МВС України

Харківський національний університет внутрішніх справ

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Збірник матеріалів

круглого столу

(09 грудня 2020 року, м. Харків)

Харків

Харківський національний університет внутрішніх справ

2020

УДК [351.74:004] (477)(08)
ББК 67.9(4УКР)301.163я43
З-36

Друкується згідно з рішенням оргкомітету
за дорученням Харківського національного університету внутрішніх справ
від 20.10.2020 № 144

З-36 **Застосування інформаційних технологій у діяльності правоохоронних органів :** зб. матеріалів круглого столу (09 грудня 2020 р., м. Харків) / МВС України, Харк. нац. ун-т внутр. справ. – Харків : ХНУВС, 2020. – 132 с.

У збірнику висвітлено погляди науковців та практиків щодо актуальних питань розробки, впровадження і використання компонентів інформаційних технологій в діяльності правоохоронних органів, проблем підготовки кадрів для інформаційно-аналітичних підрозділів правоохоронних органів.

УДК [351.74:004] (477)(08)
ББК 67.9(4УКР)301.163я43

ЗМІСТ

УДК 351.74:65.012.45
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

АКТУАЛЬНІ ПИТАННЯ ПОКРАЩЕННЯ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Стрімкий розвиток сучасного інформаційного суспільства практично повністю залежить від стану ІТ-інфраструктури, яка забезпечує всіх споживачів інформації новими інформаційними технологіями на базі широкого застосування різноманітних комп'ютерних систем. Не минула ця тенденція також Міністерство внутрішніх справ України і Національну поліцію України.

Як відомо, у 2018 році було затверджено Концепцію інформатизації Міністерства внутрішніх справ України та центральних органів виконавчої влади. Реалізація Концепції була неможливою без побудови єдиного інформаційного простору МВС, який повинен забезпечити єдиний механізм функціонування як новоутворених, так і вже запроваджених інформаційних автоматизованих систем, реєстрів, баз (банків) даних у ході їх інтеграції до ЄІС.

Крім того, інформатизацію МВС неможливо уявити без використання новітніх інформаційних технологій для надання відкритого, повного і захищеного доступу фізичним та юридичним особам до інформаційних обліків системи МВС у визначеному законодавством порядку. У свою чергу, необхідно відзначити, що нинішня інформаційна система МВС і Нацполіції є неоднорідною та мультисервісною, тому процеси отримання, обробки, передачі та зберігання інформації керуються великою кількістю різноманітних технологій, методів і протоколів залежно від підсистеми, в якій відбуваються ці процеси. Тому для поліпшення показників якості функціонування інформаційної системи необхідно використовувати як існуючі методи, так і методи, які ґрунтуються на нових принципах побудови й управління інформаційними системами.

Як відомо, наш час характеризується зростанням обсягів інформаційних потоків. Тому на перший план почали виходити завдання зниження операційних витрат і скорочення часу, необхідного на модернізацію Hardware (Software) в існуючих інформаційних системах. Крім того, постійно збільшуються витрати на управління інфраструктурою, що постійно ускладнюється. Тому сьогодні все більше уваги користувачі звертають на інтегровані програмні платформи (ІПП), які суттєво спрощують управління інфраструктурою, скорочують операційні витрати і при цьому дозволяють скоротити загальну вартість володіння ІТ-інфраструктурою та підготувати її до майбутніх потреб, що, безумовно, корисно і для інформаційної системи МВС України та Національної поліції України. Отже, підвищення оперативності процесу передачі інформації в інформаційних системах МВС України та Національної поліції України з використанням інтегрованих програмних платформ є досить актуальним науковим завданням метою нашої доповіді.

ІПП базуються на технології, що програмно визначається, в ній усі компоненти інтегровані, забезпечується можливість централізованого управління віртуалізованими середовищами за допомогою одного інтерфейсу, можливість прискореного придбання, розгортання, підтримки й управління Hardware і Software, а також пропонується масштабований підхід до побудови інфраструктури з використанням структурних блоків із можливістю простого розширення.

Під час упровадження ІПП користувачі, звісно, отримують низку переваг над традиційними платформами, таких як спрощення експлуатації, скорочення капітальних витрат завдяки використанню архітектури, що масштабується горизонтально і вертикально, підвищення адаптивності комп’ютерної системи, зниження ризику втрати даних за рахунок розподіленого зберігання інформації на всіх вузлах комп’ютерної мережі, більш просте масштабування. Однак водночас з’являються деякі недоліки, пов’язані, насамперед, із централізованим управлінням та уніфікацією вузлів. Також слід відзначити відсутність гнучкості масштабування, низку труднощів під час увімкнення та функціонування

гетерогенних компонентів і збільшення часу доступу до розподілених сховищ даних.

Тому подальші дослідження використання цього підходу до управління інформаційною системою МВС України та Національної поліції України повинні забезпечити істотне підвищення показників ефективності системи.

Одержано 05.12.2020

УДК [351.74(100):004.9](075.8)
Швець Дмитро Володимирович
доктор юридичних наук, доцент,
перший проректор Харківського національного університету внутрішніх справ
http://orcid.org/0000-0002-1999-9956

СТРАТЕГІЧНІ НАПРЯМКИ ВИКОРИСТАННЯ НОВІТНІХ ТЕХНОЛОГІЙ ЦИФРОВОГО СВІТУ В ПОПЕРЕДЖЕННІ ЗЛОЧИНІВ

Останні роки характеризуються перенесенням акцентів у діяльності правоохоронних органів розвинених країн з реактивного принципу до предикативного. Це обумовлено тим фактом, що наслідки від здійснення злочинів з використанням сучасних технологій для людства в багатьох випадках не можуть бути компенсовані будь-якою мірою покарання, особливо у тих випадках, коли йдеться про загибель десятків, сотень і більше людей. У цьому контексті керівники правоохоронних структур намагаються розробити нові стратегії та переформовувати свою діяльність саме виходячи з цієї парадигми.

Використання новітніх технологій цифрового світу в контексті злочинності має двоїстий характер. З одного боку, дані і технології використовуються злочинцями для здійснення кримінальних дій. У цьому плані нові технології входять в число драйверів злочинності. З іншого боку, технології є інструментом, що дозволяє успішно не тільки боротися, але й профілактувати кримінал. Тому вивчення зарубіжного досвіду з використання

сучасних інформаційних технологій для розкриття злочинів та запобігання їм є актуальним завданням.

Метою цієї доповіді є дослідження досвіду Великобританії у використанні сучасних технологічних інструментів для профілактики, запобігання і розкриття злочинів.

У найбільш розгорнутому вигляді це питання висвітлено в Сучасній стратегії попередження злочинності (березень 2016 р. Великобританія). Зокрема, в цьому документі зазначено, що ефективні протоколи обміну інформацією та координації дій між центральними і регіональними поліцейськими структурами, бізнесом і громадянським суспільством є ключем до підвищення ефективності боротьби з криміналом. Дані та інформаційно-комунікаційні технології є найважливішим фактором створення систем ефективного обміну відомостями і результативної взаємодії. Якщо ще кілька років тому головні зусилля правоохоронних органів були спрямовані на створення текстових баз даних про організовану і вуличну злочинність, то в цей час ситуація в корені змінилася.

Уже зараз не менше 70 % сховищ даних про кримінал займають відео і фотофайли. З переходом міст Великобританії з населенням понад 100 тис. і всіх транспортних комунікацій країни на 100-процентне охоплення відеоспостереженням (не пізніше 2018 р.) саме відеофайли стануть основним елементом даних і матеріалом для профілактики злочинності та проведення розслідувань. У цей час перед системою кримінальної юстиції та забезпечення правопорядку в Великобританії стоїть завдання не тільки технічно відповісти на цей виклик, але й оснастити засобами та інструментами, що дозволяють максимально повно використовувати відеоінформацію спільно з текстовою та аудіоінформацією.

Британська поліція використовує Великі дані і технології, причому не тільки програмні, але й фізичні технології (типу БПЛА). На відміну від ряду інших країн британський кримінал поступається поліції за своєю оснащеністю. Це дає певні переваги у веденні правоохоронної діяльності. Щоб найкращим

чином використовувати дані й технології, британська поліція планує не тільки здійснити до 2020 р. апаратне і програмне переоснащення, але й, найголовніше, провести суцільне підвищення кваліфікації поліцейських, в першу чергу, на низовому рівні, змінити культуру поліцейських розслідувань.

Найближчим часом не залишиться невисокотехнологічної злочинності взагалі. Навіть вуличні злочинці будуть використовувати ті чи інші плоди високих технологій.

Британський бізнес, особливо ключова галузь господарства – фінансова, вимагає від поліції якісного підвищення рівня протидії високотехнологічній злочинності. Для цього планується продовжити роботу щодо формування спеціалізованих підрозділів з кіберзлочинності.

Разом з тим усі британські поліцейські повинні мати доступ до баз даних і сучасних інструментів, що забезпечують ефективні комунікації, профілактику і розслідування злочинів з використанням інформаційних технологій. Настав час, коли всі британські поліцейські, незалежно від віку, повинні пройти прискорені курси підготовки в галузі використання інформаційно-комунікаційних технологій.

Такі основні проблеми та виклики є актуальними не тільки у Великобританії, але й для України, тому що злочинність досить часто не має національності.

Одержано 04.12.2020

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 Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-0240-5517

ЩОДО ЗАКОНОДАВСТВА УКРАЇНИ У СФЕРІ ПРОТИДІЇ ВИКОРИСТАННЮ ТЕХНОЛОГІЙ ДЛЯ ТОРГІВЛІ ЛЮДЬМИ

Незважаючи на те, що у 2011 р. в Україні було прийнято цільовий рамковий закон «Про протидію торгівлі людьми» [1] питання унормування правовідносин у сфері використання технологій під час торгівлі людьми лишається малоурегульованим. На теперішній час в законодавстві Україні практично відсутні норми, які встановлюють відповідальність саме за використання комп'ютерних технологій під час вчинення злочинів, пов'язаних з торгівлею людьми. В нормативних актах можна зустріти лише опосередковане згадування окремих аспектів, пов'язаних з інформаційними технологіями.

У Кримінальному кодексі України від 05.04.2001 [2] чч. 2, 4 ст. 301 «Ввезення, виготовлення, збут і розповсюдження порнографічних предметів» встановлено кваліфіковані ознаки злочину:

ввезення в Україну творів, зображень або інших предметів порнографічного характеру з метою збуту чи розповсюдження або їх виготовлення, зберігання, перевезення чи інше переміщення з тією самою метою, або їх збут чи розповсюдження, а також примушування до участі в їх створенні

ч. 2 вчинені щодо кіно- та відеопродукції, *комп'ютерних програм* порнографічного характеру, а також збут неповнолітнім чи розповсюдження серед них творів, зображень або інших предметів порнографічного характеру;

ч. 4 вчинені щодо творів, зображень або інших предметів порнографічного характеру, що містять дитячу порнографію, або примушування неповнолітніх до участі у створенні творів, зображень або кіно- та відеопродукції, *комп'ютерних програм* порнографічного характеру.

У Законі України «Про телекомунікації» від 18.11.2003 є окремі згадування обов'язків провайдерів (операторів) телекомунікацій щодо взаємодії з правоохоронними органами, а також збереження даних для вирішення завдань кримінального розслідування [3, ч. 2 ст. 39]. Останню категорію обов'язків було запроваджено з метою посилення протидії розповсюдженню дитячої порнографії у 2010 році. Натомість законодавець не визначив строки такого зберігання, що надає можливість провайдерам ухилятися від надання інформації правоохоронним органам.

Прийнятий Верховною Радою України, проте ветований Президентом України, Закон «Про електронні комунікації» [4] має замінити Закон України «Про телекомунікації». І хоча в новому Законі збереглися окремі норми про взаємодію з правоохоронними органами в частині здійснення негласних слідчих (розшукових) дій (п. 10 ч. 3 ст. 18), проте вимогу про обов'язковість збереження даних про транзакції користувачів взагалі було прибрано.

Взагалі питання взаємодії правоохоронних органів з провайдерами (операторами) телекомунікацій в рамках виявлення, попередження та розслідування злочинів у сфері торгівлі людьми, як правило, стосується провадження слідчої (розшукової) дії «Тимчасовий доступ до рей і документів» для отримання даних про клієнтів та негласних слідчих (розшукових) дій, пов'язаних з перехопленням телекомунікацій.

Пунктом 9 ст. 8 Закону України «Про оперативно-розшукову діяльність» [5] підрозділам, які здійснюють оперативно-розшукову діяльність, надається право здійснювати аудіо- й відеоконтроль особи, зняття інформації з транспортних телекомунікаційних мереж та електронних інформаційних мереж. Вказане стосується попередження злочинів. Якщо вже відкрито кримінальне провадження, то проводяться аналогічні негласні слідчі (розшукові) дії. У будь-якому випадку Закон України «Про оперативно-розшукову діяльність» містить бланкетну норму, яка встановлює, що порядок проведення таких оперативно-розшукових заходів так само як і негласних слідчих (розшукових) дій регулюється Кримінальним процесуальним кодексом.

В Україні також поступово відбувається унормування питань, пов'язаних з використанням електронних доказів. Серед іншого у 2017-2018 рр. було прийнято закон «Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів» та імплементовано стандарт ISO IEC 27037: 2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів» [6].

Під час дослідження українського законодавства стосовно інформаційних технологій в контексті злочинів у сфері торгівлі людьми слід враховувати також те, що згідно з чинним українським законодавством Рішення Європейського суду з прав людини є джерелом права в Україні [7, ст. 17], а тому мають враховуватися при винесенні рішень відповідними національними судами.

Список використаних джерел

1. Про протидію торгівлі людьми: закон України від 20.09.2011; [із змінами і доповненнями на 17.01.2019]. Офіційний вісник України. 2011. № 80 (24.10.2011). ст. 2936. URL: https://zakon.rada.gov.ua/laws/show/3739-17 (дата звернення: 07.11.2020).

2. Кримінальний кодекс України від 05.04.2001; [із змінами і доповненнями на 26.02.2019]. Офіційний вісник України. 2001. № 17 (18.04.2001). ст. 432. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 07.11.2020).

3. Про телекомунікації : закон України від 18.11.2003 : [із змінами і доповненнями на 13.02.2020]. Офіційний вісник України. 2003. № 51 (02.01.2004). Ч. 1. Ст. 2644. URL: https://zakon.rada.gov.ua/laws/show/1280-15 (дата звернення: 07.11.2020).

4. Прийнято Закон «Про електронні комунікації» // Верховна Рада України : Офіційний вебпортал парламенту України. 30.0.2020. URL: https://www.rada.gov.ua/news/Novyny/198213.html. (дата звернення: 07.10.2020).

5. Про оперативно-розшукову діяльність : закон України : від 18.02.1992 : [із змінами і доповненнями на 17.06.2020]. Відомості Верховної Ради України. 1992. № 22 (02.06.1992). Ст. 303. URL: https://zakon.rada.gov.ua/laws/show/2135-12 (дата звернення: 07.11.2020).

6. ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів. На заміну ДСТУ ISO/IEC 27037:2016 (ISO/IEC 27037:2012, IDT); Чинний від 2019-01-01. Київ : УкрНДНЦ, 2018. VI, 31 с. : рис., табл. (Національний стандарт України).

7. Про виконання рішень та застосування практики Європейського суду з прав людини: закон України від 23.02.2006. Офіційний вісник України. 2006. № 12 (05.04.2006). ст. 792. URL: https://zakon.rada.gov.ua/laws/show/3477-15 (дата звернення: 07.11.2020).

Одержано 17.11.2020

УДК 004.451+004.056.55

Бичков Сергій Олександрович
заступник завідувача відділу комп'ютерно-технічних та телекомунікаційних досліджень Харківського НДЕКЦ МВС України

ШЛЯХИ ПОДОЛАННЯ КРИПТОГРАФІЧНОГО ЗАХИСТУ ДАНИХ КОРИСТУВАЧА В ОПЕРАЦІЙНИХ СИСТЕМАХ MICROSOFT WINDOWS ТА MAC OS

На сьогодні найбільш поширені операційні системи, які обирають користувачі для своїх персональних комп'ютерів це Windows 10 та операційна система Mac OS для комп'ютерів компанії Apple. З приводу захисту особистих даних користувачів операційних систем розробники вбудували в них програмне забезпечення, що дозволяє застосувати алгоритми криптографічного захисту. Для операційних систем Windows 10 це BitLocker, для операційних систем Mac OS – це FileVault 2. Підхід який пропонується для подолання встановленого криптографічного захисту в цих зазначених операційних системах у більшому схожий але має деякі особливості з використанням стороннього програмного забезпечення та послідовністю дій на активній операційній системі, які необхідно буде виконати особі, що проводить вилучення комп'ютерної техніки.

Дії що пропонується зробити для подолання криптографічного захисту в операційних системах Windows 10.

Розробники операційних систем сімейства Windows, починаючи з версії Microsoft Windows Vista Максимальна\Корпоративна додали у функціонал своїх продуктів можливість шифрування логічних розділів диску (томів) за допомогою вбудованого в операційну систему програмного забезпечення BitLocker, який підтримує наступні алгоритми шифрування: AES 128, AES 128

с Elephant diffuser (використовується за замовченням), AES 256, AES 256 с Elephant diffuser, XTS-AES (починаючи з Windows 10 версії 1511).

Для того щоб зрозуміти ввімкнено шифрування чи ні, на активній системі персонального комп'ютера чи ноутбука, що буде вилучатися для направлення на комп'ютерно-технічну експертизу, самий простий спосіб це увійти в меню провідник або увійти в «Цей комп'ютер» (російською «Этот компьютер»), на панелі де відображається список логічних дисків можна побачити іконки логічних дисків. Логічні диски до яких застосовано шифрування за допомогою BitLocker мають іконку у вигляді зображення диску та замку біля нього. Якщо замок відчинений це означає що диск замонтовано до системи, якщо зачинений – диск не замонтовано, та для того щоб отримати доступ до даних що на ньому зберігаються необхідно ввести пароль або використати апаратний ключ.

У разі якщо застосовано шифрування функцією BitLocker, подальшим кроком, який є дуже важливим для успішного проведення дослідження у майбутньому є зняття дампу (копії) ОЗУ.

Дамп ОЗУ на комп'ютерах з операційною системою Windows можливо виготовити за допомогою спеціального програмного забезпечення, наприклад, «AccessData FTK Imager Lite Version», «Belkasoft Live RAM Capturer», «Magnet RAM Capture» та іншого. Наведене програмне забезпечення є безкоштовним та легким в користуванні.

Дуже важливо зробити дамп ОЗУ не даючи змоги власнику персонального комп'ютера його вимкнути, оскільки ОЗУ це енергозалежна пам'ять, та після вимикання комп'ютера більшість важливих даних, які містилися в неї, будуть очищені.

Таким чином, алгоритм дій має наступні ключові кроки:

1. Пересвідчитися чи застосовано до носіїв інформації комп’ютерної техніки функція шифрування даних BitLocker,

2. У разі якщо застосовано, виготовити дамп (копію) ОЗУ цього комп’ютера,

3. Надати судовому експерту для дослідження вилучену комп'ютерну техніку та виготовлений з неї дамп ОЗУ.

Дії що пропонується зробити для подолання криптографічного захисту в операційних системах Mac OS

На відміну від попередньої версії функції FileVault, яка могла захистити шифруванням лише розділ користувача, FileVault 2 здатна шифрувати як розділ диску, так і весь диск.

На стадії вилучення комп'ютерної техніки Apple, якщо вона знаходиться в активному стані (операційна система запущена, здійснений вхід до облікового запису користувача) необхідно виготовити дамп ОЗУ та надати його для подальшого дослідження експерту разом із комп'ютерною технікою, що вилучається.

Існує декілька сторонніх засобів для виготовлення дампів ОЗУ з комп'ютерів під керуванням операційною системою Mac OS, це: Goldfish, Mac Memory Reader, OSXPMem, які зможуть стати в нагоді при виготовленні дампів ОЗУ на версіях Mac OS до Mac OS X El Capitan 10.11.

Таким чином, у разі якщо виготовлення дампу ОЗУ з активної системи комп'ютера під керуванням операційної системи Mac OS завершилось успіхом, як і у випадку з операційними системами Windows, виготовлена копія пам'яті надається разом із технікою що вилучається на комп'ютерно-технічну експертизу для подальшого дешифрування та дослідження інформації судовими експертами.

Одержано 21.11.2020

УДК 004.4
Білашенко Данило Вячеславович
курсант 1 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

СПОСОБИ АНОНІМНОСТІ В ІНТЕРНЕТІ

Інтернет є надзвичайно великим джерелом інформації. Серед багатьох користувачів є ті, які прагнуть займатися незаконною діяльністю, або дивитися контент, заборонений на тій, чи іншій території. Велику загрозу у Всесвітній павутині становлять терористи, наркоторговці, торговці людьми, хакери, шахраї. Вони у відмінності від звичайних користувачів прагнуть приховати свою особистість та бути не покараними за свої дії. Працівники поліції, як ніхто інший повинні знати про ймовірні способи анонімності в інтернеті, щоб мати можливість протидіяти протиправним діям.

Початковим рівнем анонімності вважають користування Інтернетом за допомогою VPN, proxy, I2p або Tor.

VPN і proxy дають можливість змінити ip - адрес. Спосіб їх використання дає змогу обійти регіональне блокування, для відвідування заблокованих сайтів або сервісів, але стати повністю анонімним не вийде.

I2p та Tor включають у свій функціонал шифрування, заміну ip - адреси. До того ж доступні для всіх.

Осіб які користуються такими методами анонімності достатньо легко визначити, тому більшість серйозних злочинців використовують надійніші способи, а саме застосування віртуальних машин.

Віртуальна машина – це програмне забезпечення, яке допомагає встановити додаткову операційну систему у комп’ютері. Під час роботи основної системи, друга буде працювати як звичайна програма.

Якщо підключити на комп'ютері VPN, потім запустити віртуальну машину і в ній також запустити VPN – майже повна анонімність гарантована. Через те що одна ір-адреса використовується великою кількістю користувачів, друга VPN мережа не зможе точно визначити, хто підключився до неї.

Список використаної джерел

1. Полная сетевая анонимность: VPN + Виртуальная машина // whoer.net : сайт. URL: https://whoer.net/blog/ru/polnaya-setevaya-anonimnost-vpn-virtualnaya-mashina/ (дата звернення: 19.11.2020).

2. Об анонимности в интернете, жизни и её относительности // Хабр : сайт. 10.08.2019. URL: https://habr.com/ru/post/463189/ (дата звернення: 19.11.2020).

3. Галушка Д. Как стать невидимкой в Интернете: программы и сервисы для обеспечения анонимности в Сети // ITC.ua : сайт. 21.05.2014. URL: https://itc.ua/articles/kak-stat-nevidimkoy-v-internete-programmyi-i-servisyi-dlya-obespecheniya-anonimnosti-v-seti/ (дата звернення: 19.11.2020).

Одержано 20.11.2020

УДК [351.74(100):004.9](075.8)

Бортник Сергій Миколайович
доктор юридичних наук, доцент,
проректор Харківського національного університету внутрішніх справ
http://orcid.org/0000-0002-5281-6007

ПЕРСПЕКТИВИ РОЗВИТКУ АНАЛІТИЧНИХ СИСТЕМ ПРЕДИКАТИВНОЇ АНАЛІТИКИ

В останні 5–7 років у зв'язку з поступовим переходом правоохоронних органів розвинутих країн від парадигми реактивної діяльності до парадигми предикативної діяльності значно посилилася роль аналітичних систем предикативної аналітики, які зараз активно застосовуються у стратегічному і тактичному кримінальному аналізі. Передумовою цих процесів стало різке збільшення широкомасштабних терористичних актів, з одного боку, і доступність потужних технологічних інструментів для невеликих злочинних угруповань, з другого боку. Одним з основних компонентів таких систем є модуль пошуку інформації у відкритих джерелах (OSINT).

Однак темпи росту можливостей засобів сучасних інформаційних технологій в умовах розгортання четвертої промислової революції настільки стрімкі, що, за даними експертів, у найближчі декілька років ситуація докорінно зміниться.

Так, згідно з дослідженнями фахівців Массачусетського технологічного інституту за програмою DARPA «Мережеве суспільство 20-х рр.» у 2022 році структура Великих Даних суттєво зміниться і буде мати такий вигляд:

– більше 30 % інформації припадатиме на телеметрію інтернету всього (це не всі сигнали інтернету всього, а лише ті, що надходять в телеметричному або числовому вигляді. У 2022 р. число IP-адрес речей буде приблизно в 7–10 разів перевищувати число IP-адрес інтернет-ресурсів і персональних комп'ютерних пристроїв);

– не менше 35 % інформації припадатиме на дані, які генеруються виробничими, соціальними та управлінськими інфраструктурами і об'єктами;

– не менше 25 % складуть інтернет транзакцій, які вийдуть за межі інтернету грошей і охоплять транзакції, пов'язані з переуступкою прав власності, відстеженням руху цінностей і т. п.;

– разом на звичний нам текстовий та відео інтернет припадатиме в найбільш оптимістичному варіанті не більше 10 % загального обсягу інформаційних потоків. При цьому приблизно 4/5 припадатиме на відеопотоки.

Відповідно, нинішній традиційний інтернет, включаючи загальнодоступний інтернет, соціальні мережі і платформи, однорангові комунікаційні мережі, складе всього 2 % від загального інформаційного потоку.

Таким чином, ефективність працюючих потужних аналітичних систем, таких як Palantir, ePOOLICE та ін. суттєво зменшиться внаслідок зменшення кількості доступних джерел інформації.

За таких умов зростатиме роль баз даних правоохоронних органів, якість і повнота даних, які в них заносяться, ефективність інструментів пошуку й аналізу, архітектура сховищ, яка визначатиме ефективність їх функціонування. Крім того, зросте роль інтеграції інформаційних ресурсів. І в цій сфері у

Національній поліції України є певні позитивні напрацювання, навіть у порівнянні з деякими країнами Європейського Союзу. Зокрема, це перехід системи «Інформаційний портал НПУ» на дворівневу організаційну структуру з більшим акцентом на централізацію інформаційних ресурсів, а також упровадження єдиної інформаційної системи МВС України. Впровадження ЄІС дасть можливість реалізувати системну інтеграцію як основний інструмент формування приватно-державного партнерства у напрямі створення сервіс-орієнтованого інформаційного середовища.

Повноцінна реалізація цих проєктів і процесів потребує суттєвої переробки нормативної бази їх функціонування в нових умовах, координації та узгодженості з нормативною базою інших зацікавлених відомств і державних структур.

Список використаних джерел

1. Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України» : наказ МВС України від 03.08.2017 № 676 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/z1059-17 (дата звернення: 20.11.2020)..

2. Концепція програми інформатизації системи Міністерства внутрішніх справ України на 2018-2020 роки, затверджена Рішенням Колегії МВС України 05 листопада 2018 р. № 18КМ // Єдиний портал органів системи МВС України : сайт. URL: https://mvs.gov.ua/upload/file/koncepc_ya_nformatizac_mvs_12.12.2018.pdf (дата звернення: 20.11.2020).

3. Топ-10 прорывных технологий 2020 года // Национальная Ассоциация нефтегазового сервиса : сайт. 28.02.2020. URL: https://nangs.org/news/it/top-10-proryvnyh-tehnologiy-2020-goda (дата звернення: 20.11.2020).

Одержано 04.12.2020

УДК [351.74(100):004.9](075.8)
Бурдін Михайло Юрійович
доктор юридичних наук, професор,
проректор Харківського національного університету внутрішніх справ
http://orcid.org/0000-0002-6748-3321

РОЗПІЗНАВАННЯ ОСІБ ЗЛОЧИНЦІВ І ТЕРОРИСТІВ НА БАЗІ НЕЙРОННИХ МЕРЕЖ

Чому технології розпізнавання осіб будуть все більш затребувані в системах безпеки? Навіщо пам'ятати постійно зростаючу кількість паролів для різних сервісів і придумувати все більш складні способи ідентифікації себе в Інтернеті, коли у кожної людини з народження є унікальний ідентифікатор – його обличчя?

У 2014 р. ФБР США оголосило про успішний запуск в експлуатацію системи розпізнавання нового покоління (NGI). Її метою є розширення можливостей відомства з ідентифікації громадян, і вона повинна замінити стару, яка базується виключно на відбитках пальців. Із 2011 р. система працювала в експериментальному режимі.

