МВС України

Харківський національний університет внутрішніх справ

Кафедра кібербезпеки та DATA-технологій

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Матеріали

Круглого столу

м. Харків, 14 грудня 2021 року

Харків

2021

УДК [351.74:004] (477)(08)
ББК 67.9(4УКР)301.163я43
Н 34

ОРГКОМІТЕТ:

голова – ректор генерал поліції третього рангу Сокуренко В.В.;
заступник голови – перший проректор полковник поліції Швець Д.В;
секретар – професор кафедри кібербезпеки та DATA-технологій факультету № 6 Струков В.М.;
члени оргкомітету:

- декан факультету № 6 Брусакова О.В.;
- завідувач кафедри кібербезпеки та DATA-технологій факультету № 6 Гнусов Ю.В.;
- начальник відділу організації наукової діяльності та захисту інтелектуальної власності капітан поліції Абламський С.Є.;
- начальник інформаційно-технічного відділу Полховський О.М.;
- начальник відділу зв'язків з громадськістю Щербакова І.В.

Друкується за рішенням оргкомітету відповідно до доручення Харківського національного університету внутрішніх справ від 10 вересня 2021 року

Застосування інформаційних технологій у діяльності правоохоронних органів: матеріали круглого столу, м. Харків, 14 грудня 2021 р. / МВС України, Харк. нац. ун-т внутр. справ. Харків: ХНУВС, 2021. 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.

ЗМІСТ

УДК [351.74(100):004.9](075.8)

СОКУРЕНКО ВАЛЕРІЙ ВАСИЛЬОВИЧ

доктор юридичних наук, професор,

член-кореспондент Національної академії правових наук України,

заслужений юрист України,

ректор Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРАВООХОРОНІЙ ДІЯЛЬНОСТІ

Використання сучасних технологій правоохоронними структурами дає нові можливості щодо забезпечення безпеки громадян, але містить у собі загрозу правам і свободам людини.

Впровадження цифрових технологій у поліцейську діяльність багато в чому зумовлене необхідністю протистояти злочинному світу, який дедалі краще озброюється. Кримінальний світ активно використовує останні досягнення четвертої промислової революції: технології блокчейну, дрони, штучний інтелект (ШІ) тощо, а наслідки злочинів стають все більш масштабними та тяжкими, що необхідно враховувати у роботі поліції. До сучасних поліцейських структур висувається нова вимога — бути відкритими та прозорими для громадян. Застосування цифрових технологій дозволяє поліції ефективно виконувати свої прямі функції, а також підвищити довіру громадян і знизити ймовірність корупції.

Щоб ефективно боротися і з традиційною, і з кіберзлочинністю, правоохоронним органам не можна відставати, а краще йти на крок перед правопорушниками у використанні технічних досягнень. Перевагою поліції будуть насамперед збирання та обробка величезного обсягу даних, багато з яких накопичуються вже зараз, але не обробляються і не використовуються. При цьому на перший план виходить предиктивна поліцейська діяльність (predictive policing).

Основні етичні проблеми предиктивної поліцейської діяльності пов'язані не так з інформаційними, як із соціальними технологіями, зокрема з методами

збору даних та прийняттям рішень про долю громадян, для яких ШІ передбачив високу ймовірність скоєння злочину.

На Заході поліцейські служби та судові органи активно розробляють та використовують окремі елементи цифровізації та цілі системи ШІ. За даними Інтерполу та Європолу більш ніж у 70 країнах поліцейські практично використовують ті чи інші види предиктивної аналітики.

Крім вузькоспрямованих систем ШІ для поліцейської роботи створюються універсальні комплексні системи, які допомагають при розслідуванні та запобіганні злочинам.

На замовлення Євросоюзу міжнародна команда вчених розробила і в 2013 році запустила систему ePOOLICE (early Pursuit against Organized crime using environmental scanning, the Law and IntelligenCE systems). Система сканує сторінки сайтів, електронну листування, поліцейську інформацію з метою знайти ознаки діяльності організованої злочинності та оцінює ризик скоєння злочину. Для аналізу використовується відео, текстовий контент, фінансові дані, інформація із соціальних мереж, чатів тощо.

Вплив впровадження ШІ та інших цифрових технологій на чисельність поліції. Здається, що цифровізація значно скоротить штат поліції, як це відбувається, наприклад, у банківських структурах. Однак завдяки розширенню та ускладненню системи відеоспостереження поліція отримуватиме суттєво більше інформації про протиправні дії, яким треба давати кримінально-процесуальну оцінку. Потрібно збільшити штат оперативних працівників, дізнавачів, слідчих, експертів. Вже зараз потрібно підготувати багато аналітиків великих даних.

Критерії, які поліція використовує при зборі інформації про громадян за допомогою інструментів ШІ. Важливим є консенсус між поліцією та громадянським суспільством щодо цілей використання цих даних. Якщо йдеться про запобігання та розкриття тероризму, корупції, інших злочинів, то такий консенсус можна досягти. Зібрана інформація використовуватиметься для прогнозування злочинних дій на основі відповідних кримінологічних та

криміналістичних критеріїв. Якщо ж інформація стане підставою для обмеження прав і свобод громадян, для побудови рейтингів соціального кредиту, то поліція та громадянське суспільство навряд чи дійдуть згоди.

УДК [351.74(100):004.9](075.8)

ШВЕЦЬ ДМИТРО ВОЛОДИМИРОВИЧ

доктор юридичних наук, доцент,

заслужений працівник освіти України,

перший проректор Харківського національного університету внутрішніх справ

ПРОБЛЕМИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПОЛІЦІЙСЬКІЙ ДІЯЛЬНОСТІ

В даний час використання штучного інтелекту (ШІ) стало досить поширеним у різних сферах суспільного життя. Не стала винятком правоохоронна діяльність. Але одночасно з розширенням можливостей щодо запобігання та розкриття злочинів за допомогою застосування можливостей ШІ виникають різноманітні проблеми, які викликані особливостями соціальної поведінки різних груп осіб залежно від їхнього соціального статусу, освіти, національної належності, віросповідання тощо. Так наприклад, британські поліцейські побоюються помилок та необ'єктивності ШІ.

За даними Королівського об'єднаного інституту оборонних досліджень, британські поліцейські побоюються, що широке застосування ШІ у боротьбі зі злочинністю спричинить необ'єктивну оцінку ризиків, помилки в аналізі даних та кримінологічне прогнозування. Зокрема, представники малозабезпечених груп населення можуть бути віднесені ШІ до групи високого ризику лише тому, що вони частіше контактують із соціальними службами та їх дані з більшою ймовірністю можна знайти в державних базах, на основі яких ШІ саме робить аналіз та прогнози.

Дослідження «Аналіз даних та алгоритмічна похибка в поліцейській роботі» було проведено Королівським об'єднаним інститутом оборонних

досліджень на замовлення Центру етики даних та інновацій (CDEI) у рамках підготовки Великобританії до широкого впровадження ШІ у всі сфери життя. Як відзначають автори дослідження, поліцейські в Англії та Уельсі все частіше використовують у своїй роботі новітні технології, наприклад, розпізнавання осіб та аналіз відеоматеріалів, вилучення даних з мобільних телефонів, аналіз даних із соцмереж, кримінологічне прогнозування, оцінка індивідуальних ризиків тощо.

За словами експертів, використання ШІ дає значні переваги, але водночас викликає серйозні питання з етичної та юридичної точок зору через високу ймовірність помилок і, як наслідок, дискримінацію щодо окремих осіб чи груп осіб.

Але посилене патрулювання тих районів, де, за оцінкою ШІ, висока ймовірність скоєння злочинів, виявилося ефективнішим у зниженні рівня злочинності у конкретних районах, ніж стандартне патрулювання всіх районів поспіль.

Більше того, використання ШІ дозволяло вдвічі точніше прогнозувати місця ймовірного скоєння злочинів у порівнянні зі звичайним аналізом, який проводили співробітники поліції на підставі оперативних даних. Однак з якоїсь причини ця форма аналізу за допомогою ШІ використовується в поліції нечасто.

Найчастіше поліція вдається до допомоги ШІ для оцінки індивідуальних ризиків, тобто для визначення ймовірності скоєння злочинів конкретною особою — у такому разі виникає одна з проблем, на які вказують автори дослідження. Як показує досвід, кримінологічне прогнозування щодо груп осіб має досить високий рівень точності, але щодо окремих осіб точність серйозно знижується.

А якщо, наприклад, якась особа була відзначена ШІ як така, що представляє високий ризик скоєння правопорушення, то перевірити, наскільки вірним був цей прогноз, вдається не завжди — правоохоронні органи зазвичай вживають заходів, щоб у підозрілої особи в жодному разі не було можливості вчинити злочин.

Інша проблема полягає в тому, що через більший обсяг даних про людей із верств населення з низьким рівнем соціально-економічного благополуччя, з

проблемних районів тощо (а саме на основі цих даних відбувається машинне навчання) висока ймовірність помилки та ШІ буде шукатиме злочинців саме у цих групах населення.

Крім того, не виключено впливу людського фактора. За словами одного з поліцейських, опитаних експертами, «чорношкірих чоловіків частіше зупиняють на вулиці та обшукують, ніж білих, і причина цього у суб'єктивному людському сприйнятті. Але ця суб'єктивна оцінка потім потрапляє до баз даних і проявляється в результатах використання цих баз». У такому разі ШІ починає прогнозувати не злочини, а поліцейські операції.

Зараз же, за словами одного з поліцейських, використання ШІ в роботі правоохоронних органів подібно до «клаптевої ковдри, вона не скоординована, застосовується відповідно до різних стандартів у різних ситуаціях, і результати теж виходять різними».

Правозахисники зазначають, що використання ШІ в цій галузі «загрожує значними» порушеннями прав людини.

Тому методики використання ШІ у поліцейської діяльності потребує більш досконалних досліджень.

УДК 343.1 + 004

БАНДУРКА ОЛЕКСАНДР МАРКОВИЧ

доктор юридичних наук, професор,

академік Національної академії правових наук України,

заслужений юрист України,

професор кафедри теорії та історії держави і права факультету № 1 Харківського національного університету внутрішніх справ

ОКРЕМІ АСПЕКТИ ВИКОРИСТАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ У СЕКТОРІ БЕЗПЕКИ

Останнім десятиріччям спостерігається значне підвищення інтенсивності використання безпілотних літальних апаратів (БПЛА), які також називають

дронами, в усіх сферах людської діяльності. Термін дрон є акронімом від Dynamic Remotely Operated Navigation Equipment. БПЛА прийшли з військової сфери та почали активно застосовуватися у сфері безпеки. Залежно від вагової категорії усі БПЛА умовно можуть бути поділені на три класи:

Клас I (менше 150 кг) охоплює ручні моделі та багатоцільові системи. Типовий літальний апарат цього класу має тривалість польоту 1-3 години, дальність польоту близько 80 км, вантажопідйомність 5 кг та максимальну швидкість 100 км/год. Більшість апаратів цього класу використовуються для дослідницьких завдань та не мають озброєння на борту. За класифікацією НАТО цей клас містить три підкласи: мікро, міні та малий;

Клас II (150–600 кг), який також називають тактичними БПЛА, має тривалість польоту 10 годин, максимальну дальність польоту 100-200 км, вантажопідйомність до 70 кг, максимальну швидкість 200 км/год. Більшість БПЛА цього класу не мають на борту зброї, деякі оснащені легкими боєприпасами, зокрема керованими ракетами типу «повітря-земля»;

Клас III (більше 600 кг) також відомий як середньовисотний має тривалість польоту більше 24 годин, вантажопідйомність кілька сотень кг і максимальну швидкість більше 300 км/год. Деякі апарати цього класу можуть здійснювати польоти на декілька тисяч км. За класифікацією НАТО цей клас містить три підкласи: «medium-altitude long-endurance», «high-altitude long-endurance» та «trike/Combat» [1, с. IV].

Головними передумовами використання БПЛА у національному секторі безпеки є:

- складна оперативна обстановка на територіях проведення операції об’єднаних сил;

- зміна клімату, яка може призвести до раптового погіршення погодних умов на значній території України;

- потреба підвищення оперативності реагування органів та підрозділів МВС України на нові виклики;

- зменшення ризику для головних сил МВС України в умовах невизначеності;

- протидія правопорушенням.

