу на людину, а особливо незахищеною виявляється така вікова категорія як діти. Значна частина інтернет користувачів виявляється схильною до адикції, тобто залежності від соціальних мереж та Інтернету загалом, адже при використанні мережі вони знаходиться в зміненому стані свідомості – своєрідному психологічному трансі, в якому реальність набуває нечітких рис і зливається з віртуальністю. А це сприяє несвідомому засвоєнню значної кількості інформації яку нам надає мережа і створює умови для можливого її негативного впливу на свідомість дитини.

Список використаних джерел

1. Богдан М.С., Горецька О.В. Психологічні особливості спілкування залежних від соціальних мереж / Психологія і соціологія: проблеми практичного застосування : матеріали міжнародної науково-практичної конференції (м. Київ, 14-15 березня 2014 року). Херсон : Видавничий дім «Гельветика». С. 25-29.

2. Глущенко С.Д. Соціально-психологічні особливості Інтернет-адиктивної поведінки особистості / Молодь: освіта, наука, духовність : тези доповідей. Частина І. Київ : Університет «Україна», 2008. 547 с.

3. Робота з дітьми з ознаками ризикованої поведінки : методичні рекомендації / уклад.: В.П. Остапович, В.І. Барко, Н.Ю. Ярема, І.І. Пампура, В.В. Барко, І.П. Остапович; за заг. ред. В.О. Криволапчука. Київ : ДНДІ МВС України, 2017. 62 с.

Одержано 30.04.2021

УДК 004.491+004.056:343.85

ТИМЧЕНКО Леонід Леонідович,
кандидат юридичних наук,
директор з аналітики громадської спілки
«Глобальний центр взаємодії в кіберпросторі»

RANSOMWARE: ХАКЕРСЬКІ «ПУСТОЩІ» ЧИ ЕЛЕМЕНТ ГІБРИДНОЇ ВІЙНИ? ПОГЛЯД GC3

Програми-вимагачі (Ransomware) – це стрімко зростаюча загроза, що останнім часом набула масштабу глобального лиха. В результаті використання таких програм, хакери блокують комп'ютерні системи зашифровуючи дані, і, в подальшому, вимагають сплатити кошти, щоб розблокувати систему. За даними інформаційних агентств США, вказані програми за останні роки зачепили всіх – від банків та лікарень до університетів та муніципалітетів. Лише в минулому році жертвами таких атак стали майже 2400 організацій у США. Але, як стверджують експерти, зловмисники все частіше націлюються на промислові сектори, оскільки ці фірми охочіше платять, щоб відновити контроль над своїми системами.

Ransomware – це не просто програмний продукт, що призводить до фінансового вимагання, це злочин, який не зважає на бізнесові, державні, академічні та географічні межі. Діяльність таких продуктів також вплинула на галузь охорони здоров'я під час пандемії COVID-19, а також призвела до закриття шкіл, лікарень, поліцейських дільниць, урядових організацій та військових об'єктів США. Це злочин, який спрямовує як приватні, так і державні кошти до глобальних злочинних організацій. Прибутки, отримані від жертв вимагань, можуть фінансувати незаконну діяльність, починаючи від торгівлі людьми і закінчуючи розробкою та розповсюдженням зброї масового знищення.

Статистика станом на травень 2021:

– *21 день* – середній строк блокування системи в результаті атаки програми-вимагача [1];

– *287 днів* – середній строк, який потрібен компанії, щоб повністю відновитись після атаки програми-вимагача [2];

– *350 млн доларів США* – сплачено жертвами атак програм-вимагачів протягом 2020 року [3] (що на 311% більше ніж у 2019 році);

– *312,493 доларів США* – середньо статистична сума одноразової виплати за розблокування комп'ютерної системи, що зазнала атаки програми-вимагача [4] (що на 171% більше ніж у 2019 році).

Так, у березні 2021 року, компанія Acer зазнала атаки хакерів. За допомогою програми-вимагача REvil зловмисники вимагали від тайванського виробника найбільшу на сьогоднішній день відому суму викупу – 50 млн доларів США.

На початку травня 2021 року, представники американської паливної компанії Colonial Pipeline, що здійснює постачання палива на Східне узбережжя США, були вимушені призупинити деякі системи у роботі компанії, з метою локалізації загроз, що відбулись в результаті масштабної кібератаки. Компанією Colonial Pipeline щоденно транспортується близько 2,5 мільйонів барелей очищеного палива, що складає 45% від всього палива, яке споживається

на Східному узбережжі США. В результаті зупинки роботи найбільшого оператора-постачальника палива, компанії Colonial Pipeline, влада США оголосила режим регіональної надзвичайної ситуації у 18 штатах [5]. За даними профільних експертів та журналістів, до вказаної кібератаки можуть бути причетні хакери групи DarkSide, що нібито діє з території Російської Федерації.

Незважаючи на оприлюднену 10 травня 2021 року представниками DarkSide заяву про аполітичність та непричетність до будь-яких державних організацій [6], прояви атак на об'єкти критичної інфраструктури є елементом гібридної війни, що ведеться під контрольованим «невтручанням» представників спецслужб.

До цього, у лютому 2021 року, представники хакерського угрупування DarkSide були причетні до кібератак на бразильські енергетичні компанії [7].

Звертає на себе увагу той факт, що жертвами програм-вимагачів, здебільшого, стають організації або компанії з США, Великої Британії, Австралії та Бразилії (рис. 1) [8].

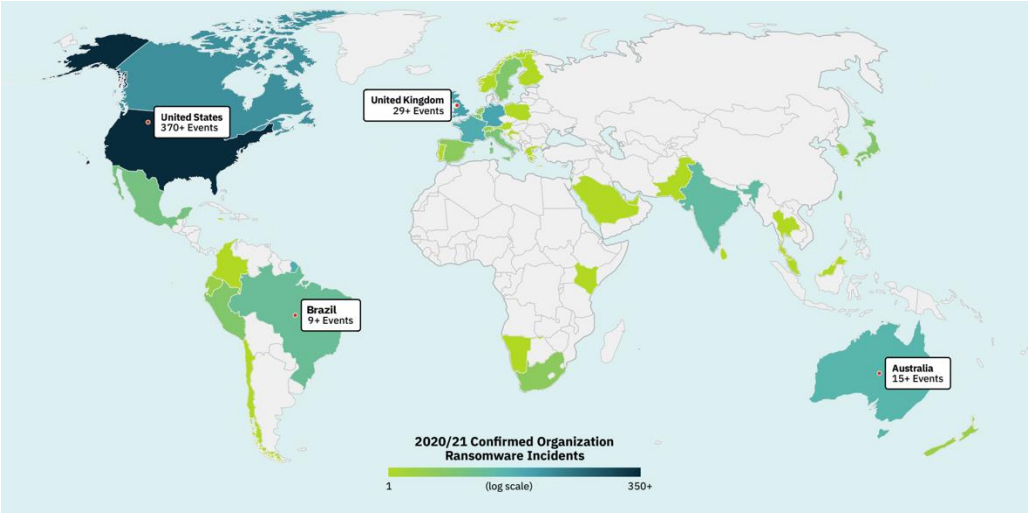

Рис. 1. Географія підтверджених випадків використання програм-вимагачів за 2020 рік – початок 2021 року

Кіберзлочинці, залучені до діяльності програм-вимагачів, процвітають завдяки уявленню про анонімність своїх злочинів. Таких осіб необхідно деанонімізувати та робити їх співіснування незручним із добропорядними громадянами.

За результатами вивчення останніх події, що призвели до втручання у роботу комп'ютерних систем за допомогою програм-вимагачів, Глобальним центром взаємодії в кіберпросторі (GC3) розроблено наступні рекомендації:

– представникам державних та приватних компаній необхідно у найкоротші строки розробити чіткий алгоритм поведінки на випадок блокування комп'ютерних систем та мереж компанії чи організації;

– обов'язково повідомляти правоохоронні органи та спеціалізовані неурядові організації про всі факти кібератак та платежі за розблокування комп'ютерних систем разом із деталями інциденту;

– якнайшвидше інформувати про проведену оплату за розблокування комп'ютерних систем, що може допомогти заблокувати кошти, для забезпечення відшкодування потерпілим та недопущення отримання грошей злочинцями;

– державним організаціям та приватним компаніям необхідно інвестувати в освіту персоналу щодо виявлення / блокування причин та умов використання програм-вимагачів, а також підготувати кожну компанію чи організацію до можливого інциденту блокування комп'ютерних систем;

– необхідно запровадити практику формування приватним бізнесом окремих коштів, що в разі необхідності будуть сплачені у якості гонорару особам-викривачам, які допомогли виявити (деанонімізувати) хакерів причетних до розробки та впровадження програм-вимагачів.

Список використаних джерел

1. Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands // Coveware : вебсайт. 01.02.2021. URL: https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020 (дата звернення: 12.05.2021).

2. The State of Ransomware in the US: Report and Statistics 2020 // Emisoft. Blog : вебсайт. 18.01.2021. URL: https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020 (дата звернення: 12.05.2021).

3. Ransomware Skyrocketed in 2020, But There May Be Fewer Culprits Than You Think // Chainalysis : вебсайт. 26.01.2021. URL: https://blog.chainalysis.com/reports/ransomware-ecosystem-crypto-crime-2021 (дата звернення: 12.05.2021).

4. Ransomware Threat Assessments: A Companion to the 2021 Unit 42 Ransomware Threat Report // PaloAlto : вебсайт. 17.03.2021. URL: https://unit42.paloaltonetworks.com/ransomware-threat-assessments (дата звернення: 12.05.2021).

5. Атаковавшие Colonial Pipeline хакеры связаны с Россией // Securitylab.ru : вебсайт. 10.05.2021. URL: https://www.securitylab.ru/news/519856.php (дата звернення: 12.05.2021).

6. Стоящие за атакой на Colonial Pipeline хакеры отрицают свою связь с политикой // Securitylab.ru : вебсайт. 11.05.2021. URL: https://www.securitylab.ru/news/519890.php (дата звернення: 12.05.2021).

7. Крупнейшие бразильские энергокомпании стали жертвами вымогательского ПО // Securitylab.ru : вебсайт. 07.02.2021. URL: https://www.securitylab.ru/news/516288.php (дата звернення: 12.05.2021).

8. Combating Ransomware. A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force // Institute for Security and Technology. 04.2021. URL: https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf (дата звернення: 12.05.2021).

Одержано 12.05.2021

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

УДК 343.983:343.34:004.77
БУРАК Марія Василівна,
кандидат юридичних наук,
старший науковий співробітник наукової
лабораторії з проблем протидії злочинності
Національної академії внутрішніх справ
https://orcid.org/0000-0002-1099-2096
ШЕВЧУК Оксана Юріївна,
кандидат юридичних наук, доцент,
доцент кафедри оперативно-розшукової
діяльності Національної академії внутрішніх справ
https://orcid.org/0000-0002-4055-1400

ВИКОРИСТАННЯ КОМП'ЮТЕРНО-ТЕХНІЧНОЇ ЕКСПЕРТИЗИ В РОЗКРИТТІ КІБЕРЗЛОЧИНІВ

З розвитком та вдосконаленням комп'ютерної техніки та програмного забезпечення особливої актуальності у розкритті кіберзлочинів набуває проведення комп'ютерно-технічних експертиз. Ці експертизи є важливим ланцюгом у доказовій базі, оскільки дозволяють побудувати цілісну систему доказів. Більш того, вони мають важливе значення для фіксації фактичних даних про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Водночас. слід враховувати, що прямими доказами використання певного обладнання із злочинною метою будуть сліди злочину, аналогічні зафіксованим на обладнанні потерпілого. Тому, обов'язковим є встановлення місцезнаходження та вилучення програмно-технічних засобів, із використанням яких було вчинено злочин, і забезпечення їх комп'ютерно-технічного дослідження.

Так, для якісного забезпечення комп'ютерно-технічних досліджень вилучають: системний блок; клавіатуру (на відбитки пальців); периферійні пристрої тощо. Обов'язково повинні досліджуватися носії інформації: жорсткий диск; зовнішні запам'ятовуючі пристрої; компакт-диски, дискети, пристрої флеш-пам'ять тощо. Крім того, на розгляд експертам надаються: інструкції з користування вилученими носіями (пристроями); опис програмного забезпечення; аркуші з нотатками правопорушника (імена, паролі, адреси тощо).

При призначенні технічного дослідження вказується серійний номер комп'ютера та його індивідуальні ознаки (конфігурація, колір, написи на корпусі), описується механізм вчинення злочину, зокрема, використане обладнання та програмне забезпечення, недоліки у комп'ютерній техніці, програмному забезпеченні та захисних системах потерпілого. Додатково описуються технічні засоби та програмне забезпечення злочинця і потерпілого, включаючи операційні системи та версії [1].

На розгляд експертів виносяться питання щодо: будови інформаційних та телекомунікаційних мереж; призначення та можливостей відповідних технічних засобів; призначення та можливостей програмних засобів; інформації, яка зберігається (зберігалася) на відповідних програмно-технічних засобах, оброблюється (оброблювалася) за їх допомогою; впливу, якого зазнали програмно-технічні засоби та інформація, що ними оброблялася.

Разом з тим, на опрацювання експертами можуть ставитись такі питання:

а) щодо технічних засобів: яке функціональне призначення наданого на дослідження апаратного засобу? Який фактичний стан (справний, несправний) наданого на дослідження

апаратного засобу? Чи є наданий на дослідження апаратний засіб носієм інформації? Який вид (тип, модель, марку) має наданий на дослідження носій інформації? Який пристрій використовується для роботи з наданим носієм інформації? Чи входить до складу досліджуваної комп'ютерної системи пристрій для роботи із вказаним носієм інформації, або його аналогами?

б) щодо програмних продуктів: яка загальна характеристика наданого на дослідження програмного забезпечення, з яких компонентів (програмних засобів) воно складається? Яке загальне функціональне призначення має програмний засіб? Який загальний алгоритм даного програмного засобу? Чи можна за допомогою даного програмного продукту реалізувати функції, передбачені технічним завданням на його розробку? Який фактичний стан програмного засобу, яка його працездатність щодо реалізації окремих функцій? Яким шляхом організовано введення вхідних даних та виведення результатів роботи у наданому на дослідження програмному засобі? Чи має програмний засіб захисні можливості (програмні, апаратно-програмні) від несанкціонованого доступу та копіювання? Яким шляхом організовані захисні можливості програмного засобу? Яка вартість програмного продукту на момент його придбання, (вилучення, проведення експертизи)? (для встановлення вартості програмного продукту експертові надається носій з копією досліджуваного програмного продукту і еталонна (дистрибутивна) копія програмного продукту, що реалізується на вітчизняному ринку програмних засобів);

в) щодо інформації, яка зберігається та оброблюється за допомогою програмно-технічних засобів: чи містить даний носій будь-яку інформацію і якщо так, то яке її цільове призначення? Які властивості, характеристики й параметри (об’єм, дата створення та редагування, атрибути та ін.) мають дані на носії інформації? В якому вигляді (явному, прихованому, видаленому) міститься інформація на носії? До якого типу відносяться виявлені дані (текстові, графічні, бази даних, електронні таблиці, мультимедійні, запис пластикової карти тощо) і які програмні засоби для їх обробки присутні на носії інформації? Які дані про власника (користувача) комп’ютерної системи (у т. ч. імена, паролі, права доступу та ін.) містить носій інформації?

Власне, убачається, що проведення комп’ютерно-технічних експертиз є найбільш вагомою та кваліфікованою формою використання спеціальних знань під час розслідування кіберзлочинів, можливості якої в процесі доказування не вичерпані й потребують комплексного дослідження, удосконалення та розроблення нових способів і методів виявлення, фіксації та вилучення слідів, а також методик їх дослідження.

Список використаних джерел

1. Попередження та розкриття кіберзлочинів : курс лекцій / Д.Й. Никифорчук, В.Г. Хахановський, Г.М. Бірюков та ін. // За загал. ред. Никифорчука Д.Й. Київ. 2012. 299 с.

Одержано 29.03.2021

УДК 343.9:[004.738.5:316.613.434]

ЄРМОЛЕНКО Богдан Сергійович,
курсант 3 курсу факультету № 4
Харківського національного університету внутрішніх справ;
КЛІМУШИН Петро Сергійович,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій і кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-1020-9399

КІБЕРБУЛІНГ В СОЦІАЛЬНИХ МЕРЕЖАХ: ВИХОВНА РОБОТА З ДІТЬМИ ТА ПІДЛІТКАМИ

Кібербулінг, мобінг, тролінг – не так давно ніхто навіть не замислювався над значенням цих слів, а сьогодні цькування в інтернеті стало предметом занепокоєння не лише на державному, та і на міжнародному рівнях. З кожним роком кількість користувачів світової мережі

неухильно зростає, а також збільшення часу до комп'ютера отримують діти, що технічно веде до збільшення можливостей стати жертвою насильства. Дослідники віртуальної спільноти відзначають, що кількість інформаційної продукції, яка пропагує насильство постійно зростає.

Мета: визначити актуальність проблеми психологічного насилля в мережі Інтернет та його впливу на соціальне життя людей та їх психічний стан.

Кібербулінг це залякування і цькування з використанням цифрових технологій, має місце в додатках для обміну повідомленнях, соціальних мережах та ігрових платформах. Метою є налякати, розсердити чи зганьбити тих, кого переслідують в мережі**.** Поширення неправдивої інформації, розміщення фотографій інтимного характеру інших осіб в соціальних мережах, відправлення непристойних повідомлень та погроз, видача себе за іншу особу і дія від його імені – все це приклади кібербулінгу.

Масово всеукраїнське опитування учнів 8 і 10 класів усіх макрорегіонів України стосовно інтернет-ризиків у контексті дослідження масштабу кібербулінгу показало, що старшокласники стикалися: 14% зі спрямованими на себе знущаннями в Інтернеті; 21% розповсюдження неправдивої інформації; 20% викрадання персональних даних [1].

Американські дослідники Робін Ковальські, С'юзан Лімбер і Патриція Агатстон виділяють вісім видів пагубної негативної поведінки в мережі Інтернет, тобто кібербулінгу:

1) флеймінг – словесна війна, яка частіше за все спалахує через непорозуміння чи образи на віртуального співрозмовника;

2) харассмент – некоректні висловлювання, жарти, дії, жести та інші вчинки, які лякають, зачіпають або принижують людину з перевантаженням особистих каналів комунікації;

3) наклеп – розповсюдження принизливої неправдивої інформації в мережі Інтернет;

4) видання себе за іншу особу – булер позиціонує себе як жертву та здійснює негативну комунікацію;

5) ошуканство – отримання персональної інформації в особистому листуванні і передача її (текстів, фото, відео) в публічну зону Інтернету або іншими шляхами третім особам;

6) остракізм – відчуження, виключення жертви з віртуального середовища;

7) кіберпереслідування – це дії з прихованого стеження за особою та її оточенням, зазвичай зроблені анонімно, з метою організації злочинних дій;

8) хепіслепінг – запис відеороликів, в яких містяться реальні напади, і які потім розміщують в Інтернеті, без жодної згоди жертви.

Доречно було б зауважити, що зараз загальна увага прикута до підліткових захоплень, так званих «груп смерті»: «Біжи або помри», «Зникни на 24 години», «Синій кит" та ін. Що це таке? Якщо не грати словами, то учасники таких «груп» – це люди, які готують власну смерть під керівництвом адміністратора групи – куратора. Їм поетапно надсилають завдання, останнім з яких є суїцид.

Куратори таких груп найчастіше самі виходять на підлітків, заводять розмову, запрошують до гри. Такі спільноти в соціальних мережах завжди закриті, що додає їм привабливості в очах підлітків – «Мене запросили, значить я – обраний!». Найпопулярніша така гра в Україні – «Синій кит». Правила цієї гри дуже прості: людина веде зворотний відлік від 50 днів, і кожен наступний день куратор надсилає завдання, на виконання якого в учасника є 24 години. На день "1" повинен скоїтись суїцид. У цей день йому присвоюється "номер" і надсилається повідомлення такого типу: "Ви кит №23, стрибок», де останнє слово є способом самогубства.

Але як уберегтися від кібербулінгу? Уникайте довірчих відносин з віртуальними знайомими, не піддавайтесь на прохання про що-небудь в онлайн-середовищі. При реєстрації на будь-яких сайтах і в соціальних мережах слід подбати про свою конфіденційність, не поширювати відомості про себе та своїх близьких. Пам'ятайте, що люди, які ображають вас, як правило, мають купу проблем, і просто намагаються відчути себе краще, нападаючи на вас [2].

У висновку хотілося б зазначити, що проблема кібербулінгу актуальна на даний момент та є серйозною загрозою для психічного здоров'я не тільки підростаючого покоління. На сьогоднішній день деякі існуючі методи боротьби з інтернет-насиллям не працюють у зв'язку з швидким розвитком і розширенням форм цього явища, тому це спонукає нас до

розробки нових форм та методів протистояння кібербулінгу. Основою цих норм повинно буди виховання та діалог. На основі отриманих знань підлітки зможуть приймати правильні рішення, знати і розуміти принципи, необхідні для того, щоб залишатися в безпеці.

Список використаних джерел

1. Найдьонова Л. А. Кібербулінг у підлітковому рейтингу інтернет-небезпек. *Психологічні науки: проблеми і здобутки*. 2018. Вип. 1. С. 141-159.

2. Міхеєва О.Ю., Корнієнко М.М. Кібербулінг як соціально-педагогічна проблема. *Молодий вчений*. 2018. № 11 (63). С. 247-251.

Одержано 19.04.2021

УДК 004.032.26+343.72

КОВТУН Вікторія Олександрівна,
курсантка 3 курсу факультету № 4
Харківського національного університету внутрішніх справ
http://orcid.org/0000-0003-1263-5970
РВАЧОВ Олексій Михайлович,
старший викладач кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
http://orcid.org/0000-0002-3500-9393

ЩОДО ПРОБЛЕМИ ОЦІНКИ ВАРТОСТІ ІНФОРМАЦІЇ

В усі часи інформація була і є одним із найважливіших ресурсів. Але при роботі з нею багато-хто не підозрює про можливі загрози щодо втрати, модифікації, крадіжки даних, а також про те, якої шкоди це можуть завдати ці інциденти [1].

Питання оцінки вартості інформації є одним з ключових для інформаційної безпеки, адже при організації захисту інформації природним чином постає питання щодо цінності інформації, яка підлягає захисту (не тільки в плані її вартості), так як витрати на захист не повинні перевищувати можливі втрати.

Але поняття вартості інформації на сьогоднішній день є мало дослідженим, а числова оцінка цієї вартості різними учасниками ринку виконується в більшості випадків на інтуїтивній основі, оскільки відсутні загальноприйняті методики [2].

Для оцінки використовуються різні, розроблені для цієї галузі, моделі цінності інформації: адитивна модель, аналіз ризику, порядкова шкала цінностей, решітка цінностей, зокрема, MLS-решітка (англ. Multilevel security) – решітка багаторівневої безпеки, що використовується в державних стандартах оцінки інформації [3].

Слід відзначити, що коли говорять про вартість інформації, то мають на увазі: по-перше, її грошове вираження, тобто ціну; по-друге, ту ціну, яку в даний момент вона має.

Поняття вартості інформації загалом розглядалося в різних літературних джерелах. Так, Л. Ф. Єжова зазначає, що «ціна інформації – вартість придбання її у зовнішньої організації» [4]. І. Г. Чалий пояснює поняття вартості інформації з точки зору бухгалтерського обліку і фінансової звітності [5]. Математичне визначення грошової суми, яку можна заплатити за отримання інформації, визначено в наказі Державного комітету статистики України від 16.03.2005 № 73. На момент затвердження наказу вартість інформації на одній сторінці становила 0,98 грн. Інформація на одній сторінці паперового носія не залежить від обсягу її заповнення, формату та виду [6].

Інформація також може бути отримана внаслідок здійснення інформаційної діяльності.

На практиці більшість компаній підходить до оцінювання витрат на інформацію, виходячи, перш за все, із своїх реальних можливостей і ціни на послуги «продавців» інформації, наприклад, компаній, що проводять маркетингові дослідження [7].

Інформаційні витрати – це витрати часу та грошей, необхідні для отримання інформації.

Розрахунок вартості витрат має бути обґрунтованим і залежати від реальних потреб та витрат розпорядника. Розмір відшкодування повинен бути встановленим в межах граничних норм, які затверджені постановою Кабінету Міністрів України від 13.06.2011 № 740. Для копіювання та друку однієї сторінки документа формату А4 передбачено не більше, ніж 0,2 відсотка розміру прожиткового мінімуму для працездатних осіб за виготовлення однієї сторінки [8]. На час ухвалення цієї постанови сума становила 0,96 грн., а на сьогодні – 4,54 грн. [9].

Можна спробувати визначити вартість інформації з точки зору бухгалтерського обліку і фінансової звітності. Наприклад, при визначенні собівартості інформації, що зберігається у певній базі даних (далі – БД) можна врахувати наступні суми витрат на:

1) знаряддя праці:
– придбання або оренда технічних засобів (комп'ютерне та мережне обладнання);
– придбання або оренда програмного забезпечення;
2) оплату праці персоналу:
– керівництва;
– програмістів;
– операторів;
– адміністраторів БД;
– охоронців;
– прибиральниць приміщень;
– тощо;
3) амортизаційні витрати на утримання приміщення;
4) оплату комунальних послуг:
– опалення;
– водопостачання;
– водовідведення;
– електричної енергії;
– тощо;

В інформаційній безпеці, коли розглядається питання захисту від витоку інформації, слід з'ясувати два головні чинники: ймовірність компрометації цієї інформації і потенційний збиток внаслідок цього.