Основною особливістю NGI є те, що вона отримує та обробляє біометричні дані автоматично. Система працює за рахунок інформації, одержуваної з камер відеоспостереження по всій країні. Вона виявляє унікальні риси обличчя тієї чи іншої людини і зберігає їх у базі даних. Потім під час розслідування злочину вона зможе провести швидкий аналіз знімків і виявити зловмисників. Для ідентифікації людини досить виявити, наприклад, характерний шрам на його обличчі або татуювання на тілі.

Таким чином побудова сучасної системи розпізнавання осіб є досить актуальним науковим завданням. **Метою цієї доповіді є** дослідження найбільш перспективних методів і засобів розпізнавання осіб з використанням технологій нейронних мереж.

Учені Інституту Макса Планка в Саарбрюккені в Німеччині демонструють спосіб ідентифікації людини за кількома фотографіями, навіть якщо на більшості з них її обличчя закрите. Розроблена дослідниками система, яку вони

називають «Безлика система розпізнавання», тренує нейронну мережу за допомогою множини фотографій, які містять як закриті від спостереження, так і добре видимі обличчя, а потім використовує ці знання, щоб ідентифікувати людину із закритим обличчям, шукаючи подібності в ділянці голови і на інших ділянках тіла. Точність системи змінюється залежно від того, скільки фотографій є в наборі з добре видимим зображенням обличчя. Навіть тоді, коли є тільки 1,25 копій зображень повністю видимого обличчя людини, система здатна ідентифікувати приховані від огляду обличчя з точністю 69,6 %; якщо є 10 копій зображень добре видимого обличчя, точність збільшується до 91,5 %.

Французька компанія Orange Labs розробила алгоритм, здатний штучно зістарювати й омолоджувати зображення осіб на фотографіях і встановлювати їх схожість із зображенням на вихідному фото. Це перший алгоритм, який генерує високоякісні зображення осіб у будь-якій заданій віковій групі зі збереженням впізнаваності людини. Для його створення дослідники використовували дві генеративні змагальні нейромережі.

У процесі навчання нейромережі проаналізували, як виглядають особи шести вікових категорій (до 18 років, 19–29, 30–39, 40–49, 50–59 років і старше). Для цього в них завантажили по 5 тис. фотографій людей з кожної вікової категорії. Таким чином нейромережи дізналися про патерни зображень, характерні для певного віку, і змогли застосувати їх для старіння й омолодження зображення.

Нейронна мережа дає набір ознак, за яким можна відрізнити одну людину від іншої (колір і форма очей, міміка та ін.). Але більшість ознак, які видає нейронна мережа, не видимі людському оку. Точність ідентифікації зображення нейронною мережею складає близько 90 %, а людиною – 25% (за обсягу бази, наприклад, 10 тис. фотографій).

Алгоритм NTechLab дає можливість порівнювати пари осіб з 99-процентним ступенем точності і проводити пошук у досить великій базі фотографій менш ніж за 0,3 секунди з точністю понад 70 %. Ця технологія була визнана кращою на світовому чемпіонаті The MegaFace Challenge,

організованому університетом Вашингтона у 2015 р. У цьому чемпіонаті взяли участь понад 100 команд з усього світу, в тому числі і команда Google.

Для пошуку людини в базі обсягом 1 млрд фотографій таким алгоритмом потрібно менше 1 секунди. Подібна швидкість пошуку може вирішити безліч завдань не тільки в масштабах міста, але й країни і навіть світу, наприклад, під час пошуку злочинця в режимі реального часу. До переваг алгоритму крім швидкості пошуку в базах фотографій глобального масштабу, належить дуже висока точність розпізнавання. Це стало можливим завдяки глибинному навчанню і правильно підібраній архітектурі нейронної мережі.

З поширенням автоматизації бізнес-процесів технології 3D-розпізнавання осіб отримують все більш широке впровадження. Рівень якості технологій (точність розпізнавання зараз перевищує 95 %) уже досить високий, а економія часу і ресурсів величезна. Трохи більше 10 років тому фотографії передбачуваних злочинців або банківських шахраїв порівнювали з наявною базою зображень вручну, і після 30-ти фотографій людина починає працювати повільніше і помилятися набагато частіше. Сьогодні всі системи розпізнавання осіб не просто автоматизовані, а використовують штучні нейронні мережі. Це дозволяє їм працювати з колосальним обсягом даних, зменшувати кількість помилок і збільшувати швидкість.

Проведення віддаленої ідентифікації – обов'язкова вимога «антивідмивного» законодавства – зараз передбачає тільки два способи: через підтвердження облікового запису клієнта на порталі держпослуг і наданням особистого набору персональних даних (паспортних даних і т. ін.).

Одержано 19.11.2020

УДК 004:03
Виганяйло Світлана Миколаївна
кандидат економічних наук,
доцент кафедри соціально-економічних дисциплін
Сумської філії Харківського національного університету внутрішніх справ
https://orcid.org/0000-0001-5350-0728

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-ПОШУКОВОЇ СИСТЕМИ «ЛІГА:ЗАКОН»

Для сучасних фахівців юридичного спрямування своєчасне володіння актуальною, достовірною та повною інформацією є надзвичайно важливим елементом їх ефективній діяльності. Сучасна юридична діяльність нерозривно пов’язана з грамотною організацією інформаційних процесів, а також освоєнням і використанням сучасних інформаційних технологій.

Актуальним залишається питання підготовки висококваліфікованих фахівців, здатних використовувати останні розробки в інформаційних технологіях для знаходження вчасної, достовірної, цілісної інформації.

Однією з найбільш популярних комп'ютерних правових систем в Україні є спеціалізована інформаційно-пошукова система «ЛІГА:ЗАКОН», яка забезпечує доступ до законодавчої та нормативної бази та складається з програмної оболонки, що забезпечує пошук документів, та інформаційного ядра - текстових баз даних нормативних документів: «Загальне законодавство», «Кодекси», «Податки в Україні», «Міжнародні угоди» та інші.

На основі ІПС «ЛІГА:ЗАКОН» розроблено тематичні комп'ютерні довідники, які містять у собі стандартний програмний комплекс і спеціалізоване інформаційне ядро - нормативні документи, консультації фахівців, огляд преси та довідкову інформацію з певних питань: «ЛІГА: Консультант БУХГАЛТЕРА», «ЛІГА:Консультант ЗЕД», «ЛІГА:ПРАКТИК-керівник» та ін. Спільні особливості систем такі: зберігання текстів документів у відповідних форматах; розміщення всіх редакцій документів у хронологічній послідовності; систематизація документів за напрямками; доступ до еталонних редакцій нормативних документів; відкритий інтерфейс.

Особливістю даного програмного продукту є:

– постійна підтримка в актуальному стані з урахуванням змін законодавства та судової практики в Україні;

– швидке знаходження нормативних документів, роз'яснення, аналітика, бланки та інструкції;

Одна з останніх версій LIGA 360 має додаткові функції як для юриста так і для бізнесу та бухгалтера:

– оновлення додаткових сервісів: хмарний сервіс (доступ з будь-якого місця із будь-якого пристрою), право України (вільний доступ до інформаційно-правової системи), вебінари (навчання роботі з продуктами);

– електронні видання: «Юрист&Закон», «Вісник МСФЗ» «Бухгалтер&Закон» та інші (електронні аналітичні видання з акцентом на практичні рекомендації та аналітику);

– можливістю використовування додаткових функцій автоматичного моніторингу документа та зміни його статусу, доступна можливість відстеження змін у окремих абзацах нормативно-правових актів та ін.

У зв'язку з необхідністю набуття студентами юридичних спеціальностей навичок володіння інформаційними технологіями даний програмний продукт детально вивчається та практично використовується в навчальному процесі.

Таким чином, в умовах зростаючої комп'ютеризації суспільства, у тому числі і правової галузі, одним із головних завдань освітнього процесу є надання курсантам, студентам, слухачам вузів МВС України таких спеціальних знань, умінь та практичних навичок з інформаційних технологій, які склали б міцний фундамент подальшого засвоєння і ефективного використання ІТ в професійній діяльності фахівців юридичного спрямування.

Список використаних джерел

1. Вишня В. Б., Косиченко О. О., Трусов В. О. Інформаційне забезпечення юридичної діяльності : навчальний посібник для студентів: у 2 ч. Дніпро : ДДУВС, 2006. Ч. 1. 164 с.

Одержано 20.11.2020

УДК 351 741 В 68
Волошин Олексій Гнатович
старший викладач кафедри криміналістичного забезпечення та судових експертиз навчально-наукового інституту № 2
Національної академії внутрішніх справ
https://orcid.org/0000-0002-3976-3887

ЗАХОДИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

В Україні спостерігається інтенсивне впровадження сучасних інформаційних технологій у різні сфери діяльності людини, зокрема у діяльність правоохоронних органів, яку вже важко уявити собі без використання сучасних засобів обчислювальної техніки. Це призводить до якісно нових можливостей несанкціонованого доступу до ресурсів і даних інформаційних систем, розширюються можливості несанкціонованих дій з інформацією і, поряд з цим, можливістю негласного знімання інформації.

З огляду на те, що проблема кіберзлочинності на сучасному етапі розвитку України набуває глобального виміру та становить загрозу інформаційному суспільству, боротьба з нею отримала відображення у нормативно–правових актах національного та міжнародного рівнів. Кібератаки значно почастішали, тому було вирішено посилити механізми захисту державних комп’ютерних систем.

15 березня 2016 року Президент України видав Указ «Про введення в дію рішення Ради національної безпеки та оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». В складі Ради національної безпеки створено робочий орган - Національний координаційний центр кібербезпеки. Поява цього органу цілком обґрунтована, адже поруч з перевагами інформаційних технологій, їх активно використовують для «здійснення терористичних актів, в тому числі шляхом порушення штатних режимів автоматизованих систем управління технологічним процесами на об’єктах інфраструктури [2].

Наказом МВС України № 575 від 07.07.2017 «Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та

підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні» і розділі XV зазначенні особливості організації взаємодії при досудовому розслідуванні кримінальних правопорушень у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку (кіберзлочинів) [3].

В Україні на базі Національного центрального бюро Інтерполу створено Національний центральний консультативний пункт по проблемам комп'ютерної злочинності. Це надало можливості накопичити матеріал про законодавче регулювання та організаційний досвід боротьби з кіберзлочинністю в різних країнах, підготувати ряд аналітичних оглядів та публікацій з цих питань, ознайомити співробітників МВС, прокуратури, суду з цим новим для України видом злочинів, внести конкретні пропозиції по удосконаленню кримінального законодавства України.

У Службі безпеки України функціонує Департамент спеціальних телекомунікаційних систем та захисту інформації. Нормативні акти СБУ потребують вмикання спеціальних ділянок захисту інформації у складі її підрозділів, органів та установ. В ряді оперативних підрозділів СБУ утворено групи, які протидіють окремим видам кіберзлочинів.

В структурі ДСБЕЗ при МВС України в 2001 році були створені підрозділи по боротьбі з правопорушеннями у сфері інтелектуальної власності та високих технологій, одним із завдань котрих є боротьба із злочинами у галузі комп'ютерної інформації, електронних рахунків і телекомунікації.

05 листопада 2015 року була створена нова Кіберполіція, як структурний підрозділ Національної поліції України. Основною метою створення кіберполіції було реформування та розвиток підрозділів МВС України, що забезпечить підготовку та функціонування висококваліфікованих фахівців в підрозділах Експертної служби МВС України, а також спеціалістів органів досудового розслідування Національної поліції України, задіяних у протидії кіберзлочинності, та здатних застосовувати на високому професійному рівні новітні технології в оперативно-службовій діяльності.

До основних завдань Кіберполіції відносять:

1. Реалізація державної політики у сфері протидії кіберзлочинності.

2. Протидія кіберзлочинам.

3. Завчасне інформування населення про появу новітніх кіберзлочинів.

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

5. Реагування на запити закордонних партнерів, що надходитимуть каналами Національної цілодобової мережі контактних пунктів.

6. Участь у підвищенні кваліфікації працівників поліції щодо застосування комп'ютерних технологій у протидії злочинності.

7. Участь у міжнародних операціях та співпраця в режимі реального часу.

8. Забезпечення діяльності мережі контактних пунктів між 90 країнами світу.

В українських реаліях також було створено волонтерський рух «Український кіберальянс». Це хакери, об’єднані спільною національною ідеєю. У цей альянс входять такі команди як «Falcons Fame», «Trinity», «ruh8». І хоча зазвичай хакерів прирівнюють до злочинців, учасники руху вважають, що діють у рамках статті 17 Конституції України: кожна військовозобов'язана людина має забезпечувати інформаційну безпеку України. По суті, це звичайні громадяни, які допомагають Україні в рамках інформаційної війни. Вони жодним чином не асоціюють себе з нинішньою владою. А інформацію передають через приватні канали до СБУ та Міноборони.

Нині кіберзлочинність становить для нашої держави більш серйозну небезпеку, ніж ще 5 років тому. Незважаючи на зусилля правоохоронних органів, спрямованих на боротьбу з кіберзлочинами, їх кількість, на жаль, не зменшується, а, навпаки, постійно збільшується. Проблема профілактики і стимулювання кіберзлочинності в Україні – це комплексна проблема. Сьогодні закони повинні відповідати вимогам, що пред'являються сучасним рівнем розвитку технологій. Пріоритетним напрямком є також організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи,

забезпечення їх необхідною матеріально-технічною базою. Жодна держава сьогодні не в змозі протистояти кіберзлочинності самостійно. Нагальною є необхідність активізації міжнародної співпраці в цій сфері.

Список використаних джерел

1. Кримінальний кодекс України : Закон від 05.04.2001 № 2341 III // Офіційний сайт Верховної Ради України. URL: http://zakon. rada.gov.ua/laws/show/2341-14/page10 (дата звернення: 19.11.2020).

2. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента від 15.03.2016 № 96/2016 // Офіційний сайт Верховної Ради України. URL: http://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 19.11.2020).

3. Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні: Наказ МВС України від 07.07.2017 № 575 // ЛІГА:ЗАКОН: главный правовой портал Украины. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/RE30805.html (дата звернення: 19.11.2020).

4. Дзюндзюк В. Б., Дзюндзюк Б. В. Поява і розвиток кіберзлочинності. *Державне будівництво.* 2013. № 1. 12 с. URL: http://www.kbuapa.kharkov.ua/e-book/db/2013-1/doc/1/01.pdf (дата звернення: 19.11.2020).

5. Скичко О. Як українців грабують в Інтернеті, банкоматах і кафе. Фахівці порадили, як врятувати свої гроші // ТСН.ua : сайт. 03.06.2015. URL: https://tsn.ua/ukrayina/yak-ukrayinciv-grabuyut-v-interneti-eksperti-ta-pravoohoronci-poradili-yak-zberegti-svoyi-groshi-431487.html (дата звернення: 19.11.2020).

6. Кібербезпека як важлива складова всієї системи захисту держави // Міністерство оборони України : офіційний вебсайт. 07.05.2018. URL: http://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html (дата звернення: 19.11.2020).

Одержано 19.11.2020

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

ДЕЯКІ АСПЕКТИ ПЕРЕХОПЛЕННЯ АУДІО ІНФОРМАЦІЇ

В сучасному світі не можливо уявити собі людину, яка б не користувалась мобільним зв'язком. Розглянемо які методи перехоплення підстерігають користувача сучасних мобільних приладів і як можна від них захиститися. Умовно їх можна розділити на кілька груп: перехоплення сигналу між телефоном і базовою станцією, впровадження апаратного або програмного «жучка» для отримання даних прямо з апарату, віддалений злом апарату для отримання контролю над ним. Окремо треба розглянути екзотичні методи перехоплення інформації, які використовують додаткові функції сучасних мобільних пристроїв.

Технічно, телефонний апарат - це звичайний приймач і передавач, абсолютно нічого не заважає приймати сигнали, якими він обмінюється з вишкою і записувати їх. Очевидно, що в цьому мало практичного сенсу, тому що дані зашифровані сучасними крипостійкість протоколами. Теоретично, є можливість поєднати перший і другий спосіб атаки, щоб отримати ключі для розшифровки сигналу з мобільного телефону.

В 2009 році, за допомогою атаки на алгоритм шифрування через райдужні таблиці для криптографічного алгоритму A5/1, який використовується в стільникових мережах стандарту GSM німецьким експертом по криптографії Карстеном Нолом було зроблено перехоплення розмови між двома абонентами. Результати були представлені в його доповіді на Chaos Communication Congress в 2009 році.

У 2013 році він зміг продемонструвати вразливість телефонів, в яких використовувалися CIM-карти застарілого зразка. На цих картах був цифровий підпис, який згенерували слабким алгоритмом і його можна було зламати за допомогою райдужних таблиць. Маючи цифровий підпис CIM-карти можна було відправити на неї сервісне повідомлення, яке змусило б телефон завантажити і виконати шкідливий код. Навіть не дивлячись на те, що Java-додатки виконуються в «пісочниці», вони все одно, як мінімум, можуть посилати СМС повідомлення на платні сервіси. Більш того, у деяких виробників карт - пісочниці були недостатньо захищені і дозволяли отримати доступ до всіх функцій і інформації на CIM-карті.

Звичайно, з появою зв'язку стандарту 4G атаки такого типу стали більш складними. У стандарті LTE були знайдено кілька десятків вразливостей різного роду, але подібні атаки на них надзвичайно складні і доступні тільки вузькому колу фахівців високого класу.

У зв'язку з тим, що LTE просувається як «стільниковий інтернет для IOT-пристроїв», з'явився відносно новий тип загроз - обладнання оператора зв'язку можна атакувати DDoS атакою і отримати над ним частковий контроль. Відповідно, є загроза створення ботнетів на основі «інтернет-речей».

Ще один складний і дорогий, але реально працюючий спосіб отримати повний доступ до всіх стільниковим даними – IMSI-пастки. Це «фальшиві» базові станції, які вбудовуються в трафік даних і стає точкою MITM між смартфоном і стільниковою вишкою. Алгоритм вибору смартфоном базової станції влаштований таким чином, що він намагається підключитися до найпотужнішої і найближчої. Природно, «фальшива сота» налаштовується так, щоб її потужність була вищою, ніж у справжніх станцій. Нічого не підозрюючи смартфони підключається до шпигунського пристрою і після хендшейка «зловмисник» може в реальному часі дивитися і слухати все, що передається: СМС, голосові розмови та інтернет-трафік, нібито він є стільниковим оператором.

Кілька років тому вчені з Массачусетського технологічного інституту продемонстрували, як можна відновити звук найнесподіванішими способами. В одному випадку відновили мелодію від вібрацій кімнатної рослини. А в іншому експерименті знімали на камеру і відновлювали аудіо, яке звучить поряд з пакетом чіпсів. Перетворити звук вдалося за допомогою високошвидкісної камери: по змінах пікселів на зображенні об'єкту, який знімався.

Влітку поточного року в Ізраїлі вчені підслухали мову, що звучить в будинку в реальному часі, по вібраціях лампочки. Спосіб назвали Lamphone. Для цього потрібен телескоп з підключеним до нього фотодиодом. Оптичний приймач перетворить падаюче на нього світло в електричний сигнал. За допомогою алгоритму сигнал переводять в мовну спектограму, з якої витягають мову співрозмовників.

Вчені з Національного Університету Сінгапуру (National University of Singapore) відкрили спосіб вловлювати звуки в приміщенні за допомогою робота-пилососа. При цьому у пилососа, який тестували фахівці, немає вбудованого мікрофона. Принцип підслуховування дещо інший - замість мікрофона використовується лідар.

Лідар складається з двох елементів: лазерний випромінювач і приймач. Лідар заміряє відстань до об'єктів з високою точністю за допомогою лазерного променя. І, як виявилося, за допомогою лазера можна відмінно чути все, що відбувається навколо робота-шпигуна, оскільки він реєструє будь які вібрації оточуючих його предметів.

Таким чином, ми бачимо появу нових, дещо екзотичних методів перехоплення аудіо інформації.

Одержано 22.11.2020

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;
Морозова Лана Юріївна
доцент кафедри природознавчих наук
Харківського національного університету радіоелектроніки
https://orcid.org/0000-0001-5317-1813

ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ В СИСТЕМАХ АДАПТИВНОГО ТЕСТУВАННЯ ЗНАНЬ

В даний час дуже важливою проблемою вищої освіти є створення методів підвищення ефективності навчання в умовах використання дистанційної форми, формування у випускників здатності застосовувати отримані знання, уміння й навички в професійній діяльності. Це, в свою чергу, робить актуальним завдання створення та впровадження технологій і засобів вимірювання рівня ефективності освіти.

Аналіз методів педагогічних вимірювань дозволяє зробити висновок про те, що одним з об'єктивних і ефективних методів контролю якості знань в умовах активного використання дистанційної форми освіти є тестовий метод, заснований на використанні педагогічних тестових матеріалів.

Дослідження показали, що, незважаючи на широке використання комп’ютерних тестів, дуже часто вони мають певні недоліки, серед яких необ'єктивність вагових коефіцієнтів тестових завдань, неоптимальна кількість тестових завдань або одноваріантність тесту, наявність зв'язку та залежностей між послідовними завданнями та ін.

На практиці дуже часто виникає ситуація, коли одна й та сама група студентів без особливих зусиль справляється з усіма тестовими завданнями або, навпаки, не може впоратися із більшістю тестових завдань. Таким чином, існує проблема коректності підбору складності тестових завдань з метою найбільш адекватної оцінки рівня знань студентів. В зв'язку зі збільшенням кількості й

недостатньою якістю тестів, що застосовуються при навчанні у ЗВО, не завжди є можливим якісно визначити рівень навчальних досягнень студента, грунтуючись тільки на тестах, в яких кількість завдань є фіксованою (так звані тести фіксованої довжини). Цей недолік можливо усунути за допомогою застосування такого виду тестування, яке здатне адаптуватися до рівня знань студентів та змінювати складність і кількість завдань в залежності від правильності відповідей на них. Подібні підходи прийнято називати адаптивним тестуванням.

При комп'ютерному адаптивному тестуванні тестові завдання формуються індивідуально для кожного студента, що екзаменується, з урахуванням результатів виконання попередніх завдань. Типи завдань, їх кількість та порядок проходження індивідуальні. Таким чином, адаптивне тестування не тільки дає більш об'єктивну оцінку знанням, умінням і навичкам студентів, але й дозволяє виявляти, які знання є помилковими або неповними, а також дозволяє формувати подальшу траєкторію навчання.

У доповіді розглянуто теоретико-методологічних аспекти використання тестових технологій у навчанні; специфіку функціонування штучних нейронних мереж та можливість їх використання при розробці педагогічних тестів з завданнями змінної складності; питання створення контрольно-вимірювальні матеріалів для адаптивного тестування; методи вдосконалення матеріалів за рахунок використання штучних нейронних мереж; методику застосування результатів, отриманих у ході адаптивного тестування, для визначення шляхів вдосконалення системи навчання.

Одержано 20.11.2020

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
Колмик Олег Олександрович
науковий співробітник
Науково-дослідної лабораторії з проблем розвитку інформаційних технологій
Харківський національний університет внутрішніх справ
https://orcid.org/0000-0003-0401-9588

НАЙПОШИРЕНІШІ ЗАГРОЗИ БЕЗПЕЦІ ВЕБДОДАТКІВ У 2020 РОЦІ

Згідно даних досліджень, які провели експерти компаній, що займаються кібербезпекою, у 2020 році знизилась доля вебдодатків, які містять у собі вразливості високого рівня ризику. Кількість вразливостей, яке у середньому доводиться на один додаток, знизилось у порівнянні з минулим роком майже у півтора рази. Не дивлячись на це, загальний рівень захищеності вебдодатків оцінюється, як низький. Спеціалісти з'ясували, що до 20 % додатків містять у собі вразливості, які надають змогу зловмисникам отримати повний контроль над системою. А отримавши доступ до всієї системи, у тому числі і до серверу, зловмисники мають можливість розміщувати на атакованому сервері власний контент, атакувати його відвідувачів, заражаючи їх комп'ютери, а також використовувати його, як майданчик для кібератак на інші системи.

Серед найпоширеніших загроз веббезпеці у 2020 році можна виділити – межсайтовий скриптінг (XSS), SQL-ін'єкції, розподілену відмову в обслуговувані (DDoS) та інше.

XSS (Cross-Site Scripting – «межсайтовий скриптінг») – дуже розповсюджена вразливість, яку можна виявити на багатьох вебдодатках [1]. Використання XSS-атак дуже популярне, вони займають перше місце серед усіх типів атак на вебсистеми. Суть технології відносно проста - зловмиснику вдається впровадити на сторінку непередбачений розробниками JavaScript-код. Цей код буде виконуватись кожний раз, коли користувачі заходитимуть на сторінку, на яку він був впроваджений. Далі можливо безліч сценаріїв.

Наприклад: зловмисник може отримати дані авторизації користувача та скористатися його акаунтом, непомітно перенаправивши користувача на іншу сторінку-клон. Ця сторінка може мати ідентичний вигляд тієї, на якій користувач розраховував опинитися, тільки належати вона буде зловмиснику. Якщо користувач введе на цій сторінці свої особисті дані, вони опиняться у зловмисника. Власне, майже все, що може JavaScript, стає доступним для киберзлочинця. За його допомогою можна отримати доступ до призначених для користувача файлів cookies, ускладнити користувачу взаємодію з сайтом чи впровадити шкідливий код в операційну систему самого користувача.

Існує два основних різновиди XSS-атак по способу взаємодії. Пасивні – які вимагають від жертви виконати певні дії, для того, щоб викликати обробник подій, котрий і призведе до запуску шкідливий скрипт. Для цього можуть використовуватися деякі елементи фішингу, наприклад: соціальна інженерія – важливий лист від «адміністрації сайту» с проханням перевірити налаштування свого акаунта, перейшовши за посиланням та виконавши деякі дії на сторінці. Як тільки користувач виконає все, що від нього вимагалось у листі, наприклад: клікнути на певному об'єкті на сторінці, запуститься шкідливий код. Якщо же жертва бездіє, код не буде активований. Активні – в цьому випадку зловмиснику на має потреби заманювати жертву за спеціальними посиланнями, тому що код впроваджується в базу даних чи в якийсь файл на сервері. Таким чином, всі відвідувачі сайту автоматично стають жертвами. Від користувача в цьому випадку взагалі не потрібно ніякої активності.

SQL injection - один з найрозповсюджених засобів злому сайтів та програм, працюючих з базами даних, заснований на впровадженні в запит шкідливого SQL-коду. Просто кажучи – це атака на базу даних, яка дозволяє виконати дії, які не планувалися в системі її розробниками [2]. Сам запит може бути будь яким: на читання, запис, модифікацію та видалення будь яких записів, а при певних умовах можна дістатися і до читання/запису локальних файлів чи навіть виконання коду. SQL- ін'єкція може призвести до втрати даних, ушкодженню

чи розголошенню конфіденційної інформації. У деяких випадках ін'єкція може призвести до повного захвату ресурса.

Distributed denial-of-service attack (DDoS attack) – комплекс дій, здатний повністю або частково вивести з ладу цільову систему, наприклад вебсайт чи додаток, зробивши його недоступним для звичайних користувачів [3]. В якості жертви може виступати будь який вебсайт, ігровий сервер чи державний ресурс. Зазвичай, зловмисники генерують велику кількість пакетів чи запитів, які в кінцевому рахунку перевантажують роботу цільової системи. На сьогоднішній день майже неможлива ситуація, коли хакер поодинці організовує DDoS-атаку. Для здійснення атаки зловмисник використовує безліч зламаних або підконтрольних джерел. У більшості випадків зловмисник використовує мережу з комп'ютерів, заражених вірусом. Мережа з таких комп'ютерів називається ботнет. Наслідки DDoS-атак можуть бути найрізноманітнішими, від відключення датацентром сервера до повної втрати репутації ресурсу. DDoS-атаки можна розділити на 3 типи:

1) атаки, спрямовані на переповнення каналу – до цього типу належать DNS ампліфікація, ICMP флуд, UDP флуд і інші атаки з ампліфікацією;

2) атаки, що використовують уразливості стека мережевих протоколів – найбільш популярними атаками цього типу є ACK / PUSH ACK флуд, SYN флуд, TCP null / IP null атака, Пінг смерті (Ping of death);

3) атаки на рівень додатків – до цього типу належать HTTP флуд, атака фрагментованими HTTP пакетами, атака повільними сесіями (SlowLoris).

Ботнет – це мережа комп'ютерів, заражена шкідливим програмним забезпеченням. Кіберзлочинці використовують ботнет-мережі, які складаються з великої кількості комп'ютерів для різних шкідливих дій без відома користувачів, таких як розсилка спаму або DDoS-атаки. Як тільки пристрій заражається, воно передає шкідливу програму на інші пристрої в мережі, тим самим роблячи мережу ще більшими. Десятки або навіть сотні тисяч пристроїв можуть становити одну бот-мережу.