На теперішній час у таких країнах як Греція, Іспанія, КНР, США, Чилі безпілотні літальні апарати використовують для гасіння пожеж, у Бельгії, Італії, Тайланді, Хорватії – для спостереження за дотриманням екологічного законодавства, в Еквадорі, Колумбії та Мексиці – для протидії наркозлочинності та контрабанді. У таких країнах як Бразилія і Франція БПЛА застосовують для спостереження за масовими заходами [1, с. XIII].

Технології використання БПЛА змінили уявлення про класичні методи і засоби збирання даних та швидкість цього процесу. Якщо раніше існували місцевості, що вважалися непридатними для ретельного аналізу, то тепер інформацію про них можна зібрати за достатньо нетривалий проміжок часу із великою точністю. При цьому системи збирання даних у важкодоступних місцях є набагато дешевшими та швидшими, аніж традиційні платформи, такі як літаки, супутники або наземні транспортні засоби [2, с. 159].

Одним з головних стримуючих факторів розвитку БПЛА є відсутність належного нормативного забезпечення, яке регламентує правила їх використання. Зокрема це стосується вирішення завдань уникнення зіткнень в повітрі, захисту персональних даних, відповідальності володільців та користувачів БПЛА.

У країнах, які вже тривалий час впроваджують роботу БПЛА на своїх територіях, законодавча база з цього питання постійно змінюється, а сама нормативна база з цього питання створена чи суттєво змінена протягом декількох останніх років. Для кожного класу БПЛА у різних країнах впроваджуються певні правила використання. Головним чином такі правила стосуються:

- визначення зони обмеження польотів відповідно до ваги дрона, висоти польоту та щільності населення тощо;

- ліцензування пілота у випадку професійного використання БПЛА;

- реєстрації БПЛА у разі професійного використання;

- регулювання використовуваних БПЛА частот;

- страхування у разі професійного використання БПЛА [3, с. 37].

В Україні польоти БПЛА здійснюються відповідно до законодавства у галузі державної авіації України. Проте законодавча база у цій сфері ще потребує суттєвого удосконалення.

Список використаних джерел:

1. Gettinger D. The Drone Databook. The Center for the Study of the Drone at Bard College, 2019. 320 p.

2. Tal D., Altschuld J. Drone Technology in Architecture, Engineering, and Construction: A Strategic Guide to Unmanned Aerial Vehicle Operation and Implementation. Wiley, 2021. 168 p.

3. Um J.-S. Drones as Cyber-Physical Systems Concepts and Applications for the Fourth Industrial Revolution and Implementation. Springer, 2019. 274 p.

УДК 004.043

БАРАБАШ ВІТАЛІЙ ОЛЕКСАНДРОВИЧ

студент 1 курсу групи Ф6-Кбдср-21-1 факультету № 6

Харківського національного університету внутрішніх справ

ТУЛУПОВ ВОЛОДИМИР ВОЛОДИМИРОВИЧ

кандидат технічних наук, доцент,

доцент кафедри кібербезпеки та DATA-технологій факультету № 6

Харківського національного університету внутрішніх справ

ДЕЯКІ ПИТАННЯ ПРЕВЕНТИВНОГО ЗАХИСТУ ПРИВАТНОСТІ ІНФОРМАЦІЇ

Метою доповіді є питання превентивності захисту приватності інформації в разі втрати або викрадення пристрою на системі Windows 10.

На теперішній час слід констатувати, що ми стали занадто довіряти звичайному паролю на своїх пристроях, завдяки яким ми можемо працювати та досить відверто спілкуватися з іншими людьми.

Як правило у нас на комп’ютері встановлені останні версії антивірусів, налаштовані брандмауери, останні збірки Windows, встановлені паролі на

облікові записи. Звісно, всі ці міри безпеки можуть захистити нас та нашу інформацію від злочинців в мережі, але не при фізичному контакті нашого пристрою з руками зловмисника. У кожного користувача є данні, які можуть нашкодити власнику, але в нашому випадку, витік даних може нашкодити безпеці інших людей.

При фізичному доступі до нашого пристрою, звичайний пароль, код, фізичний ключ або відбиток пальців може обійтися за допомогою сторонніх програм, які потребують завантаження через Dos, що дозволяє редагувати файл SAM, який, при штатній роботі системи, охороняється та контролюється процесом lass.exe від втручання, навіть від адміністратора системи.

Для вирішення цього питання на теперішній час існує два найпопулярніших рішення для таких дій, це Kon-boot та Offline NT password & registry editor. Кожен з них має свої недоліки та привілеї.

Kon-boot використовується для одноразового доступу до системи й не чіпає файлів системи, бо робота системи, при такому завантажені, схожа на Live CD в Linux.

Offline NT password редактує на постійній основі файл SAM, що дозволяє входити в систему без використання flash накопичувача з Bootloader’ром. Всі ці рішення працюють лише при вимкненому в BIOS режимі Secure Boot, його можна перемикати в будь-який час, якщо в BIOS не був встановлений пароль.

Якщо зловмиснику не потрібна робота з нашого облікового запису, а лише данні з диску, тоді можна просто дістати диск та підключити до іншого комп’ютера або використовувати Live CD образ будь-якої збірки Linux.

Таке завантаження досить часто не потребує втручання до налаштувань BIOS, так як більшість Uefi Bios та деякі Legacy, мають окреме меню для одноразового запуску з системного диску або flash носія Linux.

Дізнатися про комбінацію клавіш можна з мережі знаючи виробника ноутбуку або материнської плати ПК.

Так, Linux завантажується без єдиної підозри зі сторони BIOS, тому має доступ до наявних дисків, в тому числі й системного. Досить просто вмонтувати

диск до обраної Live CD системи та безперешкодно копіювати данні з дисків, та в окремому випадку з під root, редагувати їх.

Роблячи підсумки, слід зазначити, що для захисту приватності інформації достатньо встановити пароль до BIOS, не використовувати емуляцію Legacy на Uefi Bios, завжди тримати увімкненим Secure Boot та зашифрувати данні за допомогою BitLocker.

Ці дії не уявляють складнощів та не заважають комфортному використанню пристроїв власником. Захистити данні від монтування або звичайного підключення до іншого комп'ютера диску можна завдяки пропрієтарній Windows програмі BitLocker, що зашифрує наявну інформацію на диску.

Список використаних джерел:

1. Яка різниця між UEFI и Legacy BIOS? /gravitsapa.info: веб-сайт. URL: https://gravitsapa.info/kakie-otlichiya-mezhdu-uefi-i-legacy-biosami/ (дата звернення 12.11.2021)

УДК 339.92

БАРАНЕНКО ЄГОР ОЛЕКСАНДРОВИЧ

курсант 2 курсу факультету №4

Харківського національного університету внутрішніх справ

ОНИЩЕНКО ЮРІЙ МИКОЛАЙОВИЧ

кандидат наук з державного управління, доцент,

заст. декана факультету з навчально-методичної роботи факультету №4

Харківського національного університету внутрішніх справ

БЛОКЧЕЙН, ЯК ВАРІАНТ ЗАХИСТУ ДАНИХ

З кожним днем роль кіберпростору в нашому житті невпинно збільшується. Щороку об'єм інформації в інтернеті зростає в рази, а з ним зростає кількість конфіденційної інформації, яку необхідно захищати.

Блокчейн перетворює цифрову ідентифікацію на реальність та допомагає захиститися від крадіжки ідентифікаційної інформації. Цифрова ідентичність - це інформація, яка зберігається в цифровому форматі і сама по собі є повним ідентифікатором. Користувач, за запитом та за своєю згодою, ділиться цією інформацією з організацією. Зацікавлена організація звіряє отриманий хеш із публічним репозиторієм хешів, наприклад, Aadhaar.

Хеші.

В основі блокчейну лежить обчислення математичного алгоритму хеша від заданого набору даних. Ось деякі властивості та особливості хешу:

- Хеш - це деяка кількість певної довжини;
- Хеш може бути отриманий в результаті перетворення даних на цифровий відбиток, тобто перетворити цілу енциклопедію на набір символів фіксованої довжини;
- Використовуються захищені алгоритми хешування, наприклад: SHA256, SHA384 та SHA512.
- З обчисленого хеша важко або неможливо отримати вихідні дані, навіть знаючи алгоритми, за якими формувався хеш.

У чому взагалі сенс блокчейн-безпеки, які її «населяють»? Технологія дозволяє людям, які не довіряють один одному, ділитися цінними даними безпечним та захищеним способом. Завдяки їй досягається:

- Блокування крадіжки особистих даних;
- Блокування підробки даних;
- Блокування DDoS-атак.

Якщо хеш збігається, це говорить про те, що посвідчення використовується автентифікованою особою. Дані помітні не завжди і знаходяться в захищеному вигляді до моменту перевірки.

Блокчейн замінює секретність на прозорість, розподіляючи докази підписання документа по багатьох блокчейнах. Практично неможливо маніпулювати даними.

Перевірка ідентичності без цифрового підпису – при цьому хеші вихідних файлів зберігаються у блокчейні, виконується перевірка інших копій файлів за допомогою алгоритму хешування та порівнюється результат із хешами, що зберігаються у блокчейні.

У *Hyperledger*, який є приватним блокчейном, існує мережа, в якій всі учасники заздалегідь відомі, а нові учасники перевіряються сертифікуючими органами перед підключенням. Є незначні шанси на DDoS-атаку, але всі учасники вже відомі винуватця буде легко виявити.

DoS і **DDoS** - це атаки, при яких на сервер приходить величезна кількість запитів, що сміття, що значно збільшує час відповіді сервера для відповіді на нормальні запити. У контексті *Ethereum* за будь-який запит, що обслуговується, повинна бути виплачена певна сума у вигляді *GAS* (найменша форма *Ethereum*). Такий підхід за своєю концепцією виключає DDoS-атаку.

Маніпуляції з даними будуть швидко виявлені, оскільки вихідний хеш існує на мільйонах вузлів.

Зазначимо, що міністерство оборони США розглядає блокчейн-інфраструктуру KSI як потенційно придатну для захисту чутливих військових даних. А ще існує компанія під назвою Gem, яка допомагає використовувати блокчейн для безпечного обміну медичними даними між зацікавленими сторонами відповідно до вимог американської HIPPA.

Блокування DDoS-атак.

Розподілені атаки типу «відмова від обслуговування» (DDoS) – це проблема, яка за умовчанням виключена у блокчейні. Давайте розглянемо це в контексті *Ethereum* і *Hyperledger*, обидві технології є різними формами блокчейна — публічний і приватний блокчейн відповідно.

Підбиваючи підсумки:

Зараз, запровадження блокчейн мереж може багатократно підвищити ефективність захисту даних користувачів, в порівнянні з сьогочасними методами. Ці мережі необхідно додаткового дослідити заради їх покращення та з’ясування можливості запровадження їх в сучасних реаліях сьогодення.

УДК [342.951:351.814](477)

БЕЗПАЛОВА ОЛЬГА ІГОРІВНА

доктор юридичних наук, професор,

заслужений діяч науки і техніки України,

завідувач кафедри поліцейської діяльності

та публічного адміністрування факультету № 3

Харківського національного університету внутрішніх справ

ЗАПРОВАДЖЕННЯ ПІДГОТОВКИ ОПЕРАТОРІВ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ЯК ПЕРСПЕКТИВНИЙ КРОК У НАПРЯМІ ЗАБЕЗПЕЧЕННЯ ЕФЕКТИВНОГО ВИКОНАННЯ МВС УКРАЇНИ ПОКЛАДЕНИХ НА НЬОГО ЗАВДАНЬ

Стрімке поширення практики використання безпілотних літальних апаратів для забезпечення військових та оборонних цілей держави, проведення рятувальних операцій, здійснення моніторингу інфраструктури, забезпечення ефективного функціонування сфери сільського господарства та для виконання інших цивільних завдань (комерційного та некомерційного характеру) вимагає вироблення на законодавчому рівні дієвого механізму їх використання, а також здійснення якісної підготовки операторів таких апаратів. Підготовка операторів безпілотних літальних апаратів має відбуватися з урахуванням сфери, в якій таким операторам доведеться працювати, що зумовлюється специфікою виконання покладених на них завдань.