Наприклад, цінність деталі, створеної на заводі, визначається безліччю різних чинників, серед яких: трудовитрати, попит і стан ринку, проте ціна цієї деталі все-таки піддається осмисленню і більш-менш постійна.

Креслення цієї самої деталі також є дуже цінною інформаціє. Однак якщо креслення потрапить у відкритий доступ – вартість цього креслення стане дорівнювати нулю.

Різниця між ціною креслення і деталі полягає в тому, що забезпечити швидкий і безкоштовний доступ до нескінченної кількості деталей неможливо, а ось з інформацією, у даному випадку з кресленням, таке може статися. Таким чином, цінність інформації продиктована її обмеженістю.

Цінність інформації не дорівнює потенційному збитку від компрометації.

Наприклад, у організації є важлива інформація, така як плани логістичних процесів на складі або схема роботи конвеєрів для різної продукції, але ця інформація є важливою тільки для самої організації. Для конкурентів або зловмисників вона не представляє цінності, тому її потрапляння у відкритий доступ можна не побоюватися. Однак втрата цієї інформації може боляче вдарити по організації.

Головною загрозою у разі втрати певної цінної інформації виступає не компрометація інформації, а її втрата, внаслідок збою, помилки або дії шкідливого програмного забезпечення, наприклад, вірусів-шифрувальників.

При розгляді критеріїв оцінки вартості інформації не варто упускати суму витрат на проведення розслідування факту втрати інформації.

На практиці достовірно з'ясувати точну вартість інформації, що знаходиться у володінні організації, практично неможливо. Будь-яка оцінка буде приблизною.

Наслідки будь-якого інциденту у сфері інформаційної безпеки важкопрогнозовані. Завдання для організації – по-перше, не допустити цього інциденту, а по-друге максимально знизити потенційний збиток.

Список використаних джерел

1. Ковтун В. О. Забезпечення цілісності та конфіденційності інформації в базах даних // Тези доп. учасників XXVII наук.-практ. конф. курсантів та студентів «Сучасна наука і правоохоронна діяльність» / МВС України, Харків. нац. ун-т внутр. справ, Наук. т-во студентів, курсантів, слухачів, аспірантів, ад'юнктів, докторантів і молодих вчених. Харків : ХНУВС, 2020. С. 82-83.

2. Мачуга Р. І. Визначення вартості додаткової управлінської інформації. *Ефективна економіка.* 2014. № 8. URL: http://www.economy.nayka.com.ua/?op=1&z=3230 (дата звернення: 30.04.2021).

3. Грушо А. А., Тимонина Е. Е. Теоретические основы защиты информации. Москва : Изд-во «Яхтсмен», 1996. 192 с.

4. Єжова Л. Ф. Інформаційний маркетинг : навч. посібник. Київ : КНЕУ, 2002. 560 с.

5. Чалий І., Момот Т. Суттєвість та вартість інформації – український формат та зарубіжний досвід. *Бухгалтерський облік і аудит.* 2002. № 11. С. 29-31.

6. Про встановлення вартості одного людино-дня та вартості інформації на одній сторінці : наказ Державного комітету статистики України від 16.03.2005 № 73 // БД «Законодавство України» / ВР України : офіційний вебпортал. URL: https://zakon.rada.gov.ua/laws/show/z0334-05 (дата звернення: 30.04.2021).

7. Економіка підприємства: магістерський курс : підручник. Ч. 1 / М. В. Загірняк [та ін.] ; ред. М. В. Загірняк, П. Г. Перерва, О. І. Маслак. Кременчук : ТОВ «Кременчуцька міська друкарня», 2015. 736 с.

8. Про затвердження граничних норм витрат на копіювання або друк документів, що надаються за запитом на інформацію : постанова Кабінету Міністрів України від 13.06.2011 № 740 // БД «Законодавство України» / ВР України : офіційний вебпортал. URL: https://zakon.rada.gov.ua/laws/show/740-2011-п (дата звернення: 30.4.2021).

9. Буртник Х. Дорогий доступ до інформації: за що платять запитувачі // Центр демократії та верховенства права : вебсайт. 29.07.2019. URL: https://cedem.org.ua/analytics/dorogyj-dostup/ (дата звернення: 30.04.2021).

Одержано 30.04.2021

УДК 343.97:004.77

ЛИЗОГУБЕНКО Євген Віталійович,
кандидат юридичних наук,
доцент кафедри оперативно-розшукової діяльності
Національної академії внутрішніх справ
https://orcid.org/0000-0001-5428-7172

ДЕТЕРМІНАНТИ КІБЕРЗЛОЧИННОСТІ

Стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції.

Водночас поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення, персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави [1]. Агресія Російської Федерації, що триває, інші докорінні зміни у зовнішньому та внутрішньому безпековому середовищі України вимагають невідкладного створення національної системи кібербезпеки як складової системи забезпечення національної безпеки України.

Відтак боротьба з кіберзлочинністю не може бути ефективною без встановлення її детермінант.

В механізмі детермінації кіберзлочинності можна умовно виділити такі групи чинників: соціальні, політичні, економічні, технологічні, психологічні, а також чинники пов'язані з діяльністю правоохоронних органів та віктимною поведінкою потерпілих. Утім, доречним убачається розглядати їх не розрізнено, а в межах наступних груп: політичні, правові, економічні та психологічні детермінанти.

Так, політичні чинники виявляються у недостатньому усвідомленні урядом можливих соціальних наслідків кіберзлочинності. У зв'язку з цим, обмежуються бюджетні фінансування робіт зі створення правової, організаційної, технічної бази інформаційної безпеки держави та захисту прав і свобод громадян в віртуальному просторі. Фактично не виділяються кошти на фундаментальні та прикладні вітчизняні дослідження у сфері запобігання кіберзлочинності.

Слід сказати, що у групі правових детермінант, одразу необхідно звернути увагу на недосконаліть правового регулювання державної політики у сфері кібербезпеки. Зокрема, відповідно до Стратегії кібербезпеки України, затвердженої Указом Президента України від 5 березня 2016 року №96/2016 передбачається створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [1]. Однак, слушно зазначається, що в Україні цей документ хоча і називається стратегією, проте визначені в ньому основні засади кібербезпеки у світовій практиці не зовсім вважаються стратегічними. Головним атрибутом у закордонних стратегіях передбачається перелік конкретних проектів забезпечення кібербезпеки із кінцевим терміном їх реалізації, з виділеним фінансуванням і, що найголовніше, конкретними відповідальними. Водночас, до правових детермінант кіберзлочинності в Україні необхідно відносити недосконаліть організації системи органів, що розслідують кібернетичні злочини і притягають суб'єктів їх вчинення до відповідальності, а також некомпетентність посадових осіб цих органів. Наприклад, в Україні простий кіберзлочин – «зламування» сайту, наприклад, сторінки у соцмережі, організована групова злочинна діяльність, наприклад, атака на інтернет-банкінг це справа кіберполіції. Однак, відімкненням електростанції від міської мережі вже займається СБУ як кібертероризмом. Коли ж відбуваються кібератаки по всій країні, які супроводжуються військовою агресією, повноважним органом є Збройні сили України [2, с. 331].

Економічні чинники проявляються у значній прибутковості кіберзлочинів. Повідомлення зарубіжних науковців свідчать, що кіберзлочинність за рівнем кримінального збагачення займає третє місце після торгівлі зброєю та наркотиками. За оцінками Рахункової палати уряду США, щорічний дохід злочинців тільки від розкрадань та шахрайств, вчинених з використанням комп'ютерних технологій через інтернет, досягає 5 млрд. дол. Ці показники щорічно збільшуються пропорційно зростанню у структурі національної та міжнародної економіці сектора торгівлі та надання послуг через електроні (комп'ютерні) засоби телекомунікації.

Психологічні чинники зумовлені особливостями функціонування віртуального простору. У реальному світі існують певні стримувальні засоби, а у віртуальному – злочинці не можуть бачити своїх жертв, яких вони вибрали для атаки. Красти у тих кого ти не бачиш, до кого не можеш доторкнутися рукою, набагато легше. Немає фізичної шкоди, кровопролиття та інших атрибутів небезпеки. Злочини у мережі – це злочини на відстані. У зв'язку з цим, у винних осіб є певне усвідомлення анонімності та відсутності безпосереднього ризику бути виявленим та притягнутим до кримінальної відповідальності [2, с. 332].

Отже, на наше переконання, основними детермінантами кіберзлочинності є: соціально-економічна ситуація в країні; відсутність виваженої державної політики у сфері кібербезпеки; низький рівень формування ефективних правоохоронних структур; загострення міждержавних відносин з Російською Федерацією; не захищеність українських інтернет-банкінгу та online-магазинів; необачне використання українцями електронних грошей, а також активний розвиток хакерської субкультури тощо. Відтак подальший аналіз зазначених факторів, а також вироблення механізмів їх подолання, повинні сприяти становленню кібербезпеки в Україні.

Список використаних джерел

1. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 5 березня 2016 року № 96/2016 // БД «За-

конодавство України» / ВР України : офіційний вебпортал. URL: http://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 13.04.2021).

2. Грицюк Ю. І. Кіберінтервенція та кібербезпека України: проблеми та перспективи їх подолання. *Науковий вісник НЛТУ України*. 2016. Вип. 26.8. С. 327-337. URL: http://nbuv.gov.ua/-UJRN/nvnltu_2016_26 (дата звернення: 15.04.2021).

Одержано 15.04.2021

УДК 519.7:537.8

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

ПІДВИЩЕННЯ ПОКАЗНИКІВ ЕФЕКТИВНОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ СУДОВОЇ ЕКСПЕРТИЗИ ЗА РАХУНОК ЗАСТОСУВАННЯ ВЕЙВЛЕТ-ПЕРЕТВОРЕНЬ

У результаті аналізу даних, які обробляються при проведенні експертиз, встановлено, що стрімкий прогрес технічних засобів фотозйомки, відеозапису, телекомунікаційних технологій розширює як можливості традиційних засобів фіксації фото-, відеоданих, так і нових (мобільних, мережевих, спеціалізованих, космічних) із новими форматами даних, вимагає постійного оновлення спеціальних експертних знань у галузі дослідження цифрових фотозображень. Існуючі методи обробки зображень проте не вирішують повною мірою завдання їх ефективного представлення, що робить пошук нових ефективних методів представлення зображень актуальним. Для вирішення цього завдання запропоновано використання ортогональних перетворень. У докладі вирішена актуальна науково-технічна задача підвищення показників ефективності інформаційної системи судової експертизи за рахунок вибору більш ефективних адаптивних ортогональних перетворень інформації.

В теперішній час існує значна кількість методів обробки, фільтрації, стиску, розпізнання і передачі інформації, які відповідають завданням судової експертизи цифрових зображень. Вони дозволяють побудувати загальну схему досліджень, порядок дій експерта при попередньому дослідженні, дії при візуальному аналізі та аналізі метаданих у межах аналітичного дослідження. Однак слід зауважити, що ефективність візуального аналізу цілком залежить від кваліфікації та стану зору експерта й містить значний суб'єктивний фактор. Аналіз метаданих є ефективним лише в разі примітивних підробок, бо EXIF-дані фотографії можуть бути легко відредаговані існуючими EXIF-редакторами.

Проте за методикою, використання різних методів (ELA, PCA, wavelet та ін.) [1-5] у межах розширеного аналізу зображень означено лише концептуально без конкретних рекомендацій щодо обмежень їх використання та запобігання отримання експертом хибного висновку – визначення ознак фотомонтажу або ретушування за відсутності таких (помилка першого роду), або визначення їх відсутності в редагованому зображенні (помилка другого роду). Це змушує експертів застосовувати означені та інші методи на свій розсуд, з урахуванням свого досвіду, що призводить до протилежних висновків різних експертів за одним і тим самим провадженням.

Використання для аналізу зображень існуючих методів комп'ютерної обробки дозволяє отримати більше інформації про досліджувані зображення, визначити акти зміни зображення і істотно скоротити час, необхідний на передачу цих зображень [3-7].

Одним з найбільш перспективних засобів обробки зображень є вейвлет-перетворення сигналу, яке є сигнально-незалежним [5-7]. Октаво смужне розбиття спектра, вироблене їм, підходить для більшості, але не для всіх реальних сигналів. Бажано було б мати перетворення,

адаптоване до сигналу, подібно ПКЛ, але має швидкий алгоритм виконання. Це еквівалентно тому, що перетворення було б здатне довільно змінювати структуру розбиття частотна-часової площини в залежності від сигналу. Каскадне з'єднані блоки вейвлет фільтрів дозволяють досягти цього. Вейвлети можуть бути ортогональними, напівортогональнимі, біортогональними. Ці функції можуть бути симетричними, асиметричними і несиметричними. Розрізняють вейвлети з компактною областю визначення і не мають такої. Деякі функції мають аналітичний вираз, інші – швидкий алгоритм обчислення пов'язаного з ними вейвлет-перетворення. Вейвлети розрізняються також ступенем гладкості. Все це розмаїття визначає основний напрямок досліджень, проведених в даному докладі-аналіз застосовності різних варіацій вельвет перетворення для обробки зображень в інтересах судової експертизи.

Метою даної статті є визначення можливості використання адаптивних перетворень, що на основі введеної функції вартості реалізують довільне розбиття частотна-часовій площині сигналу.

Для досягнення поставленої мети необхідно вирішити такі приватні задачі:

– провести аналіз так званих пакети вейвлетов, або адаптації в частотної області;

– проаналізувати алгоритм подвійного дерева, або адаптацію базису розкладання як в частотній, так і в просторової областях;

– провести дослідження розмірності бібліотеки базисів для всіх перетворень і їх обчислювальної складності.

У результаті проведених досліджень були отримані такі наукові результати:

1. Було розглянуту адаптивні ортогональні перетворення, побудовані на базі вейвлет-перетворень. Під адаптивністю тут розуміється автоматичний вибір базису для сигналів як в частотній, так і в просторовій областях.

2. Проаналізовано методи, що дозволяють здійснювати адаптацію в частотній області (вейвлет-пакети – алгоритм одиночного дерева), спочатку в часовій, потім – в частотній (алгоритм подвійного дерева), одночасно в обох областях (алгоритм частотно часового дерева). Недоліком цих методів є обмеження на бінарне розбиття в часовій області. Від цього недоліку вільний метод гнучкої сегментації, заснований на динамічному програмуванні.

3. Показано кількість базисів, які перебираються кожним алгоритмом, обчислювальна складність і ефективність застосування для стиснення зображень. Загальна тенденція така, як і слід було очікувати: чим складніше обчислювальні ресурси алгоритмів, які реалізують методи, що запропоновані, тим вища їх ефективність. Таким чином, перспективи застосування того чи іншого методу залежать від їх конкретних додатків.

4. Ймовірно, кращі результати можуть бути досягнуті, якщо відокремити процес сегментації від перетворення за допомогою пакетів вейвлетів. На даний час розроблені ефективні алгоритми сегментації, які можуть бути з успіхом застосовані. Після сегментації кожен сегмент приводиться до прямокутного виду, і над ним виконується перетворення з використанням пакетів вейвлетів.

Подальші дослідження бажано присвятити вивченню застосування запропонованих методів для конкретних додатків.

Список використаних джерел

1. Gersho A., Gray R. M. Vector Quantization and Signal Compression. Kluwer Academic Publishers, Norwell, MA, 1992.

2. Goyal V. K., Zhuang J., Vetterli M. Transform coding with backward adaptive updates. *IEEE Trans. Inf. Theory.* 2000. № 46(4). pp. 1623–1633.

3. Kovacevic J., Goyal V. K., Vetterli M. Fourier and Wavelet Signal Processing. Cambridge Univ. Press, 2014.

4. Strang G., Fix G. An Analysis of the Finite Element Method. Wellesley-Cambridge Press, 2nd edition, 2008.

5. Unser M. Splines: A perfect fit for signal and image processing. *IEEE Signal Process*. 1999. № 16(6). pp. 22–38.

6. Wilkie D. Pictorial representation of Ken-dall's rank correlation coefficient. *Teachmg Statistics.* 1980. Vol. 2. pp. 76-78.

7. Kliuiev O., Uhrovetskyi O., Simakova-Yefremian E., Mozhaiev M., Mozhaiev O. Method of forensic research on image for finding touch up on the basis of noise entropy // 3rd International Conference on Advanced Information and Communications Technologies (AICT). Lviv, Ukraine. 2-6 July 2019.

Одержано 01.05.2021

УДК 343.9

OLBER Paweł,
Doctor of the Science of Law,
Senior Lecturer at the Department of Forensics and Computer Forensics,
Institute of Criminal Service, Police Academy in Szczytno, Poland

THE ROLE AND IMPORTANCE OF COMPUTER FORENSICS IN COMBATING CYBERCRIME

Cybercrime is one of the serious threats of the modern world. This phenomenon has gained strength and has become very troublesome, both for citizens and for law enforcement agencies and the judiciary. There is a reason cybercrimeis one priority of EMPACT (European Multidisciplinary Platform Against Criminal Threats) defined within the European Union Security Policy Cycle 2018-2021.

The major aim adopted assumption is to combat cybercrime by disrupting the criminal activities related to attacks against information systems, combat child sexual abuse and exploitation, including the production and dissemination of child abuse material and combat fraud and counterfeiting of non-cash means of payments [1].

With the rapid growth of cybercrime, law enforcement and justice authorities need to keep on top of the new technologies. It also needs efforts to use new technologies to combat cybercrime.

Scientific law enforcement activities in the face of cybercrime

One example of the use of pioneering solutions in the fight against cybercrime is research being conducted at the Police Academy in Szczytno, Poland. This research investigates the use of convolutional neural networks in computer forensics for images content recognition and classification [2]. The primary aim of this research is to gain new knowledge and to implement artificial intelligence algorithms for the automatic classification of multimedia files containing criminal content. The need for this research stems from the need to optimise the research process of digital data carriers carried out as part of computer forensic research. Indeed, the fight against cybercrime requires reducing the working time of law enforcement agencies concerning digital evidence analysis, which will help to increase their effectiveness.

The current state of affairs

Its time-consuming nature and diversity characterise computer forensics. This is because of the different digital data carriers that are analysed in police forensic laboratories. Another element that contributes to the time-consuming nature is that investigators secure digital evidence for a range of criminal proceedings. Digital forensic investigation is now the most important source of evidence in cybercrime cases. Computer forensic experts use binary copies of digital evidence, done using dedicated tools. Then, using specialised software, they conduct time-consuming analyses that reveal information numbering in the thousands or even millions of records. This is because of the constantly growing amount of digital content and the increasing capacity of storage devices. The exponential increase in the amount of data requiring analysis within the framework of computer forensic examinations translates into long-lasting examination times [3].

This is because of the constantly growing amount of digital content and the increasing capacity of storage devices. The exponential increase in the amount of data requiring analysis within the framework of computer forensic examinations translates into long-lasting examination times. One can suppose, following global trends, that the problems related to data growth will deteriorate with time. According to data presented by IDC, today over 5 billion consumers collect, process or exchange data every day, and by 2025 this number will reach 6 billion, or 75% of the

world's population. Projections show that in 2025 every person with access to the Internet will have at least one interaction with data every 18 seconds. Billions of networked devices generate many of these interactions around the world, which in 2025 will produce 90 ZB of data [4]. We can therefore expect that the volume of data will continue to increase, requiring complex analyses as part of digital forensic investigations. The current situation, as well as the forecasts presented for the growth of digital data, therefore encourage efforts to optimise digital investigations and reduce their duration.

One technique for optimising digital forensic investigation in content analysis of digital data carriers is removing irrelevant files. For this purpose, experts use databases containing so-called file hashes [5]. Another solution is the functionality to analyse the colour and pixel arrangements in the image, which allows the automatic classification of files. However, the expert must perform a final verification of the file contents [6, p. 668 – 669].

Proposed solution

The existing state prompts to solve the identified problem situation. Considering the capabilities of artificial neural networks in the analysis and recognition of image content, they can provide a solution to the problem in computer forensics and thus increase the effectiveness in combating cybercrime.

The analysis of the literature shows that computer forensic experts do not use neural networks to examine digital evidence. Besides, the review shows that only a few authors have undertaken scientific research in the above area. In this context, it is important to note the work of Al-Nabki et al. [7], who investigated the use of artificial neural networks in identifying criminal content recorded on file names. Artificial neural networks for text file identification and categorisation based on lexical databases are another interesting solution [8].

Conclusions

The applied solutions in computer forensics for optimising the research process are insufficient. The rapid growth of information stored in digital data storages is one of the fundamental problems of computer forensics. Solving the identified problem situation requires the use of the latest IT solutions. Artificial neural networks deserve attention, apply which by law enforcement authorities should optimise the analysis of digital evidence and thus increase the effectiveness of cybercrime fighting.

Список використаних джерел

1. EU POLICY CYCLE – EMPACT. URL: https://www.europol.europa.eu/empact (last accessed: 20.04.2021).

2. List of research tasks conducted at the Police Academy in Szczytno, Poland. URL: http://www.wspol.edu.pl/ibir/index.php/wykaz-zadan-badawczych (last accessed: 20.04.2021).

3. Central Forensic Laboratory of the Police, Computer research. URL: https://clkp.policja.pl/clk/badania-i-projekty/langnodata/badania-informaty czne/153011,Badania-Informatyczne.html (last accessed: 20.04.2021).

4. Seagate, The Digitization of the World – Data Age 2025. URL: https://www.seagate.com/pl/pl/our-story/data-age-2025 (last accessed: 20.04.2021).

5. NIST, The National Software Reference Library (NSRL), URL: https://www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl (last accessed: 20.04.2021).

6. Kowalski B., Radziszewski R. *Ekspertyza informatyczna*, (red:) M. Kała i in., Ekspertyza sądowa. Zagadnienia wybrane, Warszawa, 2017. 668 – 669 p.

7. Al-Nabki M. W., Fidalgo E., Alegre E., & Aláiz-Rodríguez R. (2020). File Name Classification Approach to Identify Child Sexual Abuse: Proceedings of the 9th International Conference on Pattern Recognition Applications and Methods – Volume 1: ICPRAM, Malta: Valletta, 2020. 228–234 p. https://doi.org/10.5220/0009154802280234.

8. Pereira M., Dodhia R., & Brown R. Metadata-Based Detection of Child Sexual Abuse Material. 2020. P. 1–9 ArXiv:2010.02387 [Cs]. URL: http://arxiv.org/abs/2010.02387 (last accessed: 20.04.2021).

Одержано 22.04.2021

УДК 378:004
ОРЛОВ Роман Русланович,
курсант 3 курсу факультету № 4
Харківського національного університету внутрішніх справ;
ОНИЩЕНКО Юрій Миколайович,
кандидат наук з державного управління, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ
http://orcid.org/0000-0002-7755-3071

ВИЯВЛЕННЯ ПІДОЗРІЛИХ ФІНАНСОВИХ ОПЕРАЦІЙ, ЯКІ МОЖУТЬ БУТИ ПОВ'ЯЗАНІ З ВІДМИВАННЯМ ДОХОДІВ, ОТРИМАНИХ У СФЕРІ КІБЕРЗЛОЧИННОСТІ

Незважаючи на винахідливість кіберзлочинців і використання широкого інструментарію для схем легалізації незаконних доходів, представляється можливим розділити фінансові операції за рівнем ризику. Більш того, можливо також визначити сфери і послуги, які мають підвищений ризик і, відповідно, вимагають підвищеної уваги. Слід зазначити, що клієнтам, які встановлюють ділові відносини з банком або користуються банківськими послугами з використанням новітніх технологій без безпосереднього контакту з банком часто встановлюється більш високий рівень ризику відмивання злочинних доходів. Індикаторами підозрілості фінансових операцій зазначеної спрямованості для банківських установ побічно можуть бути наступні фактори:

– спроба входу з забороненої / нової IP-адреси;

– спроба використання прострочених первинних / робочих або старих ключів після сертифікації нових;

– використання для банківських операцій IP-адрес або імен користувачів, щодо яких попередній моніторинг виявив причетність до шахрайських операцій;

– проведення трансакції в нестандартний час або підключення до системи у вечірній час;

– незвичайні умови або складність операції: висока частота переказів протягом невеликого періоду часу, велика кількість різноманітних джерел походження коштів і платіжних методів (інструментів);

– особа не поінформована про характер діяльності юридичної особи, яку вона представляє;

– особа не може пояснити необхідність надання тієї чи іншої банківської послуги;

– залучення до проведення операцій осіб молодого віку і / або новостворених підприємств; проведення операцій з використанням загублених документів;

– відкриття рахунку, на який зараховуються кошти в результаті несанкціонованого списання незадовго до проведення таких операцій;

– спроби зняти кошти в день їх зарахування;

– спроби клієнта отримати дві або більше банківських карт, що не відповідає суті його діяльності або обороту.