Список використаних джерел

1. Что такое XSS-уязвимость и как тестировщику не пропустить ее // Хабр : сайт. 16.07.2020. URL: https://habr.com/ru/post/511318/ (дата звернення: 16.11.2020).

2. SQL injection для начинающих. Часть 1 // Хабр : сайт. 20.07.2012. URL: https://habr.com/ru/post/148151/ (дата звернення: 16.11.2020).

3. DDoS-атака — что это такое? // DDOS-GUARD : сайт. URL: https://ddos-guard.net/ru/terminology/attacks/ddos-ataka (дата звернення: 16.11.2020).

Одержано 16.11.2020

УДК 343.85 (477)

Єрмак Олексій Вікторович
кандидат юридичних наук, головний науковий співробітник відділу наукової діяльності та міжнародного співробітництва
Академії Державної пенітенціарної служби

ДО ПИТАННЯ ПРО ВИКОНАННЯ УКРАЇНОЮ КОНВЕНЦІЇ ПРО КІБЕРЗЛОЧИННІСТЬ

Законом України «Про внесення змін до деяких законодавчих актів України щодо спрощення досудового розслідування окремих категорій кримінальних правопорушень» № 2617-VIII від 22.11.2018 розділ XVI Кримінального кодексу України було перейменовано на «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» [1].

Кримінальним проступком є передбачене КК України діяння (дія чи бездіяльність), за вчинення якого передбачене основне покарання у виді штрафу в розмірі не більше трьох тисяч неоподатковуваних мінімумів доходів громадян або інше покарання, не пов’язане з позбавленням волі [1]. Законом України «Про внесення змін до деяких законодавчих актів України щодо спрощення досудового розслідування окремих категорій кримінальних правопорушень» № 2617-VIII від 22.11.2018 у назвах розділів II-XX Особливої частини слово «злочини» замінено словами «кримінальні правопорушення» [1]. Як результат – відсутність точності і визначеності юридичної форми: формулювань речень,

словосполучень або окремих термінів нормативно-правового акта. Закон про кримінальну відповідальність містить моделі майбутніх вчинків фізичних і юридичних осіб. Розпливчатість норм КК України може негативно впливати на долі людей, тому визначення в тексті закону повинні суворо відповідати його наповненню, тобто необхідною є діалектична єдність форми і змісту [2, с. 35].

З позицією законодавця про перейменування розділу XVI Особливої частини КК України важко погодитися. Всі кримінальні правопорушення (ст. ст. 361-363-1 КК України), що передбачені цим розділом без виключення є злочинами, тому з огляду на залишення старої назви розділу I «Злочини проти основ національної безпеки України» Особливої частини КК України, назву розділу XVI КК України теж не потрібно було змінювати.

Відповідно до міжнародних правових документів, у тому числі і Конвенції про кіберзлочинність від 23.11.2001, Україна взяла на себе зобов'язання про впровадження заходів реагування на кримінальні правопорушення, що вчиняються керівниками або представниками юридичних осіб в інтересах останніх [3]. Доволі тривалий час положення про кримінально-правові заходи впливу на юридичних осіб, в інтересах яких вчинювалися кримінальні правопорушення в національне законодавство не імплементувалися. Лише Законом України «Про внесення змін до деяких законодавчих актів України стосовно виконання Плану дій щодо лібералізації Європейським Союзом візового режиму для України стосовно відповідальності юридичних осіб» № 314-VII від 23.05.2013 Загальну частину КК України було доповнено розділом XIV-1, яким були передбачені заходи кримінально-правового характеру щодо юридичних осіб [4].

Відповідно до ч. 1 ст. 12 Конвенції про кіберзлочинність від 23.11.2001 кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для забезпечення того, щоб юридична особа могла нести відповідальність за кримінальне правопорушення, встановлене відповідно до цієї Конвенції, яке було вчинене на її користь будь-якою фізичною особою, як індивідуально, так і в якості частини органу такої юридичної особи [3]. Така

фізична особа має займати керівну посаду в рамках юридичної особи, в силу: 1) повноважень представляти цю юридичну особу; 2) повноважень приймати рішення від імені цієї юридичної особи; 3) повноважень здійснювати контроль в рамках цієї юридичної особи.

Заходи кримінально-правового характеру щодо юридичної особи підлягають застосуванню судом лише поряд з однією з форм кримінальної відповідальності щодо особи фізичної, яка вчинила одне з кримінальних правопорушень, передбачених в ст. 96-3 КК України [5, с. 152]. Враховуючи широку обізнаність підростаючого покоління з ІТ-технологіями, один із злочинів, передбачених ст. ст. 361-363-1 КК України може вчинити дитина у віці до 16 років, яка відповідно до ст. 22 КК України не може бути його суб'єктом.

Вважаю такий стан речей незадовільним. Пропоную доповнити до ч. 2 ст. 22 КК України статтями 361-363-1 КК України, а також передбачити застосування заходів кримінально-правового характеру щодо юридичних осіб у разі вчинення її представником (у тому числі дитиною у віці від 14 років) одного із злочинів, передбачених розділом XVI КК України. Такі зміни в КК України відповідатимуть рівню розвитку неповнолітніх, а також безпосередньо стосуються виконання України своїх міжнародних конвенційниїх зобов'язань.

Список використаних джерел

1. Про внесення змін до деяких законодавчих актів України щодо спрощення досудового розслідування окремих категорій кримінальних правопорушень : Закон України від 22 листопада 2018 року № 2617-VIII // БД «Законодавство України» // ВР України. URL: https://zakon.rada.gov.ua/laws/show/2617-19 (дата звернення: 18.11.2020).

2. Ковальський В. С., Козінцев І. П. Правотворчість: теоретичні та логічні засади. Київ : Юрінком Інтер, 2005. 192 с.

3. Конвенція про кіберзлочинність від 23 листопада 2001 року: ратифікована Законом України № 2824-IV від 07 вересня 2005 року // БД «Законодавство України» // ВР України. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 18.11.2020).

4. Про внесення змін до деяких законодавчих актів України стосовно виконання Плану дій щодо лібералізації Європейським Союзом візового режиму для України стосовно відповідальності юридичних осіб : Закон України від 23 травня 2013 року № 314-VII // БД «Законодавство України» // ВР України. URL: https://zakon.rada.gov.ua/laws/show/314-18 (дата звернення: 18.11.2020).

5. Єрмак О. В., Куц В. М. Конфіскація як засіб кримінально-правового реагування: монографія. Чернігів : Видавець Лозовий В. М., 2018. 232 с.

Одержано 19.11.2020

УДК 343.9
Калюга Каріна Вікторівна
кандидат юридичних наук,
заступник завідувача кафедри кримінального права, процесу та криміналістики
Інституту економіки та права Класичного приватного університету

ЩОДО НАЙБІЛЬШ ЗАТРЕБУВАНИХ ІТ-ПРОФЕСІЙ СЬОГОДНІ

У сучасному світі активно розвивається ІТ-індустрія. З кожним роком все більше і більше навчальних закладів опановують освітні програми, пов’язані з цим напрямком. Світ комп’ютерних технологій дуже бистро розвивається, а професія ІТ-шника стає з кожним роком все більш затребуваною та престижною на ринку праці. Тези присвячено аналізу сучасного стану популярності комп’ютерних професій, що можуть слугувати окремим особам (правопорушникам) передумовою та інструментарієм їхніх злочинних намірів. Сучасність диктує нам перехід від фізичних дій людини до робіт, що виконуються за допомогою машин і роботехніки. Такі масштабні зміни безпосередньо зв'язані з технологічними досягненнями сьогодення: комп'ютерними технологіями, що постійно удосконалюються; штучним інтелектом; нанотехнологіями; розвитком віртуальної реальності та генної інженерії тощо. З кожним роком економіка та всі види промисловості все більше залежать від ІТ-сектора. Почнемо дослідження з аналізу сучасних комп’ютерних професій: прогнозування та передбачення можливих наслідків, застосування цих технічних досягнень під кутом зору їх використання окремими особами у власних цілях чи на замовлення.

Front-end розробник і UX / UI-дизайнер. Так, UX / UI-дизайнер проєктує і визначає, як буде виглядати, реагувати та взаємодіяти з користувачем інтерфейс. А Front-end розробник реалізує його на практиці, за допомогою написання коду. Тут можливе, корпоративне шпигунство.

Blockchain-фахівець [1]. Більшою мірою blockchain-фахівця, визначають навички в програмуванні. Наприклад, деякі з них написані на мовах. C / C / C #,

Java, Python. Інші напрямки також швидко розвиваються, що створює потенційні можливі крадіжки з банківських рахунків тощо.

IoT-інженер – їх сфера це Internet Of Things – інтернет речей. Тут створюються потенційні можливості втручання в особисте життя особи чи навіть підміна гаджетів людським ресурсом тощо.

SEO-спеціаліст. З тих пір, як інтернет став ефективним інструментом для заробітку приватних осіб і бізнесу, SEO-оптимізація була і залишається затребуваною. Тут можливі випадки протиправного маніпулювання з платіжними картками тощо.

Спеціаліст з віртуальних систем. Віртуалізація і технології автоматизації безпосередньо пов'язані з глобальною мережею. Це створює потенційну можливість створення злочинних організацій безпосередньо спрямованих на шахрайства з обслуговуванням цих систем.

Спеціаліст з кібербезпеки. Постійно відбуваються різні вірусні атаки і зломи від хакерів. Усе це робить проблему кіберзагроз, як ніколи актуальною і для простих користувачів, і для бізнесу. Фахівці здатні протистояти цим загрозам зараз особливо потрібні практично усім навіть державним структурам.

Розробник мобільних додатків. Тут спостерігаються не поодинокі випадки створення «фірм-замінників», які мімікрують (маскуються) під офіційні бренди.

З огляду на попереднє, наявна беззаперечна потреба в аналітиках у сфері IT. За нашими спостереженнями, тут практично не вирішуваною проблемою є недостатня фінансова забезпеченість державних органів (у тому числі правоохоронних) для утримання відповідних фахівців.

Мережний інженер. Сьогодні світова економіка, уряди, військові та правоохоронні відомства тощо вже не можуть працювати без обчислювальної техніки та відповідних комунікаційних мереж.

Спеціаліст з вільного програмного забезпечення. Можлива небезпека залучання таких осіб полягає в тому, що їх буде складно в подальшому притягнути до відповідальності за вчинення злочинних дій.

Менеджер із забезпечення послугами. За допомогою роботи таких менеджерів із забезпечення послугами і завдяки результатам їхньої діяльності ІТ зможе унебезпечити самостійну діяльність організацій та підприємств.

Адміністратор системи електронного медичного архіву. Це досить нова галузь, яка відповідно може містити певні підводні камені.

Спеціаліст з підбору постачальників. Як будь-яка нова технологія вона породжує нові види злочинної діяльності, так кожен новий тип злочинів вимагає нових заходів захисту і методів роботи правоохоронних органів [2].

Менеджер службових каталогів. Менеджер службових каталогів може відіграти велику роль як керівник організаційних змін при перетворенні просто корисної ІТ-організації в ІТ-компанію, сфокусовану на наданні послуг.

Інженер бізнес-процесів. Спеціаліст в області SEM-маркетингу. SMM-спеціалісти. Менеджер з планування пропускної спроможності ресурсів. Це досить нові види діяльності, які зараз стають особливо популярними [3].

Окреслимо ще три галузі, які потребують певної уваги. Архітектор інтернету промов (коли побутові пристрої, підключені до інтернету; наприклад: холодильники, можуть самі замовляти їжу, чи кросівки з wi-fi). Аналітики Big Data (означає «великі дані»), а сама спеціальність - на стику інформаційних технологій та соціології. Біотехнології та медицина. Відповідно, можливі злочинні підміни чи недобросовісні виробники, зловживання монополій на виробництво тих чи інших продуктів (в тому числі соціальних) тощо. У медичній сфері будуть затребуваними спеціалісти, які створюватимуть штучні органи на 3D-принтерах для заміни пошкоджених. Матимуть попит і розробники кіберпротезів та імплантів, які вживлятимуться в тіло людини і сприйматимуться ним як власні [4]. Що, в свою чергу тягне за собою цілу низку відповідних ймовірних зловживань. Особа комп'ютерного злочинця – це беззаперечно відмінний психолог. У ньому повинні поєднуватися високі показники емоційного та соціального інтелекту, знання тонкощів людської душі, життєвий досвід, хороші комунікативні здібності і глибокі знання в галузі ІТ: крос-функціональність та міждисциплінарність, знання в області

віртуалізації, обчислень, мережевої безпеки та соціальних мереж, IT-професіонали, які здатні застосовувати гнучкі методи роботи тощо.

Список використаних джерел

1. Blockchain – Блокчейн // It enterprise : сайт. URL : https://www.it.ua/knowledge-base/technology-innovation/blockchain (дата звернення: 17.11.2020).

2. Голубєв В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинами : монографія. Запоріжжя : ГУ «ЗІДМУ», 2003. 250 с.

3. Самые востребованные IT-профессии на 2020 год // IT Рейтинг Украины : сайт. 21.01.2020. URL : https://it-rating.in.ua/samyie-vostrebovannyie-it-professii-na-2020-god (дата звернення: 17.11.2020)

4. Юрченко О. Професії майбутнього: ТОП-7 напрямків, що будуть популярними до 2020 року // Освіторія : сайт. 31.07.2018. URL : https://osvitoria.media/experience/profesiyi-majbutnogo-top-7-napryamkiv-yaki-budut-populyarni-do-2020-roku/ (дата звернення: 17.11.2020).

Одержано 24.11.2020

УДК 351.74+343.982.33

Ковтун Вікторія Олександрівна
курсантка 3 курсу факультету № 4
Харківського національного університету внутрішніх справ
http://orcid.org/0000-0003-1263-5970
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

ІНФОРМАЦІЙНА СИСТЕМА ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ

Ефективність розслідування злочинів зумовлена рівнем інформаційного забезпечення цього процесу, можливістю оперативного отримання необхідних відомостей їх оброблення з метою прийняття слідчим оптимальних рішень.

Окремі аспекти інформаційного забезпечення розслідування злочинів висвітлені в роботах В. В. Бірюкова [1], Д. В. Дабіжа [2], С. С. Кудінова [3], Н. В. Павлюк [4] та інших науковців.

До засобів інформаційного забезпечення розслідування слід зарахувати інформаційні системи, під якими прийнято розуміти організаційно впорядковану сукупність масивів інформації про об'єкти та інформаційні технології, у тому числі засоби сучасної комп'ютерної техніки, програмне забезпечення й мережі зв'язку, що забезпечують процеси введення, опрацювання та видачі інформації.

Інформаційне забезпечення відбувається шляхом сукупності єдиної системи класифікації та кодування інформації, уніфікованих систем документації, схем інформаційних потоків, а також методології побудови баз даних; технічне – за допомогою комплексу технічних засобів, призначених для роботи інформаційної системи, а також відповідної документації на ці засоби й технологічні процеси; математичне та програмне забезпечення – завдяки сукупності математичних методів, моделей, алгоритмів і програм для реалізації цілей і завдань інформаційної системи.

Встановлено, що сьогодні особливе місце серед джерел інформації належить облікам та базам даних різних за цільовим призначенням та відомчою належністю інформаційних систем (ІПНП, ІС «ОДК», ІПС «Оріон», ІМІТС «Аркан», ІБнД про ТЗ (НАІС), АДІС «ДАКТО-2000» та «Сонда» тощо). Зокрема, під час опитування працівників правоохоронних органів 62,9 % респондентів підтвердили необхідність звернення до ІІПС за інформацією. При цьому вони наголосили, що найчастіше користуються такими обліками та автоматизованими інформаційними системами, а саме: ІІПС – 84,3 %; АДІС «ДАКТО-2000» та «Сонда» – 34,3 %; ІМІТС «Аркан» – 22,9 %; ІПС «Оріон» – 18,6 %; ІБнД про ТЗ (НАІС) – 17,1 %; ІС «ОДК» – 15,7 %; інші – 11,4 % [2].

Зазначено, що основна проблема сучасного етапу полягає вже не у збиранні й накопиченні даних, а в тому, щоб у найкоротші строки провести якісний аналіз достовірних фактів, виявити корисну інформацію, а також підготувати на її основі рішення, спрямовані на виявлення та розслідування конкретного кримінального правопорушення.

Застосування як основи для побудови інформаційних масивів криміналістичної характеристики злочинів, з використанням відомостей із завершених провадженням справ, дозволить об'єднати (консолідувати) зусилля з підвищення ефективності розкриття і розслідування злочинів криміналістичної характеристики, як елементу криміналістичної методики розслідування злочинів, та інформаційного забезпечення, як одного з основних елементів організації діяльності правоохоронних органів у боротьбі зі злочинністю. Крім того таке формування інформаційних масивів дозволить одночасно застосовувати описовий та статистичний підходи для створення якісних криміналістичних характеристик злочинів і поряд з описовими криміналістичними моделями використовувати в правоохоронній діяльності статистичні моделі злочинів.

Алгоритм формування нових інформаційних систем повинен складатися з наступних етапів:

1) виділення категорії кримінальних справ (злочинів) за якою вона буде формуватися;

2) визначення типових елементів криміналістичної характеристики для злочинів виділеної категорії на підставі чого створення структури інформаційної системи;

3) розробка інформаційних листів (анкет) для наповнення баз даних;

4) підбір та аналіз матеріалів кримінальних справ закінчених провадженням, введення даних в інформаційну систему.

До формування інформаційних масивів побудованих на підставі криміналістичної характеристики злочинів необхідним є залучення трьох суб'єктів роботи з інформацією: слідчих, інформаційно-аналітичних фахівців та працівників експертних підрозділів. Така інтеграція інформаційних можливостей слідчих, інформаційно-аналітичних фахівців та експертно-криміналістичних підрозділів дозволить збирати узагальнену (про сліди вчинення злочину, знаряддя його вчинення, осіб, що причетні до його вчинення, механізм злочинної діяльності та ін.) криміналістичну інформацію як

за певною кримінальною справою так і за сукупністю справ певної категорії. Але вочевидь що така інтеграція потребує розробки відповідних анкет (довідок) для кожного з підрозділів за напрямами діяльності, відомості з яких будуть вноситися до інформаційних масивів.

Наведене дозволяє висловити думку, що формування таких інформаційних систем для інформаційного забезпечення правоохоронної діяльності на підставі криміналістичної характеристики злочинів можуть сприяти ефективності розкриття та розслідування злочинів. Разом з тим слід зазначити, що ефективність інформаційного забезпечення буде залежати від повноти збору, якості обробки, належності зберігання, пошуку та оперативності отримання інформації, а крім того потребує окремого нормативного врегулювання.

Список використаних джерел

1. Бірюков В. В. Інформаційно-довідкове забезпечення розслідування злочинів: проблеми теорії і практики : автореф. дис. … докт. юрид. наук : спец. 12.00.09. Нац. акад. внутр. справ. Київ : НАВС, 2011. 31 с.

2. Дабіжа Д. В. Використання обліків та автоматизованих інформаційних систем при розслідуванні кримінальних правопорушень : автореф. дис. канд. юрид. наук. спец. 12.00.09. Нац. акад. внутр. справ. Київ : НАВС, 2017. 22 с.

3. Кудінов С. С. Інформаційне забезпечення розслідування злочинів: сучасний стан та шляхи вдосконалення. *Вісник Луганського державного університету внутрішніх справ*. 2011. Вип. 1. Луганськ, ЛДУВС, 2011. С. 280–285.

4. Павлюк Н. В. Інформаційні системи як засоби забезпечення розслідування злочинів корупційної спрямованості. *Науковий вісник Херсонського державного університету*. Серія Юридичні науки. 2014. Вип. 6-1. Том 4. С. 88–90.

Одержано 19.11.2020

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

НАПРЯМКИ ВИКОРИСТАННЯ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ У ЗЛОЧИННІЙ ДІЯЛЬНОСТІ

Ще 15 років тому штучні нейронні мережі могли впоратися хіба що з розпізнаванням рукописного тексту. Сьогодні ж вони допомагають безпілотним автомобілям бачити пішоходів на вулиці, розпізнають обличчя розшукуваної особи на фотографіях у соцмережах, показують на фотографії людини, як вона може виглядати в майбутньому через процес старіння (наприклад, виникнення зморшок та зміна пігментації шкіри, поява сивого волосся чи його випадіння), генерують фотографії неіснуючих людей і котів. А потрапивши до рук хуліганів, нейромережі використовуються, щоб «роздягати жінок» на фотографіях та створювати фейкове порно за участі голлівудських актрис [1].

Штучні нейронні мережі являють собою сімейство математичних програмних моделей, побудованих за принципом організації і функціонування біологічних нейронних мереж – мереж нервових клітин живого організму. Поняття штучної нейронної мережі було запропоновано ще у 1943 році У. Маккалоком і У. Піттсом [2]. Вони запропонували модель, що складалася зі штучних нейронів, у якій кожен нейрон характеризувався тим, що знаходиться у «ввімкненому» або «вимкненому» стані, а перехід у «ввімкнений» стан відбувався у відповідь на стимуляцію достатньої кількості сусідніх нейронів [3].

На сьогодні штучні нейронні мережі застосовують для розв’язання великого класу задач з обробки інформації, у тому числі великих об’ємів даних, насамперед для ідентифікації, емуляції, інтелектуального керування,

прогнозування часових рядів довільної природи за умов структурної та параметричної невизначеності.

У 2016 році команда розробників «NtechLab» з Російської Федерації запустила сервіс розпізнавання осіб «FindFace» (https://findface.pro), що дозволяв знаходити в соціальних комп'ютерних мережах сторінки людей по їх фотографіях. В основі проєкту лежала робота нейромережі «FaceN» – її алгоритм здатний за долі секунди ідентифікувати людину по одній фотографії серед тисяч інших. Для цього нейромережа враховує індивідуальні риси обличчя: ті, які сприймає людське око (розріз очей, форма брів, губ і ін.), і ті, які людина самостійно виділити не здатна [4].

Схожі технології взяли за основу творці онлайн-сервісів «FindFace.sex» (https://findface.sex) та «Porn Star By Face» (https://pornstarbyface.com). Дані вебсайти дозволяють за фотографією порноактриси знайти на порносайтах фото та відео, зняті за її участі [5].

У злочинній діяльності штучні нейронні мережі можуть застосовуватися не тільки в порно-індустрії, але й для, наприклад, генерації голосу певної людини, заміни на фото чи відео обличчя людини на обличчя іншої особи, створенні «майстер-ключів» для обходу систем, заснованих на ідентифікації за відбитками пальців тощо.

У 2018 році американські вчені продемонстрували, як штучний інтелект може створювати «майстер-ключі» для обходу систем, заснованих на ідентифікації за відбитками пальців. Згенеровані нейромережею відбитки підходили в кожному п'ятому випадку, хоча ймовірність помилки дактилоскопічних сканерів не повинна бути вище однієї на тисячу спроб [6]. Дослідження було підготовлено п'ятьма вченими Нью-Йоркського і Мічиганського університетів на чолі з Філіпом Бонтрейджером з Інженерної школи Нью-Йоркського університету [7].

У 2019 році компанія Тимура Бекмамбетова навчила нейромережу говорити голосами відомих людей. Проєкт «Vera Voice» (https://veravoice.ai) аналізує аудіозаписи голосу будь-якої людини, наприклад, артиста чи політика

й озвучує його голосом абиякі тексти. Розробники відзначають, що вже створили інструмент для захисту прав власників голосу та готові відстежувати голосових клонів-шахраїв. Як саме це буде реалізовано, вони не повідомили. Відомо, що зі знаменитостями укладуть договори про партнерство [8].

Ще однією технологією, що може застосовуватися в злочинній діяльності, є технологія «Deepfake». З допомогою штучної нейронної мережі можна створити фотографії або відео за участі обличчя певної людини, яка буде щось робити або говорити, чого вона насправді не робила.

На сервері для зберігання і поширення програмного забезпечення «Github» була викладена готова програма для Windows «Deepfacelab» (https://github.com/iperov/DeepFaceLab), розробка якої ведеться з 2018 року та яка дозволяє зробити обличчя людини молодшим, замінити обличчя чи голову особи на відеозаписі, підігнати артикуляції людини на відео під інший текст [9].

Спочатку публічне використання даної технології було ексклюзивним для обмеженого кола осіб, але це швидко стало ще одним способом створення популярних відеороликів для Інтернету. Це були, в основному, нешкідливі відеоролики, подібні до перетворення обличчя актора Білла Хадера на Тома Круза, але останнім часом популярності набувають вірусні фейкові відеоролики «за участі» таких політичних лідерів, як спікера Палати Конгресу США Ненсі Пелосі, Президента Російської Федерації Володимира Путіна. Подібні випадки спричинили численні кампанії за заборону або принаймні підвищення обізнаності про технології дипфейків [10].

Влада США стурбована поширенням deepfake-порно. У липні 2019 року в Конгрес був внесений законопроєкт «DEEPFAKES Accountability Act», що передбачає кримінальну відповідальність за поширення фейкових фотографій і відео, зроблених за допомогою нейронних мереж або комп'ютерних програм і ганьблять ту чи іншу особу.

Американський штат Вірджинія став першим, хто прийняв цей закон. Відтепер будь-якому його жителю загрожує тюремне ув'язнення, якщо він буде викритий у створенні та розповсюдженні deepfake-порно [11].

Висновки. Штучні нейронні мережі щільно увійшли в життя людини та в даний час широко використовуються при вирішенні найрізноманітніших завдань. Не виключенням є і застосування даних мереж у злочинній діяльності.

На сьогодні є потреба в розробці технологій і відповідного програмного забезпечення для перевірки фотографій, аудіо- та відеозаписів щодо виявлення факту їх створення чи обробки за допомогою штучних нейронних мереж. Особливо важливим це є для перевірки справжності наданих до суду доказів щодо причетності визначеної особи до певних дій для уникнення ситуації притягнення до відповідальності невинної особи.

Список використаних джерел

1. Батыров Т. 13 самых смешных и страшных применений нейросетей // GQ Россия : сайт. 22.07.2019. URL: https://www.gq.ru/entertainment/13-samyh-smeshnyh-i-strashnyh-primenenij-nejrosetej (дата звернення: 16.11.2020).

2. История развития искусственного интеллекта // История компьютера : сайт. URL: http://chernykh.net/content/view/261/460/ (дата звернення: 16.11.2020).

3. McCalloch W. S., Pitts W. A logical calculus of the ideas immanent in nervous activity // Bull. Math. Biophys. 1943. v. 5. pp. 115–133.

4. Дружинин А., Бережная Н. Поиск в соцсетях по фото как инструмент маркетинга // Sostav : сайт. 07.04.2016. URL: https://www.sostav.ru/publication/tekhnologii-21764.html (дата звернення: 18.11.2020).

5. Turilin A. Порно будущего: 3 технологии применения нейросетей в индустрии для взрослых // vc.ru : сайт. 28.05.2019. URL: https://vc.ru/future/69442-porno-budushchego-3-tehnologii-primeneniya-neyrosetey-v-industrii-dlya-vzroslyh (дата звернення: 16.11.2020).

6. Рождественская Я. Нейронная сеть может подделать отпечатки пальцев / А преступники — пользоваться этим // Коммерсантъ : сайт. 18.11.2018. URL: https://www.kommersant.ru/doc/3803970 (дата звернення: 16.11.2020).

7. Bontrager P., Roy A., Togelius J., Memon N., Ross A. DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution. Version 4 // Cornell University. 18 Oct 2018. 9 p. URL: https://arxiv.org/pdf/1705.07386.pdf (дата звернення: 16.11.2020).

8. Сизов И. Нейросеть заговорила голосами знаменитостей / Как мошенники могут использовать технологию синтеза речи для распространения фейк-ньюс // Коммерсантъ : сайт. 03.11.2019. URL: https://www.kommersant.ru/doc/4148142 (дата звернення: 16.11.2020).

9. Степанов Д. В Сеть выложили бесплатное ПО для подмены лиц в видео с инструкцией на русском языке // CNews : сайт. 04.09.2019. URL: https://www.cnews.ru/news/top/2019-09-04_v_set_vylozhili_besplatnuyu (дата звернення: 16.11.2020).

10. Hubert D. How Deepfake Technology Actually Works // ScreenRant : сайт. 21 Feb 2020. URL: https://screenrant.com/deepfake-videos-explained-how/ (дата звернення: 16.11.2020).

11. Кузнецов А. За deepfake-порно теперь можно угодить в тюрьму // iGuides : сайт. 02.07.2019. URL: https://www.iguides.ru/main/other/za_depfake_porno_teper_mozhno_ugodit_v_tyurmu/ (дата звернення: 16.11.2020).