МВС України є одним із суб'єктів використання безпілотних літальних апаратів у сфері забезпечення законності та правопорядку в державі. Безпілотні літеральні апарати можуть використовуватися в діяльності органів та підрозділів, діяльність яких координується МВС України, під час: моніторингу оперативної обстановки; забезпечення безпеки дорожнього руху; звільнення заручників; проведення рятувальних та пошукових операцій; проведення оперативно-розшукових заходів і негласних слідчих (розшукових) дій; забезпечення безпеки державного кордону; протидії контрабанді, торгівлі людьми та нелегальній міграції тощо. Таким чином, мають висуватися особливі вимоги до підготовки

операторів безпілотних літальних апаратів, на яких крім безпосереднього управління такими апаратами буде покладено одночасно виконання низки завдань правоохоронної спрямованості.

У зв’язку з цим важливого значення сьогодні набуває створення навчального центру підготовки операторів безпілотних літальних апаратів (далі – Центр), основною метою якого має бути здійснення підготовки операторів безпілотних літальних апаратів (літакового та коптерного типу) у правоохоронній сфері (сфері внутрішньої безпеки держави). На базі Центру повинні проходити підготовку інструктори, техніки, оператори, фахівці терміналів наземних даних та станцій наземного контролю безпілотних літальних апаратів.

На нашу думку, Центр доцільно створити на базі Кременчуцького льотного коледжу Харківського національного університету внутрішніх справ. Персонал Центру повинен буде пройти навчання на базі виробників безпілотних літальних апаратів.

Центр має бути оснащений:

– тренувальними комплексами підготовки операторів безпілотних літальних апаратів (симуляторами та тренажерами зі спеціалізованим програмним забезпеченням) із системою гарантованого електропостачання;

– пультами управління (ручним та з наземної станції);

– натурними зразками та макетами об’єктів безпілотних літальних апаратів;

– наземним комплексом управління та програмного забезпечення, необхідними для експлуатації, обслуговування та ремонту безпілотних літальних апаратів.

Для функціонування Центру необхідною є розробка відповідної нормативно-технічної документації.

Підготовка операторів безпілотних літальних апаратів повинна складатися з двох частин:

1) теоретична:

– ознайомлення із нормативно-правовими та адміністративно розпорядчими документами з питань організації та виконання польотів, з питань використання безпілотних літальних апаратів;

– вивчення структури та порядку використання повітряного простору України;

– набуття знань в області аеродинаміки і динаміки польоту безпілотних літальних апаратів, метеорології, військової топографії;

– ознайомлення з типами безпілотних літальних апаратів та вивчення їх технічних характеристик та правил безпечної експлуатації;

– вивчення теоретичних основ фотограмметрії та особливості аерофотозйомочних робіт земної поверхні, основ фото- та відеозйомки з безпілотних літальних апаратів;

– вивчення будови безпілотних літальних апаратів;

– ознайомлення з необхідністю дотримання вимог конфіденційності і недоторканності приватного життя при здійсненні заходів, належного захисту персональних даних;

2) практична:

– набуття практичних знань та вмінь з використання інженерно-авіаційного забезпечення;

– складання польотних планів за координатами для подальшого завантаження в апарат;

– проведення практичних занять з управління безпілотними літальними апаратами на різних висотах (підготовка до польоту, управління безпілотними літальними апаратами, формування завдання та аерофотознімання, ручний та напівавтоматичний політ у міських та сільських умовах, ручний та автоматичний зліт і посадка, аварійна посадка, політ за заданий координатами GPS, маневрування та обхід перешкод, коригування польотного завдання);

– робота з цифровою картою;

– здійснення навчально-тренувальних польотів з використанням симуляторів та тренажерів, справжніх літальних апаратів;

– технічне обслуговування безпілотних літальних апаратів.;

– підготовка та заправка витратних матеріалів.

Для здійснення навчально-тренувальних польотів Центр повинен погодити з обласними головними управлінням Служби безпеки та Національної поліції України зони польотів безпілотних літальних апаратів.

Навчання майбутніх операторів безпілотних літальних апаратів у Центрі дозволить забезпечити їх належну теоретичну підготовку та відпрацювати широке коло навчальних питань, пов'язаних як із безпосереднім керуванням безпілотним літальним апаратом (плануванням, коригування та виконання маршруту в різних погодних умовах), так і з їх технічним обслуговуванням та ремонтом.

По завершенню навчання оператори безпілотних літальних апаратів повинні скласти випускні кваліфікаційні іспити та за умови успішного їх складання отримати відповідні сертифікати.

Підсумовуючи викладене вище, можна дійти висновку, що важливого значення сьогодні набуває розробка галузевого стандарту, положеннями якого має бути чітко визначено необхідність підготовки операторів безпілотних літальних апаратів та затверджено процедурні питання, пов'язані з такою підготовкою, у тому числі інституційні, операційні та ліцензійні аспекти.

УДК 004.624

БІЛАШЕНКО ДАНИЛО В'ЯЧЕСЛАВОВИЧ

курсант 2 курсу факультету №4

Харківського національного університету внутрішніх справ;

ОНИЩЕНКО ЮРІЙ МИКОЛАЙОВИЧ

кандидат наук з державного управління, доцент,

заступник декана факультету з навчально-методичної роботи факультету №4

Харківського національного університету внутрішніх справ

АНАЛІЗ ІНФОРМАЦІЇ В ІНТЕРНЕТІ ЗА ДОПОМОГОЮ ПАРСІНГУ САЙТІВ

З кожним роком роль Інтернету та інформаційних технологій у житті людини стає все більшою. Відповідно, з'являється необхідність аналізу даних

на сайтах та веб-сторінках. З цією метою здійснюється «парсінг сайтів». Але, нажаль, не всі знають про його види, переваги та алгоритм.

Парсінгом називають послідовний синтаксичний аналіз інформації, яка розміщена на веб-сторінці. Цей метод використовується для оперативної обробки та копіювання великої кількості даних, якщо ручна робота потребує багато часу. Для парсінгу використовуються парсери – спеціальні програми, які здатні аналізувати контент в автоматичному режимі та знаходити потрібні фрагменти [2].

Незалежно від того якою формальною мовою програмування написано парсер, алгоритм його дії залишається однаковим:

- вихід в інтернет, отримання доступу до коду веб-ресурсу та його завантаження;
- читання, вилучення та обробка даних;
- представлення вилучених даних у зручному вигляді – файли .txt, .sql, .xml, .html та інших форматах [1, 2].

Парсери не розуміють текст, вони лише порівнюють запропонований набір слів з тим, що виявили в інтернеті і діють за заданою програмою. Те, як пошуковий робот повинен вчинити зі знайденим контентом, написано в командному рядку, що містить набір букв, слів, виразів та знаків програмного синтаксису.

Коли мова заходить про створення парсерів, всі згадують PHP і Python – саме ці мови працюють на стороні сервера. Незважаючи на те, що безліч програм все ще працює на PHP, зараз набагато вигідніше користуватися Python, який застосовується такими відомими компаніями як YouTube, Instagram, Facebook, Google, Netflix [3].

Парсінг законний, якщо стосується збору інформації, що знаходиться у відкритому доступі. Тобто все, що можна і так зібрати вручну.

Парсери просто дозволяють прискорити процес і уникнути помилок через людський фактор. Тому «незаконності» у процес вони не додають. Інша річ, як власник свіжозібраної бази розпорядиться такою інформацією [4].

Переваги парсінгу.

У порівнянні з людиною парсери можуть:

- збирати дані швидше та в будь-якому режимі, хоч цілодобово;
- слідувати всім заданим параметрам, навіть дуже тонким;
- уникати помилок від неуважності чи втоми;
- виконувати регулярну перевірку за заданим інтервалом (щотижня тощо);
- подати зібрані дані у будь-якому необхідному форматі без зайвих зусиль;
- рівномірно розподіляти навантаження на сайт, де проходить парсинг (зазвичай одна сторінка за 1-2 секунди), щоб не створювати ефекту DDOS-атаки [1].

Види парсінгу сайтів:

- наповнення сайтів текстовим або мультимедійним контентом (це найпопулярніший вид парсінгу);
- парсінг даних про товари та ціни для інтернет-магазинів;
- парсінг оголошень зі спеціалізованих ресурсів;
- збирання контактних даних потенційних клієнтів;
- робота з соціальними мережами (парсинг між спільнотами в соцмережах або збір даних із спільнот на сайт) [2].

Інформаційні технології з кожним днем все більш задіються у повсякденному житті людини. Це особливо стосується обробки даних, адже якщо передати цю роботу парсеру – аналіз буде якіснішим і менш працезатратним.

Список використаних джерел:

1. Парсінг. Що це і де використовується [Електронний ресурс]. – Режим доступу : https://ipipe.ru/info/parsing

2. Що таке парсінг сайту? [Електронний ресурс]. – Режим доступу : http://xtgamers.com/page-id-13831.html

3. Парсінг сайтів за допомогою Python: плюси та мінуси, коротка інструкція для чайників [Електронний ресурс]. – Режим доступу : https://prime-

ltd.su/blog/parsing-saytov-s-pomoshhyu-python-plyusyi-i-minusyi-kratkaya-instruktsiya-dlya-chaynikov/

4. Що таке парсінг і як правильно парсити [Електронний ресурс]. – Режим доступу : https://blog.calltouch.ru/chto-takoe-parsing/

УДК 004.42

БИЗОВ ІВАН СЕРГІЙОВИЧ

студент 6-го курсу факультету інформаційних та технічних систем Інституту цивільної авіації Харківського національного університету Повітряних Сил імені Івана Кожедуба;

ЄВСТРАТ ДМИТРО ІВАНОВИЧ

кандидат технічних наук, доцент,

доцент кафедри інформаційних технологій, Інститут цивільної авіації Харківського національного університету Повітряних Сил імені Івана Кожедуба

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ ЛЮДИНИ НА ЗОБРАЖЕННІ (ВІДЕОПОТОЦІ)

Останнім часом широкого поширення набуває технологія інформаційно-пошукових систем розпізнавання особи з метою її ідентифікації. Ця технологія поряд з технологіями розпізнавання голосу найкраще підходить для інтелектуальних середовищ нового покоління, які можуть бути використані в автоматизованих системах безпеки, наприклад, на державних пунктах пропуску, у великих аеропортах, різних громадських місцях та інших, з метою ідентифікації осіб, що розшукуються, з одночасною передачею відповідної оперативної інформації службам, що займаються встановленням особи.

Технологія ідентифікації особи на основі зображення обличчя, на відміну від використання інших біометричних показників (відбиток пальця, райдужна оболонка ока), не вимагає фізичного контакту з пристроєм та з урахуванням стрімкого розвитку цифрової техніки є найбільш прийнятною для масового застосування.

Підходи, щодо реалізації такої технології практично сформувалися. Однак, необхідно вдосконалення існуючих алгоритмів з метою оптимізації тимчасових і точних характеристик пошуку, що забезпечуються ними, за рахунок використання ключових ознак, що "витягуються" автоматично з зображення обличчя (наприклад, наявність бороди, окулярів, ракурс обличчя та ін.), і, таким чином, підвищення швидкості і точності пошуку.

В результаті проведеної роботи було спроектоване та розроблено програмне забезпечення, яке засноване на технології розпізнавання обличчя людини на зображенні. Це надає низку незаперечних переваг, а саме, можливість проводити ідентифікацію на відстані, приховану перевірку, використовувати недороге поширене обладнання, у точності, відеокамери. Враховуючи велику кількість камер у всіх сферах діяльності та аспектах життя людини, розробки у цьому напрямку стають все більш актуальними.

Програма була реалізована мовою високорівневої мови Python загального призначення, з використанням наступних бібліотек:

PyQt (інтерфейс);

NumPy;

OpenCV (з підходом "каскадами Хаара");

Face-recogntion.