Надзвичайно швидкий розвиток інформаційних і комп'ютерних технологій останнім часом призводить до стрімкого розвитку кіберзлочинності, тому особливої актуальності набувають питання попередження та протидії злочинам у кіберпросторі.

Удосконалення нормативно-правового забезпечення у сфері запобігання та протидії легалізації доходів, пов'язаних зі злочинами в сфері кіберзлочинності, можливо також за наступними напрямками: посилення відповідальності за злочини в сфері комп'ютерних та інформаційних технологій; введення обов'язкової ідентифікації при особистому контакті клієнтів, що користуються послугами дистанційного банківського обслуговування або електронних платіжних систем; визнання електронних документів та інших електронних даних в якості доказової бази при розслідуванні кіберзлочинів; регулювання питань, що стосуються юрисдикції, при наданні послуг через інтернет; зниження кількості анонімних платежів і

переказів грошових коштів; введення сертифікації електронних платіжних засобів; чітка регламентація механізмів взаємодії між клієнтом і банком, між банком відправника грошей і банком одержувача коштів у разі несанкціонованого списання коштів клієнта.

З метою попередження кіберзлочинів банківськими установами можуть впроваджуватися такі технічні та організаційні заходи: періодичний огляд банкоматів для виявлення незаконно встановлених пристроїв; впровадження для клієнтів банку карт з мікропроцесором (чіпом), як більш захищених від підробки; ведення «чорного» списку рахунків (ідентифікаційних кодів, IP-адрес) шахраїв для своєчасного блокування операцій; вимоги двохфакторної / двоканальної автентифікації; використання токенів для зберігання електронних цифрових підписів; обов'язкове інформування клієнтів про кожну проведену операцію; підтвердження платежу в телефонному режимі; генерація клієнтського ключа самим клієнтом, що робить неможливим вчинення неправомірних дій з боку працівників банку; прив'язка ключа клієнта до серійного номеру жорсткого диску / флеш-накопичувача, що унеможливлює копіювання ключів і доступ до сторінки клієнта за допомогою інших комп'ютерів; використання ряду логічних правил для типових / нетипових / підозрілих платежів в системі Клієнт-Банк; використання клієнтом окремого комп'ютера, який призначений тільки для системи Клієнт-Банк (інтернет-банкінг), з налаштованими мережевими фільтрами; статистичний аналіз трафіку (Netflow) для виявлення аномалій; введення лімітів на проведення операцій в мережі Інтернет.

Одержано 08.04.2021

УДК [004;343.6]

ПЕРЕЦЬ Олексій Вячеславович,
курсант 3 курсу факультету № 4
Харківського національного університету внутрішніх справ;
ОНИЩЕНКО Юрій Миколайович,
кандидат наук з державного управління, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
http://orcid.org/0000-0002-7755-3071

ВИКОРИСТАННЯ ВІРТУАЛЬНИХ БАНКІВСЬКИХ КАРТОК, ЯК ЗАХІД ПРОТИДІЇ ШАХРАЙСЬКИМ ДІЯМ

Завдяки зручності використання системи дистанційного банківського обслуговування (далі – ДБО) активно застосовуються майже всіма верствами населення як в Україні, так і за кордоном нашої держави. Пластикова банківська карта – платіжний інструмент, який набагато зручніше і, головне, вигідніше готівки. Але у пластикових карток є і недоліки: можливість механічного пошкодження або втрати, наприклад внаслідок крадіжки. Карту завжди можна перевипустити або заблокувати, але це зайвий клопіт. Потрібно бути обережним, розраховуючись нею на касах або знімаючи готівку в банкоматах. Різними способами шахраї при цьому можуть спробувати дізнатися реквізити картки: номер, термін дії, CVV-код, пін-код.

Пластику є альтернатива – віртуальні картки, які позбавлені цих недоліків. Це банківські карти, у яких є всі ті ж реквізити, що і у звичайних. Додавши таку карту в смартфон (технології ApplePay і GooglePay), користувач ДБО значно збільшує ступінь безпеки розрахунків за допомогою свого платіжного інструменту, що є досить актуальним у період всесвітньої пандемії, коли різко зросла кількість шахрайств, які вчиняють злочини з використанням платіжних інструментів та онлайн-сервісів у мережі Інтернет.

Віртуальну картку не потрібно носити з собою і тому неможливо втратити. У магазині ніхто не зможе підгледіти її реквізити, адже в процесі оплати держатель платіжного інструменту підносить до терміналу не карту, а смартфон. Але головне призначення віртуальних

карт – платежі в інтернеті. Сплачуючи покупки в мережі, доводиться вводити карткові дані на різних сайтах, що не завжди безпечно. Для цих цілей краще всього використовувати саме віртуальну карту. Відкрити її можна в будь-який момент, в більшості банків зробити це можна безкоштовно, і перерахувати на неї саме ту суму, яку плануєте витратити онлайн. В результаті шахраї, якщо і заволодіють реквізитами картки, то все одно не отримають ваші гроші.

Поруч із банківськими установами підрозділи Департаменту кіберполіції Національної поліції України ведуть активну превентивну діяльність щодо запобігання кіберзлочинам у банківській сфері, зокрема шахрайським діям, що вчиняються із застосуванням ДБО та платіжних інструментів. Доведення до відома населення України очевидних переваг використання віртуальних карток – важливий крок превентивного характеру у сфері запобігання шахрайським діям зловмисників.

Отже, коли справа йде про інтернет-покупки слід не забувати про такий спосіб забезпечення безпеки власних заощаджень як використання віртуальних карток. Саме популяризація серед населення даного платіжного інструменту суттєво вплине на зменшення кількості шахрайських дій у сфері електронної комерції та ДБО.

Превентивна діяльність, спрямована на запобігання злочинам у сфері ДБО, зокрема використання платіжних інструментів, повинна здійснюватися за допомогою комплексного підходу – із залученням зусиль усіх зацікавлених суб'єктів: правоохоронних органів, державних та комерційних фінансових установ, міжбанківських асоціацій, органів державної влади та представників приватного сектору, а також засобів масової інформації. Доречним вважається залучення закладів вищої освіти зі специфічними умовами навчання до проведення просвітницьких заходів щодо безпечного користування платіжними інструментами у загальноосвітніх школах під час профорієнтаційної роботи, адже фінансовій та комп'ютерній грамотності в умовах сьогодення слід навчати саме з дитячого віку.

Одержано 14.04.2021

УДК 343.13
ПОЛІТОВА Анна Сергіївна,
кандидат юридичних наук, доцент

СТАТТЯ 149 КРИМІНАЛЬНОГО КОДЕКСУ УКРАЇНИ: ЧИ НАГАЛЬНА ПОТРЕБА УДОСКОНАЛЕННЯ?

Протидія торгівлі людьми постійно привертає увагу наукової спільноти, спонукаючи вчених, представників правоохоронних органів до обговорення проблем удосконалення чинного Закону про кримінальну відповідальність. Натомість, складається враження, що ініціатори внесення змін та доповнень до КК України – народи депутати України, вносячи зміни та доповнення, криміналізуючи або декриміналізуючи суспільно небезпечні діяння «граються». Така думка виникає якщо проаналізувати Проєкт Закону про внесення змін до Кримінального кодексу України щодо посилення кримінальної відповідальності за торгівлю людьми (реєстр. № 5134 від 22.01.2021).

1. Частина 1 ст. 149 КК України «Торгівля людьми» передбачає відповідальність за торгівля людиною, а так само вербування, переміщення, переховування, передача або одержання людини, вчинені з метою експлуатації, з використанням примусу, викрадення, обману, шантажу, матеріальної чи іншої залежності потерпілого, його уразливого стану або підкупу третьої особи, яка контролює потерпілого, для отримання згоди на його експлуатації.

Така назва та редакція ч. 1 аналізуємої статті, з'явилася після того, як 06 вересня 2018 р. Верховна Рада України прийняла проєкт Закону України «Про внесення змін до статті 149 Кримінального кодексу України (щодо приведення у відповідність до міжнародних стандартів)» (реєстр. №6243 від 27.03.2017), поданий народними депутатами України

І. Луценко, О. Третьяков, В. Король, І. Геращенко, С. Войцеховська, А. Бабак, О. Кондратюк, Я. Безбах, В. Развадовський, М. Іонова, Ю Мірошниченко.

Обґрунтовуючи необхідність внесення змін до ст. 149 КК України, ініціаторами законопроєкту відзначалось, що «як засвідчив правовий аналіз вказаної статті, окремі її положення, зокрема в частині визначення поняття «торгівля людьми» не відповідають положенням Конвенції ООН проти національної організованої злочинності та Протоколу до неї про попередження і припинення торгівлі людьми, особливо жінками і дітьми, і покарання за неї. Так, положеннями національного законодавства, зокрема статтею 149 КК України не надано чіткого визначення поняттю «торгівля людьми», що ускладнює правозастосування вказаної статті КК України на практиці» [1].

2. 22 січня 2021 р. на сайті Верховної Ради України опубліковано проєкт Закону про внесення змін до Кримінального кодексу України щодо посилення кримінальної відповідальності за торгівлю людьми (реєстр. № 5134). Цей законопроєкт подано народними депутатами України Д. Лубінцем, Т. Батенко, Д. Люботою, А. Пушкаренко, С. Мандзієм, М. Перебийнісом, О. Бакумовим, Р. Умєровим, М. Нікітіною, А. Поляковим, О. Горобцем та ін.

Як запропоновано посилити кримінальну відповідальність за торгівлю людьми? Ініціатори законопроєкту вважають, що ст. 149 КК України потребує таких змін:

1) у абзаці першому частини першої статті 149 після слів «торгівля людиною» доповнити словами «або здійснення іншої незаконної угоди, об'єктом якої є людина,»;

2) у абзаці другому частини другої статті 149 слово «п'яти» замінити словом «шести»;

3) у примітці статті 149 після третього абзацу доповнити четвертим абзацом «4. Відповідальність за вербування, переміщення, переховування, передачу або одержання людини за цією статтею настає незалежно від наявності згоди цієї людини на експлуатацію, якщо до неї було використано примус, викрадення, обман, шантаж, матеріальна чи інша залежність потерпілого, його уразливий стан або підкуп третьої особи, яка контролює потерпілого, для отримання згоди на його експлуатацію» [2].

Цікавим є те, що обґрунтовуючи необхідність прийняття законопроєкту, вони відзначають, що «не зважаючи на висновки Головного науково-експертного управління Верховної Ради України та зауваження Головного юридичного управління Верховної Ради України, із диспозиції статті 149 Кримінального кодексу України було виключено поняття «здійснення іншої незаконної угоди, об'єктом якої є людина», що на практиці призвело до складнощів притягнення до кримінальної відповідальності осіб, які вчиняють дії, направлені на передачу або отримання людини, не маючи на меті її експлуатацію. Як приклад таких дій: дарування, оренда, надання у безоплатне користування, передача людини в рахунок погашення боргу тощо» [2].

Не вдаючись у глибокий аналіз щодо поняття «торгівля людьми» у міжнародно-правових актах, відзначимо, що у 2020 р. було обліковано 206 кримінальних правопорушень, серед яких у 110 кримінальних провадженнях вручено особам підозру. Чи багато це? Ні, оскільки за своєю суття торгівля людьми є латентним злочином, що має об'єктивні та суб'єктивні причини.

Але вносячи зміни до ст. 149 КК України, автори законопроєкту чомусь випадково забувають, що відповідно до Закону України від 20.09.2011 № 3739-VI «Про протидію торгівлі людьми», торгівля людьми – це *здійснення незаконної угоди, об'єктом якої є людина* (вид. А.С.П.), 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 [3].

Крім того, виходячи із Пояснювальної записки до проєкту Закону про внесення змін до Кримінального кодексу України щодо посилення кримінальної відповідальності за торгівлю людьми, вони вказують у п. 3 Загальна характеристика та основні положення законопроекту про «*виключення із об'єктивної сторони статті 149 такої форми злочинного діяння, як «здійснення іншої незаконної угоди, об'єктом якої є людина»* [2], що дає підстави вважати

цей законопроєкт «грою», адже одночасно пропонується і доповнити і виключити вищезазначене словосполучення.

Список використаних джерел

1. Про внесення змін до статті 149 Кримінального кодексу України (щодо приведення у відповідність до міжнародних стандартів) : проєкт Закону України № 6243 від 27.03.2017 // ВР України : офіційний вебпортал. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=61428 (дата звернення: 30.04.2021).

2. Про внесення змін до Кримінального кодексу України щодо посилення кримінальної відповідальності за торгівлю людьми : проєкт Закону № 5134 від 22.01.2021 / ВР України : офіційний вебпортал. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=71204 (дата звернення: 30.04.2021).

3. Про протидію торгівлі людьми : Закон України від 20.09.2011 № 3739-VI // БД «Законодавство України» / ВР України : офіційний вебпортал. URL: https://zakon.rada.gov.ua/laws/show/3739-17 (дата звернення: 30.04.2021).

Одержано 30.04.2021

УДК [004;343.6]

САЄНКО Денис Леонідович,
курсант 3 курсу факультету № 4
Харківського національного університету внутрішніх справ;
ОНИЩЕНКО Юрій Миколайович,
кандидат наук з державного управління, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
http://orcid.org/0000-0002-7755-3071

ВИДИ КІБЕРЗЛОЧИНІВ ТА СПОСОБИ ЗАХИСТУ ВІД НИХ

Зловмисна прив’язка до злому вперше була задокументована в 1970-х роках, коли ранні комп’ютеризовані телефони ставали мішенню. Підковані в техніці люди, відомі як «фрікери», знайшли спосіб оплати міжміських дзвінків за допомогою ряду кодів. Вони були першими хакерами, які навчились використовувати систему, модифікуючи апаратне та програмне забезпечення для крадіжки телефонного часу на великій відстані. Це змусило людей усвідомити, що комп’ютерні системи вразливі до злочинної діяльності, і чим складніші системи ставали, тим більш сприйнятливими вони були до вчинення кіберзлочинів.

Відомий випадок стався 1990 року, коли був викритий великий проект під назвою «Операція Сандевіл». Агенти ФБР вилучили 42 комп'ютери та понад 20000 дискет, які використовувались злочинцями для незаконного використання кредитних карток та телефонних послуг. У цій операції взяли участь понад 100 агентів ФБР, і знадобилося два роки, щоб розшукати лише кількох підозрюваних. Це був наочний спосіб показати хакерам, що за ними слідкуватимуть і будуть переслідувати.

Кіберзлочинність зростає такими ж швидкими темпами, як і кількість нових користувачів, які підключаються до цифрового світу. Подібно до того, як у реальному світі є хороші і погані люди, є користувачі інтернету, які використовують свої знання з кібербезпеки, щоб допомогти іншим (також відомі як білі капелюхи або етичні хакери). Є й ті, хто використовує свої цифрові навички для поширення страху та створення хаосу.

Кіберзлочинність в інтернеті щорічно завдає збитків організаціям, компаніям та урядам на мільярди доларів. Нажаль незаконна діяльність в інтернеті не має тенденцій уповільнення, навпаки – дедалі більше зростає. Дослідження Gallup доводить, що громадян більше турбує кіберзлочинність, аніж безпосередньо небезпечні для життя злочини, такі як вбивство чи тероризм.

Що таке кіберзлочинність? Якщо говорити просто, кіберзлочинність – це злочин, вчинений в інтернеті, в локальних мережах або навіть проти ізольованих комп’ютерів, може

впливати на будь-які цифрові пристрої (включаючи ПК, ноутбуки, смарт-телевізори, планшети, смартфони, електронні системи тощо). Кіберзлочинці загальновідомі як хакери, хоча цей термін технічно неточний, правильний термін – «зломщик».

Класифікація кіберзлочинів поділяється на чотири основні категорії, які базуються на тому, хто постраждав від цифрової злочинності.

Кіберзлочини проти фізичних осіб – злочини, що безпосередньо впливають на людину (соціальна інженерія, фішинг, переслідування електронною поштою, кіберсталінг та розповсюдження незаконних матеріалів).

Кіберзлочини проти юридичних осіб компаній (організацій): порушення даних, кібервимагання та розповсюдження warez (програм, які розповсюджується незаконним шляхом з порушенням прав правовласника) тощо.

Кіберзлочини проти суспільства: фінансові злочини проти громадських організацій, продаж нелегальної продукції, незаконна торгівля, азартні ігри в інтернеті, підробка тощо.

Кіберзлочини проти уряду, зокрема кібертероризм, проникнення в урядові системи та мережі, поширення пропаганди, розміщення у мережі контенту, що має на меті дезінформацію, залякування тощо.

Важливість кібербезпеки зростає. Принципово, що наше суспільство більш технологічно залежне, ніж будь-коли раніше, і немає жодних ознак того, що ця тенденція сповільниться. Витоки даних, які можуть призвести до крадіжки особистих даних, тепер публічно публікуються в акаунтах соціальних мереж. Конфіденційна інформація (номери соціального страхування, дані кредитної картки та реквізити банківських рахунків) тепер зберігаються в хмарних сховищах, таких як Dropbox, Google Drive тощо.

Незалежно від статусу (фізична особа, малий бізнес, велика компанія) користувачі щодня покладаються на інформаційно-телекомунікаційні та комп'ютерні системи. Зі зростанням темпів та обсягів використання хмарних сервісів, їхнім недосконалим рівнем безпеки, уразливостями операційних систем та іншого програмного забезпечення смартфонів та інтернет-сервісів маємо безліч загроз в мережі.

Більшість користувачів інтернету не усвідомлює реальність реалізації та наслідки потенційних загроз мережі (можливість зламу їх акаунтів, компрометації банківських платіжних інструментів, заволодіння персональними даними тощо) та навіть рідко змінює свої облікові дані або оновлює паролі.

Тому, актуальним залишається питання поінформованості населення щодо елементарних правил кібергігієни: необхідність проявляти пильність під час перегляду вебсайтів; ніколи не натискати на незнайомі посилання чи оголошення у листах електронної пошти, що надходять від незнайомців; за можливості використовувати VPN; перш ніж вводити облікові дані, слід переконатися, що вебсайт безпечний; оновлювати антивірусне програмне забезпечення; використовувати надійні паролі з восьми та більше символів різних типів (цифри, літери верхнього та нижнього регістрів, спеціальні символи); не встановлювати однакові паролі на різні облікові акаунти, облікові записи до інтернет-сервісів та системи дистанційного банківського обслуговування тощо.

Одержано 20.04.2021

УДК 343.3/.7
ФІАЛКА Михайло Ігоревич,
кандидат юридичних наук, доцент,
доцент кафедри кримінального права і кримінології факультету № 1
Харківського національного університету внутрішніх справ

СУТНІСТЬ ПОНЯТТЯ «ІНФОРМАЦІЇ» В РОЗДІЛІ XVI КРИМІНАЛЬНОГО КОДЕКСУ УКРАЇНИ ТА ЇЇ ВПЛИВ НА КВАЛІФІКАЦІЮ СУСПІЛЬНО НЕБЕЗПЕЧНОГО ДІЯННЯ

В кримінальному законодавстві України в межах питання охорони сфери використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку активно використовуєть поняття «інформація». Розділ XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Кримінального кодексу України (далі – КК України) містить в своїй структурі шість кримінально-правових норм (ст.ст. 361, 361-1, 361-2, 362, 363 та 363-1 КК України) в чотирьох з яких використовується цей термін [1]. Крім того, за офіційною статистичною інформацією приблизно 98% кримінальних правопорушень, які зареєстровані за останні вісім років (2013-2020 рр.), містять в собі ті які передбачають у власних складах кримінальних правопорушень поняття «інформації». Іншими словами, актуальність врахування поняття «інформації» під час кримінально-правового аналізу та майбутньої кваліфікації таких суспільно небезпечних діянь має вельми високий рівень.

Визначення змісту цього терміну, а саме – інформація, в науковому просторі характеризувалось та тлумачилось неодноразово і в певній мірі має чітко окреслене розуміння. Крім того, поняття інформації регламентовано на законодавчому рівні, а саме в ст. 1 Закону України «Про інформацію» наголошується на тому, що інформація це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [2].

Одночасно з цим, в Законі України «Про авторське право і суміжні права» закріплюються ряд нормативно-правових термінів, які активно використовуються у сфері використання електронно-обчислювальних машин (комп'ютерів), а сам: електронна (цифрова) інформація та комп'ютерна програма. При цьому, під електронною (цифровою) інформацією розуміють аудіовізуальні твори, музичні твори (з текстом або без тексту), комп'ютерні програми, фонограми, відеограми, програми (передачі) організацій мовлення, що знаходяться в електронній (цифровій) формі, придатній для зчитування і відтворення комп'ютером, які можуть існувати і (або) зберігатися у вигляді одного або декількох файлів (частин файлів), записів у базі даних на зберігаючих пристроях комп'ютерів, серверів тощо у мережі інтернет, а також програми (передачі) організацій мовлення, що ретранслюються з використанням мережі Інтернет.

Комп'ютерна програма – набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи у будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером, які приводять його у дію для досягнення певної мети або результату (це поняття охоплює як операційну систему, так і прикладну програму, виражені у вихідному або об'єктному кодах) [3].

Свого часу, аналізуючи проблему визнання комп'ютерної інформації предметом злочину, С. О. Орлов наголошував на тому, що комп'ютерна програма – це комп'ютерна інформація (дані), побудована за певними правилами (сукупність інструкцій, команд), що здатна змусити комп'ютерну систему й/або телекомунікаційну мережу виконувати ту чи іншу функцію [4, с. 82].

З наведених положень вищезазначених нормативно-правових актів ми бачимо те, що поняття «інформації» в певній мірі має багатогранний характер та зміст.

Внаслідок цього виникає певна проблема: під час юридичної оцінки суспільно небезпечного діяння який зміст поняття «інформація» використовувати і як це вплине на кваліфікацію цього діяння.

Зрозуміло те, що в межах невеликого повідомлення розкрити, обґрунтувати та надати практичні рекомендації в цьому питанні фізично неможливо. Але окреслити проблемне

питання та визначитись з основними правовими підходами його розв'язання – завдання, яке можливо виконати в межах такого невеликого наукового аналізу.

Узагальнюючи підходи до розуміння змісту поняття «інформації» можливо наголосити на тому, що даний термін в межах Розділу XVI КК України розуміється з одного боку як інформація загального розуміння (спираючись на поняття яке закріплюється ЗУ «Про інформацію»), а з іншого боку – мова йде про електронну інформацію у виді комп'ютерної програми.

Такий стан речей створює особливий підхід в питанні кваліфікації суспільно небезпечного діяння. Справа полягає в тому, що у випадку, якщо діяння, яке передбачено як суспільно небезпечне тієї чи іншої кримінально-правової норми даного розділу, посягає на електронну інформацію, то кваліфікація повинна відбуватись за тією статтею Розділу XVI КК України в якій таке діяння передбачене як ознака об'єктивної сторони. Одночасно з цим, у випадку, коли посягання відбувається на інформацію загального характеру (наприклад, здійснюється внесення недостовірної інформації в електронні документи, які зберігаються в електронно-обчислювальних машинах шляхом несанкціонованих дії з цією інформацією), то кваліфікація повинна відбуватись за сукупністю кримінальних правопорушень, а саме: за підроблення документів (ст.ст. 358 або 366 КК України) та за відповідною статтею Розділу XVI КК України.

Список використаних джерел

1. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III // БД «Законодавство України» / ВР України : офіційний вебпортал. URL: http://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 13.04.2021).

2. Про інформацію : Закон України від 02.10.1992 № 2657-XII // БД «Законодавство України» / ВР України : офіційний вебпортал. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 15.04.2021).

3. Про авторське право і суміжні права : Закон України від 23.12.1993 № 3792-XII // БД «Законодавство України» / ВР України : офіційний вебпортал. URL: https://zakon.rada.gov.ua/-laws/show/3792-12 (дата звернення: 15.04.2021).

4. Орлов С. О. Комп'ютерна інформація як предмет злочину. *Право і безпека.* 2005. № 4. С. 81-85.

Одержано 30.04.2021

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

УДК 004.7

ВОДЯНИЦЬКИЙ Кирилл Юрійович,
заступник начальника 1-го відділу (оперативного реагування)
Управління протидії кіберзлочинам в Харківській області
Департаменту кіберполіції Національної поліції України,
полковник поліції

ТЕХНОЛОГІЯ БЛОКЧЕЙН В РОБОТІ ПРАВООХОРОННИХ ОРГАНІВ

По всьому світу правоохоронні органи стикаються зі схожими проблемами: злочини стають більш технологічними, обсяг пов'язаних з ними даних безперервно збільшується, а ресурси і бюджети для вирішення поточних завдань скорочуються. При цьому підвищуються вимоги до забезпечення прозорості роботи і підзвітності громадському контролю.

Дані, які мають правоохоронні органи, в тому числі, в ході розслідувань, стають все більш різноманітними і складними, часто розподіляються за багатьма різнорідними інформаційно-технологічними системами в різних типах і форматах.