Одержано 19.11.2020

УДК 343:9

Кожевніков Олексій Андрійович
заступник завідувача відділу досліджень у сфері інформаційних технологій – завідувач сектору дослідження звуко- та відеозапису Харківського науково-дослідного експертно-криміналістичного центру МВС України
https://orcid.org/0000-0001-8976-0863

ОСОБЛИВОСТІ КОМПЛЕКСНОГО ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ ТА ТЕХНОЛОГІЙ OSINT

На сучасному етапі одним з додаткових джерел для отримання корисної та значущої (для кримінального провадження) інформації можна розглядати технологію отримання даних під назвою Open source intelligence (OSINT) – *розвідка на основі аналізу відкритих джерел інформації*. Динамічний інформаційний розвиток сучасного суспільства створив об’єктивні чинники для виникнення умов, коли все більше інформації, яка необхідна для прийняття рішення, можливо знайти у відкритих джерелах кіберпростору (Internet). Даному виду розвідки приділяється все більше уваги і у відповідних силових структурах України.

Запорукою ефективного пошуку криміналістично значущої інформації в мережі Інтернет – є гармонійне поєднання можливостей традиційних криміналістичних експертиз та сучасних технологій з пошуку інформації у відкритих джерелах (OSINT). Про необхідність залучення спеціаліста в окремих галузях криміналістичних знань, а саме портретної та фототехнічної

експертизи, в процесі моніторингу мережі Інтернет спонукають об'єктивні причини, а саме:

– необхідність оперативного ототожнення особи за елементами зовнішності із застосуванням спеціальних методів портретної експертизи але без процедури оформлення висновку експертного дослідження;

– виявлення фактів монтажу або інших штучних маніпуляцій зі змістом цифрових фотозображень;

– потреба у частковому покращенні якості цифрових фотозображень;

– встановлення змісту державних реєстраційних знаків авто, інших літерно-цифрових позначок на фото або відеозаписах, які через низьку якість не проглядаються у звичайних умовах;

– ототожнення ділянок місцевості за візуальними ознаками;

– ототожнення інших предметів матеріального світу;

– визначення інших характеристик матеріальних об'єктів, що відображені на фото або відеозаписах (наприклад: визначення зросту людини, натуральних розмірів об'єкту, марки та моделі транспортного засобу тощо).

Практично аналогічне обґрунтування надають й інші науковці (В. Ю. Шепітько, В. В. Білоус, А. О. Панасюк, О. В. Одерій) [1; 2; 3], а тому стає актуальним питання щодо форми документування такої діяльності спеціаліста. З цього приводу заслуговує на увагу позиція тих практиків, які пропонують оформлювати результати OSINT-пошуку у вигляді письмової консультації спеціаліста, де останній у вірогідній формі надає орієнтуючу інформацію про невпізнану особу (правопорушника, свідка, потерпілого тощо) та інші відомості, що мають суттєве значення для встановлення її фактичного місцезнаходження (склад сім'ї, місце реєстрації, судові рішення та інше) [4]**.** Так, у листопаді поточного року спеціалістами відділу досліджень у сфері інформаційних технологій Харківського НДЕКЦ МВС саме у форматі письмової консультації спеціаліста й було надано орієнтуючу інформацію до одного із територіальних підрозділів ГУНП в Харківській про ймовірні особисті дані причетних до скоєння майнових злочинів чотирьох

невстановлених осіб, зображення яких містились на фото. Наведена інформація була згодом підтверджена в ході проведення низки портретних експертиз за матеріалами кримінального провадження.

Таким чином, наявні позитивні результати в ідентифікації особи ймовірного злочинця шляхом проведення комплексного процесу пошуку та аналізу OSINT-інформації та використанню спеціальних знань (у галузі портретної та фототехнічної експертизи) – дають підстави вважати даний напрямок перспективним.

Список використаних джерел

1. Шепітько В. Ю., Білоус В. Роль сучасних інформаційних технологій у встановленні особи злочинця. *Теорія та практика судової експертизи і криміналістики* : зб. наук. пр. Харків, 2014. Вип. 14. С. 5-11.

2. Панасюк А. О. Алгоритмізація використання мережі Інтернет при виявленні та розслідуванні злочинів. *Правова держава*. 2019. № 34. С. 95-100.

3. Одерій О. В., Кожевніков О. А. Використання відкритої інтернет-інформації у викритті кримінальних правопорушень // Кримінологічна безпека населених пунктів : матеріали Міжнародної науково-практичної конференції (м. Маріуполь, 31 липня 2020 року). Ред. кол.: В. М. Бесчастний, М. О. Семенишин, С. С. Вітвіцький та інші ; Донецький юридичний інститут МВС України, Головне управління Національно поліції в Донецькій області. Київ : ВД «Дакор», 2020. С. 238-246.

4. Шевцов С. О., Кожевніков О. А. Консультації спеціаліста на стадії досудового розслідування : практ. посібник / М-во внутр. справ України; Експертна служба; Харківський наук.-дослід. експерт.-криміналіст. центр. Харків, 2020. 43 с.

Одержано 20.11.2020

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
Переверзєва Софія Дмитрівна
курсантка 1 курсу факультету № 1
Харківського національного університету внутрішніх справ

ФУНКЦІОНАЛЬНІ ПІДСИСТЕМИ ЄДИНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ МВС УКРАЇНИ

Відповідно до Стратегії розвитку системи Міністерства внутрішніх справ України до 2020 року, яка затверджена 15 листопада 2017 року розпорядженням Кабінету Міністрів України № 1023-р, інформатизація діяльності, а саме підвищення ефективності роботи і взаємодії через максимальне використання інформаційно-комунікаційних технологій у реалізації завдань органами системи МВС України, визначено серед основних підходів з досягнення цілей Стратегії. Одночасно розпорядженням Кабінету Міністрів України від 20 вересня 2017 р. № 649-р «Про схвалення Концепції розвитку електронного урядування в Україні», запровадження єдиної інформаційної системи МВС (положення Кабінету Міністрів України від 14.11.2018 № 1024), а також розвиток сучасних електронних технологій у найбільш актуальних напрямках діяльності органів виконавчої влади, діяльність яких координується Кабінетом Міністрів України через Міністра внутрішніх справ України, визначено серед основних завдань модернізації державного управління за допомогою інформаційно-комунікаційних технологій у сфері охорони прав і свобод людини [1].

Метою програми інформатизації системи Міністерства внутрішніх справ України на 2018-2020 роки є запровадження нової моделі єдиного спільного інтегрованого інформаційного середовища, побудованого на інтероперабельності електронних інформаційних ресурсів, а також повнофункціональна реалізація загальнодержавного сервісу електронної

ідентифікації особи на базі єдиного «наскрізного» ідентифікатора, з одночасним комплексним захистом інформації та дотриманням технологічної незалежності, використання єдиних інтерфейсів та протоколів взаємодії і обміну інформацією у режимі реального часу.

Єдина інформаційна система МВС - багатофункціональна інтегрована автоматизована система, що безпосередньо забезпечує реалізацію функцій її суб'єктів, інформаційну підтримку та супроводження їх діяльності і становить сукупність взаємозв'язаних функціональних підсистем, програмно-інформаційних комплексів, програмно-технічних та технічних засобів телекомунікації, які забезпечують логічне поєднання визначених інформаційних ресурсів, обробку та захист інформації, внутрішню та зовнішню інформаційну взаємодію.

Функціональні підсистеми єдиної інформаційної системи МВС - це сукупність технічних засобів та програмних комплексів, які автоматизують службові процеси суб'єктів єдиної інформаційної системи МВС до рівня стандартів операційних процедур та автоматизованого робочого місця користувача, забезпечують формування, зберігання, спільне використання і верифікацію інформаційних ресурсів єдиної інформаційної системи МВС [2].

Функціональними підсистемами єдиної інформаційної системи МВС є: національна система біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства; інформаційний портал Національної поліції України; Єдиний державний реєстр транспортних засобів; Реєстр адміністративних правопорушень у сфері безпеки дорожнього руху; система фіксації адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху в автоматичному режимі; система екстреної допомоги населенню за єдиним телефонним номером 112; інтегрована міжвідомча інформаційно-телекомунікаційна система щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон; інформаційно-телекомунікаційна система прикордонного контролю «Гарт-1»;

інші системи, реєстри та бази (банки) даних, створені суб'єктами єдиної інформаційної системи МВС в межах реалізації владних повноважень.

Перелік пріоритетних інформаційних ресурсів єдиної інформаційної системи Міністерства внутрішніх справ визначено постановою КМУ від 14 листопада 2018 року № 1024 «Про затвердження Положення про єдину інформаційну систему МВС та переліку її пріоритетних інформаційних ресурсів» [2].

Список використаних джерел

1. Концепція (нова редакція) програми інформатизації системи Міністерства внутрішніх справ України на 2018–2020 роки // Єдиний портал органів системи МВС України : сайт. URL: https://mvs.gov.ua/upload/file/koncepc_ya_nformatizac_mvs_12.12.2018.pdf (дата звернення: 19.11.2020).

2. Про затвердження Положення про Єдину Інформаційну Систему Міністерства внутрішніх справ та переліку її пріоритетних інформаційних ресурсів : постанова КМУ від 14.11.2018 № 1024 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1024-2018-%D0%BF (дата звернення: 19.11.2020).

3. Про схвалення Стратегії розвитку органів системи Міністерства внутрішніх справ на період до 2020 року : розпорядження КМУ від 15.11.2017 № 1023-р // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1023-2017-%D1% (дата звернення: 19.11.2020).

Одержано 20.11.2020

УДК 343.13
Корнейко Олександр Васильович
кандидат технічних наук, професор,
завідувач кафедри інформаційних технологій та кібербезпеки ННІ № 1
Національної академії внутрішніх справ
https://orcid.org/0000-0002-1882-9680
Школьніков Владислав Ігорович
старший викладач кафедри інформаційних технологій та кібербезпеки
ННІ № 1 Національної академії внутрішніх справ, т.в.о. начальника Центру
кримінальної аналітики Національної академії внутрішніх справ
https://orcid.org/0000-0003-2041-9450
Овсянюк Дмитро Іванович
начальник відділу
Департаменту кримінального аналізу Національної поліції України
https://orcid.org/0000-0002-1846-4167

ПРАКТИЧНІ МЕТОДИКИ ЗДІЙСНЕННЯ КРИМІНАЛЬНОГО АНАЛІЗУ (ДОСВІД ЦЕНТРУ КРИМІНАЛЬНОЇ АНАЛІТИКИ НАЦІОНАЛЬНОЇ АКАДЕМІЇ ВНУТРІШНІХ СПРАВ)

Сучасний розвиток технологій кримінального аналізу зумовлює впровадження новітніх методик обробки та аналізу даних з відповідних інформаційних ресурсів.

Відповідно до спільного рішення керівництва Національної академії внутрішніх справ (НАВС) та Департаменту кримінального аналізу (ДКА) Національної поліції (НП) України, на підставі рішення Вченої ради НАВС від 07 липня 2020 року в НАВС було утворено Центр кримінальної аналітики (надалі – Центр) як самостійний структурний підрозділ академії.

Одним із головних напрямків діяльності Центру є надання допомоги підрозділам НАВС, ДКА, інших підрозділів НП та правоохоронних органів України щодо впровадження в їх практичну діяльність відповідних методик та програмних засобів, що розроблені Центром для здійснення кримінального аналізу, інформаційно-пошукової та аналітичної роботи.

Центром спільно з працівниками ДКА, кафедрою оперативно-розшукової діяльності та кафедрою інформаційних технологій та кібербезпеки НАВС

підготовлено ряд практичних посібників, що детально розкривають специфічні методики проведення кримінального аналізу, а саме:

– «Кластерний аналіз інформації про телефонний трафік»;

– «Обробка та аналіз за допомогою MS Excel та IBM i2 Analyst's Notebook інформації щодо одночасного перетину кордону декількома особами»;

– «Обробка та аналіз інформації з Державного реєстру нерухомого майна Міністерства юстиції України»;

– «Обробка та аналіз інформації з інформаційно-аналітичного комплексу «Безпечне місто».

Окрім цього, Центром розроблюються методики встановлення та візуалізації спільних маршрутів перетину осіб, транспортних засобів на основі телефонного трафіку, даних з інформаційно-аналітичного комплексу «Безпечне місто» тощо. Це стало можливим внаслідок апробації геоінформаційного комплексу ArcGIS в освітню та наукову діяльність НАВС, який є найбільш потужним програмним продуктом для здійснення аналізу інформації з використання можливостей геовізуалізації.

Більш детальна інформація про впровадження геоінформаційного комплексу ArcGIS в діяльність НАВС висвітлено на XXIII щорічній конференції «ESRI Ukraine. User Conference» за посиланнями:

1. https://youtu.be/PP87OEtI_Ro?t=6500

2. https://youtu.be/PP87OEtI_Ro?t=7981

Іншим актуальним напрямком діяльності Центру є напрацювання відповідних методик обробки та аналізу інформації з відкритих джерел, у тому числі мережі Інтернет. Крім того, на сьогодні працівниками Центру розроблено алгоритми завантаження інформації про біткоїн транзакції з використанням технології API-інтерфейсу з метою подальшого аналізу цієї інформації в програмному продукті IBM i2 Analyst's Notebook.

Стрімкий розвиток сучасних інформаційно-аналітичних технологій зумовлює переосмислення змісту поліцейської діяльності, розвиток відповідних методик задля ефективного попередження, розслідування, розкриття та прогнозування кримінальних правопорушень. Тому здійснення освітньої та наукової діяльності закладів вищої освіти системи МВС України у сфері кримінального аналізу є одним із напрямів підготовки нової генерації сучасних українських поліцейських.

Одержано 22.11.2020

УДК 351.74+343.982.33
Кулак Олександра Іванівна
курсантка 1 курсу факультету № 1
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

ТЕХНОЛОГІЧНІ ЗАСАДИ ОРГАНІЗАЦІЇ МЕТАПОШУКОВИХ СИСТЕМ ДОСТУПУ ДО ДОКУМЕНТАЛЬНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

На сьогоднішній день підтримка інформаційно-аналітичної діяльності правоохоронних органів шляхом застосування методів і засобів моніторингу, адаптивного агрегування та узагальнення потоків інформації з глобальної комп'ютерної мережі є актуальною науково-практичною проблемою.

Існуючі засоби доступу до документальних інформаційних ресурсів можна умовно розділити на кілька груп: каталоги; інформаційно-пошукові системи; метапошукові системи; системи моніторингу та контент-аналізу; екстрактори об'єктів, подій і фактів; системи управління знаннями (DataMining, TextMining); спеціалізовані системи конкурентної розвідки.

Метою цього дослідження є визначення технологічних засад організації метапошукових систем доступу до документальних інформаційних ресурсів для підтримки інформаційно-аналітичної діяльності правоохоронних органів.

Традиційні глобальні пошукові системи в Інтернеті, наприклад Google, Yahoo, AltaVista, Bing, Яndex, Rambler, охоплюють мільярди вебдокументів, але не в змозі проіндексувати весь вебпростір і забезпечити можливість пошуку всіх вебсторінок. Відомо, що вони страждають від ряду обмежень. Зокрема, обумовленнями топологією мережі, обмеженнями на глибину обходу окремих вебсайтів, часом, необхідним для індексування тієї чи іншої частини вебпростору. Зростання пошукових систем призводить до того, що велика частка інформації, яка охоплюється ними, застаріває. Відритим залишається питання про масштабність сучасних технологій пошуку на всьому вебпросторі [1].

Як доповнення, до глобальних пошукових сервісів в даний час розглядаються метапошукові системи - пошукові інструменти, які посилають запити користувачів одночасно на кілька пошукових серверів і, іноді, в так званий, глибинний веб. Зібравши результати, вона видаляє дублюючі посилання і, відповідно до свого алгоритму, об'єднує / ранжує результати для надання їх в загальному списку. На відміну від інших систем, метапошукові не мають власних баз даних, де міститься індексований контент вебпростору [2].

Отже, метапошук - це процес, який підтримує уніфікований доступ до кількох пошукових систем. При цьому метапошукові системи можуть не мати власного індексу вебсторінок. Коли метапошукова система отримує призначений для користувача запит, вона спочатку передає його відповідним

пошуковим системам, сервіс яких вона експлуатує, а потім збирає (реорганізує, узагальнює) результати використаних пошукових систем.

Явною перевагою такої системи є можливість підтримки індексних даних в актуальному стані, так як кожна локальна пошукова система охоплює власний фрагмент вебпростору. Крім того, для роботи метапошукових систем потрібні набагато менші інвестиції в апаратні засоби в порівнянні з традиційними пошуковими системами типу Google, в інфраструктурі яких сьогодні використовуються тисячі серверів [3].

Для вибору підключеної пошукової системи використовується засноване на певних принципах ранжування баз даних для конкретного заданого запиту, скажімо, використовується сума коефіцієнтів подібності документів, яка перевищує певний поріг або сума зважених частот документів, які відповідають умовам запиту.

Всі ці методи ранжирування бази даних систем призначені для отримання ефективних результатів пошуку на основі деяких критеріїв оптимальності. Використана функція для ранжирування бази даних базується на схожості запиту і аналогічного документа в базі даних підключеної пошукової системи.

Для злиття результатів пошуку в більшості існуючих підходів використовуються зважені розподіли отриманих документів шляхом уявлення релевантних запитів з баз даних пошукових систем з найвищими рангами або відкориговані локальні індекси подібності документів.

Існує кілька серйозних проблем в реалізації ефективних метапошукових систем, серед яких можна назвати проблему, як-от, вибір пошукових систем, що підключаються за запитом користувача, тобто пошукових систем, які можуть містити релевантні запиту користувача документи. Наступна проблема пов'язана з об'єднанням (злиттям) результатів пошуку, ранжируванням цих результатів, забезпеченням того, щоб більш корисні для користувача документи йшли попереду інших. Ефективний метапошуковий механізм повинен забезпечувати ілюзію того, що документи знаходяться в одній базі даних; забезпечувати мінімізацію часу пошуку.

Таким чином, для підтримки інформаційно-аналітичної діяльності правоохоронних органів, необхідно знати технологічні засади організації метапошукових систем доступу до документальних інформаційних ресурсів, щоб реалізувати обґрунтовані технології, що охоплюють всі ланцюжки роботи з інформацією, включаючи моніторинг, агрегування та узагальнення потоків інформації.

Список використаних джерел

1. Додонов А. Г., Ландэ Д. В., Путятин В. Г. Компьютерные сети и аналитические исследования : монография. Киев : ИПРИ НАН Украины, 2014. 486 с.

2. Гришанова І. Ю. Аналітичний огляд методів і засобів інформаційного пошуку в Semantic Web. *Проблеми програмування*. 2016. № 1. С. 51-72.

3. Косиченко О. О. Правові інформаційні ресурси Інтернет : довідник. Дніпро : ДДУВС, 2017. 92 с.

Одержано 12.11.2020

УДК 004.056:55(043.2)

Маляренко Дмитро Сергійович
курсант 1 курсу факультету № 4
Харківського національного університету внутрішніх справ
Гнусов Юрій Валерійович
кандидат технічних наук, доцент,
завідувач кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-9017-9635

ШАХРАЙСЬКІ СХЕМИ, ЯКІ НАЙБІЛЬШ АКТИВНІ В НАШЕ СЬОГОДЕННЯ

Незважаючи на кризу, стрімко розвивається кредитно-фінансова сфера. Однак вона не завжди приносить користь для громадян, а й часто потурає аферистам, адже інновації в злочинному світі впроваджуються швидко.

Чорні брокери. Варто тільки засвітити номер мобільного телефону в інтернеті, наприклад на дошці оголошень, з великою ймовірністю він може потрапити в базу шахраїв, які почнуть регулярно дзвонити, з пропозицією поторгувати, на деякій біржі; або застосовують бота, який буде робити

прогнози та показувати куди ставити. Головним завданням «брокера», буде заставити скачати деяке програмне забезпечення, в який потрібно буде вкладати гроші й торгувати, де й відбудуться осідання. До речі, можуть запропонувати зайти в фішинговий сайт, де результат такий самий – втрата грошей. Позбутися цих дзвінків можна лише змінною SIM-картки.

Бінарні опціони. Користуючись соціальними мережами, ми бачимо успішних людей, деякі з них є несправжніми «трейдерами», які готові поділитися торговими сигналами до закритих або відкритих груп, по реферальному посиланню. Зареєструючись і після внесення депозиту, люди починають торгувати по його вказівкам на бінарних опціонах. «Трейдери» заробляють відсотки або за рахунок внесеного депозиту, але, зазвичай, за рахунок поразки жертви. Реклама опціонів може бути де завгодно. Шахраї в онлайн-оголошеннях придумують нові, різні види обману, для привласнення чужих коштів. На дошці оголошень, де розміщуються оголошення про товари, вакансії і резюме, обманюють, як покупців, так і продавців. Шахрай правдоподібно оформлює оголошення з уціненим товаром. Коли на цей товар знаходиться покупець, виникає угода, торгівля. Багато які інтернет - сервіси блокують на своїх сайтах чужі посилання, тому шахрай може попросити перенести спілкування в інші соціальні мережі, мовляв, що там більш зручніше. Вводячи в оману, повідсилає відредаговані, взяті з інших мереж фото чужого товару. Коли покупець повірить, шахрай відсилає посилання на фішинговий сайт, який зовні виконаний по одній стилістиці як справжнє онлайн-оголошення, але відрізняється лише посилання. Обдурений покупець вводить данні своєї банківської карти, номера телефону й відправляє ці данні шахраю, якому буде не складно зняти гроші з карти. Щоб не бути обманутим треба бути уважним, обов’язково читати на сайті інформацію спеціальних розділів, які допомагають впізнати шахраїв.

SCAM сайти. Це сайти де, начебто, розігруються грошові кошти: за компенсацію, проходження незначного опитування, тощо. Щоб нібито отримати ці кошти треба оплатити внески, яких буде незчисленна кількість, де і

втратить свої гроші користувач. Скільки б не було проведено транзитних операцій, дані кошти вивести неможливо. Щоб не піймались на даний проєкт, треба бути скептично налаштованим. На справжніх проєктах з виплати коштів, не треба вносити свої гроші, тому що на всі грошові операції використовуються посередні кошти з виплат.

HYIP проєкти (фінансові піраміди). Усі хочуть бути успішними та багатими, найбагатші люди планети рекомендують пасивний заробіток, тобто інвестиція. Існує думка, що кожна людина вчиться на своїх помилках, таким чином, отримуючи безцінний досвід. Але якщо в реальному житті необхідний опит, можна отримати пару раз наступивши на одні і ті, самі граблі, то у інвесторів одна помилка може призвести до втрати всього капіталу. Фінансові піраміди відрізняються від реальних проєктів тим, що у них нема реальної діяльності проєкта. За статистикою, більшість хайпів закривається протягом 6 місяців з моменту свого старту. Не можна при реєстрації використовувати той же e-mail, який ви використовуєте і для платіжних систем. Це може загрожувати тим, що якщо вашу пошту зламають – то паролі від платіжних систем і електронних гаманців зможуть без зусиль відновити і вивести гроші. І саме обов'язкова умова безпеки – для кожного нового проєкту використовуйте різні паролі. Ні в якому разі не застосовуйте один і той же пароль, це може спричинити проблеми. Злом будь-якого вашого облікового запису може дозволити шахраям отримати легкий доступ до акаунтів в інших проєктах, а згодом і крадіжку коштів.

Вішинг. Зазвичай телефонні шахраї знаходять номера постраждалих на якомусь форумі або дошці оголошень. Схема надзвичайно проста: шахраї телефонують із незнайомого номера і під різними приводами намагаються: вивідати дані платіжної карти , змусити зняти ліміти на операції по платіжній картці, відключити перевірку коду безпеки картки CVV2 або перерахувати кошти на картку шахраїв. Слід пам’ятати, що ніколи, нікому і ні за яких обставин не можна повідомляти термін дії платіжної картки і тризначний код

безпеки CVV2, а також код підтвердження операції з банківського SMS-повідомлення.

Висновки. Багато людей на жаль, думають що в інтернеті заробити гроші без вкладень можна легко і просто, але при пошуку способів заробити грошей, часто потрапляють на шахраїв або шахрайський проєкт, а способів того, як розвести і вкрасти гроші, дуже багато, чорних схем заробітку, сірі і білі схеми є, але чорних більше. Заробити гроші в інтернеті можна, без вкладень, просто треба знати де.

Одержано 20.11.2020

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

ОКРЕМІ АСПЕКТИ УНОРМУВАННЯ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ПРАВООХОРОННИМИ ОРГАНАМИ ПІД ЧАС ПРОТИДІЇ ЗЛОЧИННОСТІ

У Верховній Раді України постійно проводиться робота, щодо унормування використання технологій правоохоронними органами.

На теперішній час в комітеті Верховної Ради України з питань правоохоронної діяльності напрацьовано пропозиції до Кримінального, Кримінального процесуального кодексів України, Кодексу України про адміністративні правопорушення та Законів України «Про оперативно-розшукову діяльність», «Про телекомунікації», у вигляді законопроєкту «Про внесення змін до деяких законодавчих актів щодо імплементації положень Конвенції про кіберзлочинність та підвищення ефективності боротьби з кіберзлочинністю». У разі прийняття цього законопроєкту, фіксацію електронних доказів можна буде здійснювати за більш логічно обумовленою

процедурою, зокрема шляхом здійснення зняття інформації з електронних інформаційних систем, яке не пов'язане з подоланням системи логічного захисту. Ця процедура на теперішній час належить до категорії негласних слідчих (розшукових) дій, в законопроєкті пропонується перевести її в розряд слідчих (розшукових) дій.

Але наразі невідомо, коли цей законопроєкт приймуть, і чи взагалі це відбудеться. Крім того, при розробці вказаного законопроєкту не знайшла підтримки ідея запровадження до Кримінального процесуального кодексу такої категорії як електронні докази.

Ще один законопроєкт «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів» № 4004 було подано до Верховної Ради України 01.09.2020 [1]. У ньому передбачається запровадження інституту електронних доказів – інформації в електронній (цифровій) формі з відомостями, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження.

Згідно зі ст. 100-1 згаданого законопроєкту до електронних доказів можуть належати:

1) електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо);

2) віртуальні активи;

3) вебсайти, вебсторінки;

4) текстові, мультимедійні та голосові повідомлення;

5) метадані;

6) бази даних;

7) інша інформація в електронній (цифровій) формі.

В законопроєкті передбачається врегулювати питання:

– зберігання електронних доказів та вирішення питання про спеціальну конфіскацію;

– тимчасового доступу до інформації в електронній (цифровій) формі;

– накладання арешту на віртуальні активи;

– особливості огляду електронних доказів, а також поводження з ними під час обшуку, отримання зразків для проведення експертизи;

– установлення місцезнаходження радіоелектронного засобу за письмовою заявою власника такого засобу;

– дослідження електронних доказів.

Крім наведеного, 01.09.2020 низкою народних депутатів до Верховної Ради України було також подано законопроєкт «Проект Закону про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам» № 4003 [2], яким передбачається:

– запровадження заходу забезпечення кримінального провадження у вигляді термінового збереження інформації;

– унормування подолання системи логічного захисту електронних інформаційних систем;

– зобов’язати операторів телекомунікацій зберігати інформацію в електронній (цифровій) формі із забезпеченням її цілісності, щодо наданих користувачу послуг, у тому числі даних про рух інформації (трафіку) у такому обсязі, який достатній для ідентифікації абонента, а також достатньому для визначення джерела походження інформації (трафіку) та маршруту її передачі впродовж 12 місяців.

У разі прийняття описаних законопроєктів або хоча б їх частини вдасться нарешті заповнити прогалини, які на теперішній час існують в кримінальному процесуальному законодавстві стосовно використання електронних доказів.

Список використаних джерел

1. Проект Закону про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів // Верховна рада України : офіційний вебпортал. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771 (дата звернення: 07.10.2020).

2. Проект Закону про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам // Верховна рада України : офіційний вебпортал. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=69770 (дата звернення: 07.10.2020).

Одержано 17.11.2020

УДК 343.72:004.773+343.97
Марков В'ячеслав Валерійович
кандидат юридичних наук, старший науковий співробітник,
декан факультету № 4 Харківського національного університету внутрішніх справ
https://orcid.org/0000-0003-2024-657X
Рвачов Олексій Михайлович
старший викладач кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-3500-9393
Гельдт Станіслав Володимирович
курсант 1 курсу факультету № 4
Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ ЧАТ-БОТІВ ДЛЯ ЗАЛУЧЕННЯ НАСЕЛЕННЯ ДО ПРОТИДІЇ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ, ЩО ВЧИНЯЮТЬ ЗЛОВМИСНИКИ З ВИКОРИСТАННЯМ ЗАСОБІВ ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ ТА ЕЛЕКТРОННИХ КОМУНІКАЦІЙ

В останні роки спостерігається стала тенденція щодо збільшення серед населення як світу, так і України, користувачів інтернету.