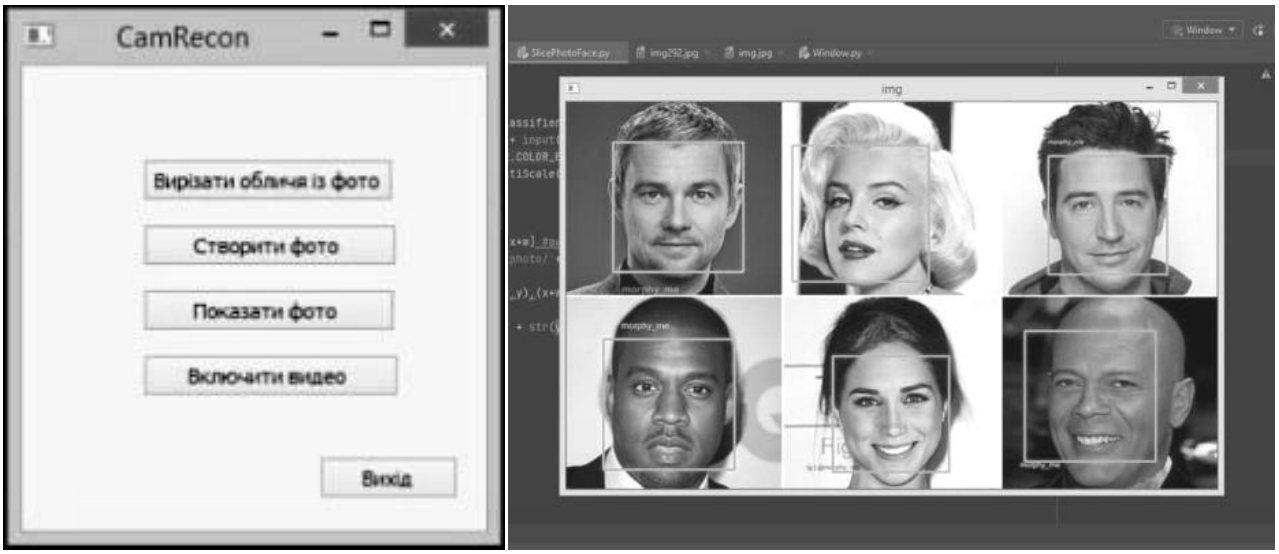

Рис. 1. Головне меню програми та результати розпізнавання облич на зображеннях

Враховуючи те, що у задачах розпізнавання обличь прийнято використовувати шаблони, що складаються зі світлих і темних областей, в основу алгоритму роботи програми покладено процедура пошуку певних шаблонів на зображенні обличчя особи.

У програмі представлено кілька функцій, зокрема: створення фото, перегляд фото, обрізки фото, знаходити всі особи на фото і вирізати їх для подальшого іменування та розпізнавання в потоковому відео, а також запуск потокового відео з розпізнаванням осіб.

Аналогом такого рішення є плагін для програми iSpy, який попередить вас, якщо в радіусі камера розпізнає обличчя людини. Плагін буде ігнорувати всі інші рухи так що, це запобіжить і знизить кількість помилкових спрацьовувань, а у разі визначення особи, вас про це сповістить. Його рішення також побудовано на бібліотеці Face-recognition та має велику базу людських обличь.

Можемо сказати, що подібні рішення мають переваги та недоліки, чудовий інтерфейс та хороші інші характеристики, однак їх використання обмежене, тому що вони були спроектовані та розроблені з адаптацією до конкретних вимог та повністю контролюються компаніями-розробниками.

Розробка власного програмного забезпечення забезпечує реалізацію необхідного функціоналу та дозволяє повністю контролювати потік даних.

Подальшим розвитком запропонованого рішення буде:

створення додаткової підсистеми вибору зображень людських обличь з відеоряду, формованого, наприклад, шляхом автоматичного зчитування з відеокамер стеження за навколишньою обстановкою, з подальшим використанням цієї інформації в якості вхідної для системи ідентифікації особи;

використання хмарних сервісів для збереження зображень, з метою збільшення швидкодії ідентифікації, за рахунок швидкого доступу до сервера з необхідними базами.

УДК 351.741:004.89

БОНДАРЕНКО ОЛЕКСАНДР ВІКТОРОВИЧ

здобувач вищої освіти Луганського державного університету внутрішніх справ імені Е. О. Дідоренка

ВИКОРИСТАННЯ SWOT-АНАЛІЗУ У ПРОТИДІЇ КОРРУПЦІЇ

В сучасних умовах протидії злочинності в Україні велике місце посідає питання організації цієї діяльності на державному рівні, що безпосередньо пов’язане з формуванням і реалізацією відповідних державних стратегічних документів, а саме: стратегії та програми протидії злочинності, своєчасність, повнота і якість розроблення та подальша реалізація яких суттєво впливає на ефективність протидії злочинності в країні[1, с.124]

Сучасна коррупція в Україні набуває великих масштабів. Якщо розглядати дані КМІС, то у 2021 році 93,5%. українців вважають корупцію серйозною проблемою для держави [2].

Аналізуючи таку статистичну інформацію, можна стверджувати, що для ефективної протидії корупції повинні бути дієві механізми. Одним із таких механізмів є використання у аналітичних відділах ***SWOT*-аналізу.**

***SWOT*-аналіз – це фактично фундаментальна, проста модель, яка аналізує те, що організація може, а що не може зробити, а також імовірні можливості та загрози. Техніка SWOT-аналізу завжди полягає в тому, щоб отримати інформацію зі зовнішнього середовища, зокрема розділити їх на внутрішні елементи – це сильні та слабкі сторони, а також зовнішні елементи – це можливості та загрози** [3, с.208]**.**

SWOT-аналіз, розроблений на базі європейських наукових шкіл, і названий так за першими літерами термінів, що характеризують суть його застосування, групування та систематизації. Це сильні (Strengths), слабкі (Weaknesses) сторони досліджуваного предмету, явища, феномену, а також його реальні та потенціальні можливості (Opportunities) і загрози (Threats), які виникають, або можуть виникнути в майбутньому стосовно нього, у ньому або через нього. До числа переваг, які властиві цьому науковому інструменту пізнання, можливо віднести доступність, оперативність, практичність у застосуванні,

універсальність використання при необхідності отримати та опрацювати первинні дані для більш ретельних та ґрунтовних досліджень, спрощений порядок його проведення, зрозумілість та доступність [4, с.14].

Отже, застосування цього методу у протидії корупції має перспективні можливості, які полягають у визначенні оптимальних стратегій реалізації і впливу на злочинність і загалом на коррупцію.

Список використаних джерел:

1. Титаренко О.О. Застосування SWOT-аналізу для визначення стратегій впливу на злочинність під час формування державної комплексної програми протидії їй. *Право та державне управління*. Запоріжжя, 2019. № 4.С.124-131.

2. Коррупция в цифрах: как меняется количество наказанных, оценка украинцев и место в рейтингах. URL: https://ru.slovoidilo.ua/2021/07/23/ infografika/obshhestvo/korrupciya-cifrax-kak-menyaetsya-kolichestvo-nakazannyx-ocenka-ukraincev-i-mesto-rejtingax(дата звернення: 15.11.2021).

3. Федчак І.В. Основи кримінального аналізу : навчальний посібник. Львів : Львівський державний університет внутрішніх справ, 2021. 288 с.

4. Бондарчук П.С. SWOT-Аналіз сучасних викликів і загроз публічного адміністрування у сфері національної безпеки з використанням ціннісного підходу. *Публічне адміністрування та національна безпека.* Київ, 2021. № 2 (18). С.13-18.

УДК [351.74(100):004.9](075.8)

БОРТНИК СЕРГІЙ МИКОЛАЙОВИЧ

доктор юридичних наук, доцент,

проректор Харківського національного університету внутрішніх справ

ОСОБЛИВОСТІ РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ПРАВООХОРОННОЇ СИСТЕМІ

Правоохоронна система тісно пов'язана з правами та свободами людини. Тому ця специфічна діяльність, особливо робота судів, дуже сприймає нові технології в Україні. Віддавати «на відкуп» штучному інтелекту найцінніше

нікому не хочеться. Але це не скасовує застарілі проблеми правоохоронної системи, у тому числі людського чинника та нестачі професіоналів. Істотно допомогти у вирішенні цих проблем цілком здатні технології штучного інтелекту, а також пов'язані з ним машинне навчання та Deep Learning.

В Україні застосування штучного інтелекту (ШІ) у правоохоронній системі розвинене недостатньо. Основним чинником, який стримує проникнення ШІ в Україні, є фінансова ситуація. Однак первинна проблема — недостатнє правове регулювання.

Нещодавно з'явилася напрацьована колегами з Мінцифри і комітету з питань ШІ Концепція розвитку ШІ в Україні. Останню потрібно затвердити на рівні уряду. Крім того, заснували Асоціацію розвитку ШІ.

Отже, і створення, і застосування ШІ має бути врегульованим – для блага всього суспільства. Саме лиш законодавче визначення поняття «штучний інтелект» відкриє доступ ШІ до нових сфер і галузей економіки.

Звичайно, лише концепції недостатньо. Необхідний передусім апробаційний період, у ході якого буде виявлено сфери нормативного регулювання, які потребують найбільшої уваги, і навіть усунуто законодавчі прогалини. Якщо говорити про сфери права, на які необхідно звернути найбільшу увагу, це громадянське законодавство (природно, як основа інтелектуальної власності), а також адміністративне право, кримінальне право. Саме регулювання лише на рівні галузей права закладе основу регулювання ШІ без прив'язки до конкретній сфері економіки чи суспільства.

Через ці основні проблеми ми поки що в основному можемо лише спостерігати, як застосовують ШІ правоохоронці в інших країнах. Досвід накопичився досить пристойний, щоб нашій країні намітити ті вузькі сфери, де можна починати застосовувати ШІ щодо безпечно:

1. Перша область, де варто застосовувати ШІ, — розслідування кіберзлочинів. Поки що у цьому напрямку ШІ застосовується лише бізнесом для раннього запобігання можливим загрозам.

2. Розпізнавання осіб. Міська система розпізнавання осіб працює у Києві вже три роки і показує відмінні результати, у Харкові система діє протягом

двох років. Старт технології дано, далі питання впирається лише у фінансовий чинник.

3. Оцінка ризиків для в'язниць та корекційних установ. Система визначення ризиків вивчає та порівнює профілі та поведінку ув'язнених до вироку та після ув'язнення, їх взаємини, їхню попередню активність в інтернеті, після чого дає рекомендації щодо розміщення у певних установах та камерах, що виключало б виникнення конфліктів. Такі дослідження проводилися США, показавши успішні результати. На даний момент система не вводиться через можливий суспільний і політичний резонанс.

4. Оцінка ризиків за умовно-дострокового звільнення. Це саме та область, де за кордоном ІІ застосовується досить активно. Ризики зазвичай визначаються такими факторами як кримінальна історія, вік, етнічна приналежність, стать і т.д. Для розрахунку ймовірності рецидиву використовується алгоритм, що класифікує ризики за рівнями: низький, середній, середньовисокий або високий. Враховуються також ставлення до соціуму, злочинні зв'язки, освіта, зайняті

5. Автоматична ідентифікація змінених відбитків пальців. Люди, пов'язані з кримінальним світом, періодично цілеспрямовано завдають пошкодження кінчикам пальців: стирають поверхню шкіри, наносять кислоту, ріжуть, роблять невеликі операції. Іноді це відбувається ненавмисно: винні умови роботи, захворювання чи медичні процедури. На даний момент використовується лише ШІ, який визначає наявність та можливі причини таких змін відбитків.

6. ШІ у роботі американських судів допомагає держслужбовцям структурувати дані з багатьох документів, а громадянам — розібратися в судовій системі, заповнювати форми документів та правильно проходити етапи судових розглядів.

7. Дослідження пострілів. Вчені працюють над розробкою алгоритмів виявлення пострілів, їх характеристик, напряму, часу, визначення кількості присутньої вогнепальної зброї, відповідності конкретних пострілів конкретної вогнепальної зброї, оцінки ймовірностей класу та калібру. Це перспективний напрямок розробок ШІ, який не має точних термінів впровадження.

8. Передбачення злочинів. Це дуже широка сфера застосування ШІ, оскільки кримінальні кодекси містять велику кількість видів злочинів. При цьому виявляються не лише можливі порушники, місця майбутніх злочинів, а й можливі жертви. Це дозволяє поліції розставляти пріоритети в управлінні ресурсами, частіше спрямовувати патрулі до місць можливих злочинів.

Зрозуміло, що ШІ й надалі впроваджуватиметься у практику правоохоронної діяльності з розвитком та розширенням доступності технологій розумного міста, датчиків, інтернету речей.