Одним з варіантів вирішення проблеми «зв'язності» і «простежуваності» даних в роботі правоохоронних органів може стати використання технології блокчейн, яка, зокрема, дає можливість створення безперервно доступних, відмовостійких розподілених систем зберігання та ідентифікації даних, пов'язаних зі злочинами та їх розслідуванням. В тому числі, цифрових даних (фото-, відео-, аудіоматеріали, тексти повідомлень, записи транзакцій тощо), а також оцифрованих ідентифікаторів матеріальних і речових доказів. На технології блокчейн також можуть бути засновані національні та міжнародні системи пошуку та ідентифікації осіб і транспортних засобів, пов'язаних зі злочинами.

Над створенням систем управління та зберігання доказів, заснованих на технології блокчейн, зараз активно працюють державні установи та IT-компанії у багатьох країнах світу: Китаї, Індії, Великобританії, Канаді, США тощо. Зрозуміло, що в разі використання розподілених технологій в правоохоронній сфері, мова йде не про застосування публічних блокчейн (Bitcoin, Ethereum, Waves тощо), а про використання приватних, «корпоративних» блокчейнів (Hyperledger Fabric, Exonum, Corda, Vostok тощо), оптимально – з можливістю верифікації та призначення користувальницьких ролей.

Наприклад, Міністерство юстиції Великобританії ретельно вивчає питання застосовності розподілених технологій в правосудді і, в цілому, вважає підтвердженими важливе значення блокчейна для створення системи для управління цифровими доказами, їх захисту і забезпечення точності ланцюжків доказів.

Простим прикладом може бути затримання підозрюваного поліцейським, який має «штатну» переносну відеокамеру. Особливої актуальності цей приклад набуває через його «органічну вбудовуваність» в концепт громадської безпеки «розумного» міста.

При роботі відеокамера створює відеофайли невеликого хронометражу і послідовно відправляє їх в захищене хмарне сховище через безпечний канал зв'язку. Одночасно з надходженням файлу в хмарне сховище в мережі блокчейн створюється його «цифровий зліпок» – на основі даних і метаданих (формат, розмір та інші технічні характеристики, яким пристроєм було зроблено запис, де і в який час тощо) криптографічний алгоритм генерує унікальний ідентифікатор малого розміру – цифровий підпис («геш»). Цей підпис, яким підтверджено файл в сховище, записується в блокчейн. Підпис використовується тільки для наступних перевірок достовірності (відповідності оригіналу), конфіденційні дані розслідування залишаються в безпеці. Перевірка справжності файлу та відповідність його оригінальному підпису буде простою і швидкою.

У міру просування розслідування (звернення до відеофайла для перегляду, копіювання, використання для створення звітів тощо) нові геш-підписи автоматично генеруються і зв'язуються з основним підписом відеофайлу, а не порушують його. У тому ж випадку, якщо станеться спроба змінити сам файл (або замінити його іншим файлом), підпис буде також безповоротно змінено і ніколи не зможе бути ідентичним первинному підпису (записаному в блокчейн).

Кінець-кінцем, суд, прокуратура, захисники зможуть самостійно перевірити історію відеодоказу, справжність якого буде підтверджена криптографічними алгоритмами.

В цілому, технологія блокчейн в роботі правоохоронних органів також може бути корисна для:

– підвищення доступності оперативних даних, включаючи також бази доказів, пов'язаних з актуальними розслідуваннями і архівними справами, з підтвердженням їх «справжності»;

– підвищення «простежуваності» і прозорості зберігання даних і, отже, підвищення рівня підзвітності та довіри до роботи правоохоронних органів.

З урахуванням все більшого використання технології блокчейн у всьому світі, його широке застосування в роботі правоохоронних органів залишається лише питанням часу.

Одержано 01.05.2021

УДК 004.056.53

ГНУСОВ Юрій Валерійович,
кандидат технічних наук, доцент,
завідувач кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
http://orcid.org/0000-0001-5435-5921
КАЛЯКІН Сергій Володимирович
викладач кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
http://orcid.org/0000-0001-5435-5921

ПРО ДЕЯКІ ПРОБЛЕМИ ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Кількість атак із використанням шкідливого програмного забезпечення з кожним роком все більше і більше зростає. У 2020 році кількість таких атак зросла на 54% щодо показника 2019 року. Тренд 2020 року в атаках на організації – застосування шифрувальників, їх доля серед шкідливого програмного забезпечення складала 45%.

Триває зростання кількості безфайлових вторгнень, боротися з якими без аналітичного механізму засобів EDR (Endpoint Detection and Response) практично неможливо. Цей тип загроз зберігає файли в оперативній пам'яті, тоді як типові антивірусні програми спрацьовують тільки при запису файлу на диск.

EDR вміє відслідковувати події на рівні системи і мережі, а технології машинного навчання і поведінкового аналізу дозволяють виявляти невідомі погрози і розширюють можливості для розслідування інцидентів. Тому EDR-рішення здатні виявити нестандартну шкідливу активність, для якої відсутні сигнатури. Тригером може стати як підозріла активність безфайлових вірусів або раніше невідомих шкідливих програм, так і, наприклад, поведінку співробітників компанії, ошуканих за допомогою методів соціальної інженерії.

EDR працює на стику автоматизації та людської участі в розслідуванні, тому може виявити навіть такі інструменти злому, які раніше не зустрічалися і були розроблені для обходу відомих існуючих засобів захисту кінцевих точок. Це ефективне рішення проти загроз, що маскуються під легітимні інструменти ОС: програми для віддаленого управління і адміністрування і подібні ім.

Відповідно до останнього звіту, який був представлений компанією Sophos, великі світові кіберзлочинні угрупування продовжують активно співпрацювати у сфері розробки шкідливого програмного забезпечення, створюючи справжні хакерські картелі.

Експерти Sophos відзначили, що оператори програм-вимагачів постійно розроблюють нові методи обходу антивірусних і захисних рішень, щоб дістатися до добре захищених резервних копій, які організації-жертви зберігають у місцях, куди шифрувальники потрапити не можуть. В рамках звіту виділено кілька основних трендів кіберзлочинності в галузі шкідливого програмного забезпечення:

– хакери продовжують впроваджувати інноваційні рішення в свої шкідливі технології;

– велика частина хакерських груп, що поширюють шкідливе програмне забезпечення, займається крадіжкою даних задля викупу за нерозголошення конфіденційної інформації;

– проведені сьогодні атаки програм-вимагачів займають від декількох десятків хвилин до декількох годин, хоча раніше на цей процес займав декілька днів;

– хакери можуть без перешкод пройти захист систем безпеки, побудованих на машинному навчанні, застосовуючи «універсальні атаки підстановки рядків» (в результаті цього системи машинного навчання сприймають програми-вимагачі і шифрувальники, вважаючи їх легальним ПО).

– недостатня увага компанії до одного або декількох базових аспектів інформаційної безпеки лежить в основі великих і найбільш руйнівних кібератак.

Компанія Cisco також опублікувала дослідження з кібербезпеки 2021 Security Outcomes Study, результати якого допоможуть ІБ-фахівцям вибрати напрямок розвитку їх відділів в 2021 році. У звіті наводяться конкретні заходи, що сприяють зміцненню кібербезпеки. Наведені в звіті рекомендації допоможуть службам кібербезпеки не тільки управляти ризиками, але також розширювати можливості бізнесу і підвищувати ефективність операцій.

Важливий фактор успішного забезпечення кібербезпеки – грамотно інтегрований технологічний стек. Це позитивно впливає практично на всі проаналізовані параметри, збільшуючи ймовірність загального успіху в середньому на 10,5%. Варто відзначити, що інтеграція також сприяє залученню і утриманню фахівців – служби забезпечення кібербезпеки вважають за краще працювати з передовими технологіями і уникати професійного вигорання.

Інтеграція також є найбільш значущим чинником формування культури кібербезпеки для всієї організації. Інвестиції в гнучкі і злагоджено функціонують технології краще звичних тренінгів з кібербезпеки, не пов'язаних з позитивною культурою.

Таким чином, можна зробити висновок, що у сфері інформаційної безпеки за допомогою технологій штучного інтелекту і машинного навчання вдалося вивести процеси автоматизації на якісно новий рівень. Але основна проблема полягає в тому, що хакери також застосовують штучний інтелект для поліпшення автоматизації при проведенні кібератак.

Одержано 30.04.2021

УДК 378.147: 004.9
ГОРЕЛОВ Юрій Петрович,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
http://orcid.org/0000-0002-0330-5008;
АМЕЛЬНИЦЬКА Анна Миколаївна,
студентка групи Ф6-КБдср-18-1 факультету № 6
Харківського національного університету радіоелектроніки

МОДЕЛІ ТА СТРУКТУРА ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ

На сьогоднішній момент Проведена безліч досліджень щодо принципів роботи штучних нейронних мереж (далі – ШНМ), алгоритмів реалізації, способів навчання, класифікацій, особливостях та використання у різних галузях науки та техніки.

ШНМ є одним з методів моделювання складних процесів, в основу організації якого покладена модель біологічних нейронних мереж, що складаються з простих, однотипних елементів (нейронів) зв'язаних один з одним синаптичними з'єднаннями (зв'язками). Але, незважаючи на стрімкий розвиток моделей ШНМ і технологій їх застосування, більшість ШНМ мають деякі загальні риси.

ШНМ складаються із простих однотипних елементів (нейронів), зв'язаних між собою певним чином, функціональні можливості яких аналогічні більшості елементарних функцій біологічного нейрона. Кожний нейрон характеризується своїм поточним станом. Він має групу синапсів – односпрямованих вхідних зв'язків, з'єднаних з виходами інших нейронів, а також має аксон – вихідний зв'язок даного нейрона, з якої сигнал (збудження або гальмування) надходить на синапси наступних нейронів. Кожен синапс характеризується величиною синаптичного зв'язку або його вагою w_i.

Наступною з загальних рис, властивих усім ШНМ, відзначимо принцип паралельної обробки сигналів, який досягається шляхом об'єднання великої кількості нейронів у так звані шари та з'єднання певним чином нейронів різних шарів, а також у деяких конфігураціях і нейронів одного шару між собою, причому обробка взаємодії всіх нейронів ведеться пошарово. Для вирішення складних завдань використовують багатошарові мережі, у яких розрізняють вхідний, схований і вихідний шари. Зазвичай, теоретично ШНМ може мати величезне число як нейронів, так і шарів. На практиці ж усе обмежується ресурсами комп'ютера. Чим складніше структура ШНМ, тим більш масштабні завдання вона може розв'язувати.

На сьогоднішній день існує багато видів ШНМ. Усі вони відрізняються своєю архітектурою: структурою зв'язків між нейронами, числом шарів, функцією активізації нейронів, алгоритмом навчання. Тому серед відомих ШНМ можна виділити: статичні, динамічні, нейронні мережі, побудовані на нечіткій логіці; одношарові й багатошарові мережі.

Властивості ШНМ визначаються її архітектурою, а також сукупністю синаптичних зв'язків та характеристик нейронів. Сучасні ШНМ демонструють цінні властивості: здатність здійснювати багатопараметричний прогноз; оперативність прогнозування ШНМ; нечутливість до недоліків апріорної інформації прогнозованого об'єкта; можливість обробки даних, представлених у різнотипних шкалах; здатність вирішувати слабко формалізовані завдання – виявлення неявних аналогій прецедентів протоколу спостережень; здатність до узагальнення – після навчання мережа стає нечутливою до малих змін вхідних сигналів і дає правильний результат на виході; можливість прогнозування стрибків і подій, що не спостерігалися раніше в навчальній вибірці спостережуваного об'єкта, може бути досягнута активізацією інтелектуальних властивостей ШНМ.

Але необхідно відзначити, що коректність роботи ШНМ прямо залежить від правильності вибору моделі ШНМ і алгоритму навчання для певного завдання.

Одержано 27.04.2021

УДК 004
LIQIANG Zhang
Intermediate grade of experimenter, teacher of College of Computer Science Neijiang Normal University Neijiang (China);
WEILING Cao,
Intermediate grade of experimenter, teacher of Department of IT information Centre Neijiang Normal University Neijiang (China);
SEMENOV Serhii,
Doctor of science, professor Faculty of Computer and Information Technologies National Technical University «KhPI»

ANALYSIS AND COMPARATIVE RESEARCH OF THE MAIN APPROACHES TO THE MATHEMATICAL FORMALIZATION OF THE PENETRATION TESTING PROCESS

A mathematical model constructing process – a formalized description of a complex of factors that significantly affect the state and/or functioning of the object under research, and corresponding to this description of information support – is usually called mathematical modeling.

The practical usefulness of mathematical modeling lies in the possibility of obtaining information about the qualitative properties and quantitative characteristics of the object under research without conducting (often complex or expensive) experiments in nature, which may justify the costs of overcoming difficulties arising in the development process or when trying to use mathematical models.

The main difficulty that one has to face in mathematical modeling is to ensure the adequacy of this model to the object under research. The user needs to find out how accurately this model reflects the real situation and how reliable quantitative estimates can be obtained in the process of working with this model.

The experience of mathematical modeling of information processes, accumulated over the past few decades, shows that the problem of adequacy in a number of cases can be successfully solved. An example of this is the systems of computer simulation of numerous software and hardware components of computing facilities.

However, on the other hand, attempts to apply mathematical modeling methods to research such a complex and important process as the process of ensuring safety, convincingly demonstrate that, despite the natural desire to take into account in the model all the factors that significantly affect the functioning of the object under research, it is extremely difficult to achieve this.

In cases where the construction of a mathematical model that takes into account with an acceptable degree of accuracy all factors that are essential for the object under research is impossible, one has to abandon the standard methodology for using the model and try to act in other ways based on changing the formulations of the problems being solved and involving the user in the process of finding solutions.

In this situation, it is very important to make a reasoned choice of methods of mathematical formalization of the processes of ensuring the security of computer systems in general and software in particular.

The purpose of this article is to analyze and comparatively research the main approaches to the mathematical formalization of one of the software security testing methods, the software penetration testing process.

The article analyzes the methods of mathematical formalization of the software penetration testing process. This software testing method is one of many approaches to testing the security of computer systems. The article substantiates the importance of the processes of preliminary prototyping and mathematical formalization. The classification is carried out and the advantages and disadvantages of the main approaches of mathematical modeling are highlighted. The list and main characteristics of dynamic and static models are presented. One of the negative factors of formalization is indicated - the neglect of the factors of a priori uncertainty in the safety parameters in static models.

Одержано 01.05.2021

УДК 004.056.53
ДЕМИДОВ Захар Георгійович,
старший науковий співробітник
Науково-дослідної лабораторії з проблем розвитку інформаційних технологій
Харківський національний університет внутрішніх справ
https://orcid.org/0000-0003-2821-8047

НАЙВІДОМІШІ ХАКЕРИ СВІТУ

Вже більше 20 років триває боротьба с кіберзлочинцями. Поки люди користуються ноутбуками і телефонами, за їх особистою інформацією, даними, розгортається справжнє полювання.

Хакери придумують віруси все більш складні, а ті, хто з ними бореться, нарощує більш надійний захист – і це перетворюється на справжню війну. Хотілося б розповісти про людей, що змінили наше розуміння комп'ютера, а також про те, як талант і творчий потенціал можуть бути витрачені даремно.

Кевін Девід Митник, хакер з Каліфорнії.

У 1995 році здобув славу самого розшукуваного кіберзлочинця в світі. У 16 років він отримав незаконний доступ до мережі Digital Equipment Corporation і вкрав програмного забезпечення на суму в 1 мільйон доларів, за що був засуджений до року в'язниці. Після звільнення він зламував комп'ютери телефонної компанії Pacific Bell, через це його переслідувала поліція, і йому довелося жити під вигаданими іменами протягом декількох років. Всі його зломи не переслідували конкретної мети. Він просто розважався. За такі дитячі пустощі йому довелося відсидіти 5 років. Ще 8 місяців він провів в одиночній камері, так як один з експертів стверджував, що цей хакер може «почати ядерну війну». Після звільнення Кевін Митник випускає книги про свої кіберзлочини, а також консультує комерційні компанії і співробітників ФБР з питань безпеки. В даний час він керує консалтинговою компанією і допомагає людям зберігати конфіденційність даних.

Джонатан Джозеф Джеймс (cOmrade), хакер з Майамі.

Перший злом він зробив ще в 15 років, отримавши доступ до комп'ютерів міністерства оборони США і до трьох тисяч повідомлень державних службовців. Імена, коди доступу, паролі – все це виявилося в руках звичайного підлітка. У мережі він був відомий під псевдонімом cOmrade. Став першим неповнолітнім, які потрапили до в'язниці за кіберзлочини. 29 червня 1999 року він влаштував потужну атаку на NASA. За допомогою звичайного комп'ютера Pentium йому вдалося викрасти вихідний код міжнародної орбітальної станції. Вкрадені у компанії документи оцінювалися в 1,7 мільйона доларів. Його спіймали в 2000 році і засудили до шести місяців домашнього арешту. Йому також заборонили користуватися комп'ютером, але він порушив це правило і потрапив до в'язниці, де пробув півроку. 18 травня 2008 року хакер наклав на себе руки, вистріливши собі в голову. Однією з причин такого рішення стали звинувачення ФБР.

Майкл Калс (MafiaBoy), хакер з Канади.

У 2000 році організував DDoS-атаки на такі всесвітньо відомі світові компанії, як Amazon, Dell, CNN, eBay і Yahoo !. Після його дій корпоративні сервери перестали відповідати, а вебсайти лягли. Це стало великим ударом для жертв атаки: збиток оцінювався в 1,2 мільярда канадських доларів. На момент злочину Майклу було всього 15 років. За таке серйозне порушення закону він відбувся невеликим штрафом і ув'язненням на 8 місяців. Через роки після звільнення Майкл випустив книгу «Як я зламав інтернет, і чому він все ще не працює». До незаконної хакерської діяльності він більше не повертався.

Гері Маккіннон, 55-річний хакер з Шотландії.

У 2002 році Гері проник в 97 комп'ютерів армії США і NASA, щоб довести, що влада приховує інформацію про НЛО. З 2001 по 2002 рік він за допомогою комп'ютера родичів зламував різні державні системи. Він один з небагатьох кіберзлочинців, який бачив у своєму

діях вище правосуддя. Гері розмістив на військових сайтах США повідомлення: «Ваша безпека – відстій». Той злом по праву вважається найбільшим в історії. Збиток від нього оцінюється в 800 000 доларів. На даний момент Гері займається SEO-підтримкою сайтів і керує власною компанією Small SEO Ltd.

Адріан Ламо, хакер з Бостона.

Прославився зломом великих компаній, таких як Microsoft і New York Times. У 2002 році, він зламав New York Times, додавши себе в список альтернативних джерел видання, а також залишивши особисті коментарі щодо вагомих публічних персон. За це він поплатився штрафом в 65 000 доларів, а також 6 місяцями домашнього арешту. Ламо був відомим журналістом і незалежним консультантом з безпеки. Він видав владі США інформатора Wikileaks Челсі Меннінга, що викликало великий суспільний резонанс. 14 березня 2018 року він помер. Подробиці його смерті невідомі.

Макс Батлер (Iceman), колишній американський консультант з комп'ютерної безпеки.

А також хакер, який відсидів 13 років за крадіжку грошей з майже 2 мільйонів кредитних карт – всього 86 мільйонів доларів. У 1998 році він написав код, який зламав тисячу військових систем США. Його засудили до 18 місяців позбавлення волі. Після виходу з в'язниці Макса позбавили можливості законно заробляти на життя – адже все боялися мати такого небезпечного співробітника. Він створив форум Carders Market, на якому хакери могли торгувати вкраденими картками. У 2007 році його заарештували. Він отримав за кіберзлочини рекордні на той час 13 років, хоча прокурори наполягали на 30 років ув'язнення. У в'язниці Макс взявся за старе. Йому вдалося роздобути телефон T-Mobile My-Touch, за допомогою якого він виходив в інтернет і отримував доступ до банківських систем MoneyGram та Western Union. Потім купив дрон і поставляв до в'язниці контрабандою гаджети, планував провести ряд злочинних кібероперацій. Зараз Макс все ще відбуває термін у в'язниці.

У кожного з нас є необмежений доступ до гігабайтів інформації, і ця добірка – яскравий приклад того, як не варто робити. Можна стати справжнім комп'ютерним генієм і здобути визнання мільйонів людей, створюючи щось інноваційне в рамках закону!

Одержано 30.04.2021

УДК 004.056.5

ЗАГОРЕЦЬКА Єлизавета Романівна,
курсантка 1 курсу факультету № 4
Харківського національного університету внутрішніх справ;
СВІТЛИЧНИЙ Віталій Анатолійович,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
http://orcid.org/0000-0003-3381-3350

ДЕЯКІ АСПЕКТИ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ В УКРАЇНІ

Крадіжки грошей з банківських карток, даних з комп'ютерів, інформацію з телефонів, запуск вірусів-вимагачів, шантаж компаній та крипто-афери – це далеко не повний перелік злочинів, які вчиняють в Україні кібершахраї. Українські кіберзлочинці «прославилися» вже і за кордоном. В Сполучених Штатах викрили мережу хакерів, яка завдала збитків людям на понад 500 мільйонів доларів, а також допомагала «відмивати» доходи. Керівник мережі – українець. У викритті злочинної організації брав участь і Департамент кіберполіції Національної поліції України.

Кількість кіберзлочинів в Україні щороку зростає на кілька тисяч. Основні види кіберзлочинів: незаконний доступ, незаконне перехоплення, втручання у дані, зловживання пристроями, шахрайство, пов'язане із комп'ютерами, правопорушення, пов'язані з дитячою порнографією тощо.

Найпоширеніший вид злочину – шахрайство в мережі Інтернет. Нашим представникам вдалося виявити 2798 таких шахрайств, з яких у 2314 випадках були пред'явлені підозри про вчинення злочину. Найчастіше шахраї створюють сайти і продають неіснуючий товар, дуже багато злочинів, які стосуються виманювання інформації з карток та онлайн-кредитування [1].

Найчастіше шахраї створюють сайти і продають неіснуючий товар, дуже багато злочинів, які стосуються виманювання інформації з карток та онлайн-кредитування.

До прикладу, фахівці наголошують, що кіберзлочинці технічно просунулися щодо крадіжки коштів за допомогою банкомату. Зараз використовують тонкі накладки, які встромлюють у слот для карти, що майже непомітно, і зчитують конфіденційні дані. Ще одна схема шахрайства із банкоматом дуже схожа на раптову його поломку. Дуже часто громадяни звертаються із заявами про викрадення криптовалюти. Ще один приклад кіберзлочину – безкоштовний Wi-Fi у кафе. Wi-Fi – це сервіс, який має слабкі сторони, і за допомогою нього можна отримати доступ до будь-якого пристрою, підключитися та скористатися інформацією в злочинних цілях [2].

Поради як вберегтися від кіберзлочинів: не надавати нікому персональні дані, паролі і коди-підтвердження з SMS для операцій з картками, не довіряти повідомленням про виграші в лотереях, перевіряти інформацію за офіційним номером банку, не скачувати в інтернеті сумнівні файли, користуватись ліцензійним програмним забезпеченням тощо. Більшість людей знають всі ці речі, але все одно потрапляють у пастки кіберзлочинців. Кіберполіція на офіційному сайті радить, як не стати жертвою вірусу-вимагача, як виявити, що злочинці втручаються в систему вашого онлайн-банкінгу, або як захиститися від телефонних шахраїв.

Список використаних джерел

1. Понад 80% звернень щодо шахрайств в Інтернеті в кіберполіції вважають розкритими // Радіо Свобода : вебсайт. 08.02.2018. URL: https://www.radiosvoboda.org/a/news/29028172.html/ (дата звернення: 30.03.2021).

2. Що варто знати про кіберзлочинців в Украйні? // Радіо Свобода : вебсайт. URL: https://www.radiosvoboda.org/a/details/29031166.html (дата звернення: 30.03.2021).

Одержано 29.04.2021

УДК 004.738.5

КЛІМУШИН Петро Сергійович,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій і кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-1020-9399
СПАСІБОВ Дмитро Вікторович,
кандидат технічних наук,
начальник відділу технічного захисту інформації
Департаменту технічного супроводження Харківської міської ради

ТЕХНОЛОГІЇ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНТЕРНЕТ-РЕЧЕЙ

Інтернет-речей (Internet of Things – IoT) – це мережа, що складається із взаємозв'язаних фізичних об'єктів (пристроїв), які мають вбудовані мікроконтролери, датчики, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між ними за протоколами зв'язку [1].

Вузли IoT пов'язані лініями дротового і бездротового зв'язку і взаємодіють під управлінням мікроконтролерів, вбудованих у фізичні об'єкти. Тобто ці взаємопов'язані об'єкти IoT мають функцію програмування та ідентифікації, які забезпечують IoT-мережу даними і виконують команди, отримані з центрів туманних обчислень або від користувача, що взаємодіє

з ними через комп'ютер, стільниковий телефон, автомобільну систему, інтелектуальний пристрій або іншу платформу.

Для отримання більшої ефективності та високої продуктивності мережа IoT будується на концепції «*туманних обчислень*» (Fog Computing) – це модель обчислення та зберігання даних між кінцевими пристроями (вузлами IoT) та традиційними центрами хмарних обчислень, а будь-який пристрій, що має обчислювальні ресурси може бути вузлом туману.

В даний час велика увага в системі IoT приділяється проблемам безпеки збережених, оброблюваних і переданих даних, захисту від копіювання інтелектуальної власності та цифрового контенту, а також захисту від клонування кінцевих IoT.