Так в жовтні 2020 року організації «We Are Social» та «Hootsuite» опублікували звіт «Digital 2020» в якому зазначено, що більше 4,66 мільярдів людей з 7,81 мільярдів населення світу користуються інтернетом, а аудиторія соціальних мереж перевалила за відмітку в 4,14 мільярда [1].

За даними дослідження щодо проникнення інтернету в Україні, що було проведено у III кварталі 2020 року дослідницьким холдингом «Factum Group Ukraine» на замовлення «Інтернет Асоціація України» 71 % населення України є регулярними користувачами інтернету [2].

Українські користувачі інтернету не тільки використовують його для спілкування, отримання корисної інформації, навчання та роботи, а серед іншого також за допомогою інтернету користуються дистанційними банківськими послугами.

Національний банк України підрахував, що за перше півріччя 2020 року українці здійснили 2 306,6 мільйонів безготівкових операцій з використанням

платіжних карток на загальну суму 982,8 мільярда гривень, у тому числі 296,2 млн. операцій з переказу коштів з «картки» на «картку» на суму 415,5 мільярдів грн., 501,8 млн. операцій з оплати товарів/послуг у мережі Інтернет на суму 226,2 мільярдів грн., 396,6 млн. операцій з переказу коштів з «картки» на банківський рахунок у мережі Інтернет (погашення кредитів, поповнення депозитів тощо) на суму 65,9 мільярдів грн [3].

Такі обсяги коштів, які зберігають та пересилають українці в безготівковій формі, привертають увагу не тільки комерсантів, які все більше пропонують своїм клієнтам сплатити кошти за товари та послуги онлайн, але й представників кримінального світу.

За підрахунками Української міжбанківської асоціації членів платіжних систем ЕМА, сумарний дохід інтернет-шахраїв за перше півріччя склав 116,5 млн грн. 93 % від цієї суми вони отримали, застосовуючи методи соціальної інженерії [4].

До основних способів незаконного заволодіння коштами користувачів інтернету, що вчиняють зловмисники з використанням сучасних електронних комунікацій, можна віднести наступні:

1) направлені на користувачів терміналів мобільного (рухомого) зв’язку (мобільних телефонів, смартфонів та інтернет-плашетів):

а) розсилка фейкових повідомлень через SMS-повідомлення;

б) фейкові телефонні дзвінки від начебто:

– банківських працівників;

– операторів мобільного зв’язку;

– правоохоронців;

– податківців;

– лікарів;

– соціальних працівників;

– працівників державних установ;

– тощо;

2) направлені на користувачів інтернету незалежно від виду пристрою, яким вони користуються для отримання доступу до мережі Інтернет:

а) розсилка повідомлень через вебсайти та програмні додатки:

– інтернет-мессенджерів;

– соціальних комп'ютерних мереж;

– електронної пошти;

б) використання фейкових вебсайтів [5, с. 151]:

– інтернет-магазинів;

– поповнення рахунків мобільних операторів;

– переказу коштів;

– банківських установ;

– маркетплейсів;

– продажу білетів на транспорті засоби, що здійснюють міжнародні пасажирські перевезення;

– компаній, що надають послуги з доставки товарів;

– компаній, що проводять розіграші товарів та послуг;

– організацій, що проводять онлайн-опитування чи дослідження;

– державних установ, що здійснюють соціальні виплати від держави;

– тощо;

в) розміщення на інтернет-ресурсах (наприклад, в соціальних комп'ютерних мережах, маркетплейсах) шахрайських оголошень про:

– продаж товарів чи послуг;

– збір благодійної допомоги, наприклад, на лікування чи для постраждалих від аварій, пожеж тощо;

г) надсилання користувачам чи розміщення на популярних інтернет-ресурсах програм чи файлів, що мають прихований від користувача шкідливий функціонал.

Для ошукування громадян кібершахраї використовують не тільки методи соціальної інженерії, але й інформаційні приводи про події, які нещодавно відбулися або повинні відбутися найближчим часом, такі як:

– спортивні змагання чи виступи відомих артистів для продажу білетів на ці заходи;

– соціальні виплати від держави для різних верст населення (багатодітним родинам, пенсіонерам, підприємцям, особам похилого віку тощо);

– ювілеї відомих комерційних установ (наприклад, банківських установ, ІТ-компаній тощо);

– взлом популярних вебсайтів (наприклад, соціальних комп'ютерних мереж, поштових серверів, державних реєстрів чи баз даних тощо);

– витік конфіденційних даних у компаній, які мають велику кількість клієнтів (наприклад, банків, кур'єрських компаній тощо);

– появу ефективних методів профілактики та лікування популярних хвороб, продаж за привабливими цінами чи безкоштовну роздачу експрес-тестів чи ліків від цих хвороб (наприклад, гострої респіраторної хвороби COVID-19, спричиненої короновірусом SARS-CoV-2) [6, с. 186].

Однією із причин втрати коштів інтернет-користувачем також може бути кібероніманія – неконтрольовані особою покупки товарів в інтернет-магазинах, без реальної необхідності їх придбання та без урахування власних фінансових можливостей, постійна участь в онлайн-аукціонах [7, с. 130].

На теперішній час українські інтернет-користувачі використовуючи наступні офіційні вебресурси державних установ можуть перевірити наявні в них дані про певну особу (наприклад, продавця чи покупця), телефонного абонента тощо щодо можливість їх причетності к шахрайствам:

1) на вебсайті Української міжбанківської асоціації членів платіжних систем ЕМА у розділі «BlackList EMA» (https://www.ema.com.ua/citizens/blacklist/) перевірити:

– посилання на вебсайти;

2) на вебсайті Департаменту кіберполіції Національної поліції України у розділі «Стоп Фрауд» (https://cyberpolice.gov.ua/stopfraud/) перевірити:

– номери банківських платіжних карток;

– номери мобільних телефонів;

– посилання на вебсайти;

3) на вебсайті МВС України:

– перевірити за серією та номером паспорта чи він не викрадений чи втрачений;

3) на вебсайті Державної міграційної служби України у розділі «Перевірка недійсних документів» (https://nd.dmsu.gov.ua/) перевірити за серією та номером чи є недійсним:

– паспорт громадянина України;

– паспорт громадянина України у формі картки;

– паспорт громадянина України для виїзду закордон;

– тимчасове посвідчення громадянина України;

– інші типи документів, що видають особам у підрозділах міграційної служби;

4) на вебсайті Міністерства юстиції України в Єдиному державному реєстрі юридичних осіб, фізичних осіб-підприємців та громадських формувань (https://usr.minjust.gov.ua/content/free-search) перевірити:

– чи займається підприємницькою діяльністю та якою самою певна фізична чи юридична особа, її юридичину адресу, хто є керівником організації;

– чи існує певна державна чи комунальні організація, установа чи підприємство, їх контактні дані.

В останні декілька років в Україні були виявлені непоодинокі факти, коли зловмисники використовували сучасні засоби електронних комунікацій для:

– незаконного збуту наркотиків у безконтактний спосіб;

– поширення порнографічних фото та відеофайлів, у тому числі дитячої порнографії;

– рекламування електронних ресурсів, що здійснювали продаж незаконних товарів та послуг;

– поширення фейкових новин і повідомлень від імені державних установ, політичних діячів, відомих публічних осіб;

– поширення неправдивої та конфіденційної інформації;

– тощо.

В 2018-2020 роках в Україні почали все частіше з’являтися для популярних інтернет-месенджерів чат-боти, що були розроблені приватними особами, громадськими об’єднаннями, державними, комунальними та комерційними установами чи організаціями. Основне призначення багатьох із цих чат-ботів – це швидка передача користувачем певної невеликої інформації власнику чат-боту, або швидкий пошук та отримання користувачем певної інформації з великих баз даних.

19 вересня 2019 року на засіданні Координаційної ради з протидії наркоманії Харківської міської ради, активними учасниками якого є представники факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ, було презентовано Telegram чат-бот «СтопНаркотик» (https://t.me/StopDrugsBot), який було розроблено курсантами та працівниками факультету № 4 [8, с. 213].

На теперішній час за безпосередньої допомоги користувачів Telegram чат-боту «СтопНаркотик» вдалося заблокувати більше 1800 електронних адрес у месенджері Telegram, що використовували зловмисники для незаконного збуту наркотиків через мережу Інтернет.

За більше року роботи чат-боту «СтопНаркотик» його авторський колектив декілька разів приймав рішення та проводив так звані «Дні протидії кібершахраям». В ці дні користувачам чат-боту замість надсилання електронних посилань на адреси, що використовують зловмисники для незаконного збуту наркотиків та на які необхідно залишити електронні скарги адміністрації месенджера Telegram, надсилались електронні адреси, що використовувались зловмисниками для:

– начебто продажу підроблених банкнот України різного номіналу;

– виманювання у користувачів банківських платіжних карток конфіденційної інформації для несанкціонованого списання коштів через фейкові чат-боти державного банку;

– розміщення фейкових новин і повідомлень від імені державних установ, політичних діячів, відомих публічних осіб;

– поширення неправдивої та конфіденційної інформації про жінок;

– поширення «порад» щодо того, як здійснювати насильство над жінками, у тому числі сексуальне [9, с. 306].

Завдяки об'єднанню зусиль небайдужих інтернет-користувачів чат-боту «СтопНаркотик» певну кількість електронних адрес, що використовували зловмисники у своїй протиправній діяльності, вдалося або заблокувати, або ці електронні адреси отримали позначку «Scam» (шахрайство).

На теперішній час на факультеті № 4 Харківського національному університеті внутрішніх справ ведуться роботи щодо створення під егідою МВС України всеукраїнського чат-боту «СтопШахрай», адмініструванням якого буде займатися Харківський національний університет внутрішніх справ.

Планується, що зазначений чат-бот повинен мати наступні функціоналі можливості:

1) отримувати від громадян та працівників правоохоронних органів електронні адреси, що використовують зловмисники з метою скоєння кібершахрайств, продажу заборонених товарів та послуг, поширення недостовірної та небезпечної інформації тощо;

2) участь користувачів чат-боту у спільному залишенні скарг на електронні адреси, що використовують зловмисники у своїй протиправній діяльності;

3) перевірка користувачами чат-боту наявної в них інформації про певних осіб, щодо їх можливої приналежності до шахрайств (за номером мобільного телефону, номером банківської картки, електронної адресою у месенджері тощо).

Використання чат-ботів є одним із методів залучення населення до протидії кримінальним правопорушенням, що вчиняють зловмисники з використанням засобів обчислювальної техніки та електронних комунікацій.

Список використаних джерел

1. Digital 2020 October Global Statshot Report (October 2020) v01 // slideshare : site. 20.10.2020. URL: https://www.slideshare.net/DataReportal/digital-2020-

october-global-statshot-report-october-2020-v01 (дата звернення: 20.11.2020).

2. Проникнення інтернету в Україні. Жовтень 2019 // Інтернет асоціація України : офіційний сайт. URL: https://inau.ua/sites/default/files/file/1910/dani_ustanovchyh_doslidzhen_iii_kvartal_2019_roku.pdf (дата звернення: 20.11.2020).

3. Розподіл безготівкових операцій з використанням платіжних карток у І півріччі 2020 року // Офіційне інтернет-представництво Національного банку України. 06.08.2020. URL: https://bank.gov.ua/admin_uploads/article/06-08-20_Cashless_operations_ua.jpg?v=4 (дата звернення: 20.11.2020).

4. Нобіуз В. Онлайн-покупки, або Як не заплатити шахраям // Mind.ua : сайт / ТОВ «Фьючер Медіа». 27.11.2020. URL: https://mind.ua/openmind/20218797-onlajn-pokupki-abo-yak-ne-zaplatiti-shahrayam (дата звернення: 20.11.2020).

5. 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: 20.11.2020).

6. Рвачов О. М., Ковтун В. О. Сучасні кібершахрайства щодо протизаконного заволодіння коштами з банківських рахунків громадян // Протидія кіберзлочинності та торгівлі людьми : зб. матеріалів Міжнарод. наук.-практ. конф. (27 травня 2020 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2020. С. 185-189. URL: http://www.univd.edu.ua/general/publishing/konf/27_05_2020/pdf/53.pdf (дата звернення: 20.11.2020).

7. Бєляєва Є. Г., Рвачов О. М. Мережа Інтернет як джерело підвищеної небезпеки для дітей // 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. 128-131. URL: http://univd.edu.ua/general/publishing/konf/23_11_2018/pdf/38.pdf (дата звернення: 20.11.2020).

8. Рвачов О. М., Лактіонов В. В., Дацюк Д. О. Сучасні методи активного залучення населення до протидії збуту наркотичних засобів, психотропних речовин або їх аналогів через мережу Інтернет // Протидія кіберзагрозам та торгівлі людьми (26 листоп. 2019 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2019. С. 210-217. URL: http://www.univd.edu.ua/general/publishing/konf/26_11_2019/pdf/65.pdf (дата звернення: 20.11.2020).

9. Марков В. В., Рвачов О. М., Ковтун В. О. Досягнення та перспективи розвитку факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ // Шлях успіху і перспективи розвитку (до 26 річниці заснування Харківського національного університету внутрішніх справ)

: матеріали Міжнар. наук.-практ. конф. (м. Харків, 20 листоп. 2020 р.) / [редкол.: Д. В. Швець (голова), О. М. Бандурка, С. М. Гусаров та ін.] ; МВС України, Харків. нац. ун-т внутр. справ. Харків : ХНУВС, 2020. С. 303-310. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/9722/Shliakh%20uspikhu_2020.pdf?sequence=3&isAllowed=y (дата звернення: 20.11.2020).

Одержано 20.11.2020

УДК [351.74(100):004.9](075.8)

Могілевський Леонід Володимирович
доктор юридичних наук, професор,
проректор Харківського національного університету внутрішніх справ
http://orcid.org/0000-0002-6994-6086

ВЕЛИКІ ДАНІ У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Великі дані виступають тут у ролі ультимативного інструменту розслідування кіберзлочинів і запобігання їм. Упроваджуючи чергову схему, зловмисники всюди залишають цифрові сліди. Окремо ці малі зміни зазвичай ігноруються. Однак на рівні Великих даних злочин з використанням мережевих технологій виглядає як характерний патерн. Повністю приховати його не вдасться, як би ретельно не маскувалися окремі прояви.

Стало набагато легше відстежити нелегальні ключі активації програмних продуктів. Раніше самі розробники виявляли тільки вкрадені однокористувальні ліцензії, коли їх намагалися одночасно використовувати кілька людей. Зараз обмін даними дозволяє побачити, що корпоративний ключ однієї з програм був украдений або відбувається перевірка генератора ключів.

За допомогою візуалізації великих обсягів спільних даних можна побачити незвичайні сплески активності на серверах реєстрації, що може вказувати на тестування вкрадених або згенерованих ключів. Без засобів візуалізації ці аномалії, скоріш за все, залишалися б непоміченими.

Традиційними засобами вебмоніторингу протидіяти піратству сьогодні вже навряд чи можливо. У світі існує понад 600 млн сайтів; з використанням

Великих даних виявлення незаконних завантажень контрафактного програмного забезпечення помітно спростилося.

Однак піратство – далеко не єдине явище, з яким борються в DCU. Сьогодні на технологіях аналізу Великих даних Microsoft створює цілу інфраструктуру для запобігання будь-якій нелегальній мережевій активності.

Таким чином, проблема використання систем аналізу Великих даних для запобігання та виявлення кіберзлочинів є досить актуальним науково-технічним завданням.

Метою цієї доповіді є дослідження використання технології аналізу Великих Даних для забезпечення глобальної інформаційної безпеки.

Застосовуючи технології аналізу Великих даних, у Microsoft розробляють алгоритми, що спрощують визначення керівних серверів і перехоплення контролю над ними. Також провайдери попереджаються про те, що комп'ютери їхніх абонентів заражені. Така співпраця допомагає узнати додаткові деталі про мережеву активність і обчислити подальші кроки злочинної групи.

Компанії, котрі займаються забезпеченням кібербезпеки, завжди покладалися на все більш складні програми, які на прикладі відомих їм вірусів навчалися розпізнавати нові, невідомі. До них додавалися алгоритми, які стежать за роботою інших програм і сповіщають про небезпеку, якщо в цій роботі відбувається щось несподіване.

Деякі системи захисту розміщають програми, які підозріло поводять себе, у віртуальний контейнер і за допомогою різних методів намагаються «декодувати» шкідливий код і виявити його наміри.

Поява великих обсягів інформації дозволила зробити важливий крок на шляху до створення програм захисту, які дозволяють перехоплювати 60–70 % вірусів, що залишилися б непоміченими традиційним антивірусним «софтом». Технології Machine Learning дозволяють виявити ДНК вірусних сімейств, а не просто окремі віруси.

Цей підхід був почерпнутий зі світу даталогії (науки про дані), і виявився дуже результативним завдяки величезній базі, швидко зібраній компаніями, які

почали відстежувати поведінку заражених вірусами комп'ютерів. Автоматизація виявлення таких аномальних кроків необхідна тому, що людина або навіть велика група людей не зможуть виявити їх досить швидко.

Кримінальні схеми постійно змінюються. Щоб вчасно реагувати на них і відстежувати нові тенденції, зараз важливо розробляти універсальні аналітичні інструменти, здатні працювати з будь-яким набором Великих даних.

Аналітичний підрозділ Microsoft по боротьбі зі злочинами у сфері високих технологій Digital Crimes Unit (DCU) було створено в листопаді 2013 р.

Важливим моментом тут залишається дотримання прозорості схеми отримання даних. У користувачів не повинно залишатися сумнівів щодо переслідуваних цілей і типів використовуваних відомостей.

Корпорація IBM оголосила, що пристосувала суперкомп'ютер Watson, здатний працювати з інформацією на природній мові, для використання у сфері інформаційної безпеки.

Фахівці IBM і дослідники з восьми американських університетів планують завантажити в систему, що самонавчається, вміст бібліотеки X-force, яка включає матеріали, що охоплюють два десятиліття досліджень в сфері інформаційної безпеки, детальну інформацію про 8 млн спамерських та фішингових атак і опис більше 100 тис. вразливостей.

На перших порах документи для Watson будуть підбирати і розмічати вручну, але потім машина стане справлятися з цим завданням без допомоги людей. На це в IBM і розраховують. Передбачається, що після завершення навчання Watson буде оперативно збирати і зіставляти загальнодоступні відомості про нові загрози, в тому числі інформаційні бюлетені, статті, звіти компаній, відео, навіть публікації в блогах. Він буде в курсі всього, що відбувається, і за рахунок цього зможе самостійно впізнавати проблеми і пропонувати рекомендації щодо їх вирішення.

Одержано 20.11.2020

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
Буслов Павло Володимирович
здобувач Харківського національного університету радіоелектроніки
Мелащенко Оксана Петрівна
старший викладач кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-4550-6879

ДІАГНОСТИКА ФУНКЦІОНУВАННЯ РОЗПОДІЛЕНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ СУДОВОЇ ЕКСПЕРТИЗИ

Розподілений характер інформаційних систем судової експертизи і значимість інформації, що обробляється системою, пред'являють підвищені вимоги як до структури самої системи, так і до якості передачі даних між різними підсистемами. Отже, вдосконалення існуючих систем передачі інформації і проєктування нових телекомунікаційних систем є важливим фактором підвищення якості обслуговування всієї ІС судової експертизи.

Метою даної доповіді є аналіз існуючих моделей і типів інформаційних систем судової експертизи і можливість підвищення показників QoS комп'ютерної мережі за рахунок досягнення потенційної точності оцінювання частот двох радіоімпульсів, що одночасно прийшли, при використанні методу сверхрелеевского дозволу в акустооптичних аналізаторах спектра.

Результати досліджень, які наведені в доповіді, показали, що практично в усіх напрямках інформаційного забезпечення судової експертизи є ефективні інформаційні системи. Ці інформаційні системи мають розподілений характер і для забезпечення основних показників якості функціонування висувають високі вимоги до якості функціонування телекомунікаційного обладнання відповідних комп'ютерних мереж (КМ). Адже поки не можна констатувати, що інформаційні системи забезпечення судової експертизи (ІСЗСЕ) мають

властивості штучних інтелектуальних систем, якими володіють експертні системи.

Для вирішення цього складного завдання необхідно докласти зусиль у всіх аспектах функціонування ІСЗСЕ, в тому числі і для підвищення показників якості QoS КМ. Метою доповіді є аналіз можливих шляхів підвищення QoS за рахунок використання сучасних методів визначення параметрів сигналу, що поширюється в комп'ютерній мережі [1].

Завдання вимірювання параметрів поширення сигналів ускладнюється тим, що сучасні радіотехнічні комплекси під час роботи можуть змінювати основні параметри випромінювання, такі як: частота, тривалість імпульсу, період проходження імпульсів і багато інших. Для оперативного розпізнавання і визначення параметрів радіосигналів все частіше використовуються методи обробки, що використовують акустооптичні взаємодії. Це обумовлено специфічними можливостями таких методів: паралельною, високою швидкістю і частотою обробки оптичних сигналів і т.д. [2].

Перераховані вище можливості реалізовані в акустооптичних аналізаторах спектра (АОАС), що відрізняються простотою конструкції і паралельною обробкою сигналів у широкій смузі частот і практично в реальному масштабі часу [3]. Переваги використання АОАС для вирішення завдань спектрального аналізу і розширення смуги одночасно аналізованих частот обумовлює необхідність більш глибокого аналізу роздільної здатності цих приладів.

У більшості робіт, присвячених дослідженню роздільної здатності акустооптичних аналізаторів спектра, ці дослідження проводяться з використанням критерію Релея [2; 3]. Так склалося історично, за аналогією з роздільною здатністю більшості оптичних приладів, наприклад, телескопів.

Дуже часто частоти вимірюваних в АОАС радіоімпульсів настільки близькі, що розрізнити їх як за допомогою критерію релея, так і інших методів не представляється можливим. Але в імпульсної радіолокації існує метод сверхрелеевского дозволу вузько смугових імпульсів по часу їх приходу. Основою цього методу є ідеалізація сигнальної суміші без шумової складової та

її аналітичним поданням поліномом, ступінь якого дорівнює числу джерел сигналу, а коріння однозначно пов'язані з їх параметрами [4].

У доповіді показано, що залежність середньоквадратичної помилки оцінювання розладу по частоті від її величини носить періодичний характер. Це природно, оскільки складові є також періодичними функціями. Однак при зменшенні величини періодичність на обраному інтервалі стає менш помітною. При малому числі дискрет (n = 10) і невеликій величині расстройки $\delta < 0.4$ середньоквадратична помилка оцінюваного параметра порівнянна з його величиною. Це означає, що отримання достовірних оцінок в цих умовах малоймовірно. Зі збільшенням числа дискрет на обраному інтервалі (n = 100) величина середньоквадратичної помилки становить менше 10% від величини оцінюваного параметра на всьому інтервалі.

Висновки. У доповіді наведені результати аналізу інформаційних систем судової експертизи та встановлено, що вони мають розподілений характер. Проведено аналіз підсистем, які складають інформаційну систему судової експертизи та визначені ті, які мають основний вплив на показники якості. Наведено аналіз методів підвищення якості функціонування КМ ІСЗСЕ за рахунок використання сучасних методів визначення параметрів сигналу, що поширюється в комп'ютерній мережі.

У доповіді обґрунтовується можливість застосування сверхрелеевского дозволу імпульсів по частоті в акустооптичних спектроаналізаторів. Отримано вираз для оцінки потенційної точності величини розладу по частоті двох імпульсів. Аналіз розрахунків потенційної точності показує, що для практичного використання ідеї сверхрелеевского дозволу імпульсів по частоті в акустооптичних спектроаналізаторів необхідно забезпечити потрібну частоту дискретизації вибірки.

Список використаних джерел

1. Mozhaiev M., Melashchenko O., Roh V., Usatenko M. Means of improving the quality of service of the computer network of the forensic information system. *Innovative Technologies and Scientific Solutions for Industries.* 2020. № 2(12). P. 57-65. DOI: https://doi.org/10.30837/2522-9818.2020.12.057.

2. Rudnytsky V., Mozhaiev M., Kuchuk N. Method for the diagnostics of

synchronization disturbances in the telecommunications network of a critical used computer system. *Innovative Technologies and Scientific Solutions for Industries.* 2020. № 1(11). P. 172-180. DOI: https://doi.org/10.30837/2522-9818.2020.11.172.

3. Mozhaiev M., Kuchuk N., Usatenko M. The method of jitter determining in the telecommunication network of a computer system on a special software platform. *Innovate Technologies and Scientific Solutions for Industries.* 2019. № 4 (10). P. 134-140. DOI: https://doi.org/10.30837/2522-9818.2019.10.134.

4. Yasechko M. M., Mozhaiev M. O. Temporary and energy criteria for protection of radioelectronic means (automated systems and telecommunication systems) from the destructive influence of electromagnetic radiation // Scientific and technical progress in European countries and the contribution of higher education institutions : Collective monograph. Riga : Izdevnieciba "Baltija Publishing", 2020. P. 288-301. DOI https://doi.org/10.30525/978-9934-588-65-5.16.

Одержано 19.11.2020

УДК 519.7:537.8

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

СТВОРЕННЯ ТА ВИКОРИСТАННЯ ВІДЕО ВИСОКОЇ ЧІТКОСТІ У НАЦІОНАЛЬНІЙ ПОЛІЦІЇ УКРАЇНИ

Для систем ідентифікації особистості для потреб органів правопорядку в даний час застосовують різні підходи. У тому числі і системи телебачення високої чіткості (ТВЧ), які дозволяють істотно підвищити показники якості розпізнавання об'єктів різної фізичної природи, в тому числі і розпізнавання особистості. Тому необхідно провести аналіз особливостей систем ТВЧ для використання в інтересах Національної поліції України. Перехід на ТВЧ в

Європі відрізнявся від Японії і США. Вперше дослідження ТВЧ почалося в Японії на громадському телебаченні. Вони прагнули отримати зображення з насиченим кольором в більшому форматі і високої роздільної здатності. Ця система отримала назву MUSE (Multiple sub-nyquist Sampling Encoding), яка була несумісна з їх традиційним телебаченням. В Європі інженери почали працювати над проєктом HD-MAC для розробки стандарту, що сумісний з традиційним телебаченням (PAL системи). Передача ТВЧ потребує високошвидкісних каналів передачі інформації. Тому стає *актуальна науково-практична задача* забезпечення потрібної пропускної здатності для каналів передачі інформації ТВЧ.

Основна проблема при передаванні відео через інтернет є пропускна здатність мережі. Необхідно використовувати алгоритми з високим ступенем стиснення відео для низької пропускної здатності [1]. Є багато методів кодування. Деякі засновані на просторовому стисненні зображенні (наприклад, Motion-JPEG), інші, такі як H.261 і H.263, працюють на основі тимчасового стиснення відеопослідовності.

Їх мета полягає в досягненні гарної якості зображення, і при цьому мають високу ступінь стиснення. Стисле відео дозволяє знизити тимчасові витрати при передаванні і сприяє його поширенню. Однією з кращих систем стиснення, яка пропонує хорошу якість із сильною компресією зображення є MPEG 4.

Для створення відео може бути використана програма для нелінійного монтажу Adobe Premiere Pro CS5.5 [1]. Перш за все, був налаштований проєкт з параметрами обраної системи HD -MAC 1250 ліній по горизонталі (1280x720 пікселів) зі співвідношенням сторін 16: 9 і 50 кадрів в секунду.

Була розглянута технологія створення відео високої чіткості без використання камери, яка дозволяє знімати з високою якістю. Також розглянуті кілька доступних кодеків для стиснення відео. Нестислий відеофайл високої чіткості з розміром 3,86 ГБ має розмір 5,71 МБ, при стисненні використаний бітрейт 800 Kbps для 1 проходу і 52 MB, коли він стискається за допомогою бітрейт в 5000 Kbps для 2 - проходів.

Була виявлена аномалія для кодека XviD – при бітрейте 2000 Kbps, продуктивність кодека при цьому значенні вище. Отриманий час, необхідний для стиснення секунди відео за 1 прохід має більше значення, ніж при 2 проходу. Розглянуті кодеки стиснення дозволять зменшити час кодування відео і зберегти вільний простір на жорсткому диску.