УДК [351.74(100):004.9](075.8)

БРУСАКОВА ОКСАНА ВАЛЕРІЇВНА

доктор юридичних наук, доцент,

декан факультету № 6

Харківського національного університету внутрішніх справ

ОСОБЛИВОСТІ ВИКОРИСТАННЯ НОВІТНІХ ТЕХНОЛОГІЙ У ПОПЕРЕДЖЕННІ І РОЗКРИТТІ ЗЛОЧИНІВ У ПРАВООХОРОННИХ СТРУКТУРАХ ВЕЛИКОБРИТАНІЇ

Останні роки характеризуються перенесенням акцентів у діяльності правоохоронних органів розвинених країн з реактивного принципу до предикативного. Це обумовлено причинами тим, 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, сотен і більше людей. В цьому контексті керівники правоохоронних структур намагаються розробити нові стратегії і переформатувати свою діяльність саме виходячі 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. В цьому плані

нові технологи входять в число драйверів злочинності і детально розглянуті вище. З іншого боку, технології є інструментом, що дозволяє успішно не тільки боротися, але і профілактувати кримінал. В цьому докладі будуть розглянутий досвід Великобританії у використанні сучасних технологічних інструментів для профілактики, запобігання і розкриття злочинів.

У найбільш розгорнутому вигляді дане 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 злочинності, то в даний 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%-ве охоплення відеоспостереженням (не пізніше 2018 г.) саме відеофайли стануть основним елементом даних і матеріалом для профілактики злочинності та проведення розслідувань. В даний час перед системою кримінальної юстиції та забезпечення правопорядку в Великобританії стоїть завдання не тільки технічно відповісти на цей виклик, але і оснастити засобами та інструментами, що дозволяють максимально повно використовувати відеоінформацію спільно з текстовою і аудиоінформацією.

Британська поліція використовує великі дані і технології, причому не тільки програмні, але і 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 та технології, британська поліція планує не тільки

здійснити до 2020 р. апаратне і програмне переоснащення, але найголовніше - провести суцільне підвищення кваліфікації поліцейських, і в першу чергу на низовому рівні, змінити культуру поліцейських розслідувань.

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

Разом з тим всі британські поліцейські повинні мати доступ до баз даних і сучасних інструментів, що забезпечують ефективні комунікації, профілактику і розслідування злочинів з використанням інформаційних технологій.

УДК [351.74(100):004.9](075.8)

БУРДІН МИХАЙЛО ЮРІЙОВИЧ

доктор юридичних наук, професор,

проректор Харківського національного університету внутрішніх справ

ІНТЕЛЕКТУАЛЬНІ ТЕХНОЛОГІЇ У ПРОТИДІЇ ЗЛОЧИННОСТІ

Одним із видів спеціального програмного забезпечення, що використовується у правоохоронній діяльності, є експертні системи (ЕС) – системи підтримки прийняття рішень. Основне застосування ЕС знайшли у слідчій практиці.

У процесі розслідування злочинів використовуються такі види експертних систем:

- ЕС прогнозування злочинів, призначені для визначення залежності між особистісними якостями злочинців та вибором місця скоєння злочину;

- ЕС виявлення прихованих злочинів (наприклад, виявлення ознак крадіжок з виробництва);

- ЕС пошуку та встановлення особи злочинця, призначені для генерування типових версій про особу підозрюваного за первинною інформацією з місця злочину.

Інформаційно-модельна система «STOP кілер», головне призначення якої полягає у можливості побудови версій щодо особи вбивці та мотивів учиненого злочину в автоматизованому режимі. Автоматизована система «STOP кілер» адаптована до законодавства України, містить значну за обсягом базу даних, яка дозволяє отримувати більш репрезентативні результати та відрізняється новаторським підходом до побудови самих версій щодо особи вбивці та мотивів учиненого злочину. Отже, автоматизована інформативно модельна система «STOP кілер» призначена передусім для застосування співробітниками органів кримінальної юстиції під час розслідування конкретних вбивств як допоміжний ресурс для побудови слідчих версій, а також при плануванні досудового розслідування з метою найбільш ефективного провадження слідчих (розшукових) дій [1, с. 167].

Унікальна інтелектуальна система кримінального аналізу даних «RICAS», яка об’єднала в єдиному просторі основні і найсучасніші методи і методики кримінального аналізу та аналітичного пошуку в реальному часі, що дозволяє значно підвищити ефективність і результативність розкриття злочинів по гарячих слідах і нерозкритих раніше злочинів [2].

Експертні системи використовуються також для прогнозування можливих наступних місць злочинів, які скоюють серійні злочинці. На основі введених у програму вихідних даних про декілька скоєних злочинів (зазвичай п'ять-шість), на думку слідчих, пов'язаних між собою, експертна система на основі проведеного аналізу видає можливі місця скоєння нових злочинів.

У загальному вигляді ЕС є програми для вирішення завдань, які традиційно відносяться до сфери діяльності людського інтелекту. Це завдання, як планування, прогнозування, класифікація, прийняття рішень тощо.

На підвищення якості функціонування ЕС нині отримало використання штучних нейронних мереж.

Штучні нейронні мережі запропоновані для завдань, що тягнуться від управління боєм до нагляду за дитиною, Потенційними додатками є ті, де людський інтелект малоефективний, а звичайні очищення трудомісткі або

неадекватні. Цей клас додатків, принаймні, не менший за клас, що обслуговується звичайними обчисленнями, і можна припускати, що штучні нейронні мережі займуть своє місце поряд зі звичайними обчисленнями як доповнення такого ж обсягу і важливості.

В останні роки над штучними нейронними мережами домінували логічні та символьно-операційні дисципліни. Наприклад, широко пропагувалися експертні системи, які мають багато помітних успіхів, аналогічно до того, як і невдач. Дехто каже, що штучні нейронні мережі замінять собою сучасний штучний інтелект, але багато свідчить про те, що вони існуватимуть, об'єднуючись у системах, де кожен підхід використовується для вирішення тих завдань, з якими він краще справляється. Ця думка підкріплюється тим, як люди функціонують у нашому світі.

Розпізнавання образів відповідає за активність, яка потребує швидкої реакції. Так як дії відбуваються швидко і несвідомо, то даний спосіб функціонування важливий для виживання у ворожому оточенні. Уявіть тільки, що було б, якби наші предки змушені були обмірковувати свою реакцію на хижака, що стрибнув? Коли наша система розпізнавання образів неспроможна дати адекватну інтерпретацію, питання передається у вищі відділи мозку.

Вони можуть запросити додаткову інформацію і займуть більше часу, але якість отриманих в результаті рішень може бути вищою. Можна уявити штучну систему, що наслідує такий поділ праці. Штучна нейронна мережа реагувала б у більшості випадків відповідним чином на зовнішнє середовище. Так як такі мережі здатні вказувати довірчий рівень кожного рішення, то мережа «знає, що вона не знає» і передає даний випадок для вирішення експертної системи. Рішення, прийняті на цьому вищому рівні, були б конкретними і логічними, але вони можуть потребувати збору додаткових фактів для отримання остаточного висновку.

Комбінація двох систем була б більш потужною, ніж кожна із систем окремо, дотримуючись при цьому високоефективної моделі, що дається біологічною еволюцією.

Право належить до складної та недостатньо структурованої галузі людської діяльності, у зв'язку з цим дуже важливо пам'ятати, що ЕС слід використовувати тут як засіб, що полегшує і доповнює можливості фахівця, а не замінює саму людину.

Список використаних джерел:

1. Шепітько В. Ю. Автоматизовані інформаційні системи як засіб удосконалення розслідування вбивств / В. Ю. Шепітько, В. А. Журавель, Г. К. Авдєєва, С. В. Стороженко // Вісник Національної академії правових наук України. − 2017. − № 1. − С. 161-172. − Режим доступу: http://nbuv.gov.ua/UJRN/vapny_2017_1_17.

2. Інформаційно-аналітичний комплекс «RICAS – Realtime intelligence crime analytics system» [Електронний ресурс]. − Режим доступу: https://ricas.org/uk/.

УДК 378:003

ГАЙДАМАКА МИХАЙЛО СЕРГІЙОВИЧ

курсант групи Ф-4-302 факультету № 4

Харківського національного університету внутрішніх справ

ОНИЩЕНКО ЮРІЙ МИКОЛАЙОВИЧ

кандидат наук з державного управління, доцент,

доцент кафедри протидії кіберзлочинності факультету № 4

Харківського національного університету внутрішніх справ

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

Сьогодні, як ніколи постає важливим питанням застосування інформаційних технологій в діяльності правоохоронної системи України. Розвинення інформаційних технологій сприяє, як на розвиток кіберзлочинності та торгівлі людьми, так і на боротьбу з цими злочинами. До використання

технологій, рекрутери залежать від особистих соціальних зв’язків, спокуси багатства і романтичних відносин для вербування жертв. Крім того, жінки і дівчата, вже пов'язані з торговцем людьми, допомагатимуть торговцю у вербуванні інших жертв. Один із способів, яким технологія змінює цю динаміку, - це дозволити рекрутерам працювати під завісою анонімності. Торговці часто ведуть розмови через Dark Web за допомогою браузеру Tor, а також месенджеру Telegram. Згідно з оцінкою загрози організованої злочинності в Інтернеті, проведеної Європолом приблизно 40 відсотків платежів між злочинцями відбувається у Bitcoin, децентралізованії цифровій валюті, без центрального банку. Роль технологій в торгівлі людьми стає все більш тривожною, враховуючи здатність відстежувати кожен рух жертви. Це може потенційно включати використання технології GPS;

Однак нові технології стають все більш витонченими і грають ключову роль в боротьбі торгівлі людьми. Деякі використовуються для виявлення і порятунку жертв, інші - для виявлення злочинців. Багато з цих досягнень починають давати правоохоронним органам можливість знайти корінь мереж торгівлі людьми та зупинити діяльність, що лежить в її основі.

В основі кожного випадку торгівлі людьми лежить жертва, але дізнатися особистість цієї жертви складно. Сотні зображень людей, які зазнали насильства, публікуються в Інтернеті кожен день - навіть якщо всі вони відзначені прапорцями, багато хто з них будуть дублікатами вже порушених справ. Зрозуміти, чи є зображення дублікатом або новою фотографією, що потребує нової реакції з боку правоохоронних органів, складно, оскільки такі зображення важко відстежити. Тепер технології використовуються, щоб перехитрити торговців людьми і швидше розрізняти нові і існуючі зображення. Наприклад, Microsoft PhotoDNA накладає дрібну сітку на зображення і присвоює кожному квадрату числове значення, що представляє «хеш» - як підпис ДНК для зображення. Замість того, щоб сканувати цілі зображення, програма зіставляє числовий хеш з базою даних відомих незаконних зображень, щоб миттєво зіставити повторювані зображення.

Щоб допомогти правоохоронним органам перетворити це нововведення в позитивні дії, Thorn - технологічний стартап, заснований Ештоном Катчером і Демі Мур для боротьби з сексуальним насильством над дітьми і торгівлею ними, - уклав партнерську угоду з Microsoft, щоб дозволити організаціям додавати і отримувати доступ до централізованої бази даних обміну хешамі. . Нові зображення, які не були хешировані, повідомляються як нові жертви - це означає, що правоохоронні органи отримують повідомлення про нову жертву раніше. Це прискорює виявлення жертви.

Торговці людьми можуть використовувати технології, щоб приховати свою діяльність, але технології також еволюціонують то, як правоохоронні органи знаходять злочинні мережі. Ключовим моментом є об'єднання точок інформації від неурядових організацій, джерел новин, баз даних відомих торговців людьми та інформації про них.

Традиційний людський інтелект збирається на місцях в конкретній країні благодійними організаціями, переглядаючи джерела новин, чутки і інші ресурси, що знаходяться в їх розпорядженні. Оскільки багато благодійних організацій діють тільки в одній країні, а торгівля людьми відбувається між країнами, цю інформацію часто необхідно передати урядовим і внутріурядової організаціям, щоб скласти профіль торгівця людьми або діяльності в більш широкому сенсі. Однак цього традиційного інтелекту зазвичай недостатньо для швидкого виявлення мережі торговців людьми. Використовуючи великі дані, програмне забезпечення штучного інтелекту здатне знаходити зв'язки між людьми і їх транзакціями, адресами, партнерами і зв'язками компаній, а також масу іншої відповідної інформації, яка може вказувати на протиправну діяльність. Розбираючи ці окремі сутності, технологія ІІ може побудувати детальну картину злочинної мережі, помістивши окрему транзакцію або відносини в більш широкий контекст. Використовуючи поєднання людського інтелекту і зібраної в цифровому вигляді інформації, правоохоронні органи можуть ідентифікувати торговців людьми і їх зв'язку.