Коли мова заходить про захист таких систем, «шифрування» часто ототожнюється з терміном «безпека», хоча це лише один з елементів безпеки. Для створення безпечного середовища перш за все необхідно виявити і ідентифікувати елементи, підключені до мережі. Спочатку потрібно визначити, хто саме хоче підключитися до мережі, тому що без попередньої автентифікації шифрування і захист транспортного рівня (наприклад, протоколи SSL / TLS) дозволяють захистити тільки тих, хто не повинен знаходитися у мережі. Тобто, слід зазначити, що підтвердження справжності вузла (автентифікація) стає критично важливим фактором в забезпеченні безпеки інтернет-речей. Крім того, IoT-пристрої привносять нову парадигму в мережеву взаємодію, оскільки вони дуже компактні і прості, практично не взаємодіють з людиною.

Суворі заходи безпеки передбачають три основні елементи (в англомовній літературі позначаються абревіатурою CIA (Confidentiality, Integrity, Authenticity) [2]:

– конфіденційність – дані, що зберігаються або передаються в повідомленні, повинні бути доступні тільки уповноваженим особам або об’єктам;

– цілісність – відправлене повідомлення не повинно змінюватися при транспортуванні до місця призначення;

– справжність – потрібно бути впевненим, що відправник повідомлення - той, за кого себе видає.

Завдання полягає в тому, щоб забезпечити безпеку IoT вузлів, залишаючись у вузьких межах доступних ресурсів з точки зору обчислювальної потужності, пам'яті та енергоживлення.

Негативний вплив на безпечність вузла IoT можливий за чотирма способами:

– через мережу, в наслідок використання: вебінструментів, наприклад, як Shodan, які сканують мережу і можуть ідентифікувати кожен незахищений вузол; за помилками в реалізації TLS для вузла IoT; поганого генерування випадкових чисел в криптоалгоритмах; шкідливого програмного забезпечення, агресивних протокольних атак з встановлених експертних вузлів; слабких місць протоколів обміну даними; оновлення прошивки оригінального програмного забезпечення кодом, написаним зловмисником.

– через зовнішні порти, які надають можливість доступу до вузла IoT в тому числі через невикористані порти, на відміну від мережевого порту для захисту цих портів не існує встановленого стандарту;

– за допомогою безконтактних атак (Proximity Attack), які також називають атаками «за бічним каналом», наприклад, підключившись до лінії живлення або вимірюючи рівень випромінюваних перешкод або вібрації на незахищеному пристрої, можна витягти інформацію про криптографічні ключі;

– шляхом фізичного проникнення в пристрій, тобто зловмисник може фізично розібрати пристрій IoT, намагаючись досліджувати внутрішні ланцюга (з напругою живленням або без напругі живлення), або навіть видалити і відключити мікросхему для вивчення вмісту вбудованої пам'яті.

Слід пометати, що наслідки успішної атаки можуть піддати ризику мережу цілком і все, що підключено до неї. Тому комплексна безпека вузлів IoT повинна захищати від усіх цих способів атак.

Існує ряд способів підтримки важливих елементів CIA [3]:

– справжність – підтверджуйте особистість будь-якого користувача, який заходив у мережу або ідентифікуйте будь-які додаткові пристрої, які намагаються підключитися до вузла;

– конфіденційність – шифруйте повідомлення;

– цілісність – додавайте код автентифікації повідомлення (Message authentication code, MAC) до всіх повідомлень, щоб підтвердити, що ніхто не змінив повідомлення за маршрутом.

Крім того, можуть бути вжиті заходи захисту від безконтактних атак, які носять практичний характер і можуть бути реалізовані у всій системі або тільки в вузлі IoT:

1) зберігайте ключі в захищеному обладнанні, щоб не було електричного доступу до ключа;

2) екрануйте систему, щоб запобігти витоку ключової інформації шляхом детектування електромагнітного випромінювання;

3) додайте спеціальні схеми для того, щоб запобігти спробам контролю над напругою живлення або іншими сигналами. Це можуть бути фіктивні лічильники або схеми з вбудованими елементами генерування випадкових сигналів для шифрування корисної інформації;

4) зашифруйте ключ в сховище. Навіть якщо ключ не доступний з електричної точки зору, зловмисник може спробувати фізично розкрити пристрій, щоб прочитати вбудовану Flash-пам’ять і витягти ключ. Шифрування нейтралізує цю атаку;

5) по можливості відмовтеся від зовнішніх портів.

Таким чином, важливо захищати ключі протягом усього циклу їх життя – від генерації, використання, зберігання до знищення. Перевірена методологія – використання апаратних модулів безпеки (Hardware Security Module, HSM), які зберігають ключі в зашифрованому вигляді і в захищеному обладнанні. Всі операції зашифровування і розшифрування даних, що надходять ззовні, відбуваються всередині пристрою. При цьому криптографічні ключі ніколи не залишають захищений периметр всередині пристрою, в якому вони були створені.

Список використаних джерел

1. Горбовський А. І., Войтович О. П. Дослідження безпеки у інтернеті речей // Матеріали XLVI науково-технічної конференції підрозділів ВНТУ, Вінниця, 22-24 березня 2017 р. URL: http://ir.lib.vntu.edu.ua/bitstream/handle/123456789/17277/2805.pdf?sequence=3 (дата звернення: 23.04.2021).

2. Smarter Security For Your Everything, Atmel Has You Covered // Microchip : вебсайт. 2019. URL: https://www.microchip.com/design-centers/security-ics (дата звернення: 23.04.2021).

3. Асангханва Ю., Ий Р., Сыров А. Повышение уровня безопасности граничных узлов интернета вещей с помощью микросхем ATECC608A компании microchip. *Электроника НТБ*. 2019. № 7 (00188). С. 60-64.

Одержано 01.05.2021

УДК 004.5+004.65

КОЛІСНИК Тетяна Петрівна,
кандидат педагогічних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-74428136
ЮЩЕНКО Ярослав Вікторович,
курсант 2 курсу факультету № 4
Харківського національного університету внутрішніх справ

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ: НЕБЕЗПЕКА СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В КІБЕРПРОСТОРІ

Сьогодні людський фактор в інформаційній безпеці грає набагато важливішу роль, ніж декілька років тому, коли інтернет не був так поширений і його користувачами були лише фахівці. Прогрес мережі з кожним роком все збільшується, а разом і з ним шахрайські методи

збору інформації. Засоби протидії кіберзлочинам, які ми звикли використовувати: засоби ідентифікації, пристрої шифрування, прилади знаходження мережевих атак та інші – малоефективні в протистоянні хакерам, які застосовують процедуру соціальної інженерії. І саме тому на сьогоднішній день, проблемність захисту конфіденційної інформації є однією з необхідніших у кібербезпеці.

Мета: визначити використання психологічних прийомів та методів соціальної інженерії для отримання доступу до приватної інформації особи, а також вберегти себе від шахрайства.

В сучасному світі найбільшу цінність та значимість несе інформація, а самим слабким місцем у її захисті є ж самі люди. Технології стрімко розвиваються, а разом з ними збільшується чисельність злочинів у кіберпросторі. Все більше хакерів намагаються отримати дані з осіб, фірм та різних організацій у своїх інтересах. І з кожним разом вони застосовують різні підходи для отримання бажаного результату. Існують безліч методів та способів пов’язаних з шахрайством в цифровому середовищі, проте одним з найнебезпечніших та найбільш ефективних вважається соціальна інженерія (далі – СІ).

СІ являє собою метод несанкціонованого доступу до інформації або системам зберігання інформації завдяки взаємодії з людиною. Вона стала універсальним способом управління діями людини з мінімальним використанням технічних засобів. Метод заснований на використанні слабкостей людського фактора з впливом на психіку об’єкта, і тому представляє найбільшу загрозу для інформаційної безпеки [1]. В її основу покладено психологічне управління людиною, а саме, емоційний стан:зацікавленість, стурбованість,страх, довіра тощо. Основною метою СІ є отримання допуску до конфіденційної інформації, паролів, електронної почти, банківських даних і інших захищених систем.

Сьогодні найефективнішою схемою психологічного впливу на особу, яку застосовують шахраї у соціальній інженерії є схема Шейнова, яка складається з наступних етапів: 1) формування цілі та мети впливу на об’єкт; 2) пошук та збір з різних джерел інформації про об’єкт; 3) виявлення найбільш зручних мішеней впливу; 4) створення необхідних умов для впливу на об'єкт; 5) примус до потрібної для соціального інженера дії; 6) очікування корисного результату.

Найпоширеніша атака соціальної інженерії і найпоширеніша техніка, що використовується в таких атаках, це уособлення людини,тобто прямий підхід. Зловмисники прикидаються кимось, ким вони не є, наприклад надійним колегою або відомим продавцем, і вони надсилають електронні листи або втягуються в довіру до жертви для того, щоб вкрасти гроші або конфіденційні дані [2]. Більшість співробітників організацій та звичайних користувачів навіть не підозрюють про наявність загроз, пов'язаних з соціальним інжинірингом. Вони мають доступ до конфіденційної інформації, не розбираючись в властивостях цієї інформації, і не усвідомлюючи важливість оброблюваної інформації, паролів, логінів тощо. Шахраї найчастіше обирають собі за мету особу з низьким рівнем володіння комп'ютером**,** адже якщо людина менше розуміє в мережі, то швидше видасть необхідні дані, аніж більш досвідченіший.

Різновидів злочину з використанням психіки людини дуже багато, але для стурбованості нема підстав, якщо знати як їх уникнути. Звісно не можливо вберегтися від всіх інтернет-шахрайств, але виконувати виконання елементарних правил техніки безпеки при роботі в мережі,а зокрема: 1) нікому і нізащо не повідомляти свої персональні дані; 2) не переходити на підозрілі посилання та за спливаючими вікнами; 3) використовувати надійні паролі та періодично змінювати їх; 4) не заходити на ненадійні сайти та не завантажувати з них програмне забезпечення для використання на своєму комп’ютері; 5) при роботи з конфіденційної інформацією використовувати захищені канали інтернет-зв’язку.

У висновку потрібно зазначити, що кібербезпека відіграє важливу роль у житті користувачів інтернет, шахрайство із застосуванням соціальної інженерії стає більш розповсюдженим і небезпечним. Для того щоб побудувати систему протидії таким атакам в цілях профілактики необхідно здійснювати техніку безпеки в мережі, а також залучати у критичних випадках професійних експертів з кібербезпеки. Звісно потрібно пам’ятати, що можливості мережі є не лише приємним джерелом задоволення потреб, знань та спілкування, але й джерелом підвищеної небезпеки, особливо в випадках коли є сторона, яка зацікавлена вашою діяльністю.

Список використаних джерел

1. Яковенко В. С., Казеян Н. К. Соціальна інженерія в Інтернет-просторі. *Інформаційні технології та моделювання економічних процесів*. 2016. Вип. III-IV (63-64). С. 119-126.

2. Махницький О. В. Використання соціальної інженерії для крадіжки особистих даних // Використання сучасних інформаційних технологій в діяльності Національної поліції України : матеріали Всеукр. наук.-практ. семінару (23 листопада 2018 р., м. Дніпро). Дніпро : ДДУВС, 2018. С. 55-60.

3. Цуркан О., Герасимов Р., Крук О. Методи протидії використанню соціальної інженерії. *Information Technology and Security*. 2019. Vol. 7, Iss. 2 (13), pp. 161-170.

Одержано 01.05.2021

УДК 65.012.8 + 004

МАНЖАЙ Олександр Володимирович,
кандидат юридичних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
http://orcid.org/0000-0001-5435-5921
МАНЖАЙ Ірина Андріївна
завідувач навчального відділу Харківського університету

ЩО ТАКЕ КІБЕРГІГІЄНА?

Сьогодні безпека роботи з інформацією як ніколи є актуальною. Зростаючі кібератаки на державні та приватні підприємства, установи й організації тільки посилюють цей тренд. Окрема категорія загроз стосується громадян, які все частіше стають об'єктом прискіпливої уваги правопорушників. Враховуючи викладене, поступово набуває поширення відносно нова концепція необхідності самостійного дотримання елементарних правил безпеки користувачами. Такий підхід дає змогу значно посилити систему колективної безпеки суспільства та держави в цілому. Агентство Європейського Союзу з мережної та інформаційної безпеки (European Union Agency for Network and Information Security) відзначає, що кібергігієна повинна розглядатися так само, як особиста гігієна, і після належної інтеграції в організацію стати простою повсякденною процедурою, яка забезпечить стан кіберздоров'я організації в оптимальному стані [1, p. 4].

Порушення правил кібергігієни може призвести для згубних наслідків не лише для окремої людини. Досить часто від дій зловмисників страждає і роботодавець жертви. Навіть великі держави можуть зазнати величезної шкоди від необачного ставлення до вимог безпеки однієї людини. Часто порушники використовують окрему особу як лаз для проникнення на об'єкти критичної інфраструктури, викрадення чутливих державних даних, створення умов для скоординованих повномасштабних атак.

Таким чином, недотримання вимог кібергігієни здатне нанести значну матеріальну та моральну шкоду. А крім того, суттєво вплинути на Вашу особисту репутацію!

У світі існує достатньо велика кількість тлумачень слова «кібергігієна». Вони, як правило, відображають найбільш значущі аспекти цього терміну, важливі для конкретної галузі знань. Серед останніх оприлюднених визначень можна навести такі:

– правила кібербезпеки, яких мають дотримуватися онлайн користувачі з метою забезпечення цілісності та убезпечення своїх персональних даних на мережних пристроях від компрометації у випадку кібератаки [2];

– сукупність практик, спрямованих на захист від негативного впливу на певні об'єкти ризиків, пов'язаних з кібербезпекою [3];

– способи заохочення користувачів комп'ютерних технологій до безпечної поведінки в інтернеті [4].

Більш спрощена інтерпретація цього терміну дозволяє представити ***кібергігієну*** як дотримання правил безпечної поведінки у кіберсфері.

Така поведінка обумовлена наявністю загроз, які виникають під час роботи користувачів з інформацією в електронному вигляді. Спроби реалізації загроз називаються атаками.

Як і на рибалці або полюванні зловмисники можуть заздалегідь обирати цілі, які вважають цікавими для себе, а можуть навпаки розставити пастки і чекати, доки жертва попадеться в одну з них. Теж саме стосується ситуацій, коли порушники випадковим чином обирають жертву, стосовно якої намагаються реалізувати свої наміри.

Виділяють декілька типів *інформаційних атак*: соціальна інженерія, одержання віддаленого доступу за допомогою вірусів, вплив на інфраструктуру стільникового зв'язку, маніпуляція через ЗМІ, атаки відмови в обслуговуванні, атаки на енергетичні системи та комунікації, політичний спамінг, атаки на системи управління та провайдерів тощо [5, p. 416].

Перед тим, як напасти, зловмисниками можуть здійснюватися підготовчі дії. Це виражається у підшукуванні працездатних схем нападу, збиранні інформації про жертву різними способами, створенні умов для реалізації атаки.

Для того щоб мінімізувати ризик успішної реалізації таких атак, як раз і потрібна кібергігієна. По суті це рутинний процес. І для того, щоб полегшити його, потрібно використовувати допоміжний інструментарій. Якщо у класичній гігієні такими інструментами є мило, шампунь, зубні щітка тощо, то для забезпечення її кібернетичного аналогу використовуються спеціальні програми як от антивіруси, фаєрволи, захищені браузери та багато інших застосунків і сервісів.

Важливим моментом в роботі з інструментами кібергігієни є правильне їх застосування. Це приблизно те саме, що і правильне підрізання нігтів ножицями або зачісування волосся гребінцем. З одного боку все просто, а з іншого потрібно чітко визначити для себе елементарний порядок дій з певними програмами, щоб не потрапити у халепу. Просте озброєння купою застосунків для захисту інформації як правило не приносить користі. Без знання правил роботи з такими програмами вони стають просто набором коду, який навряд чи зможе Вас захистити.

Так само потрібно мати на увазі, що чим меншою буде кількість інформації, яку Ви хочете вберегти, тим менше Вам потрібно буде вживати дій для її убезпечення. Тому під час продукування фотознімків, написання повідомлень в мережі, спілкування телефоном з незнайомими та навіть знайомими людьми подумайте, чи дійсно це є необхідним і наскільки шкідливим може бути використання відповідної інформації проти Вас.

Саме тому бажано користуватися перевагами інтернету в частині забезпечення анонімності та використання вигаданих даних. Особливо це стосується мережних ресурсів, у безпеці яких не можна бути впевненим. У випадку атаки на Вас, зловмисники зможуть отримати доступ лише до вигаданих даних. Це може стати ще одним додатковим ешелоном, який убезпечить Вас від протиправних посягань.

Немаловажним принципом забезпечення кібергігієни є періодичне резервування даних. Можна використовувати мережне резервування або дублювання даних на фізичних запам'ятовувальних пристроях. Усе залежить від чутливості даних, які потрібно зберегти, та відповідних знань предметної області. Так, наприклад, другорядні дані цілком можуть бути перенесені у хмару. Це дозволить зменшити кількість інформації, що потребує захисту на локальних пристроях, і таким чином тримати їх у чистоті.

Найкращий варіант, якщо Ви зробите кібергігєну своєю повсякденною звичкою. При цьому вона не потребує суттєвих витрат коштів і часу. Згодом Ви звикнете до виконання відповідних процедур і відчуєте їх корисність як в особистих, так і в службових справах.

Список використаних джерел

1. Review of cyber hygiene practices (December 2016). European Union Agency For Network and Information Security (ENISA) URL: https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/-fullReport (last accessed: 17.03.2021).

2. Vishwanath A., Neo L. S., Goh P., Lee S., Khader M., Ong G., Chin J. Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*. 2020. Vol. 128 (DOI: 10.1016/j.dss.2019.113160).

3. Maennel K., Mäses S., Maennel O. Cyber Hygiene: The Big Picture. In: Gruschka N. (eds) Secure IT Systems. NordSec 2018. Lecture Notes in Computer Science. 2020. Vol. 11252. Springer, Cham. (DOI: 10.1007/978-3-030-03638-6_18).

4. Pfleeger S. L., Sasse M. A., Furnham A. From Weakest Link to Security Hero: Transforming Staff Security Behavior. *Journal of Homeland Security and Emergency Management*. 2014. Vol. 11. Iss. 4. pp. 489-510. (DOI: 10.1515/jhsem-2014-0035).

5. Sharma S. Gupta J. N. D. Securing Information Infrastructure from Information Warfare. *Logistics Information Management*. 2002. № 15(5/6). P. 414-422.

Одержано 17.03.2021

УДК 004.04:004.67:004.77

МОЖАЄВ Олександр Олександрович,
доктор технічних наук, професор,
професор кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-1412-2696
ЗВІРЯНСЬКИЙ Геннадій Володимирович,
кандидат юридичних наук,
заступник декана факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-6687-8575

ВИКОРИСТАННЯ НЕЧІТКИХ КРИТЕРІЇВ ПІД ЧАС ПОБУДОВИ СОЦІАЛЬНОГО ПРОФІЛЮ

Процес прийняття рішень – це певна послідовність дій, орієнтованих на вирішення проблем системи, який містить аналіз ситуацій, генерацію альтернатив, прийняття рішень.

Прийняття рішень, які ліквідують розрив між сьогоденням і майбутнім станом системи являє собою обґрунтований вибір з наявних альтернатив напрямів діяльності.

При більш детальному розгляді, основні фази прийняття рішень в соціально-економічних системах полягають у наступному:

– збір інформації про можливі проблеми;
– виявлення та визначення джерел виникнення проблем;
– постановка цілей вирішення проблем;
– обґрунтування стратегії вирішення проблем;
– пропозиція альтернатив рішень;
– вибір оптимального варіанта;
– внесення коректівів і узгодження рішення;
– реалізація рішення.

Ефективність прийнятого рішення при здійсненні управління соціально-економічною системою базується на наступних принципах:

– обґрунтованість – управлінські рішення повинні прийматися на підставі максимально вичерпних і достовірних даних;

– своєчасність – рішення не повинні ні відставати, ні випереджати потреби і завдання соціально-економічної системи;

– повнота змісту – рішення повинні охоплювати всю соціально-економічну систему;

– повноважність – суб'єкт управління повинен строго дотримуватися тих правил і повноважень, які йому присвоєно;

– узгодженість з раніше прийнятими рішеннями – забезпечення чіткого причинно-наслідкового зв’язку розвитку системи;

– гнучкість – використання численних можливостей, тобто наявність точних критеріїв, ясних цілей і вичерпної інформації.

На даний час володіння інформацією про соціальні профілі як особистості, так і соціальної групи в цілому становить значну зацікавленість в більшості сфер діяльності людини і суспільства: економіці, освіті, політиці, безпеці, забезпеченні комфортних умов життєдіяльності тощо.

Тому побудова соціального портрета індивідуума, групи, а також всього суспільства в цілому є важливою науковою задачею, на вирішення якої спрямовані численні дослідження.

Одним із найважливіших аспектів дослідження є точна оцінка важливості соціальних об’єктів, яка ускладнюється проблемами верифікації, суб'єктивністю експертних оцінок і чутливістю даних до впливу людського фактору. Формалізованими критеріями можна вважати тільки рейтинги або оцінки, представлені в числовому або процентному вигляді.

Таким чином, виникає актуальне наукове завдання вибору апарату формалізації об'єктів дослідження і визначення критеріїв значущості складових інформації соціального профілю.

При виборі засобів і методів вирішення поставленої перед пропонованими дослідженнями мети автори зупинили свій погляд на апараті теорії нечіткої логіки.

Емпірично були підібрані параметри, що впливають на значимість окремих характеристик соціального профілю, і визначені наступні їх характеристичні функції:

– актуальність (ні, та, частково) – «свіжість» інформації, що залежить від часу появи інформації в досліджуваній вибірці;

– авторитетність (відсутня, низька, висока) джерела – ключовий параметр, що впливає на оцінку висловлювання експертами при ускладненнях визначення його достовірності наявними у експертів доказовими засобами;

– важливість (не має відношення, другорядна, важлива, критична) інформації – показує ступінь пов'язаності з іншими характеристиками соціального профілю;

– аргументованість (недостатньо, досить) – враховує наявність доказів і посилань з метою виявлення інформаційного шуму і бездоказових заяв;

– унікальність (раніше невідомо, відомо, широко відомо) інформації – дозволяє відокремити факти від бездоказових висловів;

– достовірність (брехня, правда) – висловлювання при наявності протилежних думок залежить від найбільш авторитетної з них.

У доповіді розглянуті властивості розроблених моделей забезпечують можливість подальшої алгоритмізації аналітичних функцій для підтримки осіб, які приймають рішення, в межах нової методики соціального профілювання. Надана можливість врахування природи і основних характеристик зібраних відомостей спрощує виявлення явних і неявних зв'язків між елементами соціального середовища.

Таким чином, в результаті проведених досліджень розроблені нечіткі критерії для визначення значущості складових інформації соціального профілю, що дозволить істотно підвищити адекватність моделі соціального профілю.

Одержано 01.05.2021

УДК 004.04:004.67:004.77
МОЖАЄВ Олександр Олександрович,
доктор технічних наук, професор,
професор кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-1412-2696
ПЕРЕСІЧАНСЬКИЙ Валерій Миколайович,
старший викладач кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-0130-9339
РОГ Вікторія Євгеніївна,
старший викладач кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-7443-5125

АНАЛІЗ ВИКОРИСТАННЯ ҐРІД-МЕРЕЖ ДЛЯ ПОТРЕБ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Перед Національною поліцією України стає дуже складне завдання забезпечення зниження рівня злочинності та покращення і поліпшення профілактики можливих правопорушень. Це вимагає значного збільшення обсягу інформації, що потрібно обробити. Для обробки такої різноманітної інформації в теперішній час використовуються значна кількість методів обробки значних даних. Але існуючі методи та технічні засоби не завжди відповідають рішенню цих задач у повному обсязі. Тому аналіз можливості використання технології ҐРІД-мереж для потреб Нацполіції України є досить актуальною науково-технічною задачею, що буде досліджена у наступній доповіді.

Концепція ҐРІД-мереж породила нову модель організації різних форм обробки даних, запропонувавши технології видаленого доступу до ресурсів різних типів, незалежно від місця їх розташування в глобальному мережевому середовищі. ҐРІД-технології дали можливість виконувати програмні коди на одному або відразу декількох «чужих» комп'ютерах, стали всюди доступними сховища даних із структурованою (бази даних) і неструктурованою (файли) інформацією, джерела даних (датчики, інструменти спостереження) і програмно керовані пристрої.

Найбільш зацікавленим споживачем цієї технологічної концепції виступила саме наукова громадськість. Спочатку створювалися національні ҐРІД-мережі, а після збільшення наукомістких завдань, ці мережі об'єднувалися.