Висновки. В докладі було наведено результати аналізу використання систем телебачення високої чіткості в системах ідентифікації особистості.

Проведені дослідження методів забезпечення потрібної пропускної здатності для каналів передачі інформації ТВЧ.

Проаналізовані проблеми, які виникають при реалізації запропонованих методів та запропоновані засоби підвищення якості функціонування системи ТВЧ.

Список використаних джерел

1. Adobe Premiere Pro // Adobe Systems : сайт http://www.adobe.com/products/premiere/ (дата звернення: 19.11.2020).

Одержано 19.11.2020

УДК 004

Моргай Крістіна Сергіївна
курсантка 2 курсу факультету № 1
Харківського національного університету внутрішніх справ

ФОРМУВАННЯ ЦИФРОВОЇ КОМПЕТЕНТНОСТІ СУЧАСНОГО ПОЛІЦЕЙСЬКОГО

Інформаційні технології кардинальним чином змінили життя мільйонів людей. Інформація стала найважливішим стратегічним ресурсом поряд з іншими – людським, економічним, фінансовим, матеріальним. Використання інформації складає необхідну основу ефективного функціонування і розвитку різних сфер економіки та суспільного життя.

Інформатизація та автоматизація процесів проникла в усі сфери діяльності поліції: починаючи від оперативних підрозділів і закінчуючи юридичними та кадровими підрозділами.

У сучасній світовій педагогіці виокремлюються основні напрямки розвитку професійних навичок, які підходять і до підготовки сучасного фахівця-поліцейського.

Формування цифровий компетентності – це одна з основних вимог сучасної освіти поліцейського. З'являються нові форми інформаційного забезпечення діяльності поліції, які в деяких випадках дають можливість розкривати злочини, не виходячи зі службового кабінету.

Вважаємо, що кожен сучасний поліцейський на сьогодні повинен вміти:

– користуватися електронним документообігом (з використанням цифрового підпису);

– користуватися службовою електронною поштою;

– використовувати бази даних та інформаційні ресурси органів внутрішніх справ та інших державних органів;

– використовувати цифрові технології у своїй службовій діяльності в залежності від спеціалізації (наприклад, експерт);

– мати навички в області інформаційної безпеки і захисту інформації.

Усе це диктує нові вимоги до підготовки сучасного поліцейського: формування цифрової компетентності поряд з базовими юридичними знаннями.

Глибоко переконані, що завдання закладу вищої освіти МВС України щодо формування цифрової компетентності – дати уявлення курсантам і слухачам про можливості сучасних технологій, ознайомити їх з «новинками» в цифровому світі, сформувати навички роботи на сучасному програмному забезпеченні, які вони потім зможуть застосувати на практиці.

З метою боротьби зі злочинністю необхідно ознайомити курсантів і слухачів із тими способами злочинної діяльності, які використовують «просунуті» представники злочинного світу. Зросла цифрова компетентність населення, що породжує і нові темпи зростання злочинів, скоєних за

допомогою інформаційних технологій. Кількість кіберзлочинів зростає, способи їх здійснення розвиваються, стають більш професійними. Унаслідок цього кіберзлочини несуть загрозу не тільки громадянам та юридичним особам, але також є небезпечними для окремих держав і світової спільноти в цілому.

У практику роботи правоохоронних органів необхідно активно впроваджувати можливості мережі Інтернет та інших високих комп'ютерних технологій не тільки по виявленню та розслідуванню злочинів, але і по координації роботи підрозділів. Для забезпечення такої роботи необхідним є проведення спеціальних наукових досліджень з кримінології та криміналістики в аспекті застосування цифрових технологій у протидії злочинності.

Інформаційні технології стали невід'ємною частиною всіх сфер діяльності суспільства та держави. Їх ефективне застосування є фактором прискорення економічного розвитку держави та формування інформаційного суспільства. Для професійної підготовки поліцейського формування цифрової компетентності є наскрізною основою для застосування набутих знань, умінь і навичок у сучасному інформаційному середовищі.

Одержано 14.11.2020

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

СУЧАСНИЙ СТАН СИСТЕМ ІНТЕЛЕКТУАЛЬНОГО ВІДЕОСПОСТЕРЕЖЕННЯ, ЯКІ ВИКОРИСТОВУЮТЬСЯ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Для забезпечення громадської безпеки, збору доказів злочину, пошуку і затримання злочинців, охорони власності, дотримання правил дорожнього руху т.і. Національна поліція України (далі – НП України) використовує системи відеоспостереження силових структур і приватних власників [1].

1. Патрульна поліція України використовує нагрудні відеокамери (відеореєстратори), системи відеоспостереження, встановлені на службових транспортних засобах, і стаціонарні системи відеоспостереження. Основною метою використання відеореєстраторів є забезпечення об’єктивної оцінки дій патрульного під час виконання ним своїх обов’язків, ретельний збір доказів правопорушення.

2. Управління силами та засобами патрульної поліції здійснюється за допомогою системи централізованого управління нарядами патрульної служби «ЦУНАМІ». До складу цієї системи входить система стаціонарного відеоспостереження, яка забезпечує оперативний візуальний контроль за основними криміногенними місцями, вулицями, майданами, транспортними

потоками, об’єктами що охороняються. НП Україні використовує інформацію з понад ніж 24 тис. відеокамер, з яких майже 2,8 тис. це так звані «розумні».

3. За допомогою систем відеоспостереження, встановлені на службових транспортних засобах функціонує інформаційна підсистема «Гарпун». Система «Гарпун» використовує спеціалізоване аналітичне програмне забезпечення створене для розшуку викрадених транспортних засобів та номерних знаків, виявлення одночасного перебування номерних знаків на різних транспортних засобах, фактів використання знищених номерних знаків, а також для автоматизованого інформування про такі факти чергових диспетчерів патрульної служби. «Гарпун» є підсистемою інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України».

4. До Єдиного аналітичного сервісного центру Головного управління Національної поліції в Донецькій області належить система UASC, в якій використовують інтелектуальні відеокамери. Система проводить ідентифікацію автомобіля, на який встановлений державний номер і виявляє відповідність номера автомобіля згідно з реєстрацією, розпізнає тип і марку автомобіля та його колір, перевіряє чи знаходиться автомобіль у розшуку, чи відповідає державний номер автомобіля, ідентифікує осіб, які знаходяться на передньому сидінні. Система виявляє скупчення людей, може фіксувати їх неадекватну поведінку, розпізнає заборонений або нетиповий рух автотранспорту т.і.

5. В структурі апарату НП України створено Управління організації діяльності підрозділів поліції на воді та повітряної підтримки (УПВП). Його запроваджено для організації, координації й контролю службової діяльності підрозділів поліції на воді та забезпечення повітряної підтримки підрозділів НП України. Підрозділи поліції застосовують БпЛА для: висотного спостереження під час проведення масових святкувань, політичних демонстрацій, спортивних заходів, а також під час припинення масових заворушень; висотного спостереження при загрозі нападу на стратегічні об’єкти та об’єкти, які знаходяться під охороною; виявлення злочинів та адміністративних правопорушень; організації відео документування; забезпечення зв’язку й

управління наземними нарядами поліції; організації взаємодії підрозділів поліції з іншими силовими структурами; забезпечення та контролю безпеки дорожнього руху; проведення спостереження при здійсненні оперативних заходів, відстеження оперативної обстановки під час виконання службових завдань; пошуку підозрюваних, які намагаються сховатись; пошуку зниклих людей.

6. КАСКАД – комплексна система контролю автомобільних доріг (Київ). Єдиний повнофункціональний пристрій що впроваджений в експлуатацію, та розроблений під особливості національного технічного регулювання, законодавчу базу. Встановлені комплекси фіксують події з ознаками порушень ПДР: швидкісний режим; проїзд на забороняючий сигнал світлофора; порушення розмітки, перетин суцільної смуги; порушення правил паркування; рух смугою громадського транспорту. Дані передають до системи збору та обробки даних.

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 18.11.2020

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

ДЕЯКІ АСПЕКТИ ІДЕНТИФІКАЦІЇ АКТУАЛЬНИХ КІБЕРЗАГРОЗ В КОМП'ЮТЕРНИХ МЕРЕЖАХ ОРГАНІВ МВС УКРАЇНИ

В кожному центральні органі виконавчої влади, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України [1], існують структурні підрозділи, які забезпечують

функціонування відомчих комп'ютерних мереж інформаційно-телекомунікаційних систем, а саме:

– Департамент інформаційно-аналітичної підтримки Національної поліції України (ДІАП НПУ);

– Головний центр зв'язку, автоматизації та захисту інформації Державної прикордонної служби України (ГЦЗАЗІ ДПСУ);

– Центр оперативного зв'язку, телекомунікаційних систем та інформаційних технологій Державної служби України з надзвичайних ситуацій (ЦОЗТСЗІ ДСУНС);

– Об'єднаний вузол зв'язку Національної гвардії України (ОВЗ НГУ);

– Департамент інформатизації, телекомунікацій та захисту інформації Державної міграційної служби України (ДІТЗІ ДМСУ);

– Управління інформатизації Головного сервісного центру МВС України (УІ ГСЦ МВСУ).

На Департамент інформатизації МВС (ДІ МВС), окрім іншого, покладена задача [2] організації впровадження та забезпечення контролю функціонування в системі МВС систем управління інформаційною безпекою, аналізу стану кібербезпеки, вживання заходів щодо профілактики кібератак та кіберінцидентів, протидії кіберзагрозам, забезпечення кіберзахисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури системи МВС.

З метою системного вирішення цієї задачі ДІ МВС доцільно організувати впровадження і контролювати функціонування в органах МВС відкритої платформи ідентифікації кіберзагроз - Malware Information Sharing Platform (MISP) [3], яка призначена для автоматизованого збору, обміну, зберігання та співвіднесення індикаторів вторгнення (indicators of compromise, IOCs), інформації про наявні: кіберзагрози (threat intelligence); схеми шахрайства (fraud); вразливості (vulnerability) апаратно-програмного забезпечення.

Кінцевими споживачами сервісів MISP є адміністратори систем кібербезпеки, які відповідним чином налаштовують конфігурацію систем

захисту і реагують на виявлені кіберінциденти, та системи виявлення/запобігання вторгнень (Snort, Suricata, Zeek IDS), в яких автоматизовано оновлюються правила та сигнатури виявлення вторгнень.

На сьогодні [4], в Ситуаційному центрі забезпечення кібербезпеки Служби безпеки України вже впроваджено платформу MISP-UA, яка, перш за все, забезпечує [5]: розкриття (розслідування) кіберзлочинів і кіберінцидентів та негласну перевірку готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів.

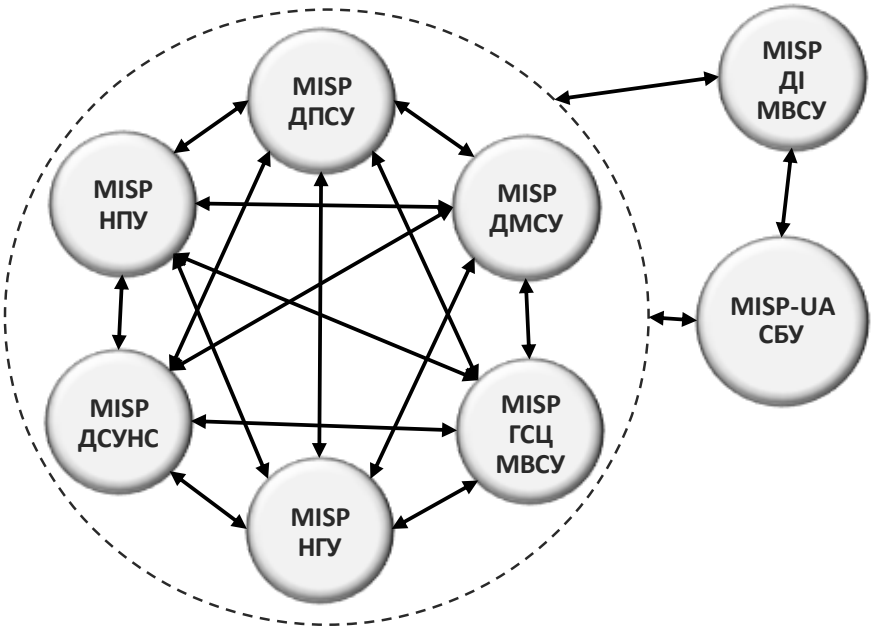

Рисунок 1 – Децентралізоване з'єднання MISP органів МВС та MISP-UA СБУ

Розгортання і впровадження MISP в органах МВС (MISP-MIA) відповідними структурними підрозділами з огляду на особливості платформи краще здійснити за децентралізованою схемою, де в кожному органі МВС будуть власні MISP, але горизонтально з'єднані, як між собою, так і з MISP-UA СБУ (рис. 1).

MISP, як система ідентифікації актуальних кіберзагроз, існує з 2011 року, постійно розвивається за фінансуванням Європейського Союзу і впроваджується в країнах ЄС та НАТО.

Список використаних джерел

1. Органи МВС // Єдиний портал органів системи МВС України : сайт. URL: http://mvs.gov.ua/ua/structure (дата звернення: 18.11.2020).

2. Департамент інформатизації // Єдиний портал органів системи МВС України : сайт. URL: http://mvs.gov.ua/ua/structure/Departament-%D1%96nformatizats%D1%96ii.htm (дата звернення: 18.11.2020).

3. MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing // MISP project : сайт. URL: https://www.misp-project.org (дата звернення: 18.11.2020).

4. Для протидії кіберзагрозам СБУ вводить в дію оновлену версію платформи MISP-UA // Служба безпеки України : сайт. 16.07.2020. URL: https://ssu.gov.ua/novyny/7800 (дата звернення: 18.11.2020).

5. Ситуаційний центр забезпечення кібербезпеки Служби безпеки України. Основні завдання // Служба безпеки України : сайт. URL: https://sbu.gov.ua/ua/pages/330 (дата звернення: 18.11.2020).

Одержано 19.11.2020

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

ПРАВООХОРОННІ ОРГАНИ В БОРОТЬБІ З РОЗПОВСЮДЖЕННЯМ НАРКОТИЧНИХ РЕЧОВИН ЧЕРЕЗ МЕРЕЖУ ІНТЕРНЕТ

В даний момент говорити про онлайн-торгівлю наркотиками в рамках якоїсь однієї країни не представляється можливим в силу того, що така система нелегальних продажів вже давно набула глобального масштабу. Користуючись можливостями мережі, дилери організували інтернаціональну доставку бажаних товарів поштою або кур'єрською службою. Люді, які торгують нелегальними товарами, знають толк в конспірації, і навряд чи їх сайт можна знайти в пошуковій видачі Google і Yandex. У них є свої портали і магазини. Вони вже давно облюбували анонімну мережу Tor (The onion router, «Цибулева маршрутизація»). За допомогою неї користувачі можуть зберігати анонімність в інтернеті при відвідуванні сайтів, заборонених в різних країнах, при публікації матеріалів, надсилання повідомлень. Встановити IP-адреса комп'ютерів

користувачів проблематично, користувачі «лушпиння мережі» запускають проксі-сервер на своїй машині, дане програмне забезпечення підключається до серверів і використовує криптографію багаторівневим способом.

Зайшовши в мережу, користувач легко може знайти будь-який наркотик: до його послуг Hidden Wiki (каталоги сайтів на будь-який смак), пошукові системи по кублах, електронні торгові майданчики. Найпопулярнішою майданчиком, свого роду величезним ринком будь-яких психотропних речовин була площадка Silk Road («Шовковий шлях»). Цей ресурс став безсумнівним лідером нелегального ринку, купити пару грам героїну або ЛСД, АК-47 або гранатомет там було простіше простого. Оплата здійснювалася біткоїнами (криптовалюта). У Європейському союзі 1 грудня 1989 року було створено Європейську комісію по боротьбі з наркотиками (CELAD), що складається з 12 представників держав-членів ЄС. За пропозицією CELAD метою збору та систематизації об'єктивної інформації з виробництва, розповсюдження та споживання наркотиків в країнах ЄС в 1993 році був створений Європейський центр моніторингу наркотиків і наркозалежності (EMCDDA)

Відповідно до рішень Європейської ради, комісія розробила всеосяжну стратегію боротьби з наркотиками, представивши антинаркотичну стратегію.

Для правоохоронних органів боротьба з розповсюдженням наркотиків через інтернет - завдання не з легких. У кожній країні існують свої закони, а сам інтернет не знає державних кордонів, дозволяючи оформляти замовлення в інших країнах. Експерти-криміналісти відзначають не тільки зростання обсягів збуту наркотиків через інтернет кінцевим споживачам. Злочинці, користуючись лазівками в законодавстві, організовують поставку сировини, а також координують транспортування і оптові продажі. Щоб поставити ефективний заслін діяльності такого роду угруповань, необхідні спільні зусилля на міжнародному рівні.

В цілому, політика лібералізму по відношенню до наркотиків у світі, відносна доступність заборонених продуктів онлайн стимулює зростання споживання наркотиків, що особливо важливо, серед молоді – основних

користувачів глобальної мережі. Боротися з такими підпільними мережами силами однієї держави неможливо, і все більше аналітиків приходять до висновку, що тільки спільні зусилля правоохоронних органів та влади інших держав можуть побороти цю інтернет-мафію.

Одержано 08.11.2020

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

ПРОБЛЕМНІ ПИТАННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ ТА ЗВО ЗІ СПЕЦИФІЧНИМИ УМОВАМИ НАВЧАННЯ

Сьогодні, як ніколи постає важливим питанням застосування інформаційних технологій в діяльності правоохоронної системи України, а також закладів вищої освіти зі специфічними умовами навчання. Рівень розвитку людства показує стрімке зростання технологій, які допомагають в повсякденній діяльності правоохоронців. Важко собі уявити діяльність судів, органів прокуратури, Національної поліції України, Служби безпеки України, органів митного контролю без застосування сучасних комп’ютерних засобів.

З метою підвищення ефективності діяльності правоохоронних органів створюються державні бази та реєстри. У статті 10 Закону України «Про інформацію» надано вичерпний перелік видів інформації, а саме: інформація про фізичну особу; інформація довідково-енциклопедичного характеру; інформація про стан довкілля; інформація про товари і послуги; науково-

технічна інформація; податкова інформація; правова інформація; статистична інформація; соціологічна інформація; інші види інформації [1].

В державних базах даних можна знайти ти інформацію про: обліково-реєстраційні дані громадян; правопорушення і кримінальні події; правопорушників і злочинців; викрадені і вилучені речі, а також предмети антикваріату; власників авто-, мототранспортних засобів; власників вогнепальної зброї; громадян, що знаходяться в розшуку та безвісті зниклих громадян; інша інформація, що підлягає зберіганню. В державних реєстрах зберігається інформація щодо: фізичних осіб платників податків, нормативно-правові акти, громадські об'єднання, цивільний стан громадян, нотаріусів, довіреності, юридичних осіб та фізичних осіб-підприємців, осіб, які вчинили правопорушення, інформація про підприємців щодо яких порушено провадження щодо банкрутства та інше.

Таким чином можна сказати, що правоохоронні органи володіють певною кількістю інформації, що допомагає їм м в розкритті, протидії та запобіганні злочинам у різних сферах суспільного життя. З метою систематизації такої кількості інформації створено автоматизовані інформаційні системи (АІС) для швидкого пошуку потрібних даних [2].

Для закладів вищої освіти зі специфічними умовами навчання застосування інформаційних технологій у навчальному процесі є важливим аспектом виховання майбутніх працівників правоохоронної системи. Безумовно для цього є необхідним відповідне матеріальне забезпечення, яке дасть можливість створення сучасних комп'ютерних класів та лабораторій для того, щоб такі заклади вищої освіти могли готувати висококваліфіковані кадри для боротьби зі злочинністю. У процесі навчання важливою є не сама інформаційна технологія, а методи її реалізації для досягнення освітніх цілей. Застосування інформаційних технологій є однією з основних тенденцій розвитку освітнього процесу. Тому, необхідно проводити постійні тренінги для викладачів з метою підвищення їхнього кваліфікаційного рівня. Адже сучасній освітній системі потрібні такі науково-педагогічні працівники, які зможуть підготувати якісні

кадри для правоохоронної системи, що допоможе знизити рівень злочинності, як в суспільстві, так і в інтернет-просторі.

Згідно Закону України «Про Концепцію Національної програми інформатизації» інформатизація освіти спрямовуватиметься на формування та розвиток інтелектуального потенціалу нації, удосконалення форм і змісту навчального процесу, впровадження комп'ютерних методів навчання та тестування, що дасть можливість вирішувати проблеми освіти на вищому рівні з урахуванням світових вимог. Серед основних результатів інформатизації освіти має бути: розвиток інформаційної культури людини (комп'ютерної освіченості), скорочення терміну та підвищення якості навчання і тренування на всіх рівнях підготовки кадрів; кадрове забезпечення усіх напрямів інформатизації України шляхом спеціалізації та інтенсифікації підготовки відповідних фахівців. Першочерговим завданням є створення глобальної комп'ютерної мережі освіти та науки [3].

Тому, застосування інформаційний технологій працівниками правоохоронної системи та науково-педагогічними працівниками і курсантами закладів вищої освіти зі специфічними умовами навчання є критичним питанням, яке потребує постійної уваги та вдосконалення. На державному рівні потрібно розробити стратегію вирішення цього питання, яка б за максимально короткий термін реформувала систему правоохоронних органів та закладів вищої освіти зі специфічними умовами навчання щодо запровадження сучасних інформаційних технологій в повсякденній професійній діяльності правоохоронців, студентів, курсантів та викладачів. Адже в сучасному світі неможливо уявити роботу системи МВС України без застосування баз і банків даних, державних реєстрів, як необхідної складової для ефективної діяльності.

Список використаних джерел

1. Про інформацію : Закон України від 02.10.1992 № 2657-XII // БД «Законодавство України» / ВР України. URL: http://zakon4.rada.gov.ua/laws/show/1906-15 (дата звернення: 15.11.2020).

2. Бабаскін В. В., Жалгунова С. А. Проблемні питання інформаційного забезпечення діяльності ОВС. *Науковий вісник ЮА МВС*. 2005. № 3. С. 32-38.

3. Про Концепцію Національної програми інформатизації : Закон України

від 04.02.1998 № 75/98-ВР // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80 (дата звернення: 15.11.2020).

Одержано 19.11.2020

УДК 342.9

Осипчук Іван Іванович
здобувач Науково-дослідного інституту публічного права

ДЕЯКІ ПИТАННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ ЩОДО ЗАБЕЗПЕЧЕННЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Останнім часом посилюються загрози для критичної інфраструктури, пов’язані з погіршенням її технічного стану, відсутністю інвестицій в її оновлення та розвиток, несанкціонованим втручанням у її функціонування, зокрема фізичного і кіберхарактеру, триваючими бойовими діями, а також тимчасовою окупацією частини території України [1]. Отже, з урахуванням потреб національної безпеки і необхідності запровадження системного підходу до розв’язання проблеми на загальнодержавному рівні створення системи захисту критичної інфраструктури є одним із пріоритетів у реформуванні сектору оборони і безпеки України.

Варто звернути увагу, що у теорії управління під інформаційним забезпечення розуміють діяльність, що організовується в рамках управління, спрямована на проєктування, функціонування та вдосконалення інформаційних систем, що забезпечують ефективне вирішення завдань управління [2, с. 21]. Р. А. Калюжний та В. О. Шамрай виділяють три основні значення поняття «інформаційне забезпечення»: забезпеченість системи управління відповідною множиною інформації; діяльність, пов’язана з організацією збору, реєстрації, передачі, зберігання, опрацювання і представлення інформації; діяльність щодо формування цілеспрямованої суспільної й індивідуальної свідомості суб’єктів

суспільних відносин щодо управління у конкретній сфері суспільних відносин [3, с. 39].

На сьогодні, відповідно до Законів України «Про Службу безпеки України», «Про контррозвідувальну діяльність» Служба безпеки України має широкі повноваження задля вчинення заходів, направлених на недопущення, швидке реагування та припинення правопорушень у сфері забезпечення національної безпеки, проведення контррозвідувальних та оперативно-розшукових заходів та виконання повноважень, встановлених у статтях 1, 2 Закону України «Про Службу безпеки України». А, функція СБУ щодо контррозвідувального захисту критичної інфраструктури має здійснюватися у виключній відповідності із контррозвідувальними заходами, визначеними Законом України «Про контррозвідувальну діяльність».

В той же час, в нормотворенні інформаційного забезпечення повинні брати участь колективи працівників різного фаху (юристи, інженери-електронники, програмісти-математики, системотехніки, при цьому провідна роль належить відповідно підготовленим юристам, які спеціалізуються на інформаційному праві). При цьому у комплексі повинні вирішуватися проблеми, які досліджуються щодо відносин з приводу того, як виробляється і використовується інформація, яка її якість, за допомогою яких засобів, технологій, носіїв вона обробляється, переробляється тощо.

З точки зору теорії права, інформаційне забезпечення, як діяльність, яка пов’язана з інформацією, – суть інформаційних правовідносин. В той же час інформаційні відносини в процесі нормотворення – це діяльність суб’єктів і об’єктів управління, яка пов’язана із збором та використанням інформації. Від якості збору і обробки інформації залежить якість підготовки та прийняття нормативно-правових актів.

Варто звернути увагу, що несьогоднішній день існує проєкт Закону України «Про критичну інфраструктуру та її захист», який чітко визначає об’єкти критичної інфраструктури, до яких віднесено підприємства, установи, організації незалежно від форми власності, які: 1) провадять діяльність та

надають послуги в галузях енергетики, хімічної промисловості, оборонно-промислового комплексу, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах; 2) надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, централізованого водовідведення, постачання теплової енергії, гарячої води, електричної енергії і газу, виробництва харчових продуктів, охорони здоров'я; 3) включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави; 4) підлягають охороні та обороні в умовах надзвичайного стану і особливого періоду; 5) є об'єктами підвищеної небезпеки; 6) є об'єктами, які мають загальнодержавне значення, розгалужені зв'язки та значний вплив на іншу інфраструктуру; 7) є об'єктами, порушення функціонування яких призведе до кризової ситуації регіонального значення.

В зв'язку з викладеним, чітке законодавче визначення об'єкта критичної інфраструктури має важливе значення, оскільки від цього залежить об'єм відповідних повноважень Служби безпеки України у сфері захисту критичної інфраструктури. Розширення меж діяльності Служби безпеки України може призвести до порушення прав і свобод, законних інтересів громадян та суб'єктів господарювання, а також створенню певних правових колізії між нормами законодавства.

Список використаних джерел

1. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14.09.2020 № 392/2020 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/go/392/2020 (дата звернення: 13.11.2020).

2. Воскресенский Г. М. Теория и практика информационного обеспечения управления в органах внутренних дел : учеб. пособ. Москва, 1985. 121 с.

3. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії і практики : монографія / за ред. Р. А. Калюжного та В. О. Шамрая. Київ : КВІЦ, 2002. 296 с.

Одержано 13.11.2020

УДК 378+349
Пашковська Марина Віталіївна
кандидат юридичних наук, старший науковий співробітник,
старший науковий співробітник наукової лабораторії з проблем превентивної діяльності та запобігання корупції Національної академії внутрішніх справ
https://orcid.org/0000-0002-9087-0290
Федоровська Наталія Володимирівна
старший науковий співробітник наукової лабораторії з проблем превентивної діяльності та запобігання корупції Національної академії внутрішніх справ
https://orcid.org/0000-0003-2019-778X

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ІНТЕРАКТИВНИХ МЕТОДІВ НАВЧАННЯ ПРИ ПІДГОТОВЦІ ПОЛІЦЕЙСЬКИХ

Наука невпинно прямує вперед, відкриваючи для її здобувачів нові перспективи та горизонти. На рівні освітніх закладів відбувається вдосконалення тактик та методик викладання, здійснюється пошук нових способів у доступній, цікавій та пізнавальній формі.

Завданням вищого навчального закладу із специфічного навчання є здійснення освітньої, наукової, методичної та організаційної діяльності пов’язаної з підготовкою поліцейських і цивільних осіб.

Особливе місце в освітньому процесі займає використання інтерактивних методів навчання, на заняттях у навчально-тренувальних полігонах серед яких: криміналістичний, «кілер-хауз», блокпост, «Протидія домашньому насильству», «Зелена кімната», кабінет працівника поліції («Поліцейська станція»), Центр поліграфологічних досліджень, «Нарколабораторія», «Зал судового засідання», тир, чергова частина, ізолятор тимчасового тримання, скалодром, спеціальна смуга перешкод, автодром, кімната психоемоційного розвантаження.