УДК.004

ГНЕДЮК ВОЛОДИМИР ЛЕОНІДОВИЧ

Головний спеціаліст

Українського науково-дослідного інституту

спеціальної техніки та судових експертиз

Служби безпеки України

АКТУАЛЬНІ ПИТАННЯ ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРАВООХОРОННУ ДІЯЛЬНІСТЬ

Нині в розвинених країнах світу приділяється велика увага питанням інформатизації суспільства. Все більшим стає розуміння того, що держава, яка буде володіти потужними інформаційними ресурсами, ефективною системою їх реалізації, буде знати динаміку й перспективи їх розвитку, опиниться на гребні науково-технічного прогресу і зможе його ефективно використовувати. Не залишається осторонь цих процесів і Україна, в якій відбувається інтенсивне впровадження сучасних інформаційних технологій майже в усі сфери життєдіяльності суспільства, зокрема, в правоохоронну діяльність. Формуючи і ефективно використовуються різні інформаційно-пошукові системи, бази та банки даних, системи електронного документообігу. Новітні інформаційні технології дають можливість працівникам правоохоронних органів отримати багатоцільову довідкову, аналітичну та статистичну інформацію, що сприяє продуктивному виконанню ними різних оперативно-службових завдань .

Оптимізація вирішення завдань пошуку, відбору та систематизації інформації, необхідної в діяльності поліції, базується на конструкті єдиного інформаційного простору системи МВС України, який логічно визначити як сукупність спеціалізованих баз і банків даних, технологій їх ведення та використання, інформаційно-телекомунікаційних систем і мереж, суб’єктів інформаційно-аналітичної діяльності, які функціонують на основі єдиних принципів і за загальними правилами забезпечують інформаційну взаємодію системи Міністерства внутрішніх справ України і громадян [3, с. 266–267].

Одною з ключових вимог до успішної роботи інформаційних технологій у разі взаємодії правоохоронних органів є їх уніфікація та стандартизація. Під час здійснення взаємодії правоохоронних органів уніфікація дає можливість: здійснювати розробку програмних та аналітичних систем на єдиній платформі; отримувати однакову і безперебійну роботу апаратного та програмного забезпечення; здійснювати оцінку, аналіз поточної та майбутньої обстановки у сферах взаємодії [2, с. 100].

Завданнями інформаційного забезпечення публічного адміністрування в органах Національної поліції України слід визначити:

- узгодження дій суб'єктів здійснення публічного адміністрування;
- сприяння прийняттю ефективних управлінських рішень, спрямованих на оптимізацію та розвиток системи Національної поліції України;
- створення інформаційних систем, спрямованих за внутрішнє забезпечення публічного адміністрування та взаємодію із зовнішнім середовищем та його інформаційним простором (системами) [1, с. 139].

Розвиток інформаційних технологій у системі правоохоронної діяльності корелятивний розвитку злочинності, виробленню нових методів приховування злочинів і результатів злочинної діяльності. У сучасному світі намагання правоохоронних органів інтегрувати у свою діяльність інформаційні технології зумовлено організованою злочинністю, яка характеризується високою координацією та конспіративністю, ієрархічною структурою, стійкою взаємодією. Найбільш високотехнологічними є механізми протиправної діяльності у фінансовій сфері.

Варто вказати, що забезпечення функціональної діяльності правоохоронних органів – не єдина причина, що породжує необхідність розвитку та впровадження hi-tech технологій. Відповідно до Стратегії кібербезпеки України створення безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави досягається взаємодією державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів,

громадських об’єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та / або є власниками (розпорядниками) об’єктів критичної інформаційної інфраструктури. Стратегія вимагає не тільки створення та використання інформаційно-телекомунікаційних систем і баз даних правоохоронними органами в процесі їх взаємодії, а й забезпечення безпеки, безперебійності роботи таких технологій, надійності обміну відомостями [2, с. 100–101].

Висновок. Отже, інформаційне забезпечення правоохоронних органів є комплексною категорією, яка об’єднує як процес збору, оброблення, аналізу та збереження інформації, так і систему відомостей, зафіксованих у встановленому порядку. На сьогодні основні напрями такого інформаційного забезпечення регламентовані законодавством, але вони потребують уточнення в напрямі конкретизації їх у сфері адміністративно-юрисдикційної діяльності, а також чіткого визначення порядку обміну інформацією між різними суб’єктами такої діяльності. Крім того, в законодавстві, що регулює таку діяльність, доцільно закріпити вимоги до інформації та порядок її оброблення і збереження.

Список використаних джерел:

1. Бугайчук К. Інформаційне забезпечення публічного адміністрування в органах Національної поліції. / К. Бугайчук// Підприємництво, господарство і право.- 2019. - № 6.- С. 135–141.

2. Мамчур Л. О. До питання про міжсуб’єктну взаємодію правоохоронних органів з використанням інформаційних технологій. / Л. О. Мамчур // Право і суспільство.- 2018. - Т. 2, №6.- С. 97–103.

3. Шорохова Г. М. Інформаційне забезпечення діяльності територіальних органів поліції України. / Г. М. Шорохова // Юридичний науковий електронний журнал. – 2018 - №6. - С. 264–267.

УДК 004.49: 004.056.57

ГОЛОВНЯ АМІНА ІГОРІВНА

Курсантка 3 курсу факультету №4

Харківського національного університету внутрішніх справ.

ГНУСОВ ЮРІЙ ВАЛЕРІЙОВИЧ

кандидат технічних наук, доцент,

завідувач кафедри кібербезпеки та DATA-технологій факультету №6

Харківського національного університету внутрішніх справ

ЗАХИСТ ВІД ВІРУСІВ-ШИФРУВАЛЬНИКІВ

Сьогодні найпоширеніша проблема в світі цифрових технологій є віруси-шифрувальники. Вони шифрують всі файли на комп'ютері таким чином, що власник втрачає до них доступ. Вірус-шифрувальник (шифратор, криптор) – особливий різновид шкідливих програм-здирників, чия діяльність полягає в шифруванні файлів користувача і, в подальшому, вимоги викупити засіб розшифровки. Суми викупу починаються десь від $200 і досягають десятків і сотень тисяч.

Частіше за все, такий вірус може потрапити на Ваш ПК через електронну пошту, якщо точніше, через файли та посилання, прикріплені до повідомлення. Перейти по них/завантажити файл змушує текст повідомлення: «Терміново погасіть борг по кредиту», «Ой, це ти на фото?», «Позовна заява подана до суду», «Сплатіть штраф / внесок / податок», «Донарахування комунального платежу», «Лена попросила терміново передати це тобі» та інші провокуючі фрази. Існують і інші шляхи завантаження вірусу: соціальні мережі, розсилка у месенджерах, шкідливі і заражені веб-ресурси, банерна реклама, розсилка через месенджери зі зламаних акаунтів, сайти розповсюджувачі кейгенів і кряків, сайти з порнографічним контентом, магазини додатків і контенту.

Як діяти для того, щоб зберегти важливі файли та не потрапити в пастку?

По-перше, якщо Ви – директор фірми чи підприємства, для якого є не бажаним описана вище ситуація, поясніть своїм підлеглим про можливість настання такої ситуації, про можливість загрози та наслідки, що чекають на

Вашу кампанію у разі успішної атаки. Важливо вказати на те, що не можна переходити по невідомим посиланням та завантажувати не перевірені файли.

Якщо ж Ви - рядовий користувач ПК, Вам теж не слід забувати про вказані вище речі. Не переходьте за посиланнями, якщо не впевнені в їх безпечності. Та не встановлюйте файли чи документи.

По-друге, бажано створити резервну копію всіх файлів, що буде зберігатися на сервері. Та будь-які нові файли також довантажувати на цей сервер.

По-третє, за можливості, працювати лише у віртуальному, ізольованому середовищі.

Розуміння можливостей вірусу – перший крок в його подоланні. Отож, будучи освідомленим у цьому питанні, та слідуючи представленим вказівкам, Ви будете відчувати себе захищеним.

УДК 004.942:004.946

Д'ЯКОВ АНДРІЙ ВОЛОДИМИРОВИЧ

кандидат технічних наук,

доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів

Львівського державного університету внутрішніх справ

ВИКОРИСТАННЯ СИСТЕМ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ, ЯК ПОТУЖНИЙ ЗАСІБ ПІДГОТОВКИ ФАХІВЦІВ МВС

Вдосконалення системи підготовки кадрів МВС, зокрема пошук найбільш дешевих та в той же час ефективних форм і методів підготовки є найголовнішою задачею розвитку Національної поліції та Національної гвардії України. Економічні аспекти з одного боку та розвиток інформаційних технологій з іншого вимагають застосовувати разом з традиційними нові форми і методи організації проведення підготовки. Цими новими формами, в тому числі і як показує досвід провідних країн НАТО, є заходи підготовки з

використанням засобів імітаційного моделювання, зокрема комп'ютерні командно-штабні навчання, комп'ютерні командно-штабні тренування, різні види навчальних занять (тактико-стройові, практичні тощо) із використанням засобів імітаційного моделювання.

Застосування засобів імітаційного моделювання суттєво знижують умовність дій за рахунок створення віртуального бойового середовища, де усі сили і засоби діють на реальній місцевості та як в реальній бойовій обстановці. Результати імітації усіх конфліктуючих сторін враховуються у реальному масштабі часу. Реалії такого протистояння надають можливість відповідним командирам та начальникам приймати рішення на відповідні дії, а також вести підготовку до дій як в реальних бойових умовах.

Вищою формою спеціального математичного і програмного забезпечення управління силами та засобами у сучасному збройному протистоянні є моделі операцій (бойових, спеціальних дій та інш.). Найбільш повними і адекватними є імітаційні моделі. Теоретично за їх допомогою можна представити та завчасно програти операцію (бій та інш.) з будь-яким ступенем точності, в цьому випадку тільки технічні засоби виступають тут обмежувальним фактором.

Застосування засобів імітаційного моделювання в ході комп'ютерних навчань дозволяє моделювати оперативно-тактичну обстановку, різні бойові ситуації, а також проводити розрахунки та готувати дані для прийняття рішення та планування спеціальних дій. Все це дозволяє відпрацьовувати різноманітні варіанти застосування підрозділів в інтересах широкого спектра задач (бойових, миротворчих, спеціальних). Відмінністю від традиційних форм проведення навчань є забезпечення відпрацювання слухачами всебічно обґрунтованих рішень на застосування підрозділів та ефективного управління при виконанні поставлених задач за рахунок проведення оперативно-тактичних розрахунків і математичного моделювання бойових дій в єдиній інформаційно-моделюючому середовище, а також забезпечення автоматизованої розробки

навчально-методичних документів, планів нарощування обстановки та розигришу імітації спеціальних (бойових) дій.

Слід зауважити, що органи управління , відповідальні за підготовку та проведення заходів оперативної підготовки, отримують можливість шляхом математичного (в т.ч. імітаційного) моделювання здійснювати об'єктивний прогноз розвитку обстановки у відповідності із рішенням конфліктуючих сторін та при цьому враховується значно більша кількість факторів у порівнянні із методами абстрактно-логічного прогнозування.

Широке поширення застосування засобів імітаційного моделювання отримало у збройних силах провідних країн світу, в тому числі і у Збройних Силах України. На сьогодні існує так звана *LVC*- концепція підготовки військ, яка базується на комплексному використанні трьох видів моделювання: «живої» бойової реальності (*Live*), віртуального (*Virtual*) та конструктивного (*Constructive*) моделювання. При цьому кожен сегмент моделювання фактично визначає особливості побудови засобу моделювання та область його застосування.

Так, моделювання «живої» бойової реальності (*Live Simulator, L-сегмент*) передбачає використання реальних військовослужбовців та реальних систем при проведенні тактичних навчань різних рівнів. У процесі виконання заходів спеціальної (бойової) підготовки або при проведенні навчального процесу використовується реальне озброєння та військова техніка в реальних умовах. Ефекти взаємодії можуть бути визначені підіграванням протилежного боку. Даний вид моделювання характерний для застосування на полігонах, навчальних центрах, тощо.

Віртуальне моделювання (*Virtual Simulator, V-сегмент*) передбачає роботу реальних людей з системами, що імітуються в інформаційно-моделюючому середовище, тобто використання різних видів і типів тренажерів при проведенні заходів бойової підготовки, спрямованих на одиночну підготовку слухачів, навчання та злагодження підрозділів. Цей вид

моделювання застосовується у місцях постійної дислокації при проведенні тренувань, тактико-стройових занять, тощо.