ҐРІД-мережі з’явилися як реалізація програми Національного наукового фонду США (NSF), 1985-1995 рр. Результат – створення розвиненої комунікаційної інфраструктури і декількох суперкомп’ютерних центрів для підтримки академічних робіт і досліджень. У 1998 році був створений інструментальний пакет Globus Toolkit, який є технологічною базою створення ҐРІД-інфраструктури. У 1999-му році сформувалося(і активно діє) міжнародне наукове ҐРІД-співтовариство Global Grid Forum (GGF). GGF і IBM в 2000-му році представили нову системну розробку – Open Grid Service Architecture (OGSA). У 2002-му створено об'єднання Enterprise Grid Alliance (EGA). А в 2006-му році GGF і EGA оголосили про злиття і утворення Open Grid Forum (OGF) [1-4].

У основі ҐРІД-мереж лежать обчислювальні потужності комп'ютерів, сховища даних, що об'єднані в єдину мережу і утворюють ҐРІД-вузол. Набір ҐРІД-вузлів є ҐРІД-мережею (ҐРІД-сайт), а набір ҐРІД-мереж у свою чергу утворює ҐРІД-систему. Можливі об'єднання ҐРІД-систем усередині країни, між країнами. Такі об'єднання виникають, як правило, на основі ҐРІД-ініціатив. ҐРІД-проекти включає велика кількість географічно розподілених ҐРІД-систем на міжнародному рівні. Окрім цього, існує поняття «Віртуальне ҐРІД-співтовариство», яке є створюваною на певний час віртуальною організацією (В) під актуальне завдання і з використанням ресурсів набору ҐРІД-систем. У ролі зв’язки між ҐРІД-

системами і В виступають координаційні центри (координаційна організація, К), що управляють виділенням/розподілом ресурсів.

Інструментарій Globus Toolkit є стандартом для ҐРІД-мереж, визнаним як науковим співтовариством, так і провідними компаніями комп'ютерної індустрії. Завдяки тому, що GT із самого початку мав і як і раніше зберігає статус відкритого програмного забезпечення, до теперішнього часу накопичений значний досвід його застосування у великих проектах. Використовуючи інструментальні засоби GT, різні колективи розробили додаткові служби: реплікації файлів, авторизації, диспетчеризації завдань та ін.

Стандарт OGSA (Open Grid Services Architecture) визначає служби як абстрактні об'єкти, але не містить ніяких приписів про спосіб їх реалізації [5, 6]. У OGSA не зачіпаються питання програмної моделі служб і виконавчого середовища їх функціонування, що, звичайно, має сенс, оскільки робить стандарт незалежним від реалізаційної платформи. Наприклад, в GT3, ҐРІД-служби реалізуються в компонентних середовищах – контейнерах, розроблених для вебслужб. Так, на платформі J2EE (Java 2 Enterprise Edition) застосовуються різні типи контейнерів: EJB (Enterprise JavaBeans) – специфікація технології написання і підтримки серверних компонентів, JSP (JavaServer Pages) – технологія, що дозволяє веброзробникам легко створювати вміст, який має як статичні, так і динамічні компоненти, сервлети і аплети. Роль контейнерів – розміщення служб, забезпечення життєвого циклу, підтримка безпеки.

Якщо цих функцій контейнера вистачає для вебслужб, то для ҐРІД- служб потрібно більше – спосіб реалізації цих служб повинен забезпечувати віртуалізацію ресурсів:

– розраховане на багато користувачів обслуговування, що динамічно адаптується до навантаження, що міняється, шляхом породження безлічі екземплярів служб;

– автоматичний розподіл ресурсів між екземплярами служб, що виконують обробку потоку запитів.

Загальні стани способу побудови ҐРІД-мережі на базі локальних систем управління розподіленими ресурсами виглядають таким чином:

– модель служб OGSA розглядається як майбутній стандарт усієї інформаційної індустрії, на основі якого будуватимуться просторово-розподілені застосування. За посередництва служб додатка дістають уніфікований дистанційний доступ до ресурсів віртуальної організації;

– єднальне програмне забезпечення ҐРІД-мережі «склеює», тобто робить доступними споживачам, географічно рознесені, такі, що належать різним адміністративним доменам ресурсні пули;

– засоби ҐРІД-мережі для збору і зберігання інформації забезпечують віртуальну організацію метаданими про ресурси, послуги і умови їх надання. OGSA специфікує формат описів і спосіб зберігання метаданих в реєстрах. На основі метаданих працюють різні комунальні ҐРІД-служби;

– захист у віртуальній організації базується на стандарті інфраструктури безпеки, ґрунтованому на сертифікаті X.509.

Таким чином, у результаті досліджень встановлено можливість використання технології ҐРІД-мереж для потреб Нацполіції України.

Список використаних джерел

1. Kazymyr V. Prila O., Rudyi V. Grid workflow design and management system. *International Journal «Information Technologies & Knowledge»*. 2013. Vol. 7, № 3. pp. 241 – 255.

2. Hirales-Carbajal A., Tchernykh A., Yahyapour R. et al. Multiple Workflow Scheduling Strategies with User Run Time Estimates on a Grid. *Journal of Grid Computing*. 2012. Vol 10. Iss. 2. pp. 325 – 346.

3. Melnyk A. Multiple DAGs Scheduling with Deadline Driven Coordinator in Grid // Second International Conference “Cluster Computing”. (Lviv, Ukraine, 2013. June 3-5). pp. 127 – 130.

4. Казимир В. В., Бивойно П. Г., Прелая О. А., Гуза Т. А. Методи планування потоків задач в GRID-середовищі. *Математичні машини і системи*. 2013. № 4. С. 70-81.

5. Державна цільова науково-технічна програма впровадження і застосування ҐРІД-технологій на 2009–2013 роки. *Офіційний вісник України*. 2009. № 75. С. 2556.

6. Chen Y., Qiao Zh., Davis S., Jiang H., Li K.-Ch. Pipelined Multi-GPU MapReduce for Big-Data Processing. *Computer and Information Science*. 2013. Vol. 493. pp. 231-246.

Одержано 01.05.2021

УДК 351.741:[621.397.4+004]
МОРДВИНЦЕВ Микола Володимирович,
кандидат технічних наук, доцент,
провідний науковий співробітник
Науково-дослідної лабораторії з проблем розвитку інформаційних технологій
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-7674-3164
ХЛЄСТКОВ Олексій Володимирович,
старший науковий співробітник
Науково-дослідної лабораторії з проблем розвитку інформаційних технологій
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0001-8777-8269
НИЦЮК Сергій Павлович,
старший науковий співробітник
Науково-дослідної лабораторії з проблем розвитку інформаційних технологій
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0001-8251-642X

ТЕНДЕНЦІЇ СВІТОВОГО РОЗВИТКУ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ ЗАДЛЯ ЗАБЕЗПЕЧЕННЯ ПУБЛІЧНОЇ БЕЗПЕКИ

В розвинених країнах світу для забезпечення публічної безпеки масово використовують системи відеоспостереження. На базі цих пристроїв створюються інтелектуальні системи, що дозволяють не тільки аналізувати обстановку, але і прогнозувати розвиток подій і в найкоротші терміни генерувати рекомендації для управління силами і засобами, які забезпечують публічну безпеку. Все частіше в США, Західній Європі, Китаї, Росії з метою забезпечення публічної безпеки використовуються системи зі штучним інтелектом (далі – ШІ) які поєднуються з системами відеоспостереження [**Ошибка! Источник ссылки не найден.**].

Досвід Китаю. Правоохоронні органи Китаю користуються допомогою багатьох високотехнологічних ШІ-компаній (розробки в сфері штучного інтелекту). До кінця 2021 року на китайський ринок надійдуть 450 млн нових камер. Понад 400 банків Китаю вже впровадили технологію розпізнавання облич мережах банкоматів.

Китайські вчені вже розробили систему розпізнавання облич, яка здатна виявити в натовпі потрібну людину з точністю до 99,8 % з 91 ракурсу. Програма може знаходити відмінності між ідентичними близнюками, розпізнавати дуже загримованих осіб, а також ідентифікувати людину, щільно укутану в одяг.

Китайська поліція тестує технологію розпізнавання людей за ходою. Програмне забезпечення може ідентифікувати людину на відстані 50 м від точки зйомки, навіть якщо в неї приховано обличчя або віна стоїть до відеокамери спиною.

Необхідно відзначити, що для боротьби з поширенням коронавірусу в цій країні широко застосовуються звичайні та інфрачервоні камери з використанням систем ШІ для вимірювання температури тіла людини і фіксації лиця з метою подальшого його визначення в натовпі. Вони широко застосовуються в місцях з високою щільністю пасажиропотоку, таких як метрополітен, автобусні станції, залізничні станції та аеропорти і дозволяють швидко ідентифікувати людей, які можуть мати підвищену температуру тіла, а також виключити з ними фізичний контакт.

Досвід Сполучених Штатів Америки. Крім системи розпізнавання облич, в США застосовується система ShotSpotter. Це система пов’язаних між собою акустичних датчиків, здатних забезпечити покриття міста. Система, оснащена кількома звуковими датчиками, може виявляти тип вогнепальної зброї згідно із зафіксованими звуками, а алгоритм машинного навчання, використовуючи тріангуляційні алгоритми, визначати координати місця події.

Досвід Ізраїлю (віброкамери). Ізраїльська компанія «Cortica», яка працює в сфері безпеки і досліджень ШІ, проводить аналіз терабайтів даних, переданих з камер відеоспостереження у

громадських місцях. Її метою є підвищення безпеки у громадських місцях. Використання ШІ у системах відеоспостереження спрямоване насамперед на попередження злочинів. Дослідження та виробництво систем «Cortica» направлені на пошук поведінкових аномалій у рухах людини, які сигналізують про те, що вона збирається вчинити злочин.

Досвід Росії (віброкамери). В Росії інтенсивна розробляються системи віброкамер. Віброкамера реєструє мікрорухи, на основі аналізу яких можна отримати будь-яку інформацію про людину. Кожна частина тіла людини здійснює власні рухи, по-своєму вібрує. Око може цього не помітити. Віброкамера фіксує всі незначні (десятки мікрон) мікрорухи людини, потім за частотою вібрацій система аналізує її психологічний стан.

Віброкамери встановлені в аеропортах, на стадіонах, у метрополітені й у великих супермаркетах, де вони не лише стежать за безпекою покупців, а й виявляють потенційних правопорушників.

В Україні прийнято ряд законів, інструкцій та інших документів, що регламентують впровадження системи відеоспостереження в Національній поліції. Створено Управління організації діяльності підрозділів поліції на воді та повітряної підтримки, ефективно працює Єдиний аналітично-сервісний центр (UASC) в Донецькій області, патрульна поліція використовує персональні відеореєстратори, їх автомобілі обладнані системами відеозапису.

Список використаних джерел

1. Коршенко В. А., Чумак В. В., Мордвинцев М. В., Пашнев Д. В. Стан систем безпеки з використанням технічних засобів відеозапису та відеоспостереження: зарубіжний досвід, перспективи впровадження в діяльність Національної поліції України. *Право і безпека*. 2020. № 2(77). С. 86-92.

Одержано 26.04.2021

УДК 004.9 +343.1

НОСОВ Віталій Вікторович,
кандидат технічних наук, доцент,
професор кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-7848-6448
МАНЖАЙ Олександр Володимирович,
кандидат юридичних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
http://orcid.org/0000-0001-5435-5921

ЗМІСТ ТА МЕТОДОЛОГІЯ ПРАКТИЧНОГО НАВЧАННЯ З ПИТАНЬ КІБЕРГІГІЄНИ

У національних і міжнародних нормативних документах, рекомендаціях і кращих практиках з кібербезпеки зазначається необхідність реалізації в організаціях програм підвищення обізнаності (awareness) з основ кібербезпеки. Дотримання основ кібербезпеки користувачами інформаційно-телекомунікаційних систем зокрема отримало відносно новий термін «кібергігієна», який мабуть вперше в законодавчому полі був вжитий в законі США «Promoting Good Cyber Hygiene Act of 2015» [1], а Агентство з мережної та інформаційної безпеки Європейського Союзу (ENISA) в 2016 році опублікувало огляд існуючих практик із кібергігієни в країнах ЄС [2].

На початку 2021 року на порталі «Дія. Цифрова освіта» Міністерства цифрової трансформації України було розміщено освітній серіал «Основи кібергігієни» [3], який є курсом Координатора проектів ОБСЄ в Україні у рамках проекту «Посилення спроможностей українських державних органів у сфері кібергігієни та кібербезпеки» як частина загальної короткострокової програми підвищення кваліфікації для державних службовців та посадових осіб місцевого самоврядування у співпраці з Українською школою урядування. Розробники

теоретичної частини цього курсу визначили 9 тем (напрямів) інформування з основ кібербезпеки: 1) соціальна інженерія; 2) безпечне користування мережею Інтернет; 3) безпечне користування електронною поштою; 4) шкідливе програмне забезпечення; 5) безпека користування соціальними мережами; 6) безпека мобільних пристроїв; 7) фізична безпека; 8) убезпечення від неправдивих повідомлень; 9) правові засади кібергігієни.

За вищезазначеними темами для проведення практичних тренінгів з «Основ кібергігієни» державних службовців та посадових осіб місцевого самоврядування з урахуванням кращих практик було розроблено такі практичні вправи:

1. «Захист від фішінгових атак», «Аналіз поштового повідомлення».

2. «Безпечний перегляд вебсторінок», «Способи організації безпечного з'єднання в мережі», «Накладання електронного підпису».

3. «Двофакторна автентифікація поштового облікового запису», «Парольний менеджер», «Перевірка факту компрометації поштової адреси», «Електронний підпис та шифрування повідомлень».

4. «Вбудована в ОС Windows 10 система захисту від вірусів і загроз», «Антивірус "Zillya!"»; «Антивірус "ZoneAlarm"».

5. «Двофакторна автентифікація облікового запису Facebook», «Видалення метаданих фотозображень», «Двофакторна автентифікація облікового запису Instagram та Twitter».

6. «Налаштування захисних механізмів у мобільному пристрої».

7. «Створення захищеного флеш-накопичувача», «Блокування доступу до операційної системи за відсутності активності», «Автовідтворення під час підключення знімних носіїв».

8. «Інструменти виявлення неправдивих повідомлень».

9. «Правове забезпечення у сфері інформаційної безпеки та кібербезпеки».

Методологія проведення тренінгу передбачає:

– проведення обговорення, виконання групових вправ та рольових ігор за темами № 8, 9;

– наведення прикладів створення та використання фішингових ресурсів і прихованого віддаленого доступу за темами № 1, 4;

– зразкове виконання тренером практичних завдань, за яким слідують учасники;

– створення презентацій, де зазначені: тема, цілі, від яких кіберзагроз будемо вчитися захищатися, коротка ідея щодо відповідних методів та засобів захисту і практичні завдання для виконання.

Передбачається, що кожен учасник тренінгу заздалегідь отримує електронний та паперовий варіант порядку виконання практичних завдань. За наявності технічної можливості на комп'ютерах учасників тренінгу встановлюються віртуальні машини, на яких виконуються усі завдання, що дозволяє за необхідністю їх швидке відновлення до початкового стану. Виведення інформації з екрана смартфона на персональний комп'ютер і проектор здійснюється за допомогою або спеціальних програм (Vysor, LonelyScreen) або апаратних можливостей проектора (Wi-Fi-підключення).

Зміст та методологія проведення тренінгу з «Основ кібергігієни» було апробовано на «Тренінгу для тренерів з питань кібергігієни» [4].

Список використаних джерел

1. Promoting Good Cyber Hygiene : HR3664 Act of 2015 // Congress.gov : вебсайт. URL: https://www.congress.gov/bill/114th-congress/house-bill/3664 (дата звернення: 04.04.2021).

2. Review of Cyber Hygiene practices. December 2016. European Union Agency For Network and Information Security (ENISA) URL: https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport (дата звернення: 04.04.2021).

3. Основи кібергігієни : освітній серіал // Дія. Цифрова освіта / Міністерство цифрової трансформації України. URL: https://osvita.diia.gov.ua/courses/cyber-hygiene (дата звернення: 04.04.2021).

4. Кібергігієна для держслужбовців // Українська школа урядування : вебсайт. 22.03.2021. URL: https://usg.org.ua/kibergigiyena-dlya-derzhsluzhbovcziv (дата звернення: 04.04.2021).

Одержано 19.04.2021

УДК 381.74.[343.575:004]
ОРЛОВ Роман Русланович,
курсант 3 курсу факультету № 4
Харківського національного університету внутрішніх справ;
ГРИЩЕНКО Денис Олександрович,
старший викладач кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0001-5066-7389

ОСНОВНІ ТРЕНДИ У СФЕРІ КІБЕРБЕЗПЕКИ З ЗАХИСТУ БАНКІВСЬКИХ ПЛАТЕЖІВ

Організація Payment Card Inductry Security Standards Council (PCI SSC) – це міжнародний регулюючий орган по стандартам безпеки індустрії платіжних карт. Рада PCI SSC була створена колективним рішенням міжнародних платіжних систем VISA, MasterCard, American Express, JCB, Discover. У компетенції ради PCI SSC входять розробка і підтримка стандартів забезпечення безпеки даних індустрії платіжних карт.

Ключовим активним стандартом зараз є PCI DSS версії 3.2. Фокус уваги в ньому, в порівнянні з попередніми версіями, зважаючи на зростання популярності сервісних моделей в IT, зміщений на розширення відповідальності сервіс-провайдерів і критерії оцінки всіх учасників, залучених в обслуговування транзакцій, закріплені обов'язки по регулярному тестування систем платежів і вимоги до маскування номера рахунку. Стандарт PCI DSS містить в собі дванадцять розділів перевірки безпеки систем:

– захист обчислювальної мережі;
– конфігурація компонентів інформаційної інфраструктури;
– захист збережених даних про власників карт;
– захист переданих даних про власників карт;
– антивірусний захист інформаційної інфраструктури;
– розробка і підтримка інформаційних систем;
– управління доступом до даних про власників карт;
– механізми аутентифікації;
– фізичний захист інформаційної інфраструктури;
– протоколювання подій і дій;
– контроль захищеності інформаційної інфраструктури;
– управління інформаційною безпекою.

Стандарти PCI SSC не закріплені на державному рівні як обов'язкові, точніше, тільки деякі штати в США ввели їх на законодавчому рівні. Але, завдяки вимогам платіжних систем, вони виконуються у великій кількості організацій. Дослідження компанії Cisco по виконанню стандарту в США від 2011 виявило наступне:

З усіх галузей краще за всіх виконують вимоги PCI DSS підприємства роздрібної торгівлі та фінансові організації; роздрібна торгівля найсерйознішим чином поставилася до впровадження і реалізації цього стандарту. При цьому 85% опитаних вважають, що в даний момент їх організації здатні успішно пройти аудит PCI DSS, а 78% успішно пройшли такий аудит з першого разу. Найбільш високі результати в цій галузі показали державні організації: 85% держустанов успішно пройшли аудит PCI DSS з першого разу. Найгірше проходили такий аудит медичні організації (72%). 67% опитаних керівників компаній і членів рад директорів вважають PCI DSS вельми важливою ініціативою; крім того, 60% опитаних підтвердили, що стандарт PCI DSS може стимулювати інші проекти, пов'язані з мережами і мережевою безпекою. 10 років тому компанія «Verizon» почала відстеження виконання стандарту PCI DSS серед компаній. Звіт «Verizon PCI Report» від 2019 року показує, що динаміка підтримки відповідності знаходиться на межі від 22% (2009 р.) до 7,5% (2011 р.) і 55,4% (2016 р.). Через 15 років після виходу стандарту, більше 35% підтримують системи захисту в

повністю актуальному, відповідному стандарті, багато компаній знаходяться в процесі опрацювання подібних процедур.

В даний час найбільшу загрозу в сфері платежів являє шахрайство на основі соціальної інженерії, тому важливо виховання технологічної грамотності серед користувачів банківських послуг.

Рекомендації в якості заходів цифрової гігієни для кінцевого користувача платіжних систем:

– не зберігати платіжні дані на сумнівних сервісах, оцінювати ризики і необхідність введення платежів на ресурсах, які не підтримують стандарт 3D Secure (він вимагає підтримку не тільки від платіжної системи та фінансової організації, але також і від самого торгово-сервісного підприємства);

– уникнути фактів зберігання або запису коду CVV зі зворотного боку картки на будь яких носіях інформації, не повідомляти нікому код з SMS, Push-повідомлення, PIN-код карти – їх не має права запитувати ніхто – ні співробітник банку, ні служба технічної підтримки, ніхто інший, ви використовуєте ці коди тільки в процесі певних платіжних операцій;

– уникати шахрайства: бути пильними, не довіряти телефонним дзвінкам. Не розкривати свої персональні дані: ПІБ, місце і рік народження, дані паспорта. Співробітники банку мають доступ до цієї інформації при необхідності, і, якщо хтось намагається дізнатися у вас ці дані, – це підозріло, тому не вступає в подальшу розмову, вішайте трубку, у разі необхідності або сумніву самостійно здійснить виклик на номери служби підтримки фінансової установи;

– якщо ви стали жертвою шахрайства: слід негайно повідомити банк про сумнівні платежі і виконувати всі надані фінансовою установою вимоги. Своєчасне повідомлення дозволить тимчасово заблокувати платіж для з'ясування його легітимності. У разі втрати або крадіжки картки необхідно чинити так само;

– не викачувати і не встановлювати програми на мобільні пристрої на прохання незнайомих осіб, і, тим більше, не повідомляти їм коди доступу до програм. Необхідно добре розуміти, що ви встановлюєте і навіщо. Бажано уважно керувати правами, затребуваними програмами, і мінімізувати їх.

Одержано 22.04.2021

УДК 621.34

ТУЛУПОВ Володимир Володимирович,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0003-4794-743X

ВИКОРИСТАННЯ МЕТОДІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ ДЛЯ ОТРИМАННЯ ІНФОРМАЦІЇ ШАХРАЙСЬКИМ ШЛЯХОМ

На теперішній час фахівці з кібербезпеки в основному зосереджені на виявленні та виправленні вразливостей у програмному забезпеченні, у той час як кінцеві користувачі залишаються найслабшою ланкою у кіберпросторі.

У кіберсфері існує метод соціальної інженерії такий як фішинг – це один із різновидів інтернет-шахрайства, який дозволяє обманним шляхом отримувати різну цінну інформацію, маскуючи комунікації так, ніби вони надійшли з надійного джерела (користувача). Інформація за допомогою фішингу може бути використана для доступу до пристроїв або мереж. Фішинг є цілеспрямованою шахрайською атакою, яка спирається на використання особистої інформації об'єкта (жертви), що робить атаку більш надійною та успішною.

Як правило зловмисники використовують різні методи фішингу у своїх атаках а саме: обманні вебпосилання, інтернаціональні доменні імена, клонування вебсайтів, підробку та перенаправлення трафіку, створення вікон, що спливають, голосовий та текстовий фітинг.

Використання методу обманних вебпосилань полягає в тому, що шахраї маскують зловмисне вебпосилання як вказівку на легітимне або довірене джерело. Ці типи фішингових атак можуть приймати будь-яку кількість форм, наприклад, застосування шахрайських URL-адрес, створення піддомену для зловмисного вебсайту або експлуатація дуже схожих доменів.

Також шахраями можуть використовуватися так звані – IDN (інтернаціональні доменні імена) для створення заплутано схожих доменних імен, дозволяючи використовувати не ASCII-символи. Такі візуальні подібності між символами в різних сценаріях, які називаються гомогліфами, застосовують для створення доменних імен, що візуально неможливо диференціювати. Це спонукає користувачів приймати один домен за інший.

Відомо, що вебсайти вразливі до атак типу межсайтовий скриптинг (XSS), тому зловмисниками використовуються методи клонування вебсайтів, підробки та перенаправлення трафіку для запису власного контенту на інший вебсайт. Такі атаки XSS (межсайтовий скриптинг) можуть застосуватися для перехоплення даних, введених на скомпрометованому сайті (включно з ім'ям користувача та паролем), які зловмисники використають пізніше.

Як правило, частіше такі атаки використовують для створення вікон, що спливають, які походять з вразливого вебсайту, але притому завантажують сторінку, що контролюється зловмисниками. Часто такий тип прихованого пере направлення трафіку відкриває форму для входу з метою збору реєстраційних даних. Через поширення цього типу атак більшість браузерів тепер показують адресний рядок у вікнах, що спливають.

Для отримання інформації про обліковий запис зловмисники також використовують телефонні дзвінки та текстові повідомлення (голосовий та текстовий фітинг.

Так, за даними компанії Check Point Research (дослідницька компанія Check Point) Software Technologies Ltd., нещодавно опублікувала звіт про фішинг бренду за другий квартал 2020 року. Цифри звіту говорять самі за себе про зростання цієї шахрайської практики, навіть за часів пандемії. Дослідження показало, що топ-5 найбільш використовуваних брендів в цих фішингових атаках: Google і Amazon – по 13%, WhatsApp і Facebook – по 9% і Microsoft – по 7%. У порівнянні зі звітом за перший квартал минулого року відбулися значні зміни: Apple очолила список і тепер посідає сьоме місце – всього 2% [1].

На жаль, проти фішингових атак не існує надійних засобів, адже майже всі подібні атаки значною мірою покладаються на соціальну інженерію, з метою переконати користувачів негайно вжити заходів і, тим самим, блокуючи можливість та бажання детального аналізу ситуації. Через це найкращим захистом від фішингу є навчання кінцевих користувачів правилам безпеки.