Навчально-науковий інститут № 3 Національної академії внутрішніх справ здійснює підготовку фахівців за спеціальністю «Правоохоронна діяльність», посилюючи кадровий потенціал підрозділів ювенальної превенції, дільничних офіцерів поліції, патрульної поліції, психологічної служби. З метою підвищення рівня підготовки та професіоналізму розроблено фахівцями

академії навчальні інформаційно-довідкові програми «Автоматизоване робоче місце працівника підрозділу ювенальної превенції», «Автоматизоване робоче місце дільничного офіцера поліції» (АРМ), який представляє собою цифровий носій, на якому міститься мережа науково-методичної інформації (яка систематично оновлюється), яка використовується у повсякденній діяльності працівників підрозділів під час виконання службових обов'язків.

На особливу увагу заслуговують використання в освітньому процесі навчально-тренувальних полігонів, серед яких:

- «Зелена кімната» з метою закріплення практичних навичок роботи поліцейських із дітьми, які постраждали внаслідок насильницьких чи сексуальних злочинів або стали свідками таких подій. Курсанти-психологи мають можливість відпрацьовувати вміння спілкування з дітьми, тим самим формувати професійні навички роботи практичного психолога, які неодмінно знадобляться їм у подальшій професійній діяльності;

- «Протидія домашньому насильству» відпрацювання навчальних сценаріїв з метою набуття навичок діяльності дільничного офіцера поліції, працівника ювенальної превенції, патрульної поліції на закріпленій дільниці обслуговування, що максимально наближені до реальних умов.

В свою чергу, використання інноваційних методів навчання сприяє підвищенню якісного професійного рівня здобувачів вищої освіти, що в комплексному та системному застосуванні дасть змогу отримати висококваліфікованих кадрів.

Підсумовуючи, слід зазначити, що впровадження методичних інновацій та інформаційних технологій вдосконалює освітній процес в Національній академії внутрішніх справ з урахуванням сучасних потреб професійної діяльності майбутніх спеціалістів-юристів з відповідного напряму.

Одержано 19.11.2020

УДК 343.98
Расторгуєва Наталія Олегівна
курсантка 3 курсу факультету № 1
Харківського національного університету внутрішніх справ;
Загуменна Юлія Олександрівна
кандидат юридичних наук, доцент,
професорка кафедри теорії та історії держави і права факультету № 1
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0003-0617-8363

БОРОТЬБА З КІБЕРЗЛОЧИННІСТЮ В УМОВАХ ПАНДЕМІЇ COVID-19

Реалії сьогодення становлять перед правоохоронними органами нові виклики та завдання. Так 2020 рік ознаменувався поширенням нової коронавірусної пневмонії SARS-CoV-2. Станом на 17 листопада 2020 року в світі за даними американського університету Джонса Гопкінса зафіксовано 55 147 032 підтверджених випадків, із яких 1 329 556 смертельних [1]. Не оминула ця хвороба й Україну. Станом на 17 листопада 2020 року в Україні зареєстровано 11 968 нових випадків інфікування COVID-19, усього з початку пандемії викликаною захворюваністю на SARS-CoV-2 кількість підтверджених випадків становить 557 657, з них 9 856 летальних [2]. Тому 11 березня 2020 року КМУ прийняв постанову № 211 «Про запобігання поширенню на території України коронавірусу COVID-19» [3], якою був запроваджений карантин на всій території нашої держави. Карантинні обмеження викликані поширенням коронавірусної пневмонії стали не тільки рушійною силою діджиталізації суспільства, але й створили плацдарм для активізації діяльності кіберзлочинців.

Окрім безпосередньої шкоди від можливих випадків несанкціонованого доступу до приватної чи комерційної інформації, інформації з обмеженим доступом, зростають випадки фішингу, DDOS-атак, інформаційних кібератак пов’язаних із маніпулюванням ситуації з COVID-19, актів кібершпигунства, витоку персональних даних громадян та інших злочинів у цій сфері. При цьому ми можемо спостерігати негативну тенденцію підвищення суспільної небезпеки зазначених діянь.

Жертвами кіберзлочинців стають не тільки пересічні громадяни, компанії чи установи, але й цілі корпорації, а також об’єкти критичної інфраструктури, та дедалі частіше - лікарні. Надзвичайною є загроза кібератак, що спрямовані на підрив нормального функціонування закладів охорони здоров’я в умовах пандемії. Так 12 березня 2020 року в результаті кібератаки на заклад охорони здоров’я «University Hospital» (м. Брно, Республіка Чехія) лікарня була змушена відкласти термінові хірургічні операції та перенаправити нових гострих пацієнтів до сусідніх відділень. Цього ж дня дві інші лікарні «Children’s Hospital» і «Maternity Hospital» також постраждали від хакерських атак [4]. В травні 2020 року в результаті кібератаки постраждав ряд об’єктів Національної системи охорони здоров’я (NHS) Великобританії. Хакери вимагали викуп за відновлення роботи комп’ютерних мереж медичних установ в період COVID-19 [5]. Зазначені кібератаки мають тенденцію до зростання і не завжди правоохоронні органи спроможні успішно протидіяти цим злочинним посяганням. Це викликає необхідність здійснення широкомасштабних, довгострокових, системних та науково – обґрунтованих запобіжних заходів як на державному, так і на транснаціональному рівні, що охоплюватиме організаційно – управлінський, кримінально – правовий, адміністративний, медичний та інші напрямки і передбачатиме:

1) удосконалення національного та міжнародного законодавства, що регулює протидію кіберзлочинності, з урахуванням нових сучасних ризиків викликаних захворюваністю на COVID-19. Динамічність поширення комп'ютерних технологій та їх метаморфози зобов'язують законодавця і правоохоронні органи, що протидіють комп'ютерній злочинності, збільшувати швидкість реакції на появу нових способів протиправної діяльності в даному напрямку, на випередження злочинів;

2) підвищення ефективності взаємодії між правоохоронними органами України і ряду зарубіжних країн. Чітка взаємодія, як форма взаємозв’язку та взаємної підтримки, значення якої важко переоцінити, полягає у тому, що правоохоронні органи у цілому, конкретні їх служби та структурні підрозділи

або працівники у взаємодії один з одним досягають значно більших результатів у менші строки із найменшими витратами сил;

3) посилення співпраці із спеціалізованими органами інших країн в питаннях протидії кіберзлочинності, що повинно проявлятися не лише в обміні досвідом, а також в проведенні спільних операцій, спрямованих на виявлення, попередження та розслідування будь-яких фактів кіберзлочинності, що мають міжнародний характер;

4) забезпечення правоохоронних органів, які уповноважені здійснювати заходи протидії кіберзлочинності новітніми засобами техніки на всіх рівнях роботи. Адже складність виявлення дій комп'ютерного злочинця полягає в його можливості скоювати злочини в кіберпросторі, у якого немає державних кордонів, що багаторазово збільшує ступінь їх суспільної небезпеки;

5) підвищення професіоналізму кадрового складу підрозділів, що займаються питанням протидії кіберзлочинності. Отримання і аналіз доказів у справах про злочини у сфері комп’ютерної інформації – одне з основних і важко вирішуваних на практиці завдань. Це вимагає не лише розробки тактики проведення слідчих і організаційних заходів, але і наявності спеціальних знань у сфері комп’ютерної техніки і програмного забезпечення, а також внесення поправок до чинного законодавства. Співробітники, які безпосередньо займаються розслідуванням даного роду злочинів, і працівники судової системи часто не володіють спеціальними знаннями у сфері нових комп’ютерних технологій, що часто ускладнює процес розслідування злочинів;

6) використання у діяльності підрозділів боротьби з кіберзлочинністю результатів наукових розробок з тематики, що стосується протидії кіберзлочинам. На практиці часто виникають помилки при кваліфікації та документуванні злочинних діянь, частими причинами чого є відсутність достатньої кількості методичних рекомендацій і роз’яснень із розслідування цих злочинів, узагальненої судової практики.

Список використаних джерел

1. COVID-19 Dashboard by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University (JHU). URL:

https://gisanddata.maps.arcgis.com/apps/opsdashboard/index.html?urUJ3qaOQGhVbzc6Z_muZ5mzCLU#/bda7594740fd40299423467b48e9ecf6 (дата звернення: 19.11.2020).

2. Коронавірус в Україні : офіційний інформаційний портал КМУ. URL: https://covid19.gov.ua/ (дата звернення: 19.11.2020).

3. Про запобігання поширенню на території України коронавірусу COVID-19 : Постанова КМУ від 11.03.2020 № 211 // Урядовий портал : єдиний вебпортал органів виконавчої влади України. URL: https://www.kmu.gov.ua/npas/pro-zapobigannya-poshim110320rennyu-na-teritoriyi-ukrayini-koronavirusu-covid-19 (дата звернення: 19.11.2020).

4. Cimpanu C. Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak // ZdNet : site. 13 march 2020. URL: https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/ (дата звернення: 19.11.2020).

5. Gayle D., Topping A., Sample I., Marsh S., Dodd V. NHS seeks to recover from global cyber-attack as security concerns resurface // The Guardian : site. 13 May 2017. URL: https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack (дата звернення: 19.11.2020).

Одержано 22.11.2020

УДК 340.132.83

Саніна-Мокренко Ольга Володимирівна
викладач-методист вищої кваліфікаційної категорії
Харківського фахового коледжу інформаційних технологій
Державного університету телекомунікацій
https://orcid.org/0000-0002-0696-2441
Мокренко Григорій Олексійович
викладач-методист вищої кваліфікаційної категорії
Харківського фахового коледжу інформаційних технологій
Державного університету телекомунікацій
https://orcid.org/0000-0001-8498-9706

ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАХОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУБ'ЄКТІВ РИНКУ ТЕЛЕКОМУНІКАЦІЙ В УМОВАХ ГЛОБАЛЬНОЇ ДІДЖИТАЛІЗАЦІЇ ІНФОРМАЦІЇ

У сучасному світі, в умовах прискорених інформаційних потоків, глобалізаційні процеси сучасної цивілізаційної епохи здебільшого набувають вияву в інформаційній сфері. Вони засновані на телекомунікаційному підґрунті

та спричиняють неоднозначні для життєдіяльності людини, суспільства й держави наслідки.

З використанням новітніх інформаційних технологій у кінці XX століття виникли глобальні системи масової комунікації,. Цьому сприяла діджитальна революція в інформаційних технологіях, яка призвела до глобальної (планетарної) діджиталізації інформації.

Діджиталізація – це способи приведення будь-якого різновиду інформації в цифрову форму [2, с. 259].

Отже, діджиталізація інформації – це трансформація (запис, обробка та передача) будь-якої інформації в цифрову форму за допомогою бінарнокодованих знаків, що використовуються у комп'ютерній техніці.

Конституцією України (ст. 3) безпеку людини проголошено найвищою соціальною цінністю, що визначає зміст і спрямованість діяльності держави [1].

В умовах переходу сучасної цивілізації до нової стадії свого розвитку – інформаційного суспільства – особливого значення набуває проблема забезпечення інформаційної безпеки людини у сфері телекомунікацій (електрозв'язку).

В контексті революційних змін у галузі телекомунікацій, розвитку мережі Інтернет, соціальних медіа, мобільної телефонії, стрімкої діджиталізації тощо, значно посилюється роль глобальної комунікації у таких сферах життєдіяльності людства, як культура, політика, економіка та кібербезпека.

Наразі діджитальна комунікація не лише заміщує безпосереднє спілкування між людьми, а й нестримно перетворюється на домінуючий у глобальних масштабах різновид соціальної взаємодії.

Саме телекомунікаційні послуги й технології, за допомогою яких діджитальна комунікація набуває реалізації, забезпечують як глобальний доступ до інформації, виступаючи своєрідним усесвітнім «посередником» у наданні та споживанні інформаційних послуг, так і реалізацію абсолютної більшості інших видів інформаційної діяльності (на жаль, і злочинного характеру в їх числі).

Узагальнюючи наявні закономірності, можна впевнено стверджувати, що нині інформаційне піднесення будь-якої нації засноване на телекомунікаційному підґрунті та спричиняє неоднозначні для буття людини, суспільства й держави наслідки [3, с. 2].

Обравши курс на євроінтеграцію, Україна поклала на себе також зобов'язання проводити ефективну комунікаційну політику.

Згідно Закону України «Про телекомунікації», споживач телекомунікаційних послуг (споживач) – юридична або фізична особа, яка потребує, замовляє та/або отримує телекомунікаційні послуги для власних потреб [4].

З огляду на масштабність і динамічність проникнення телекомунікацій у всі сфери життєдіяльності особи, суспільства та держави в процесі приєднання нашої країни до глобальної інформаційної цивілізації безперечної актуальності й вагомого практичного значення набуває системне відшукування та комплексне розроблення новітніх і донині не вивчених проблемних аспектів забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг в Україні.

В цьому контексті:

– *по-перше,* необхідно забезпечити інформаційну безпеку телекомунікаційних мереж (захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації);

– *по-друге*, налагодити ефективну комунікацію між усіма суб'єктами ринку телекомунікацій (оператори, провайдери телекомунікацій, споживачі телекомунікаційних послуг, виробники та/або постачальники технічних засобів телекомунікацій);

– *по-третє*, продумано впроваджувати системи електронного врядування як на національному, так і регіональному та місцевому рівнях, а також готувати для цього фахівців з необхідними цифровими навичками;

– *по-четверте*, враховуючи, що споживання телекомунікаційних послуг не лише заміщує життєву необхідність безпосереднього спілкування між людьми, а й нестримно перетворюється на домінуючий у глобальних масштабах різновид соціальної взаємодії, для роз'яснення суті діджитальної комунікації та пов’язаних з нею ризиків, необхідно впроваджувати у закладах освіти курси, спрямовані на формування у здобувачів освіти, як споживачів телекомунікаційних послуг, цифрової компетентності, яка сьогодні стає однією з найважливіших soft-skils, які потрібно розвивати для успішного формування цілісної цифрової культури особистості.

Список використаних джерел

1. Конституція України від 28.06.1996 № 254к/96-ВР // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 05.11.2020).

2. Куприна К. А., Хазанова Д. Л. Диджитализация: понятие, предпосылки возникновения и сферы применения. *Вестник научных конференций*. 2016. № 5-5 (9). Качество информационных услуг: по материалам международной научно-практической конференции (31 мая 2016 г., Тамбов). С. 259-262.

3. Сулацький Д. В. Організаційно-правові засади забезпечення інформаційної безпеки людини як споживача телекомунікаційних послуг : автореф. дис. ... канд. юрид. наук : 12.00.07 / Міжнар. ун-т бізнесу і права. Херсон, 2011. 20 с.

4. Про телекомунікації : Закон України від 18.11.2003 № 1280-IV // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1280-15t (дата звернення: 05.11.2020).

Одержано 11.11.2020

УДК 004.056.5
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 ПИТАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ, РЕАЛІЗОВАНІ В МОБІЛЬНІЙ ОПЕРАЦІЙНІЙ СИСТЕМІ ANDROID 11

У міру того, як смартфони стають швидше і розумніші, вони грають все більш важливу роль в нашому житті, виступаючи в якості нашої розширеної пам'яті, нашої зв'язку зі світом в цілому і часто будучи основним інтерфейсом для спілкування з друзями, родиною, різними соціальними мережами. Цілком природно, що в рамках цієї еволюції ми стали довіряти нашим телефонами свої персональні дані, конфіденційну інформацію і в багатьох відносинах ставитися до них як до розширення нашої цифрової та фізичної ідентичності.

Мобільна операційна система (ОС) Android відносно молода платформа, яка постійно привертає підвищену увагу кіберзлочинців. Як відомо, Android – це ОС, яка заробила свою репутацію за відносну відкритість в порівнянні з iOS. Вона дозволяє завантажувати APK файли (англ. Android Package – додатки для ОС Android) з будь–яких джерел. Користувач може налаштувати root–доступ на пристрої і встановити іншу систему на базі Android [1]. При цьому, чим більше активно модифікується ОС, тим більша ймовірність завдати шкоди вашому пристрою, ніж можуть з успіхом скористатися кіберзлочинці.

Однак, в останні роки розробниками були представлені досить ефективні поліпшення безпеки системи, наприклад, вбудований антивірус Google Play Захист. Тому резонно постає питання: чи потрібно встановлювати сторонній антивірус? Однозначно 15–20 років тому наявність додаткового засоби захисту було життєвою необхідністю, зараз часи змінилися, і сучасні операційні системи стали в значній мірі самодостатніми з точки зору безпеки.

Компанія Google в 2017 році представила систему безпеки Play Захист, яка використовує технології машинного навчання для сканування магазину

додатків Google Play на предмет шкідливих додатків. Google Play Захист також вміє аналізувати додатки локально на конкретному смартфоні. Користувач може активований перевірку вручну – для цього потрібно перейти в додаток Play Маркет> Мої додатки та ігри> Оновлення та натиснути іконку поновлення у верхній частині екрану [2]. Google Play Захист вбудована в сервіс Play Маркет, і за словами розробників «допомагає вам зберегти ваш пристрій в безпеки і недоторканності». Google Play Захист, по суті є пакетом програм безпеки, який не тільки сканує на предмет зараження вірусами і іншим шкідливим софтом додатки, завантажувані з Play Маркета, але також досліджує ваші вже встановлені додатки і ваш пристрій в комплексі.

За багато років Android перетворився в досить надійну ОС. Google Play Захист – це в цілому відмінна функція захисту, але вона не гарантує абсолютну безпеку. Іноді буває, що деякі шкідливі програми залишаються в магазині Play Маркет протягом півроку. Так, наприклад, в минулому році на майданчику були виявлені будильники і сканери QR кодів, які містили троян AsiaHitGroup – на той момент їх встигли завантажити кілька десятків тисяч користувачів. Цей троян виконував корисне навантаження з метою отримати повний доступ до пристрою і контроль над персональними даними користувача. Нове «що не видаляється» шкідливе програмне забезпечення xHelper заразило 45 000 Android пристроїв. Раніше в минулому році дослідники з компанії Trend Micro (це світовий лідер в області рішень для захисту корпоративних даних і кібербезпеки для бізнесу, центрів обробки даних) виявили в Google Play 36 фальшивих антивірусів, які встановлювали шкідливе програмне забезпечення на пристроях, викликали неправдиві попередження і показували рекламу. Ці додатки також схильні запитувати невиправдано велике число дозволів доступу з метою крадіжки персональних даних [3]. Також варто брати до уваги швидкість і фрагментацію процесу оновлення Android. У той час як пристрої на чистому Android (без надбудов) отримують оновлення безпеки відразу після виходу, відомо, що виробники деяких пристроїв з модифікованими версіями системи затримують вихід патчів на кілька днів або навіть тижнів.

Так само, як і Apple в своїй iOS 14, Google попрацювала над безпекою в своїй системі. Головні зміни стосуються сховища. Відтепер сторонні додатки не можуть отримувати доступ до папок Android/obb/ і Android/data/. Таке обмеження може, наприклад, ускладнити установку сторонніх програм з кешем. Крім цього, дозвіл на доступ до сховища перейменовано: тепер запитується доступ до файлів і медіа. Важливі зміни торкнулися і механізму дозволів. Так, в Android 11 користувач може надати одноразовий доступ додатки до місця розташування, мікрофона або камері. В системі з'явився автоматичне скидання деяких дозволів. Він відбувається, якщо конкретним додатком не користуватися кілька місяців. А кнопка «Відхилити» в діалоговому вікні дозволів на увазі під собою дію «Не питати знову». Крім того, APK додатків в Android 11 можна видавати одноразовий доступ до мікрофона, камери або даних про місцезнаходження [4]. Наступного разу, коли з додатком знадобиться доступ, воно запросить його знову. Якщо користувач давно запускав програму з раніше виданими набором дозволів операційна система автоматично їх відкличе, повідомивши про це. Зрозуміло, при необхідності права доступу можна буде відновити в будь-який момент.

Компанія Google ще в 10 версії Android змінила підхід до поширення оновлень в рамках Project Mainline. В останній Android 11 додані 12 додаткових модулів оновлення системи через Google Play. Таким чином, безпосередньо через магазин Play Маркет надходитиме більше виправлень, що стосуються безпеки та конфіденційності операційної системи. Крім того, вони будуть виходити частіше, і користувачеві не доведеться чекати виходу повного оновлення ОС.

Інша справа, якщо користувач завантажує APK додатки зі сторонніх джерел. В цьому випадку, вбудований в Android антивірус Google Play Захист вже не може допомогти. Якщо немає впевненості в надійності джерела додатки, то необхідно задуматися про встановлення антивірусу для Android, щоб дозволить забезпечити додатковий захист. Звідси випливає дуже проста порада – не завантажуйте додатки, якщо ви не впевнені в їх надійності та безпеки.

Шкідливе програмне забезпечення – це найсерйозніша загроза для безпеки Android, тому слід завжди перевіряти легітимність додатки до його завантаження.

Список використаних джерел

1. Как работает антивирус Google Play и как его отключить // Trashbox : сайт. 15.08.2017. URL: https://trashbox.ru/topics/112068/kak-rabotaet-antivirus-google-play-i-kak-ego-otklyuchit (дата звернення: 19.11.2020).

2. Представляем Android 11 // Android : сайт. URL: https://www.android.com/intl/ru_ru/security-center/ (дата звернення: 19.11.2020).

3. i-Intelligence GmbH : сайт URL: http://www.i-intelligence.eu (дата звернення: 19.11.2020).

4. Загальні рекомендації щодо зменшення наслідків від впливу шкідливого програмного забезпечення // CERT-UA: Computer Emergency Response Team of Ukraine : сайт. 21.07.2020. URL: https://cert.gov.ua/recommendation/2502 (дата звернення: 19.11.2020).

Одержано 21.11.2020

УДК 004.49

Семчук Андрій Олегович
курсант 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

ПОНЯТТЯ DDOS-АТАК ТА ЇХ КЛАСИФІКАЦІЯ

Атака на відмову в обслуговуванні (англ. Denial-of-Service attack – DoS attack. Якщо атака відбувається одночасно з великої кількості IP-адрес, то її називають розподіленою (англ. Distributed Denial-of-Service – DDoS). У розподіленій атаці на відмову одночасно можуть брати участь від кількох одиниць до кількох сотень тисяч, а іноді - кількох мільйонів хостів [1]. Мета атаки: зробити так, щоб система перестала працювати, і користувачі не могли отримати доступ до системних ресурсів. Щоб DDoS-атака була успішною, атакуючому потрібно посилати більше запитів, ніж може обробити сервер.

Види DDoS-атак

1. DDoS-атаки на рівні каналу зв'язку.

Такі DDoS-атаки включають в себе:

– UDP-флуд: Під час такої атаки сервер-жертва отримує величезну кількість підроблених UDP-пакетів від широкого діапазону IP-адрес. Сервер-жертва або мережеве обладнання перед ним переповнюється підробленими-UDP пакетами [2]. Через атаки займається вся смуга пропусків перевантажує мережеві інтерфейси;

– ICMP-флуд: Атакуючі направляють на сервер помилкові ICMP-пакети, які відправляються з широкого діапазону IP-адрес. В результаті такої атаки ресурси сервера вичерпуються і не можуть обробляти запити. Через це сервер перезавантажується або дуже повільно працює;

– ping-флуд: Атакуючі направляють на сервер помилкові ping-пакети з великого діапазону IP-адрес. Найбільший недолік цієї атаки для власників сайтів - те, що її можна переплутати зі звичайним трафіком.

2. DDoS-атаки на рівні протоколу

Цей тип атаки споживає ресурси сервера або іншого апаратного обладнання мережі під час обробки інформації. Це призводить до нестабільної роботи системи. У цих атаках сервера-мішені відправляють або більше пакетів, ніж він може обробити, або більше трафіку, ніж мережеві порти можуть обробити.

DDoS-атаки, що використовують уразливості протоколів, включають:

– пінг смерті: Серверу-жертві відправляється занадто великий пакет розміром більш 65535 байт, що призводить до помилок і відключення сервера. Цей вид атаки був дуже популярний в 90-х роках XX століття. Сьогодні такі атаки спрямовані на додатки або апаратне обладнання. В результаті такої атаки сервер перезавантажується або повністю ламається;

– синхронна атака: Атакуючі використовують уразливості TCP-протоколу в процесі рукостискання між клієнтом, хостом і сервером. Принцип атаки полягає в тому, що зловмисник, посилаючи запити на підключення, переповнює

чергу на сервері. Задача зловмисника полягає в тому, щоб підтримувати чергу заповненою таким чином, щоб не допустити нових підключень. Через це клієнти або не можуть встановити зв'язок з сервером, або встановлюють його з великими затримками.

3. DDoS-атаки на рівні додатків

Такі атаки зазвичай націлені проти додатків типу вебсерверів, наприклад, Windows IIS, Apache. Однак атаки на прикладному рівні вже поширюються і на CMS-платформи – WordPress, Joomla !, Drupal, Magento.

Мета такої атаки - вимкнути додаток, онлайн-сервіс або сайт. Зазвичай ці атаки невеликі, особливо в порівнянні з атаками на рівні мережі, але вони можуть завдати такої ж шкоди [2].

Атаки на рівні додатків включають:

– атаки на DNS-сервер: У результаті такої атаки за помилковими IP-адресами буде ходити не окремий клієнт-жертва, а всі користувачі, які звернулися до атакованому DNS. Для атаки хакер посилає запит, який змушує сервер звертатися до інших вузлів мережі і чекати від них відповіді. Відправивши запит, зловмисник починає атакувати DNS потоком помилкових відповідних пакетів. Коли сервер отримує помилкову відповідь пакет з підходящим ID, він починає сприймати хакера як DNS і дає клієнтові IP-адресу, надану атакуючим комп'ютером. Потім запит заноситься в кеш, і при наступних подібних запитах користувачі будуть переходити на підставний IP;

– Layer 7 HTTP-флуд: атака, яка перевантажує окремі частини сайту або сервера. Такі атаки складно ідентифікувати, оскільки запити виглядають як звичайний трафік. Запити, надіслані атакуючими, споживають ресурси сервера і призводять до падіння сайту [1]. Такі запити також можуть відправлятися ботами, що робить атаки більш потужними. Цікаво, те, що ці атаки мало залежать від пропускної здатності каналу. За рахунок цього атакуючі можуть легко вивести сервер з ладу. В залежності від вебсервера і стоку додатків навіть невелика кількість запитів в секунду може уповільнити роботу додатків і баз

даних серверної частини. В середньому атаки, які посилають більше ніж 100 запитів в секунду можуть вимкнути сайти середніх розмірів.

Все сказане дозволяє зробити висновок, що різні види атак можуть залишити різні цифрові сліди, а отже буде легше зрозуміти, де їх шукати.

Список використаних джерел

1. Світличний В. А. Дослідження атак на відмову в обслуговуванні інформаційно-телекомунікаційних систем // Кібербезпека в Україні: правові та організаційні питання : матеріали всеукр. наук.-практ. конф., м. Одеса, 30 листопада 2018 р. Одеса : ОДУВС, 2018. С. 88-89.

2. DDoS-атака: что это, как работает и виды атак // VPS.ua : сайт. 27.08.2018. URL: https://vps.ua/blog/ddos-attacks-and-their-types/ (дата звернення: 19.11.2020).

Одержано 21.11.2020

УДК 621.34

Скарбенчук Ірина Віталіївна
студентка 4 курсу факультету № 6
Харківського національного університету внутрішніх справ
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

АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В СУЧАСНИХ МЕРЕЖАХ РУХОМОГО ЗВ'ЯЗКУ

В основі забезпечення захисту інформації в мережах рухомого зв'язку лежать законодавчі та нормативно-правові норми, морально-етичні звичаї суспільства, організаційні та апаратно-програмні засоби та способи функціонального забезпечення інформаційної безпеки цифрових систем, каналів, мереж зв'язку.

Необхідно зауважити, що забезпечення надійного захисту інформації в мережах рухомого зв'язку перш за все, залежить від наявності певних чинників, які безпосередньо забезпечують та впливають на ступінь захищеності інформації в мережі, а саме:

– врахування особливостей відповідної технології зв’язку в процесі розробки необхідної моделі комплексного захисту інформації згідно способів та властивостей передавання/приймання фізичного сигналу, самого фізичного середовища – каналу, мережі, апаратно-програмних засобів цифрових систем зв’язку;

– наявність математичної моделі сигналу або каналу, в якій закладено параметри якісного і кількісного рівнів взаємозв’язку вхідного і вихідного сигналу.

У розвинених країнах світу продовжується перехід до інформаційної сервісно-технологічної економіки. Враховуючи особливості кожного стандарту необхідно використовувати притаманні лише йому технології, методи та засоби захисту інформації.