Конструктивне моделювання (*Constructive Simulator, С-сегмент*) включає модель особового складу, озброєння та військової техніки, підрозділи. Реальні посадові особи контролюють відтворення, де взаємодіють змодельовані війська, техніка та озброєння. Така система моделювання використовується для проведення навчальних заходів при підготовці органів управління, штабів підрозділів. Даний вид моделювання застосовується при проведенні командно-штабних навчань, починаючи із тактичної ланки.

Аналіз існуючих методів моделювання та способів застосування засобів імітаційного моделювання у підготовці (від органів управління до окремого службовця) передбачає висновок, що імітаційне моделювання повинно стати потужним засобом у підготовці фахівців МВС.

УДК 351.741 (477) :004

ЄВТУШОК ВОЛОДИМИР АНАТОЛІЙОВИЧ

старший викладач кафедри тактичної

та спеціальної фізичної підготовки факультету № 3

Харківського національного університету внутрішніх справ

АКТУАЛЬНІ ПИТАННЯ ВИКОРИСТАННЯ КОМПОНЕНТІВ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

З прогресом у галузі інформаційних технологій також зростає кількість шляхів їх використання у сферах різноманітних професій. Слід визнати, що використання інформаційних технологій полегшують роботу працівників правоохоронних органів закордонних країн та України, разом з полегшенням виникають також питання розробки, удосконалення, впровадження і використання інформаційних технологій у діяльності правоохоронних органів.

Останні роки характеризуються перенесенням акцентів у діяльності органів правопорядку у розвинених країнах з принципу реагування на злочини, до принципу попередження злочину. Використання компонентів інформаційних технологій у сфері боротьби зі злочинністю набуває все більших обертів з моменту реформування правоохоронних органів.

Застосування, розробка та впровадження компонентів інформаційних технологій у діяльності органів правопорядку є не тільки опцією, а і необхідністю, це пов’язано з використанням вищевказаних засобів представниками кримінального світу. Найближчим часом не залишиться невисокотехнологічної злочинності, навіть рядовий кишеньковий злодій буде мати у своєму арсеналі новітній гаджет, створений для полегшення здійснення процесу крадіжки.

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-відсоткове охоплення відеоспостереженням (не пізніше 2018 р.) саме відеофайли стануть основним елементом даних і матеріалом для профілактики злочинності та проведення розслідувань.[1, с. 9.]

Боротьба з розповсюдженням наркотичних речовин через мережу інтернет – була і залишається якщо не основною, то точно однією з головних проблем у боротьбі зі злочинністю в кіберпросторі. Закон існує у кожній країні, але інтернет – явище яке не має кордонів у часі та просторі, що дозволяє обходити законодавчу систему задля купівлі, продажу та розповсюдженні наркотичних засобів і прекурсорів.

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. [2, с. 94.]

Законодавче впровадження і використання таких компонентів наразі є однією з проблем інформаційних технологій та їх компонентів, бо документально внести систему використання, застосування та подальшу підтримку програмного забезпечення є нелегкою задачею. Не допомагає цьому і затяжне прийняття законопроектів пов'язаних з правоохоронними органами.

Основними тенденціями розвитку інформаційних технологій у правоохоронній сфері є: 1) удосконалення форм та методів управління Застосування інформаційних технологій у діяльності правоохоронних органів. Харків, 2020. 130 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 [3, с. 130.]

Наразі можемо констатувати, що рівень компонентів інформаційних технологій на використанні у діяльності правоохоронних органів України потребує вдосконалення, інновацій та порад експертів на тему використання інформаційних технологій з більшою користю.

Список використаних джерел.

1. Швець Д.В. СТРАТЕГІЧНІ НАПРЯМКИ ВИКОРИСТАННЯ НОВІТНІХ ТЕХНОЛОГІЙ ЦИФРОВОГО СВІТУ В ПОПЕРЕДЖЕННІ ЗЛОЧИНІВ. // Застосування інформаційних технологій у діяльності правоохоронних органів : зб. матеріалів кругл. столу / МВС України, Харків. нац. ун-т внутр. справ. – Харків : ХНУВС, 2020.

2. Орлов Р.Р., Грищенко Д.О. ПРАВООХОРОННІ ОРГАНИ В БОРОТЬБІ З РОЗПОВСЮДЖЕННЯМ НАРКОТИЧНИХ РЕЧОВИН ЧЕРЕЗ МЕРЕЖУ ІНТЕРНЕТ. // Застосування інформаційних технологій у діяльності

правоохоронних органів : зб. матеріалів кругл. столу / МВС України, Харків. нац. ун-т внутр. справ. – Харків : ХНУВС, 2020.

3. Федоренко О.А. ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ДІЯЛЬНІСТЬ ПРАВООХОРОННИХ ОРГАНІВ. // Застосування інформаційних технологій у діяльності правоохоронних органів : зб. матеріалів кругл. столу / МВС України, Харків. нац. ун-т внутр. справ. – Харків : ХНУВС, 2020.

УДК 343.85 (477)

ЄРМАК ОЛЕКСІЙ ВІКТОРОВИЧ

кандидат юридичних наук, головний науковий співробітник 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 Україні 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 № 2617-VIII. URL: https://zakon.rada.gov.ua/laws/show/2617-19#Text (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. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (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 №314-VII від 23 травня 2013 року. URL: https://zakon.rada.gov.ua/laws/show/314-18#Text (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.

УДК 355.451:004.7

ЖАРОВ ЛЕВ ВОЛОДИМИРОВИЧ

курсант 3 курсу факультету №4

Харківського національного університету внутрішніх справ

ГНУСОВ ЮРІЙ ВАЛЕРІЙОВИЧ

кандидат технічних наук, доцент,

завідувач кафедри кібербезпеки та DATA-технологій факультету №6

Харківського національного університету внутрішніх справ

ОСНОВНІ ВИДИ КІБЕРШАХРАЙСТВА ТА СПОСОБИ ПРОТИДІЇ

На сьогоднішній день багато людей користуються мережею інтернет та вважають, що вони достатньо освічені в сфері «кібершахрайства». Такі люди помиляються, що для уникнення обману зі сторони досвідчених шахраїв їх знань буде достатньо.

Я зараз перерахую типові схеми якими нікого з вас не здивую:

1) Залякування – шахраї дзвонять жертві та представляючись робітниками державних органів і повідомляють, що хтось із знайомих має деякі неприємності та вимагають хабара [1].

2) Виграш – шахраї повідомляють про деякі виграші, перерахунки пенсій або інших виплат, повернення кредитів. Зазвичай, злочинці називаються працівниками банків, та силових структур [1].

3) Проблеми з карткою – шахрай видає себе за покупця, телефонує продавцю і просить відіслати йому інформацію за картами, бо іншим способом переказати гроші чомусь не виходить. Також шахраї можуть всі реквізити та

іншу інформацію за якою можно отримати доступ до рахунку (СМС від банку, паролі від сервісів, дати та інше) [1].

Навіть знаючи що це з великою вірогідністю шахрайство люди ведуться і скоюють помилки за які потім жаліють. Одним з принципів протидії таким видам злочинів - превенція. Шляхом повторного роз'яснення способів і методів скоєння, запобігання шахрайських дій. Таким чином це зменшить кількість жертв від такого виду злочинів.

Упродовж 2020 року до кіберполіції за формою зворотного зв'язку надійшло більше 41 тисячі звернень громадян, із них понад 80% - щодо шахрайств [2].

«Близько 78% населення України у віці 16 років та старше (приблизно 25 млн осіб) користується інтернетом. З них приблизно 500 тисяч щодня стикаються з кіберзлочинцями. Наймасовішою схемою шахраїв у 2020 став фішинг — відправлення посилань на сайти-підробки. Практично у всіх випадках злочинці використовують методи соціальної інженерії: прикидаються продавцями, покупцями та навіть співробітниками банку, а потім застосовують маніпуляцію, щоб жертва сама віддала свої платіжні дані», — розповів Віктор Нобіуз, керівник відділу бізнес-аналітики компанії OLX Україна [3].

Більш сучасні вид шахрайства:

– Отримання посилки – до вас приходить смс, що для вас прибула посилка, лист і вам потрібно прийти та забрати її, але ви нічого не замовляли. Прийшови на почту вам потрібно сплатити за посилку, лист який в основному коштує до 300грн. Сплативши в ньому ви можете знайти якісь предмет або записку яка не коштує ту суму яку ви потратили за отримання посилки.

– Віруси та інше шкідливе ПЗ – шкідливі програми які потрапляючи на ваш комп'ютер або на телефон ворують всі ваші данні включаючи всі паролі та логіни від усіх сервісів.

– Інтернет-жебрацтво – фейкові сторінки благодійних організацій які прохають про матеріальну допомогу від усіх небайдужих для всіляких добрих цілей, але на справді всі кошти зберігаються у шахраїв.

Отже в інтернеті дуже багато способів для шахрайства і не варто вважати, що ти не потрапиш в халепу від цих шахраїв. Аби убезпечитися від подібних видів шахрайства, кіберполіція радить:

– не передавайте нікому дані своєї банківської картки (особливо CVV-код та пін-код), адже працівники банку ніколи не запитують таку інформацію;

– для безпечного онлайн-шопінгу використовуйте лише перевірені ресурси та обирайте післяплату;

– у разі купівлі на платформі оголошень, обговорюйте деталі угоди тільки в чаті цієї платформи і не переходьте в сторонні месенджери;

– зверніть увагу, що сайти, які приймають онлайн-платежі, мають бути захищеними, для цього в назві адреси вони мають містити https:// та значок «замочок».

– уважно перевіряйте правильність назви необхідного сайту. Один непомітний символ на панелі адреси може означати, що ви потрапили на фішинговий сайт;

– не переходьте за сумнівними посиланнями [2].

Список використаних джерел:

1. Різновиди шахрайства у кіберпросторі. Що потрібно знати для власної кібербезпеки. Частина 1 [Електронний ресурс]. – Режим доступу : https://cybermediatrack.com/kiber-kibershahrajstvo-kiberbezpeka .

2. У 2020 році до кіберполіції надійшло понад 30 тисяч звернень щодо шахрайства в Інтернеті (15 січня 2021 р. 09:54) [Електронний ресурс]. – Режим доступу : https://cyberpolice.gov.ua/news/u--roczi-do-kiberpolicziyi-nadijshlo-ponad--tysyach-zvernen-shhodo-shaxrajstva-v-interneti-8412 .

3. За рік інтернет-шахраї вкрали 252 мільйони гривень в українців: головні методи злочинців (09 лютого 2021, 15:14) [Електронний ресурс]. – Режим доступу : https://business.rayon.in.ua/news/344808-za-rik-internet-shahrayi-vkrali-252-milioni-griven-v-ukrayintsiv-eksperti-nazvali-golovni-metodi-zlochintsiv .

УДК 004.056

ЗАГОРЕЦЬКА ЄЛИЗАВЕТА РОМАНІВНА

курсантка 2 курсу факультету №4

Харківського національного університету внутрішніх справ

КАЛЯКІН СЕРГІЙ ВОЛОДИМИРОВИЧ

викладач кафедри протидії кіберзлочинності факультету №4

Харківського національного університету внутрішніх справ

ПРОБЛЕМА ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ

В останні роки особливо загострилася проблема захисту інформації в мережі. Це спричинила різка необхідність використовувати різні ресурси для дистанційного навчання, онлайн роботи та іншого. Internet і інформаційна безпека несумісні по самій природі Internet. Платою за користування Internet є загальне зниження інформаційної безпеки, тому для запобігання несанкціонованому доступу до своїх комп'ютерів всі корпоративні і відомчі мережі, а також підприємства ставлять фільтри між внутрішньою мережею і Internet, що фактично означає вихід з єдиного адресного простору [1].

Природно, комп'ютерні атаки можуть принести і величезний моральний збиток. Поняття конфіденційного спілкування давно вже стало притчею. Зрозуміло, що ніякому користувачу комп'ютерної мережі не хочеться, щоб його листи крім адресата одержували ще 5-10 чоловік або, наприклад, весь текст, що набирається на клавіатурі ЕОМ, копіювався в буфер, а потім, при підключенні до Інтернету, відправлявся на визначений сервер. А саме так і відбувається в тисячах і десятках тисяч випадків.