Крім того, виробники захисних рішень розробили спеціальні фільтри з метою виявлення фішингових атак в електронних листах. Втім, в деяких повідомленнях шахраї використовують зображення тексту замість звичайного текстового формату, щоб уникнути цих фільтрів у пошті. Крім того, фішингові вебсайти часто покладаються на методи заплутування коду, щоб запобігти детектуванню зловмисної активності з боку систем захисту. Зазвичай фішингові атаки застосовують шифрування на базі алгоритмів AES-256 або Base64 у JavaScript, або ж інші методики, що ускладнюють аналіз базового вихідного коду.

Нещодавно дослідники компанії Proofpoint розкрили фішинговий інструментарій, який заплутує отримувача листа за допомогою шифру заміщення, який спирається на спеціальний шрифт. Цей інструментарій використовує незвичайну версію шрифту Arial з окремими транспонованими літерами; при завантаженні фішингової сторінки контент виглядає нормально, але коли користувач або програма намагаються прочитати вихідний текст на сторінці, він показується змішаним [2].

Проаналізовано факт того, що кількість доступних даних про фішінг постійно збільшується тому, правоохоронним органам необхідно більш активно користуватися існуючими інструментами з кібербезпеки щодо виявлення та розкриття кіберзлочинів.

Список використаних джерел

1. Фішинг: Статистика за другий квартал 2020 року // Find your digital self : вебсайт. 15.10.2020. URL: https://blog.fyself.com/ru/%D1%84%D0%B8%D1%88%D0 %B8%D0%BD%D0%B3-%D1%81%D1%82%D0%B0%D1%82%D0%B8%D1%81 %D1%82%D0%B8%D0%BA%D0%B0-

%D0%B2%D1%82%D0%BE%D1%80% D0%BE%D0%B9-%D0%BA%D0%B2%D0%B0%D1%80%-D1%82%D0%B0% D0%BB-2020/ (дата звернення: 16.04.2021).

2. Proofpoint. Enterprise Email Security // SPRO : вебсайт. URL: https://spro.com.ua/products/-proofpoint/proofpoint-enterprise-protection-for-email-security (дата звернення: 16.04.2021).

Одержано 28.04.2021

УДК 004

SEMENOV Serhii,
Doctor of science, professor Faculty of Computer and Information Technologies
National Technical University «KhPI»;
LIQIANG Zhang,
Intermediate grade of experimenter, teacher of College
of Computer Science Neijiang Normal University Neijiang (China);
WEILING Cao,
Intermediate grade of experimenter, teacher of Department
of IT information Centre Neijiang Normal University Neijiang (China)

THE SOFTWARE SECURITY TESTING FIRST STAGE MATHEMATICAL MODEL

Ensuring the security of computer systems, in the context of an increase in the intensity of cyberattacks, is associated with the need to conduct prompt and accurate control of the level of security of their software (SW). The relevance of this issue is due to the shift in the vector of interests of cyber attackers towards the information and software component of computer systems (CS), as well as a significant increase in possible losses in the event of cyber threats on the software and information support of the CS.

Studies have shown that one of the direct mechanisms for controlling the level of software security are methods and means of identifying vulnerabilities. At the same time, it can be noted that currently the process of identifying threats to software vulnerabilities has a number of drawbacks (limited scope, low efficiency and incomplete control of the real state of software, low reliability of vulnerability identification results, etc.). To a large extent, these negative factors are caused by insufficient attention of developers to the issues of a reasoned choice of testing methods, as well as models and methods for identifying vulnerabilities.

The analysis of software security testing methods, as well as models and methods for identifying vulnerabilities has been carried out. The problem of a reasoned choice of modeling approaches at various stages of the software security testing process and identification of its vulnerabilities is revealed, which reduces the overall accuracy of the simulation results. Two stages of the process of identifying software vulnerabilities have been identified. An improved algorithm for checking compliance with the security criterion has been developed, a distinctive feature of which is the choice of distribution laws and parameters describing individual transitions from state to state for individual branches of GERT networks. Developed a GERT network for the security testing preparation process. A GERT network has been developed for the process of checking the source code for cryptographic and other data protection methods. A GERT model of the first stage of software security testing has been developed. In the aggregate, a mathematical model of the process of preparing for security testing has been developed, which differs from the known theoretically justified choice of generating functions of moments, when describing transitions from state to state, as well as taking into account the stage of checking the source code for cryptographic and other methods of data protection.

Одержано 01.05.2021

УДК 004.056
СОЛЯНИК Тетяна Миколаївна,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0003-3695-0019
БОЛЬШОВ Роман Сергійович,
студент групи Ф6-КБдср-20-2 факультету № 6
Харківського національного університету внутрішніх справ

ТЕХНОЛОГІЯ BLOCKCHAIN ЯК ОДИН З СУЧАСНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

Захист інформації – важливе та актуальне питання сучасності, для вирішення якого використовуються значні фінансові та людські ресурси, залучаються новітні розробки в галузі апаратного та програмного захисту об'єктів критичної інформаційної інфраструктури. Наявність широкого спектру методів та засобів захисту інформації обумовлено великою кількістю її різновидів, різноманіттям сфер її застосування, типом середовища передачі інформації типом фізичного носія інформації тощо.

В наш час дуже багато інформації різного контенту та значення зберігається у цифровому вигляді, починаючі з персональних даних і закінчуючи електронними грошима або криптовалютою. Одним з сучасних методів захисту або збереження даних в електронному вигляді стає технологія Blockchain.

Блокчейн (англ. *Blockchain, Block chain*, від block – блок, chain – ланцюг) – ланцюжок блоків транзакцій – розподілена база даних, що зберігає впорядкований ланцюжок записів (так званих блоків). Кожен блок містить часову позначку, хеш попереднього блока та дані транзакцій, подані як хеш-дерево [1].

Основна ідея технології *Blockchain* – це використання криптографічних даних, які постійно доступні та захищені одночасно, без будь-якого централізованого сервера чи сховища, з записами змін, які включаються до кожної нової версії даних. Це робить застосування *Blockchain* привабливим для компаній, що працюють в різних сферах.

Технологія має багато плюсів: вона децентралізована, її практично неможливо зламати, і вся інформація, яка формується в блоки, автоматично зашифрована. До кожного блоку можна додати будь-яку інформацію: персональні дані, результати виконання фінансових операцій, інформацію щодо права власності тощо.

Для убезпечення даних від підробки та спотворення в *Blockchain* використовується складна система захисту та веріфікацій.

Базова система *Blockchain* – це постійно зростаюча послідовність блоків, які розподіляються між учасниками системи за допомогою пірінгових мереж. У кожен блок додається часова відмітка (хеш-сума), унікальність та призначення якої найпростіше порівняти з унікальністю відбитка пальця. Ці блоки строго в певному порядку створюють ланцюжки. Якщо спробувати переставити послідовність блоків, то система відкине ланцюг через невідповідність структури і хеш-сумми. Для захисту часової позначки, а також унеможливлення перерахунку хеш-суми, яка буде правильною з точки зору системи, технологія блокчейн використовує кілька способів захисту, а саме: Proof of Work (PoW, доказ роботи) і Proof of Stake (PoS, доказ володіння).

Proof of Work (PoW) – це форма криптографічного доказу з нульовим знанням, в якому одна сторона (перевіряючий) доводить іншим (верифікаторам), що певну кількість обчислювальних зусиль було витрачено для досягнення певної мети [2].

Proof-of-stake (PoS) – метод захисту в технології блокчейн, заснований на необхідності доказу зберігання певної кількості активів на рахунку. При використанні цього методу алгоритм з більшою ймовірністю вибере для підтвердження чергового блоку в ланцюжку обліковий запис з великою кількістю активів на рахунку [3].

Незважаючи на порівняно невисокий ступінь використання технології блокчейн, вона постійно удосконалюється. В даний час вже існує ряд розширень для розробки бізнес-додатків на *Blockchain*.

Окрім базових функцій, вони можуть надавати такі можливості для [4]:

– роботи з мережею: зберігання інформації щодо користувачів мережі та параметрів доступу до мережних ресурсів; виконання ролі «єдиного адміністратора»;

– зберігання конфіденційної цифрової інформації, що унеможливлює несанкціоноване читання, розповсюдження чи змінювання будь-яких цифрових сертифікатів;

– швидкого укладання будь-яких двосторонніх угод з миттєвим підтвердження права власності;

– автоматичного визначення та фіксування часу проведення операції (наприклад, створення документів), що вирішує завдання у галузі авторських прав тощо;

– верифікації відповідності продукту (товару) за допомогою надійно захищеного сертифіката під час його сертифікації.

Незважаючи на те, що зараз технологія блокчейн застосовується здебільшого для роботи з криптовалютами, очікується зростання її застосування в інших сферах, тому що незмінна база даних, яка може безпечно зберігати і передавати цифрові активи, відкриває багато можливостей для спільного використання по всьому світу.

Список використаних джерел

1. Груша В. Що таке blockchain? / Nachasi : вебсайт. 02.06.2017. URL: https://nachasi.com/2017/06/02/blockchain-faq/ (дата звернення: 19.04.2021).

2. Proof of work // Wikipedia : вебсайт. URL: https://en.wikipedia.org/wiki/Proof_of_work (дата звернення: 19.04.2021).

3. Proof of stake // Wikipedia : вебсайт. URL: https://en.wikipedia.org/wiki/Proof_of_stake (дата звернення: 19.04.2021).

4. Як працює технологія Blockchain? // Guland : вебсайт. URL: https://guland.com.ua/-kryptovalyuta/blockchain/shcho-take-blokcheyn.htm (дата звернення: 19.04.2021).

Одержано 19.04.2021

УДК 004.056.5

СТРУКОВ Володимир Михайлович,
кандидат технічних наук, доцент,
професор кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0003-4722-3159
ГУДІЛІН Владислав Владиславович,
курсант 3 курсу факультету № 4
Харківського національного університету внутрішніх справ

ЗАХИСТ ВІД АТАК ПІДВИЩЕННЯ ПРИВІЛЕЇВ В КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

У більшості корпоративних інформаційних систем для швидкого адміністрування мережі використовується програмне забезпечення Active Directory – служба каталогів корпорації Microsoft для операційних систем сімейства Windows Server. Захист Active Directory є актуальним аспектом забезпечення безпеки корпоративних інформаційних систем. Реальність така, що кількість вразливих корпоративних інформаційних систем становить 73% від загального числа. У даній роботі розглянуті деякі актуальні методи атак на корпоративні інформаційні системи, пов’язані з отриманням прав адміністратора домена в Active Directory, а також сформульовані методи захисту від них.

Щоб скомпроментувати контролер домену, хакеру необхідно не тільки знайти відому вразливість, отримати реєстраційні дані користувача або знайти помилку в налаштуванні політики безпеки. Це забезпечить лише деякий мінімальний доступ з обмеженими дозволами. Тому мета атаки хакера – отримання підвищених системних привілеїв в Active Directory.

У роботі розглянуті наступні методи проведення атак для отримання привілейованих прав доступу: 1) пошук паролів в налаштуваннях SYSVOL і групових політиках, 2) атака Kerberoasting та 3) підвищення привілеїв з групової політики DNSAdmins.

Пошук паролів в налаштуваннях SYSVOL і групових політиках GPP виконується в загальнодоступній директорії SYSVOL. SYSVOL – це загальнодоменний ресурс Active Directory, до якого у всіх, хто пройшов перевірку користувачів є доступ для читання. SYSVOL містить такі дані: сценарії входу, групові політики та інші дані домену, які можуть виявитися доступними всюди, де є контролер домену, сервер, який контролює комп'ютерну мережу. Директорія SYSVOL автоматично синхронізується і використовується всіма контролерами домена. Як правило, всі групові політики домену зберігаються в файловій системі за наступним шляхом: \\<Домен>\SYSVOL\<Домен>\Policies\. Коли створюється нова групова політика, в SYSVOL створюється пов'язаний XML-файл з відповідними даними конфігурації, і якщо вказано пароль, він шифрується за допомогою алгоритму шифрування AES-256-біт. У більшості випадків наступні XML-файли будуть містити облікові дані: groups.xml, ScheduleTasks.xml та Services.xml. Але корпорація Microsoft опублікувала ключ шифрування AES, який неважко використати з метою дешифрування пароля (рис. 1):

Рис. 1. Ключ

Будь-який користувач в домені може шукати в загальному ресурсі SYSVOL файли XML, значення яких містить зашифрований пароль AES (рис. 2):

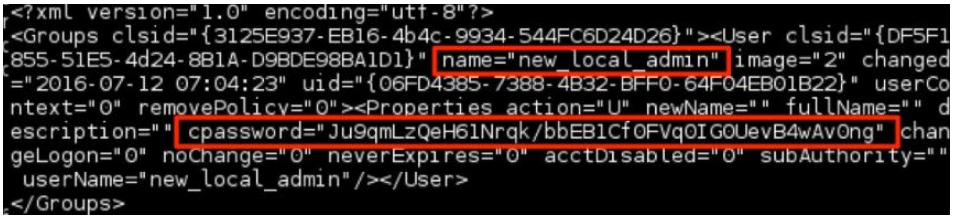

Рис. 2. Зашифрований пароль

Це відбувається через те, що авторизовані користувачі мають доступ для читання SYSVOL. Таким чином, отримавши доступ до XML-файлу, який містить пароль, хакер може використати закритий ключ AES для дешифрування пароля групової політики.

Kerberoasting – це метод, який дозволяє зловмисникові вкрасти квиток KRB_TGS, зашифрований за допомогою алгоритму RC4_HMAC_MD5, щоб зробити повний перебір хешу для отримання пароля. Мережевий протокол Kerberos використовує хеш NTLM для шифрування квитка KRB_TGS. Коли користувач домену відправляє запит на квиток TGS контролеру домену KDC для будь-якої служби, яку зареєструвала SPN, KDC генерує KRB_TGS без ідентифікації даних для авторизації користувача запитуваної служби. Зловмисник може використовувати цей квиток в автономному режимі для підбору пароля облікового запису служби, так як квиток був з використанням NTLM-хешу облікового запису служби.

Загальний план атаки виглядає наступним чином:

1. Отримання доступу до клієнтської системи доменної мережі.

2. Виявлення або сканування зареєстрованого SPN.

3. Запит на квиток TGS для виявленого SPN.

4. Отримання квитка TGS, який може бути у форматі .kirbi, ccache або бути службовим хешем (в деяких випадках).

5. Перетворення .kirby або ccache в необхідний формат для злому.

6. Перебір хеша по словнику.

Підвищення привілеїв з групової політики DNSAdmins. Microsoft не тільки реалізувала власний DNS-сервер, але і впровадила для нього протокол управління, що дозволяє інтегрувати DNS-сервер з доменами Active Directory. За замовчуванням контролери домену також є DNS-серверами, тому DNS-сервери повинні бути доступні кожному користувачеві домену. Це, в свою чергу, відкриває потенційну можливість для атаки на контролери домену: з одного боку ми маємо сам протокол DNS, а з іншого – протокол управління, заснований на RPC.

Користувач, що входить до групи DNSAdmins або має права на запис в об'єкти DNS-сервера, може завантажити на DNS-сервер довільну DLL. Це дуже небезпечно, оскільки багато корпоративних мереж використовують контролер домену в якості DNS-сервера (рис. 3):

Рис. 3. Параметри користувача

Таким чином, для реалізації атаки ми можемо просто завантажити на DNS-сервер довільну бібліотеку за допомогою команди dnscmd (шлях \\ops-build\dll повинен бути доступний для читання DC). Щоб перевірити, чи була завантажена DLL, можна використати наступну команду: Get-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Services\DNS\Parameters\-Name ServerLevelPluginDll.

Так як користувач – член групи DNSAdmins, можливо перезапустити службу DNS:

sc \\ops-dc stop dns

sc \\ops-dc start dn

Після перезапуску DNS-сервера буде виконано код з завантаженої бібліотеки. Така бібліотека може містити скрипт PowerShell для зворотного підключення (рис. 4):

Рис. 4. Код бібліотеки

Після успішного виконання скрипта буде отримано зворотне підключення з правами system (рис. 5):

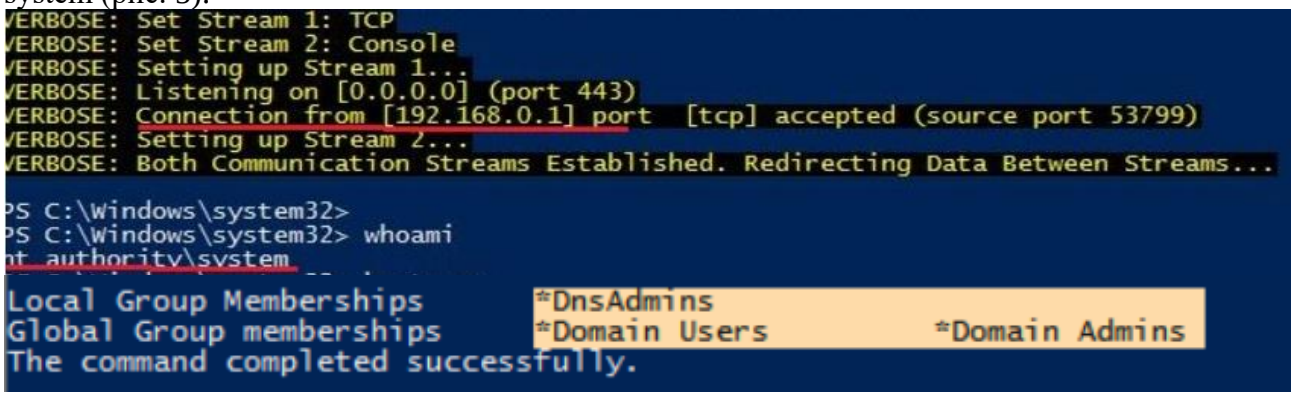

Рис. 5. Зворотне підключення

Для запобігання атак, заснованих на пошуку паролів в налаштуваннях SYSVOL, потрібно керуватися наступними рекомендаціями: розмежовувати доступ до файлів, що містять паролі, видалити існуючі XML-файли групових політик в SYSVOL, які містять паролі, своєчасно встановлювати останні оновлення з центру оновлень Windows.

Оскільки в атаці Kerberoasting протокол автентифікації Kerberos використовується звичайним чином, найкраща міра захисту від атаки – використання складних паролів для службових облікових записів, пов'язаних з Kerberos та SPN. Крім того, слід налаштувати MS SQL-сервер або будь-яку іншу службу без використання облікових записів із системними привілеями, а також доцільне використання спеціального захисного програмного забезпечення для зберігання паролів.

Щоб запобігти атаці підвищення привілеїв з групової політики DNSAdmins, слід перевірити список управління доступом ACL щодо відсутності привілеїв на запис об'єктів в DNS-сервер та членство в групі DNSAdmins. Очевидні показники в log-файлах DNS-сервера, такі як перезапуск служби DNS, події DNS-сервера з ідентифікатором 150 для помилки та 770 для успішного виконання можуть слугувати для детектування атаки. Моніторинг змін реєстру HKLM:\SYSTEM\CurrentControlSet\services\DNS\Parameters \ServerLevelPluginDll також допоможе детектувати спробу несанкціонованого отримання системних прав.

Таким чином, були розглянуті деякі з актуальних можливих методів проведення атак на корпоративні інформаційні системи, які засновані на використанні служби каталогів Active Directory і метою яких є отримання прав адміністратора домену, а також було надано практичні рекомендації із захисту та детектування проаналізованих видів атак.

Список використаних джерел

1. Metcalf S. Finding passwords in SYSVOL and exploiting group policy preferences // Active Directory Security : вебсайт. 28.12.2015. URL: https://adsecurity.org/?p=2288 (дата звернення: 15.04.2021).

2. Medin T. Attacking Kerberos: Kicking the Guard Dog of Hades // Red Siege Information Security. 08.2008. URL: https://www.redsiege.com/wp-content/uploads/2020/08/Kerberoastv4.pdf (дата звернення: 19.04.2021).

3. Metcalf S. Cracking Kerberos TGS tickets using Kerberoast – exploiting Kerberos to compromise the Active Directory Domain // Active Directory Security : вебсайт. 31.12.2015. URL: https://adsecurity.org/?p=2293 (дата звернення: 20.04.2021).

4. Metcalf S. Detecting Kerberoasting activity. // Active Directory Security : вебсайт. 05.02.2017. URL: https://adsecurity.org/?p=3458 (дата звернення: 23.04.2021).

Одержано 28.04.2021

УДК 519.859
ЧУГАЙ Андрій Михайлович,
доктор технічних наук, старший науковий співробітник,
провідний науковий співробітник
відділу математичного моделювання та оптимального проектування
Інституту проблем машинобудування імені А. Підгорного НАН України;
ШЕХОВЦОВ Сергій Борисович,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ;
ЯСЬКОВ Георгій Миколайович,
доктор технічних наук, старший науковий співробітник,
старший науковий співробітник
відділу математичного моделювання та оптимального проектування
Інституту проблем машинобудування імені А. Підгорного НАН України

ЗАСТОСУВАННЯ ПАРАЛЕЛЬНИХ ОБЧИСЛЕНЬ В ЗАДАЧАХ ОПТИМІЗАЦІЇ ІНФОРМАЦІЙНИХ СИСТЕМ

У нелінійних масштабних задачах оптимізації, що виникають у сфері штучного інтелекту та кібербезпеки, як правило, область допустимих розв'язків задачі описується величезною кількістю нелінійних нерівностей та змінних. Через це одним із важливих питань є розробка сучасних технологій, що дозволяють підвищити ефективність алгоритму розв'язання задачі оптимізації. Основна ідея запропонованої методики базується на алгоритмі декомпозиції, який зводить масштабну задачу оптимізації до послідовності підзадач значно менших розмірів.

Стратегія оптимізації включає наступні етапи: формування допустимих початкових точок, із області припустимих розв'язків; послідовна побудова підобластей; формування системи активних рівності; пошук локальних екстремумів у вибраних підобластях.

Слід зазначити, що залежно від значення параметра декомпозиції, число підзадач може бути досить великим, а обчислювальний час великий. Це пов'язано з тим, що для генерації підзадачі потрібно замінити отриману вихідну точку в систему нерівності, яка описує здійсненну область вихідної великомасштабної задачі та формує нову підсистему нерівностей. Оскільки система нерівностей, що описує обрану підобласть, визначається великою кількістю нелінійних нерівностей, то для обчислення таких нерівностей і формування нової підсистеми потрібен тривалий час.

Алгоритм формування підсистеми, що задає область припустимих розв'язків підзадачі, можна представити у вигляді графа у ярусно-паралельній формі (ЯПФ). Для ЯПФ графа алгоритму важливим є той факт, що операції, яким відповідають вершини одного ярусу, не залежать одна від іншої (не перебувають у відношенні зв'язку), і тому можлива паралельна реалізація алгоритму, в якій вони можуть бути виконані паралельно.

На першому ярусі розташовані процедури для обчислення функцій, які описують область припустимих розв'язків. Задачі перших трьох ярусів підтримують паралелізм даних, оскільки для їх виконання використовуються однакові обчислювальні процедури, але над різними масивами даних. Задачі четвертого ярусу підтримують паралелізм задач, оскільки задачі цього ярусу реалізуються окремими процедурами.

Для реалізація паралельних обчислень за представленою ЯПФ алгоритму необхідно забезпечити синхронізацію виконання паралельних задач другого та третього ярусів, оскільки результати процедур цих ярусів залежать від результатів, отриманих на третьому та четвертому ярусах відповідно.

Отже для реалізація представленої схеми паралельних обчислень необхідно застосувати сучасні засоби паралельних обчислень, які забезпечать програму механізмами автоматичної генерації паралельних обчислювальних потоків, масштабування задача, синхронізацію потоків.

Оскільки програмне забезпечення створювалось за допомогою середовища .NET Framework, то як засоби паралельних обчислень була обрана бібліотека розпаралелювання задач (TPL). Ця бібліотека дозволяє значно удосконалити багатопоточне програмування за рахунок двох основних способів. По-перше, вона спрощує створення і застосування багатьох потоків. І, по-друге, вона дозволяє автоматично використовувати кілька процесорів. Іншими словами, TPL відкриває можливості для автоматичного масштабування додатків з метою ефективного використання ряду доступних процесорів. Завдяки цим двом особливостям бібліотеки TPL вона рекомендується в більшості випадків до застосування для організації багатопотокової обробки, адже вони дають можливість легше використовувати системні ресурси. Застосовуючи TPL, паралелізм в програму можна ввести двома основними способами: за допомогою паралелелізму даних та паралелізму задач. Застосування бібліотеки TPL надає можливість автоматично масштабувати виконання коду на кілька процесорів. Бібліотека TPL дозволяє автоматично розподіляти навантаження додатків між доступними процесорами в динамічному режимі, використовуючи пул потоків CLR. Бібліотека TPL займається розподілом роботи, плануванням потоків, управлінням станом і іншими низькорівневими деталями. В результаті з'являється можливість максимізувати продуктивність додатків .NET.

Результати проведених числових експериментів показали, що використання технологій паралельних обчислень дозволило скоротити час розв’язання задач на 30%.