Найпоширенішим стандартом стільникового зв’язку в Україні є стандарт зв'язку четвертого покоління LTE (Long Term Evolution), який вважається перспективним. За даними, наприклад компанії HUAWEI, LTE забезпечує швидкість до 326,4 Мбіт/с від базової станції до користувача і до 172,8 Мбіт/с у зворотному напрямку.

З точки зору безпеки таких LTE мереж враховуючи різні технології ускладнює пошук її вразливостей. В мережах 4G весь трафік проходить через єдину архітектуру EPC (Evolved Packet Core) за протоколом IP.

З фізичної точки зору в мережах LTE використовуються великі смуги частот, високорівнева модуляція сигналу, технологія MIMO (Multiple Input Multiple Output) яка дозволяє збільшити смугу пропускання каналу, при якому для передачі даних використовуються дві і більше антени і така ж кількість антен для прийому. Разом вони забезпечують адекватну завадостійкість, високі швидкості передачі даних і ємність мережі. Важливою особливістю мережі 4G є те, що з її архітектури зникло поняття контролера радіомережі (RNC), який в 3G виконував основну функцію з управління комунікаційними ресурсами. Тому базові станції в LTE стали більш інтелектуальними і самостійними - вони отримали можливість маршрутизувати трафік, що дозволило організовувати

з'єднання між абонентами безпосередньо, минаючи ядро мережі. Щоб звести до мінімуму атаки на конфіденційну інформацію, базова станція повинна забезпечити виконання таких важливих операцій, як кодування та розшифрування користувачів даних, а також зберігання ключів.

Стандарт LTE виділяє п'ять основних груп безпеки це, насамперед:

– архітектура безпеки мережі повинна забезпечити користувачів надійним доступом до сервісів і захист від атак на інтерфейси;

– мережевий рівень повинен дозволяти вузлам мережі безпечно обмінюватися як даними користувачів, так і керуючими даними і забезпечувати захист від атак на провідні лінії;

– користувальницький рівень повинен забезпечувати безпечний доступ до мобільного пристрою;

– рівень додатків повинен гарантувати безпечний обмін повідомленнями;

– видимість і можливість зміни налаштувань безпеки повинна дозволяти користувачеві дізнаватися, чи забезпечується безпека і включати різні режими для її забезпечення.

Щодо методів захисту, необхідно зауважити, що багатьма країнами та операторами стільникового зв’язку активно використовується шифрування (RSA), яке в подальшому вимагає коди автентифікації абонента. З точки зору безпеки таких LTE мереж враховуючи різні технології ускладнює пошук її вразливостей. В мережах 4G весь трафік проходить через єдину архітектуру EPC (Evolved Packet Core) за протоколом IP.

З фізичної точки зору в мережах LTE використовуються великі смуги частот, високорівнева модуляція сигналу, технологія MIMO (Multiple Input Multiple Output) яка дозволяє збільшити смугу пропускання каналу, при якому для передачі даних використовуються дві і більше антени і така ж кількість антен для прийому. Разом вони забезпечують адекватну завадостійкість, високі швидкості передачі даних і ємність мережі.

Важливою особливістю мережі 4G є те, що з її архітектури зникло поняття контролера радіомережі (RNC), який в 3G виконував основну функцію з

управління комунікаційними ресурсами. Тому базові станції в LTE стали більш інтелектуальними і самостійними - вони отримали можливість маршрутизувати трафік, що дозволило організовувати з'єднання між абонентами безпосередньо, минаючи ядро мережі.

Щоб звести до мінімуму атаки на конфіденційну інформацію, базова станція повинна забезпечити виконання таких важливих операцій, як кодування та розшифрування користувачів даних, а також зберігання ключів.

Стандарт LTE виділяє п'ять основних груп безпеки це, насамперед:

– архітектура безпеки мережі повинна забезпечити користувачів надійним доступом до сервісів і захист від атак на інтерфейси;

– мережевий рівень повинен дозволяти вузлам мережі безпечно обмінюватися як даними користувачів, так і керуючими даними і забезпечувати захист від атак на провідні лінії;

– користувальницький рівень повинен забезпечувати безпечний доступ до мобільного пристрою;

– рівень додатків повинен гарантувати безпечний обмін повідомленнями;

– видимість і можливість зміни налаштувань безпеки повинна дозволяти користувачеві дізнаватися, чи забезпечується безпека і включати різні режими для її забезпечення.

Список використаних джерел

1. Ткаченко О. С., Тулупов В. В. Безпечне використання сучасного стандарту LTE у мережах рухомого зв’язку // The 1st International scientific and practical conference «Science, society, education: topical issues and development prospects» (December 16-17, 2019) SPC «Sci-conf.com.ua». Kharkiv : 2019. С. 276-280. URL: https://sci-conf.com.ua/wp-content/uploads/2020/01/science-society-education_topical-issues-and-development-prospects_16-17.12.2019.pdf (дата звернення: 12.11.2020).

Одержано 20.11.2020

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
Загорецька Єлизавета Романівна
курсантка 1 курсу факультету № 4
Харківського національного університету внутрішніх справ

РОЗВИТОК ФІШИНГ-АТАК ТА МЕТОДІВ БОРОТЬБИ З НИМИ

Як відомо, на сьогоднішній день, кількість технічних пристроїв (комп'ютерів, планшетів, смартфонів тощо) стала значно переважати кількість людей. Розвиток інтернет-ресурсів і сервісів, що надаються користувачам, провокує злочинців переходити в кіберпростір для здійснення різних протизаконних дій з метою отримання особистої вигоди. Одним з популярних видів злочинів в цій області став фішинг.

Фішинг (англ. Phishing, від fishing – риболовля, видобування і password - пароль) – вид інтернет-шахрайства, мета якого – отримати ідентифікаційні дані користувачів. Сюди відносяться крадіжки паролів, номерів кредитних карт, банківських рахунків та іншої конфіденційної інформації [1, 2] Собівартість однієї фішинг-атаки становить до 2 тисяч доларів, а прибуток, одержуваний шахраями, може досягати десятків тисяч [2]. Особливістю фішингу є те, що жертва шахрайства надає свої конфіденційні дані добровільно. Аби досягти мети, хакери використовують різні інструменти: фішингові сайти, e-mail розсилку, фішингові landing page, спливаючі вікна, таргетовану рекламу. Найбільш часті жертви фішингу – це банки, електронні платіжні системи, аукціони.

Крадіжка конфіденційних даних – не єдина небезпека, що виникає при фішинг-атаці. Дуже часто, слідуючи за шкідливим посиланням, можна отримати програму-шпигуна, кейлоггер або троян. На початку 2016 року, згідно зі статистикою сайту PhishMe, в 93 % фішингових листів шахраї надсилали шкідливі програми [3].

В залежності від цілей кіберзлочинців, об'єктів атаки і використаних технічних засобів і методів, прийнято виділяти такі види фішингу [4]:

1. Цільовий фішинг – атаці піддаються «цінні» жертви і компанії. Цільовий фішинг дуже ефективний, так як атака відбувається з урахуванням індивідуальних особливостей одержувача.

2. Уейлінг-шахрайство – це фішингова атака, націлена на топ-керівництво компанії. Інформація, яку вони можуть вкрасти, цінніше, ніж та, яку може запропонувати звичайний працівник.

3. Компрометація корпоративної пошти – це злом / підміна корпоративної пошти співробітників вищого ешелону управління.

4. Клонований фішинг – це копіювання справжніх повідомлень. «Шкідливий» лист відправляється з пошти, яка схожа на пошту справжнього відправника, а тіло листа виглядає в точності, як попереднє повідомлення від нього ж з прикріпленим «шкідливим» файлом або посиланням.

5. Вішинг – це фішинг за телефоном. Зазвичай жертва отримує голосове повідомлення нібито від фінансової установи.

6. Фармінг – це шахрайство через офіційні вебсайти. Фармери замінюють на серверах DNS цифрові адреси легітимних вебсайтів на адреси підроблених, в результаті чого користувачі перенаправляються на сайти шахраїв.

7. SIM-Jacking – це активація номера «жертви» на інший SIM-карті, якою володіє злочинець. Шахраї зв'язуються з колл-центром мобільного оператора жертви і переконують їх у тому, що "сімка" зламана і що необхідно перенести телефонний номер на іншу карту– ту саму, якою вже володіє зловмисник [1].

Серед ефективних методів боротьби з фішингом можна виділити наступні:

1. Антивірус з останньої базою антивірусів. Як правило, у всіх сучасних антивирусах передбачений захист від шпигунських і шкідливих програм. Соціальні мережі і браузери також попереджають користувачів про перехід на підозрілий сайт.

2. Використання захищеного з'єднання https. Необхідно перевіряти сертифікат для HTTPS при встановленні з'єднання.

3. Контроль адресного рядка посилання. Незначні зміни в електронній адресі можуть привести на абсолютно інший сайт.

4. Не використовувати точки доступу громадського Wi-Fi для входу в банківські акаунти. Шахраї можуть перехопити ваші особисті дані. Краще скористатися мобільним інтернетом або захищеним з'єднанням.

5. Не відкривати листи з невідомих адрес, які «тиснуть на емоції» або носять екстрений характер.

В останні роки кількість випадків фішингу йде на спад. Це пов'язано з тим, що великі компанії приділяють все більше уваги захисту конфіденційних даних користувачів. Кілька років тому була створена Anti-Phishing Working Group (APWG) – група з боротьби з фішингом, в яку входять як компанії- «мішені» фішерів, так і компанії, які розробляють анти-фішингове / анти-спамерське програмне забезпечення. В рамках діяльності APWG проводяться ознайомчі заходи для користувачів, також члени APWG інформують одна одну про нові фішерських сайтах і погрози.

Список використаних джерел

1. Чорненький Р. Фишинг в 2019 году: какие виды угроз будут преобладать и как от них защититься? // Delo.ua : сайт. 22.02.2019. URL: https://delo.ua/special/fishing-v-2019-godu-kakie-vidy-ugroz-budut-preob-350360/ (дата звернення: 19.11.2020).

2. Что такое фишинг и фишинговая атака // HOSTiQ : сайт. URL: https://hostiq.ua/blog/internet-phishing/ (дата звернення: 19.11.2020).

3. PhishMe: Q1 2016 Sees 93 % of Phishing Emails Contain Ransomware // Businesswire : сайт. 06.06.2016. URL: https://www.businesswire.com/news/home/20160606005677/en/PhishMe%C2%A0Q1-2016-Sees-93-Phishing-Emails-Ransomware (дата звернення: 19.11.2020).

4. Как распознавать различные виды фишинговых атак // vps.ua : сайт. 13.11.2017. URL: https://vps.ua/blog/how-to-identify-phishing-attacks/ (дата звернення: 19.11.2020).

Одержано 19.11.2020

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

ТЕХНОЛОГІЯ ОТРИМАННЯ ЦИФРОВОГО ВІДБИТКУ ПРИСТРОЮ ЯК СПОСІБ ІДЕНТИФІКАЦІЇ ОСОБИ В МЕРЕЖІ ІНТЕРНЕТ

Однією з найважливіших задач, що постає перед кіберполіцією, є ідентифікація користувача в мережі Інтернет. Актуальність цієї задачі обумовлена необхідністю ідентифікації суб'єктів мережі з метою подальшого оперативного виявлення місцезнаходження злочинців. Метою доповіді є визначення способу ідентифікації, що дозволяє підвищити достовірність ототожнення користувачів з наявними записами в базі даних інформаційного ресурсу.

Для сучасних інформаційних систем застосовуються способи ідентифікації, засновані на зберіганні IP-адрес комп'ютерів відвідувачів сайту і записі на комп'ютер користувача даних Cookie. До недоліків першого способу відноситься широка поширеність динамічних IP-адрес, що виділяються з пулу провайдера в момент підключення користувача, а також можливість використання мереж проксі-серверів, анонімайзерів і механізму NAT (Network Address Translation), що знижує ступінь достовірності ідентифікації користувача. Недоліком другого способу є прив'язка Cookie до конкретного браузеру, що знижує вірогідність ідентифікації при використанні декількох браузерів. Іншим недоліком використання даної технології є можливість підміни і знищення даних Cookie, а також можливість відключення самого механізму користувачем. Таким чином, обидва способи не дозволяють в ряді випадків досягти необхідного ступеня достовірності ідентифікації.

Але існує інший спосіб ідентифікації користувачів. Він характеризує робоче середовище користувача й називається технологією отримання цифрового відбитку пристрою (Fingerprint). Fingerprint збирає всі унікальні налаштування і дані про браузер, операційну систему й апаратну частину комп'ютера, групує їх в єдиний рядок, робить з них ідентифікатор й хешує його. Отриманий хеш і є цифровим відбитком пристрою. Основною сферою використання даної технології є налаштування персоналізованої реклами, аналітика, захист від шахрайства.

Для цього при кожному відвідуванні користувача сайту за допомогою вбудованих скриптів для відстеження збираються такі дані:

1. Рядок-ідентифікатор User Agent, який містить у собі назву браузера та його версію, інформацію про операційну систему, мову та кодування.

2. Набір плагінів браузера, визначаються за допомогою технології Javascript.

3. Найменування операційної системи та її версії, визначення якої засноване на аналізі пакетів TCP-протоколу.

4. Список встановлених шрифтів, зібраний за допомогою фреймворка ActiveX і мультимедійної платформи Flash.

5. Параметри екрану, які визначаються за допомогою мови програмування Javascript та CSS.

6. Часовий пояс, що визначається за допомогою технології Javascript.

7. Параметри відеокарти, які визначаються за допомогою Canvas Fingerprint.

8. Рядок-ідентифікатор ETag (кеш-браузера).

9. MAC-адреса – визначається за допомогою мови програмування Java.

Всі зібрані ознаки можна розділити на програмні і апаратні. До апаратних можна віднести MAC-адресу, одержану за допомогою технології Java, а також інформацію про параметри відеокарти, отриману за допомогою унікальності відтворення відеокартою тіней та шрифтів. До програмних – всі інші.

Сукупність перерахованих ознак (ідентифікаторів) отримала назву кортежу. Іменований кортеж ознак, що відноситься до конкретного користувача, в даній роботі називається профілем користувача. Очевидно, що та чи інша ознака в різній мірі сприяє процесу ототожнення кортежу з тим чи іншим профілем.

До мінусів використання такої технології ідентифікації слід віднести те, що вона тягне за собою збільшення обсягу трафіку, що призводить до зростання часу завантаження сайтів.

Але дослідження впливової американської правозахисної організації Electronic Frontier Foundation, що була створена з метою захисту закладених у Конституції США і Декларації незалежності прав у зв'язку з появою нових технологій зв'язку, в рамках проєкту Panopticlick показало, що унікальність методу отримання цифрового відбитку пристрою для ідентифікації складає близько 94%.

Технологію цифрового відбитку для ідентифікації користувачів використовує сайт президента США (www.whitehouse.gov), сайт міжнародної платіжної системи з провідними технологіями для здійснення захищених платежів MasterCard, а також сервіси Google та Amazon.

Таким чином, з урахуванням вищевикладеного, вважаємо за доцільне використання технології отримання цифрового відбитку пристрою в підрозділах кіберполіції Національної поліції України з метою ідентифікації підозрюваних осіб.

Список використаних джерел

1. Alejandro Gómez-Boix, Pierre Laperdrix, Benoit Baudry. Hiding in the Crowd: an Analysis of the Effectiveness of Browser Fingerprinting at Large Scale: The 27th International World Wide Web Conference, Lyon, France, 2018. Pp. 1-10.

2. Sami Azam, Navpreet Kaur, Krishnan Kannoorpatti, Kheng Cher Yeo, Bharanidharan Shanmugam. Browser Fingerprinting as user tracking technology: The 11th International Conference on Intelligent Systems and Control (ISCO) Coimbatore, India, 2017. Pp.103-111.

3. Pierre Laperdrix, Nataliia Bielova, Benoit Baudry, Gildas Avoine. Browser Fingerprinting: A survey: eprint arXiv:1905.01051, 2019. 32 p.

Одержано 17.11.2020

УДК 378.091.3:159.9-051
Супрун Дар'я Миколаївна
доктор пед. наук, професор,
професор кафедри спеціальної психології та медицини факультету спеціальної та інклюзивної освіти Національного педагогічного університету ім. М. П. Драгоманова
https://orcid.org/0000-0003-4725-094X

ФОРМУВАННЯ ІНШОМОВНОЇ КОМПЕТЕНЦІЇ ПРАЦІВНИКІВ ПРАВООХОРОННИХ ОРГАНІВ В УМОВАХ ВІРТУАЛЬНОГО ОСВІТНЬОГО ПРОСТОРУ – ВИМОГА СЬОГОДЕННЯ

Тенденції розвитку світового суспільства зумовлюють істотне посилення уваги до проблеми інноваційного (перетворювального) потенціалу особистості. Сучасна психолого-педагогічна наука розглядає професійну сферу самоздійснення фахівця як інтеграцію загальних сфер самозростання людини: інтелектуальної, моральної, духовно-культурної у контексті трансформації професійної підготовки в умовах інтенсифікації та інтернаціоналізації вищої освіти в умовах віртуального освітнього простору, що забезпечується першочерговою вимогою включення до професійної підготовки іншомовного аспекту.

У сучасних умовах віртуального освітнього простору знання іноземної мови є засобом успішної професійної та наукової діяльності, а рівень володіння нею виступає одним з показників становлення професійної культури особистості. Доцільною і методично виправданою є професійна, комунікативно-спрямована підготовка з іноземної мови, кінцева мета якої відповідає окресленим уявленням про майбутню професійну діяльність (предметність діяльності), стимулює відповідними заходами потребу у вивченні іноземної мови (вмотивованість діяльності), призводить у співзвуччя навчальну діяльність іноземною мовою з особистою метою (цілеспрямованість діяльності), а також сприяє актуальному усвідомленню необхідності вивчення іноземної мови як запоруки стати освіченою, культурною, професійною, конкурентноспроможною та успішною людиною (усвідомленість діяльності) [4, с. 108].

Сучасне навчання іноземній мові в умовах віртуального освітнього простору – це цілісний процес, система, яка складається з цілого ряду підсистем, кожна з яких виконує свою функцію. Кожен етап навчання має свою специфіку. Ця специфіка проявляється в лінгвістичному і психологічному планах. У першому – матеріал змінюється за структурою, складністю змісту. Щодо другого – передбачається розвиток мотиваційних компонентів діяльності, вдосконалення процесів і операцій мислення, формування професійних інтересів. Основними питаннями у застосуванні інноваційних технологій є структура навчальних комп'ютерних програм, їх зміст і оптимальна організація Web-простору.

Комп'ютеризоване навчання іноземним мовам має цілий ряд переваг. Наведемо деякі з них: можливість вийти за межі традиційних методів навчання; розширення можливостей використання різних систем аналізаторів в процесі роботи; створення різноманітних ситуацій спілкування; підвищення інтересу й загальної мотивації до навчання завдяки новим формам роботи; індивідуалізація навчання (кожен працює в режимі, який його задовольняє) та об'єктивність контролю; формування вмінь та навичок для різноманітної творчої діяльності; виховання інформаційної культури; оволодіння навичками оперативного прийняття рішень у складній ситуації тощо. Використання віртуального освітнього простору націлене на створення повністю англомовного середовища, тому не передбачає у формулюванні завдань (Tasks) до вправ і в обговоренні дискусивних питань (Dilemma & Discuss) використання рідної мови. Вправи презентуються за допомогою інноваційних комп'ютерних технологій і спрямовані на розвиток лексичних, граматичних та комунікативних навичок. Складовою забезпечення впровадження в роботу викладачів і психологів освітніх установ сучасних технологій навчання є розробка транс- і міждисциплінарних спецкурсів, таких як «Management – a component of psychologists' professional training (Менеджмент – складова професійної підготовки психологів)», який має систему методичного поділу за цільовим призначенням (Themes and materials for studies, Language skills, Career

skills, Vocabulary, Dilemma & Discuss, Listening etc.). Запропонований спецкурс впроваджується також з застосуванням основних видів комп'ютерних навчальних програм (поетапне читання, реконструкція тексту, Conversation Techniques, Self-Discovery, Pieces of Good Advice, Puzzle Stories, «Learn to Speak English», «Tell me more», «Business English» тощо.

Беззаперечно, що інтернаціоналізація стимулює розвиток вітчизняної Вищої школи. Вагомий внесок в позитивні зрушення робить загальна тенденція професійної підготовки фахівців з належним рівнем розвитку управлінських вмінь та навичок і відповідною англомовною комунікативною компетенцією, що уможливить їх конкурентоздатність на світовому рівні. Вважаємо за необхідне впровадження зазначених аспектів при професійній підготовці. Підтверджуються наявні суперечності між суспільними вимогами до компетентності фахівців в контексті європейської інтеграції та традиційним підходом до організації професійноорієнтованої підготовки кадрів правоохоронних органів іноземною мовою в умовах віртуального освітнього простору. Відтак підготовка зазначеної категорії потребує суттєвої науково обґрунтованої модернізації, зокрема, запровадження окремих on-line спецкурсів, тренінгів, мастер-класів іноземною мовою, що уможливить вирішення актуальних завдань щодо інтеграції до Європейського простору загалом, та відповідності чинної системи підготовки кадрів досліджуваної категорії фахівців щодо кращих світових зразків та провідних тенденцій, зокрема [1, с. 2].

Список використаних джерел

1. Синьов В. М., Пометун О. І., Кривуша В. І., Супрун М. О. Основи теорії виховання : навч. посіб. Київ : МП «Леся», 2000. 140 с.

2. Супрун Д. М. Професійна підготовка психологів в галузі спеціальної освіти : монографія. Київ : Вид-во НПУ імені М. П. Драгоманова, 2017. 392 с.

3. Супрун Д. М. Теорія та практика професійної підготовки психологів в галузі спеціальної освіти : дис. ... д-ра пед. наук: 13.00.03. Київ, 2018. 657 с.

4. Супрун Д. М. Management – a component of psychologists' professional training (Менеджмент – складова професійної підготовки психологів) : навч.-метод. посіб. для студентів, слухачів магістратури та практикуючих психологів. Київ : Вид-во НПУ ім. М. П. Драгоманова, 2016. 250 с.

Одержано 20.11.2020

УДК 351.74(477)(075.8)
Федоренко Оксана Анатоліївна
молодший науковий співробітник
наукової лабораторії з проблем протидії злочинності ННІ № 1
Національної академії внутрішніх справ
https://orcid.org/0000-0002-4048-5060

ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ДІЯЛЬНІСТЬ ПРАВООХОРОННИХ ОРГАНІВ

Глобалізація та інформаційна ера змінили спосіб нашого життя та роботи в суспільстві. Характер загрози, з якою ми стикаємось сьогодні, складніший, ніж будь-коли в історії. Злочинні організації вільно пов'язані між собою мережею людей, які ховаються під, здавалося б, нормальним життям, чекаючи майже безмежних можливостей створити хаос і страх у суспільстві. Громадська безпека та ефективне правозастосування повинні бути залучені до інноваційного процесу, щоб не відставати від кримінальних проблем [1].

Згідно Закону України «Про національну програму інформатизації» у ст. 1 інформаційна технологія - це цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування [2].

Інформаційне забезпечення органів поліції – це комплекс методів, заходів, засобів різного характеру, які забезпечують створення та функціонування інформаційних технологій, а також їх ефективне використання для вирішення покладених на поліцію завдань. Інформаційні підсистеми як складові системи інформаційного забезпечення призначені для збирання, накопичення, зберігання та обробки інформації з певних напрямів обліків і орієнтовані на використання в діяльності більшості правоохоронних структур, мають загальний характер і належать до загальновідомих інформаційних систем [3]

Основними тенденціями розвитку інформаційних технологій у правоохоронній сфері є: 1) удосконалення форм та методів управління

системами інформаційного забезпечення; 2) централізація та інтеграція комп'ютерних банків даних; 3) впровадження новітніх комп'ютерних інформаційних технологій для ведення кримінологічних та криміналістичних обліків; 4) розбудова та широке використання ефективних та потужних комп'ютерних мереж; 5) застосування спеціалізованих засобів захисту інформації; 6) налагодження ефективного взаємообміну кримінологічною інформацією на міждержавному рівні. Все це забезпечує суттєве підвищення рівня боротьби зі злочинністю [4].

Розвиток інформаційних систем в Україні на сучасному етапі можна охарактеризувати як низький і прийти до висновку, що впроваджені інформаційні системи на сьогодні не здатні в повному обсязі реалізувати своє призначення у процесі діяльності правоохоронних органів, тому їх вдосконалення набуває набуває особливої актуальності

Використання інформаційних технологій, наприклад, у криміналістиці сприяють швидкому поширенню даних на великі відстані. Тому IT-інструменти дозволяють поліції та іншим службам реагувати швидше на події. Завдяки технології вирішення цієї проблеми, Forensic Pathways дозволяє поліції проаналізувати загальну картину. Зібрані дані, підключені до мережі, дозволяють аналітикові одночасно бачити підключення тисяч мобільних пристроїв та зв'язок між ними. Ця технологія виходить за рамки здатності мозку представляти зв'язки, які зазвичай важко підхопити.

Україна, обравши євроінтеграційний курс, має орієнтуватися на стратегію розвитку країн-учасниць Європейського Союзу в усіх напрямах життєдіяльності суспільства, зокрема в інформаційній сфері.

Серед основних європейських нормативно-правових актів, що регулюють суспільні відносини у сфері побудови інформаційного суспільства - Окінавська хартія глобального інформаційного суспільства від 22 липня 2000 року. У преамбулі даного міжнародного договору зазначається, що «…інформаційне суспільство дозволяє людям ширше використовувати свій потенціал та реалізовувати свої спрямування».

Значну увагу в даному документі приділяється допомозі становленню інформаційного суспільства і входженню до глобального інформаційного простору країнам, що розвиваються. Зазначається, що держави, які не встигають за високими темпами розвитку ІТ, позбавлені можливостей у повному обсязі брати участь у житті інформаційного суспільства та економіки. Для вирішення цієї проблеми необхідно враховувати різнорідність умов та потреб цих країн. Важливу роль при цьому мають відігравати власні ініціативи щодо прийняття послідовних національних програм з метою реалізації політичних заходів, спрямованих на підтримку ІТ та конкуренції у цій сфері, а також створення нормативної бази, використання ІТ в інтересах вирішення завдань у сфері розвитку і в соціальній сфері, розвитку людських ресурсів, що мають навички роботи з ІТ [5].

Список використаних джерел

1. Brakujące połączenie – wykorzystanie technologii informacyjnej przez terrorystów // Mediarecover : сайт. 27.04.2014. URL: https://mediarecovery.pl/brakujace-polaczenie/ (дата звернення: 18.11.2020).

2. Про національну програму інформатизації : Закон України від 04.02.1998 № 74/98-ВР // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80 (дата звернення: 18.11.2020).

3. Шорохова Г. М. Організаційно-правові аспекти використання сучасних інформаційних технологій в службовій діяльності територіальних органів поліції. *Порівняльно-аналітичне право*. 2017. № 3. С. 169-172.

4. Кудінов В. А., Смаглюк В. М., Ігнатушко Ю. І., Іщенко В. А. Інформаційні технології в правоохоронній діяльності : посібник. Київ : НАВСУ, 2013. 82 с.

5. Мирошниченко О. В. Сучасний стан та перспективи розвитку інформаційного забезпечення України : лекція з дисципліни «Інформаційні системи та інформаційне забезпечення правоохоронної діяльності». Дніпро : ДДУВС. 2019. 16 с. URL: https://dduvs.in.ua/wp-content/uploads/files/Structure/ library/student/ lectures/2020/eib/re/z004.docx (дата звернення: 18.11.2020).

Одержано 18.11.2020

Наукове видання

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Збірник матеріалів

круглого столу

(09 грудня 2020 року, м. Харків)

Відповідальні за випуск: *П. С. Клімушин*

Коригування списків бібліографічних посилань: *О. М. Рвачов*

Комп'ютерне верстання: *П. С. Клімушин, О. М. Рвачов*

Формат 60х84/16. Папір офсетний. Гарнітура Times ET. Умов. друк. арк. 7,67.
Наклад 60 прим. Замов. № 1216/10-20. Ціна договірна.

Надруковано з готових оригінал-макетів у друкарні ФОП Петров В. В.
Єдиний державний реєстр юридичних осіб та фізичних осіб-підприємців.
Запис № 2400000000106167 від 08.01.2009 р.
61144, м. Харків, вул. Гв.Широнінців, 79в, к. 137, тел. (057) 78-17-137.
e-mail:bookfabrik@mail.ua