Одержано 01.05.2021

РОЗДІЛ 4.
МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

УДК 341.4:341.176(4)
ВОЙЦІХОВСЬКИЙ Андрій Васильович,
кандидат юридичних наук, доцент,
професор кафедри конституційного і міжнародного права факультету № 4
Харківського національного університету внутрішніх справ

ДІЯЛЬНІСТЬ РАДИ ЄВРОПИ У ПРОТИДІЇ ТОРГІВЛІ ЛЮДСЬКИМИ ОРГАНАМИ

Торгівля людськими органами є проблемою міжнародного масштабу, яка певним чином порушує основні права і свободи людини, її гідність, і є прямою загрозою здоров'ю, фізичної цілісності і найчастіше – життя людей. Вона підриває довіру суспільства до існуючих систем трансплантації, тим самим посилює глибинну причину – дефіцит людських органів. Цей вид діяльності часто пов'язаний з діяльністю транснаціональних груп організованої злочинності, які користуються уразливим становищем донора. Міжнародні кримінальні угруповання отримують значні фінансові прибутки, зважаючи на велику прогалину між попитом на людські органи та їх пропозицією.

Торгівля людськими органами є проблемою, яка вимагає реагування з боку держав і міжнародних організацій. У зв'язку з цим у межах Ради Європи була прийнята ціла низка міжнародно-правових актів, а саме: Рекомендація Комітету Міністрів R (97) 16 про трансплантацію печінки від споріднених живих донорів, Рекомендація Комітету Міністрів Rec (2001) 5 щодо регулювання списків очікування на трансплантацію органів та часу очікування та Рекомендація Комітету Міністрів Rec (2003) 12 про реєстри донорів органів.

Принцип, відповідно до якого тіло людини та його частини не повинні бути об'єктом отримання фінансової вигоди, є частиною правових принципів Ради Європи. Він закріплений у Резолюції Комітету Міністрів (78) 29 про приведення у відповідність законодавств держав-учасниць з питань вилучення, пересадки та трансплантації матеріалів організму людини та підтверджений Заключною декларацією Третьої конференції європейських міністрів з охорони здоров'я 1987 р., а також закріплений у ст. 21 Конвенції про права людини та біомедицину 1997 р. Згодом, цей принцип був закріплений у Додатковому протоколі до Конвенції про права людини та біомедицину про трансплантацію органів та тканин людського походження 2002 р.

Проте вирішення цієї проблеми також вимагає від держав-членів Ради Європи вчинення певних дій на національному рівні, а саме завдяки багатосторонній співпраці об'єднати зусилля міністерств охорони здоров'я, внутрішніх справ та юстиції європейських країн.

У світлі вищезазначеного 25 червня 2003 р. Парламентська асамблея Ради Європи прийняла Рекомендацію 1611 (2003) про торгівлю органами в Європі. У документі містяться рекомендації державам, які можна поділити на чотири групи: діяльність стосовно всіх держав-членів Ради Європи; діяльність стосовно так званих «країн-донорів»; діяльність стосовно так званих «країн-попиту»; діяльність стосовно відповідних органів Ради Європи.

Що стосується всіх держав-членів Ради Європи, то Комітетові Міністрів рекомендувалося запросити їх до підписання та ратифікації Конвенції про права людини та біомедицину 1997 р. та Додаткового протоколу до неї про трансплантацію органів та тканин людського походження 2002 р; Конвенції ООН про транснаціональну організовану злочинність 2000 р. та Протоколу до неї про попередження та припинення торгівлі людьми, особливо жінками та дітьми, і покарання за неї 2000 р.; Факультативного протоколу до Конвенції про права дитини у сфері запобігання торгівлі дітьми, дитячій проституції та дитячій порнографії 2000 р., а також Конвенції Ради Європи про заходи з протидії торгівлі людьми 2005 р., оскільки

проблема торгівлі людськими органами тісно пов'язана з торгівлею людьми. Згадані міжнародно-правові акти направлені на визнання загальної відповідальності за мінімізацію ризику торгівлі органами шляхом посилення існуючих механізмів співпраці на рівні Ради Європи.

«Країнам-донорам» рекомендується посилити діяльність щодо запобігання торгівлі людськими органами шляхом проведення спільно з неурядовими організаціями та відповідними міжнародними установами інформаційних компаній, викладацької діяльності, особливо у сільській місцевості, у тому числі через ЗМІ. «Країни-донори» повинні вживати заходи для встановлення нелегальних донорів та надання їм медичної реабілітації, а також покращувати рівень першої медичної допомоги. У разі необхідності держави повинні внести зміни або доповнення до кримінального законодавства щодо передбачення відповідальності осіб, винних у торгівлі людськими органами, включаючи санкції для медичного персоналу, який брав участь у нелегальній трансплантації органів, отриманих злочинним шляхом.

«Країнам-попиту» рекомендується приймати та застосовувати суворе законодавство до випадків трансплантації від неспоріднених живих донорів. Держави повинні забезпечити суворий контроль за прозорістю реєстрів органів та списків очікування, а також посилити механізми співпраці щодо включення органів до процедури донорства.

9 липня 2014 р. Комітетом Міністрів Ради Європи була схвалена Конвенція про боротьбу з торгівлею людськими органами. Цей міжнародно-правовий документ став найважливішим етапом у протидії незаконній практиці в сфері трансплантації. У поєднанні з існуючими міжнародно-правовими інструментами, спрямованими на протидію торгівлі людьми, в тому числі торгівлі людьми з метою вилучення органів, Конвенція містить комплексні рамки для протидії різним типам злочинів, пов'язаних з трансплантацією.

Конвенція має глобальний характер: вона відкрита для підписання і ратифікації не лише для держав-членів Ради Європи і держав-спостерігачів, а й для будь-якої держави світу. Церемонія підписання Конвенції відбулася в Сантьяго-де-Компостела (Іспанія) 25 березня 2015 р. Після церемонії відбулася Міжнародна конференція високого рівня, присвячена протидії торгівлі людськими органами.

З огляду на складний характер торгівлі людськими органами, для протидії цьому злочину надзвичайно важливо виходити з багатодисциплінарного підходу. Для забезпечення ефективності Конвенції, слід брати до уваги думки і зацікавленість багатьох сторін, які беруть участь у виявленні, інформуванні, розслідуваннях, запобіганні та переслідуванні подібних злочинів. Ще один найважливіший аспект Конвенції – це захист жертв, оскільки саме жертви торгівлі людськими органами знаходяться в уразливому становищі.

Найширше приєднання держав до Конвенції матиме велике значення для боротьби з цим злочином, бо в більшості випадків ці злочини мають транснаціональний характер. Конвенція надає унікальну можливість для скоординованих дій на глобальному рівні шляхом гармонізації національного законодавства, виявлення різних актів, які представляють собою торгівлю людськими органами, а також створення основ для міжнародного співробітництва.

Одержано 28.04.2021

УДК 343.431
МАКАРЕНКО Вікторія Сергіївна
кандидат юридичних наук,
старший викладач кафедри поліцейської діяльності
та публічного адміністрування факультету № 3
Харківського національного університету внутрішніх справ;
МАКАРЕНКО Павло Валентинович,
кандидат психологічних наук, доцент,
заступник декана з навчально-методичної роботи факультету № 4
Харківського національного університету внутрішніх справ

ТОРГІВЛЯ ЛЮДЬМИ ЯК СУСПІЛЬНО-НЕБЕЗПЕЧНЕ СОЦІАЛЬНЕ ЯВИЩЕ В ПІВДЕННО-АФРИКАНСЬКІЙ РЕСПУБЛІЦІ

Торгівля людьми – складне явище, що підживлюється колосальним зростанням світового секс-ринку. Подібна експлуатація викликана бідністю, нерівномірним розвитком, корупцією в державних органах, гендерною дискримінацією, шкідливими традиційними і культурними звичаями, громадськими заворушеннями, стихійними лихами і відсутністю політичної волі до її припинення. Світова «епідемія» торгівлі людьми з року в рік продовжує залишатися глобальною проблемою, незважаючи на розробку і ратифікацію 2000 року Протоколу Організації Об'єднаних Націй 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 [1].

Торгівля людьми, є третім за величиною видом міжнародної злочинності після незаконного обігу наркотиків та зброї, та щорічно приносить мільярди доларів. Рушійною силою торгівлі є попит на сексуальну експлуатацію в комерційних цілях. Сімдесят дев'ять відсотків всієї світової торгівлі людьми здійснюється з метою сексуальної експлуатації [3]. Число дітей серед жертв торгівлі людьми з метою сексуальної експлуатації або в якості дешевої робочої сили у всьому світі щорічно складає близько 1,2 мільйона осіб [2].

Масштаби діяльності у сфері торгівлі людьми в Південній Африці достеменно невідомі, але щорічно велика кількість людей стають жертвами торгівлі людьми як всередині країни, так і за її межами. Діти особливо уразливі для торгівлі людьми і залишаються незахищеними від експлуатації в сексуальних і трудових цілях [4, с. 3].

Торгівля людьми зазвичай відбувається на двох рівнях: внутрішньому (всередині країни) і зовнішньому (вивезення жертв за межі країни). Існує також класифікація у межах якої країни поділяються на три види: 1) «країна походження або відправлення» – звідки відправляються діти; 2) «країна транзиту» – де дітей можуть перевезти і тимчасово залишити на шляху до кінцевого пункту призначення; 3) «країна призначення» – де врешті-решт опиняються діти [4, с. 3-4]. Залежно від причини торгівлі людьми деякі країни можуть відноситись тільки до першого типу, а інші – і до першого і до другого. А деяким країнам властиві всі три. Південна Африка, зокрема, є країною походження, відправлення та транзиту, і південноафриканські діти також продаються у країні.

Внутрішня торгівля людьми відбувається в Південно-Африканській Республіці через високий рівень безробіття і бідності; багато сімей змушені дозволяти дітям переїжджати з сільської місцевості до міста, довіряючи обіцянкам освіти, догляду або можливостей працевлаштування. Дитячий секс-туризм, з метою якого дітей продають всередині країни і за її межі, також значною мірою залишається поза увагою. Дівчат в Південній Африці в основному продають в сексуальних цілях і в якості домашньої прислуги.

Південноафриканців вивозять в Ірландію, на Близький Схід і в Сполучені Штати в якості працівників. Жінок і дівчат з інших африканських країн вивозять в Південну Африку з метою комерційної сексуальної експлуатації, домашнього рабства та інших робіт в сфері послуг; іноді таких жінок вивозять до Європи. Тайських, філіппінських, китайських та східноєвропейських

жінок продають до Південної Африки з метою комерційної сексуальної експлуатації, пов'язаної з борговими зобов'язаннями [5].

Діти особливо уразливі для торгівлі людьми, тому що вони часто недостатньо освічені, їх легко переконати і легко переконати в тому, що вони зобов'язані виконувати вказівки дорослих. Діти також можуть опинитись в положенні, коли, на їхню думку, вони повинні допомагати своїм сім'ям, і для цього їх можуть продати або відправити за кордон. Безхатьки, діти з таборів біженців, і тим про кого нема кому піклуватися в групі високого ризику. Це може відбуватися через недосконаліть законодавства або його неналежне дотримання, або через те, що діти менш поінформовані про небезпеку торгівлі людьми та їх легше обдурити.

Хоча Південна Африка і ратифікувала основні міжнародні конвенції, пов'язані з торгівлею дітьми, вона повинна продовжувати належним чином звітувати і дотримуватися рекомендацій комітетів, оскільки вона погодилася зробити це в якості країни, що підписала відповідні конвенції. Західні партнери вважають, що Південна Африка повинна розробити і реалізувати національний план дій по боротьбі з торгівлею людьми, який встановлює стандартну процедуру розгляду справ про торгівлю людьми (також з упором на внутрішню торгівлю людьми), особливо для поліпшення ідентифікації жертв [4, с. 5]. Крім того, уряд повинен підвищувати обізнаність відповідних державних посадових осіб на всіх рівнях про їхню відповідальність за забезпечення захисту жертв, а також регулярно складати національну статистику про кількість порушених в судовому порядку справ про торгівлю людьми і допомоги жертвам, як це робиться стосовно інших злочинів.

Список використаних джерел

1. Najemy L.B. South Africa's Approach to the Global Human Trafficking Crisis: An Analysis of the Proposed Legislation and the Prospects of Implementation. *Washington University Global Studies Law Review*. 01.2010. Vol 9. Iss 1. URL: https://openscholarship.wustl.edu/law_globalstudies/vol9/iss1/7 (дата звернення: 01.05.2021).

2. UNICEF calls for increased efforts to prevent trafficking of children // UNICEF : вебсайт. 15.06.2007. URL: http://www.unicef.org/media/media_40002.html (дата звернення: 01.05.2021).

3. Global Report on Trafficking in Persons : UNODC, 02.2009 // UNODC : вебсайт. URL: https://www.unodc.org/documents/human-trafficking/Global_Report_on_TIP.pdf (дата звернення: 01.05.2021).

4. ECPAT International. Stop Sex Trafficking of Children and Young People. Bangkok. 2007.

5. Trafficking in Persons Report 2008 : US State Department // US State Department : вебсайт. URL: https://2009-2017.state.gov/documents/organization/105501.pdf (дата звернення: 01.05.2021).

Одержано 01.05.2021

УДК 351.745.7

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

ДІЯЛЬНІСТЬ МІЖНАРОДНИХ ПРАВООХОРОННИХ І БЕЗПЕКОВИХ ОРГАНІЗАЦІЙ ЩОДО КООРДИНАЦІЇ ЗУСИЛЬ У СФЕРІ ПРОТИДІЇ ТОРГІВЛІ ЛЮДЬМИ

Важливе значення для координації зусиль у сфері протидії торгівлі людьми й іншим злочинам транснаціонального характеру має діяльність міжнародних правоохоронних, поліцейських та безпекових організацій, зокрема Інтерполу та Європолу.

Міжнародну організацію кримінальної поліції (Інтерпол) в Україні представляє Національне центральне бюро (НЦБ) Інтерполу, яке є центром координації взаємодії правоохоронних органів України з компетентними органами зарубіжних держав щодо протидії злочинності, що

має транснаціональний характер або виходить за межі країни. Водночас підрозділом, на який безпосередньо покладається організація виконання функцій МВС України як НЦБ Інтерполу, є Департамент міжнародного поліцейського співробітництва Національної поліції України.

Основними завданнями Генерального Секретаріату Інтерполу щодо протидії злочинам, пов'язаним з торгівлею людьми, є: координація співробітництва правоохоронних органів держав-членів Інтерполу у справах щодо злочинів, пов'язаних з торгівлею людьми; створення та формування спеціалізованих банків даних щодо осіб, причетних до торгівлі людьми; запровадження та реалізація аналітичних проектів у сфері торгівлі людьми; організація та проведення міжнародних науково-практичних заходів з проблем протидії торгівлі людьми (конференцій, тренінгів, оперативних зустрічей) [1].

Європейський поліцейський офіс (Європол) є міжнародною правоохоронною організацією, що бере активну участь у протидії злочинності в рамках Європейського Союзу. Оперативна та стратегічна угода між МВС України та Європолом щодо розширення співробітництва у боротьбі з транскордонною злочинною діяльністю підписана 14 грудня 2016 року. На підставі даної угоди Україна створила національний контактний пункт, який є центральним пунктом обміну інформацією між Європолом та правоохоронними органами України. Крім того, в МВС України встановлено спеціальний захищений канал зв'язку «SIENA» для обміну інформацією з Європолом. Важливе значення для протидії торгівлі людьми мають наступні проекти Європолу: AP Phoenix (справи по торгівлі людьми); AP Twins (злочинність, пов'язана з сексуальною експлуатацією та насильством дітей).

Завданням Європейської організації з питань юстиції (EUROJUST) є сприяння органам кримінального переслідування держав-членів Євросоюзу у боротьбі проти транскордонної злочинності. З цією метою EUROJUST координує обмін інформацією, надання правової допомоги та процес видачі правопорушників. Угода про співробітництво між Україною та EUROJUST підписана у червні 2016 року [2].

У травні 2019 року Україною підписано новий План співробітництва з Європейською Агенцією з прикордонної та берегової охорони (FRONTEX). До основних завдань FRONTEX належить: аналіз даних, пов'язаних з ситуацією на зовнішніх кордонах ЄС та за їх межами з метою визначення міграційних структур та тенденцій в транскордонній злочинній діяльності; координація та організація спільних операцій та заходів швидкого реагування для надання допомоги державам-членам; підтримка держав-членів в проведенні ідентифікації та мігрантів, допомога в примусовому поверненні осіб.

Організація з безпеки і співробітництва в Європі (ОБСЄ) займається широким спектром питань, що мають відношення до торгівлі людьми: права людини і верховенство закону; корупція і боротьба зі злочинністю; дискримінація та нерівність; питання економічної, трудової та міграційної політики. У 2003 році Організація створила Бюро і заснувала посаду Спеціального представника і координатора по боротьбі з торгівлею людьми, щоб допомогти державам-учасницям у розробці і здійсненні ефективної політики у сфері протидії торгівлі людьми.

Група експертів із протидії торгівлі людьми (GRETA) складається з 15 незалежних експертів, які відслідковують, як країни-учасниці Конвенції Ради Європи «Про заходи щодо протидії торгівлі людьми» реалізують взяті на себе зобов'язання. Зазначена Конвенція набула чинності в Україні в березні 2011 року.

Міжнародна організація з міграції (МОМ) / Агенція ООН з питань міграції співпрацює з Державною міграційною службою та Державною прикордонною службою України для вдосконалення системи ідентифікації потенційних постраждалих від торгівлі людьми на кордонах України і покращення співпраці зі спеціалізованими підрозділами поліції.

Міжнародна організація праці (МОП) встановлює трудові стандарти, розробляє політику та програми, що сприяють гідній праці для всіх жінок та чоловіків. За оцінками МОМ, 40,3 млн людей перебувають у сучасному рабстві, включаючи 24,9 млн примусових робіт та 15,4 млн у примусових шлюбах. Це означає, що на 1000 людей у світі припадає 5,4 жертви сучасного рабства [3].

Управління ООН з наркотиків та злочинності (UNODC) є основним органом ООН щодо реалізації співробітництва у сфері боротьби зі злочинністю, нелегальним виробництвом і споживанням наркотиків, терористичною загрозою, корупцією, торгівлею людьми.

Отже, співробітництво Національної поліції України з міжнародними правоохоронними та безпековими організаціями має важливе значення для подолання такого ганебного у сучасному світі явища як торгівля людьми.

Список використаних джерел

1. Офіційний вебсайт Інтерполу URL: https://www.interpol.int/ (дата звернення: 15.03.2021).

2. Євроюст // Посольство України в Королівсті Нідерланди : офіційний вбесайт. 23.10.2020. URL: https://netherlands.mfa.gov.ua/spivrobitnictvo/ spivrobitnictvo-z-mizhnarodnimi-organizaciyami/spivpracya-z-yevroyustom (дата звернення: 19.03.2021).

3. Forced labour, modern slavery and human trafficking // International Labour Organization : вебсайт. URL: https://www.ilo.org/global/topics/forced-labour/lang--en/index.htm (дата звернення: 20.03.2021).

Одержано 07.04.2021

УДК [351.74(100):004.9](075.8)

ОСТАВЧУК Дину,
доктор права, доцент кафедры
уголовного процесса, криминалистики и информационной безопасности
Академии «Штефан чел Маре» МВД Республика Молдова;
РУСНАК Константин,
доктор права, доцент кафедры
уголовного процесса, криминалистики и информационной безопасности
Академии «Штефан чел Маре» МВД Республика Молдова

ПОЛИТИКА РЕСПУБЛИКИ МОЛДОВА В ОБЛАСТИ ПРЕДОТВРАЩЕНИЯ ТОРГОВЛИ ЛЮДЬМИ

Торговля людьми – это нарушение свободы и достоинства личности и серьезная форма преступления, которая имеет серьезные последствия для жизни и здоровья людей, но при этом продолжает представлять угрозу безопасности и устойчивому развитию современного общества. В условиях глобализации типы и формы проявления торговли людьми становятся все более сложными и латентными [1].

Политика предотвращения торговли людьми является неотъемлемой частью политики современного демократического государства.

Политика в области предотвращения торговли людьми и борьбы с ней определяет содержание законодательства в этой области. А именно принципы и тенденции политики предотвращения торговли людьми определяют области предотвращения, организационные аспекты проведения профилактики и контроля, основные направления деятельности в области предотвращения и борьбы с торговлей людьми и т. д.

Из вышесказанного следует, что сфере создания правовых норм принадлежит важнейшая роль [2, с. 160] в реализации политики в области предотвращения и противодействия торговле людьми. В этом контексте хотелось бы особо отметить мнение автора А. Зосима, в котором говорится, что ошибки на этапе разработки политики являются наиболее опасными, поскольку они влияют на реализацию политики и, таким образом, имеют последствия для общества в целом.

Теоретически, как закон является высшей силой в государстве, управляемом верховенством закона, так и законодательная политика должна быть выше практики обеспечения соблюдения закона: обусловливать и направлять последний [3, с. 178].

В настоящее время Национальная стратегия предотвращения и борьбы с торговлей людьми на 2018-2023 годы фокусируется на устойчивом развитии национальной системы предотвращения торговли людьми и борьбы с ней через призму парадигмы 4Р (предотвращение, защита, преследование, партнерство).

Текущий вектор политики в области предотвращения торговли людьми направлен на обеспечение преемственности государственной политики по реформированию национальных и транснациональных отношений сотрудничества между государственными, некоммерческими и межправительственными организациями для реализации мер по предотвращению и борьбе с торговлей людьми, продвижение прав жертв и предполагаемых жертв торговли людьми в соответствии с принципами соблюдении прав человека и равных возможностей для женщин и мужчин. Цели политики достигаются посредством следующих мероприятий:

1. Координация действий по предупреждению и борьбе с торговлей людьми – на национальном уровне разработан механизм, обеспечивающий согласование национальной политики в сфере противодействия торговле людьми, деятельности правоохранительных органов в сфере борьба с преступлениями торговли людьми и деятельность по прямому оказанию помощи жертвам и потенциальным жертвам торговли людьми.

2. Развитие профессиональных способностей специалистов – является важным компонентом обеспечения эффективной реализации политики в данной области. Отметим, что учебные модули для специалистов государственных учреждений профильного профиля включены в систему непрерывного обучения и профессиональной переподготовки.

3. Исследования – систематический сбор статистических данных осуществляется компетентными учреждениями по предотвращению торговли людьми и борьбе с ней. В целях усиления потенциала анализа рисков на национальном уровне в области борьбы с трансграничной преступностью, торговлей людьми и нелегальной миграцией готовятся полугодовые аналитические отчеты в этой области.

4. Предупреждение торговли людьми является важным компонентом политики в области торговли людьми, которая достигается за счет: а) информирования широкой общественности через средства массовой информации; б) снижения уязвимости; в) административный контроль.

5. Укреплять институциональный потенциал компетентных органов в области оптимизации идентификации жертв и предполагаемых жертв всех форм торговли людьми, их социальной защиты и их репатриации.

6. Наказание за торговлю людьми направлено на усиление процесса расследования, уголовного преследования и судебного процесса в соответствии с международными стандартами уголовного правосудия.

7. Укреплять сотрудничество между компетентными органами разных стран в целях оптимизации предотвращения торговли людьми и борьбы с ней.

В заключение следует отметить, что политика в области предотвращения торговли людьми должна осуществляться с соблюдением принципа научного подхода к процессу разработки нормативных актов, регулярная проверка всего спектра нормативных актов, выражающих политику в данной области, с целью устранения ошибок и противоречий, никоим образом не под влиянием личных интересов высших должностных лиц, а также под влиянием международных организации.

Список використаних джерел

1. Hotărârea Guvernului privind Strategia naţională de prevenire şi combatere a traficului de fiinţe umane pentru anii 2018-2023, nr.461 din 22 mai 2018. Publicat: Monitorul Oficial al Republicii Moldova din 25.05.2018, nr. 167-175.

2. Rusnac C. P. Aspecte ale prevenirii erorilor în procesul elaborării şi reali-zării politicii în domeniul expertizei judiciare. În: Anale ştiinţifice ale Academiei „Ştefan cel Mare” a MAI al Republicii Moldova, Ştiinţe juridice, nr. 10, Chișinău, 2019, 248 p.

3. Zosim Al. V. Aspecte ale prevenirii erorilor în procesul elaborării şi realizării politicii penale. În: Criminalitatea în spațiul Uniunii Europene şi al comunității statelor independente: evoluție, tendințe, probleme de prevenire şi combatere. Materiale ale conferinței ştiințifico-practice internaționale, Chişinău, 12-13 iunie 2012, 401 p.

Одержано 23.04.2021

Наукове видання

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

Збірник матеріалів
Міжнародної науково-практичної конференції
(м. Харків, 18 травня 2021 року)

Відповідальні за випуск: *О. В. Манжай*
Комп'ютерне верстання: *К. О. Сологуб*

Формат 60х84/8. Ум. друк. арк. 10,7. Обл.-вид. арк. 7,4.
Тираж 10 пр. Зам. № 2021-14.
Видавець і виготовлювач –
Харківський національний університет внутрішніх справ,
просп. Л. Ландау, 27, м. Харків, 61080.
Свідоцтво суб'єкта видавничої справи ДК № 3087 від 22.01.2008.