Існує безліч суб'єктів і структур, дуже зацікавлених у чужій інформації і готових заплатити за це високу ціну. Так, вартість пристроїв підслуховування, що продаються тільки в США, становить в середньому близько 900 млн. дол. у рік. Сумарні втрати, нанесені організаціям, проти яких здійснювалося прослуховування, складають щорічно в США близько 8 млрд. дол. Але ж існують і, відповідно, здобуваються пристрої для несанкціонованого доступу до інформації і по інших каналах: проникнення в інформаційні системи,

перехоплення і дешифрування повідомлень і т.д. У результаті, за даними SANS Institute, середній розмір збитку від однієї атаки в США на корпоративну систему для банківського і IT-секторів економіки складає біля півмільйона доларів.

Аналіз стану інформаційної безпеки України показує, що до основних проблем забезпечення інформаційної безпеки належать проблеми загальносистемного характеру, пов'язані з відсутністю наукового обґрунтування і практичної апробації політики і методології державної системи інформаційної безпеки. За характером це правові та нормативно-правові, науково-технічні, (економічні, організаційні, кадрові проблеми тощо [2].

Ситуація, що склалася в інформаційній сфері України, вимагає невідкладного рішення таких комплексних проблем:

1) розвиток науково-практичних основ інформаційної безпеки, а саме, визначення основних положень стратегії держави в сфері створення і забезпечення умов формування і використання інформаційного ресурсу, підтримка високих темпів його наповнення і заданих критеріїв якості (доступність, достовірність, своєчасність, повнота), розробка сучасних інформаційних технологій і технічних засобів для вирішення задачі захисту інформації в інформаційних системах;

2) створення законодавчої і нормативно-правової бази забезпечення інформаційної безпеки, а саме, нормативно-правової бази щодо розподілу і використання персональної інформації з метою створення умов для інформаційних стосунків між органами державної влади і суспільства, формування передумов досягнення соціального компромісу, створення умов становлення соціального партнерства як основи демократичного розвитку суспільства, розробки регламенту інформаційного обміну для органів державної влади і управління, реєстру інформаційних ресурсів, закріплення відповідальності посадових осіб, громадян за додержання вимог інформаційної безпеки;

3) розроблення механізмів реалізації прав громадян на інформацію загального користування;

4) визначення основних положень стратегії держави у сфері використання засобів масової інформації на засадах досліджень процесів формування суспільної свідомості, удосконалення та розвиток індустрії інформування населення країни, розробка методів і форм інформаційної політики держави [3];

5) розробка методів і засобів оцінки ефективності систем і засобів інформаційної безпеки та їх сертифікація.

Отже, інформаційна безпека України залежить від вирішення проблем формування і керування процесами суспільної свідомості, виробництва та репродукції інформаційних ресурсів і доступу до них, створення цивілізованого ринку інформаційних продуктів та послуг, реалізації прав громадян на інформацію.

Список використаних джерел:

1. А.М. Гафіяк Сучасні проблеми захисту інформації, 2018 (Електронний ресурс) / Режим доступу : http://www.rusnauka.com/21_NIEK_2007/Informatica/23650.doc.htm

2. Є.О. Бокіна, Технологія захисту інформації. Проблеми захисту інформації в сучасних іс. Основні види сучасних комп'ютерних злочинів. Засоби захисту інформації, 2016 Електронний ресурс) / Режим доступу : https://shag.com.ua/tema-tehnologiya-zahistu-informaciyi-problemi-zahistu-informac.html

3. А.Б. Баутов, Эффективность защиты информации, 2003 (Електронний ресурс) / Режим доступу :https://www.osp.ru/os/2003/07-08/183282

УДК 004.056.5, 004.7

КАЛАНЧА АНДРІЙ АНДРІЙОВИЧ

курсант 1 курсу факультету №4

Харківського національного університету внутрішніх справ;

СВІТЛИЧНИЙ ВІТАЛІЙ АНАТОЛІЙОВИЧ

кандидат технічних наук, доцент,

доцент кафедри протидії кіберзлочинності факультету №4

Харківського національного університету внутрішніх справ

ЗАСОБИ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ В МЕРЕЖІ

Згідно статті 11 і 21 Закону України «Про інформацію» до конфіденційної інформації про фізичну особу, зокрема, належать дані про її національність, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження. Хоча сьогодні інформація про інтереси користувача - гарячий товар. Її збирають про кожного, хто спілкується в цифровому світі, використовують самі та/або перепродують. Таргетована реклама, відстеження усієї мережевої активності інтернет-провайдерами, стеження зі сторони держави та інші негативні соціальні явища, що порушують нашу конфіденційність вже стали буденними для кожного. Забезпечити власну безпеку (анонімність) в мережі - тяжка праця, що вимагає масивного обсягу знань. Навіть кращі знавці у цій сфері не завжди можуть впоратися. Перше що потрібно розуміти, так це те, що 100% анонімність - це міф, бо повна анонімність може бути тільки при відсутності пристрою взагалі [0].

Проксі-сервери

Глобально, коли говорять «проксі-сервер», то мають на увазі щось, що виступає посередником між клієнтом і адресатом.

У розрізі забезпечення анонімності проксі-сервери бувають:

• HTTP-(веб)-проксі-сервери. Такі сервери пропускають через себе тільки HTTP-трафік;

• SOCKS-проксі-сервери. На відміну від HTTP-проксі-серверів, SOCKS передає всю інформацію, нічого не додаючи від себе;

• окремо варто згадати CGI-проксі або «анонімайзери», які по суті становлять собою web-сервер з формою, де клієнт вводить адресу потрібного

сайту. Після чого відкривається сторінка запитаного ресурсу, але в адресному рядку браузера видно адресу CGI-проксі. CGI-проксі, як і будь-який web-сервер може використовувати https для захисту каналу зв'язку між собою і клієнтом [2].

Схему роботи проксі-серверу ви бачите на рисунку 1.

Рисунок 1. — Схема роботи проксі-сервера

Переваги проксі-серверів:

• проксі дешеві, в мережі можна знайти багато безкоштовних проксі.

Недоліки проксі-серверів:

• треба довіряти проксі-серверу;

• для http-проксі треба фільтрувати HTTP-заголовки;

• необхідність налаштування проксі-сервера для кожної програми або використання окремих програм-соксифікаторів, наприклад, Proxifier.

VPN/SSH

Йдеться про VPN, маючи на увазі також і SSH-тунелі. Оскільки, не зважаючи на деякі відмінності, основний принцип у них однаковий. Схема роботи VPN показана на рисунку 2.

Рисунок 2. — Схема роботи VPN

Наразі комерційними провайдерами пропонуються такі протоколи VPN:

• PPTP - використовується найбільш широко, швидкий, легко налаштовується, проте вважається «найменш захищеним» порівняно з іншими;

• L2TP + IPSec. L2TP забезпечує транспорт, а IPSec відповідає за шифрування. Ця зв'язка має більш сильне шифрування, ніж PPTP, стійка до вразливостей PPTP, забезпечує також цілісність повідомлень і автентифікацію сторін;

• OpenVPN - безпечний, відкритий, а отже, поширений, дозволяє обходити блокування, але вимагає окремого програмного клієнта;

• SSTP - такий же безпечний, як і OpenVPN, окремого клієнта не вимагає, проте сильно обмежений у платформах: Vista SP1, Win7, Win8.

Окремо варто відзначити сервіси, що надають «DoubleVPN», коли перед тим, як вийти в Інтернет, трафік проходить 2 різних VPN-сервери в різних країнах, або навіть «QuadVPN», коли використовується 4 сервери, які користувач може вибрати сам і розташувати в довільному порядку [2].

Переваги VPN/SSH:

• швидко і зручно, не треба окремо налаштовувати програми.

Недоліки VPN/SSH:

• потрібно довіряти VPN/SSH-серверу/провайдеру.

Tor

Це система маршрутизаторів, в якій клієнт з'єднується з Інтернетом через ланцюжок вузлів. Як правило, ланцюжок складається з трьох вузлів, кожному з них невідомі адреси клієнта і ресурсу одночасно. Крім того, Tor шифрує повідомлення окремо для кожного вузла, а відкритий трафік видно тільки вихідному роутеру [2]. Схема роботи Tor показана на рисунку 3.

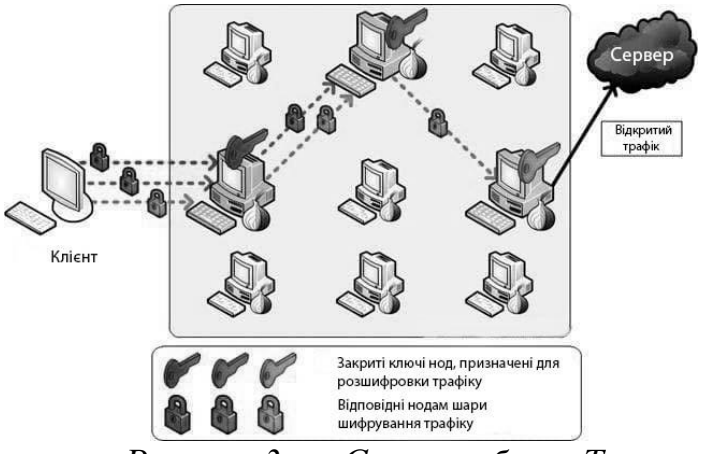

Рисунок 3. — Схема роботи Tor

Переваги Tor:

• високий ступінь анонімності клієнта при дотриманні всіх правил;

• простота використання (завантажив Tor Browser Bundle, запустив і користуйся).

Недоліки Tor:

• вихідний трафік прослуховується;

• низька швидкість;

• наявність керуючих серверів.

Висновки. Анонімність - соціокультурне явище, що побудоване довкола поняття приватності та свободи кожної людини в Мережі. Зараз інформація про інтереси користувача – це гарячий товар. Її збирають про кожного, хто спілкується в цифровому світі, використовують самі та/або перепродують. Як збирають інформацію і кому це може бути цікаво – нікому не відомо, оскільки ними може бути як продавець таргетованої реклами, так і правління, яке активно відслідковує кожен наш крок в житті за допомогою геолокації і пошуковий запит в мережі Інтернет; інформація про те, хто і про що говорив, яку думку має. Тож дотримуватися анонімності в мережі, можливо, наш єдиний спосіб уберегтися від «Великого Брата», тобто від паноптикуму, і хоча б у кіберпросторі залишатися тими, ким ми є справді і не боятися переслідувань за власну думку, інтереси та бажання. Інтернет – місце, де кожен може бути вільним у всіх розумінням цього слова.

Список використаних джерел:

1. Практичний посібник з анонімності в онлайні [Електронний ресурс]. – Режим доступу : https://habr.com/ru/company/vdsina/blog/556914/

2. Методи аномності у мережі [Електронний ресурс]. – Режим доступу : https://blog.agronavtika.ru/2016/03/18/metodyi-anonimnosti-v-seti-chast-1-pros/

УДК 004.4

КАЛАНЧА АНДРІЙ АНДРІЙОВИЧ

курсант 1 курсу факультету № 4

Харківського національного університету внутрішніх справ

ЯНОВ ВАСИЛЬ ВІКТОРОВИЧ

кандидат технічних наук, доцент,

доцент кафедри протидії кіберзлочинності факультету № 4

Харківського національного університету внутрішніх справ

ЗАБЕЗПЕЧЕННЯ БАЗОВОЇ АНОНІМНОСТІ В МЕРЕЖІ ІНТЕРНЕТ

Згідно статті 11 і 21 Закону України «Про інформацію» до конфіденційної інформації про фізичну особу, зокрема, належать дані про її національність, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження. Анонімність є одним із аспектів конфіденційності.

Пересічні користувачі мережи Інтернет фактично не захищені від сбіру про них інформації. Безліч організацій збирають різноманітною інформацію про інтереси користувачів які знаходяться та спілкуються у цифровому світі для використання для своїх цілей або для перепродажі. Таргетована реклама, відстеження усієї мережевої активності інтернет-провайдерами, стеження зі сторони держави та інші негативні соціальні явища, що порушують нашу конфіденційність вже стали буденними для кожного.

Для забезпечення власній анонімності у мережі треба володіти певним обсягу знань. Але, забезпечення базової анонімності в мережі Інтернет можливо за допомогою проксі-сервера, VPN, Tor.

У розрізі забезпечення анонімності проксі-сервери бувають:

HTTP-(веб)-проксі-сервери. Такі сервери пропускають через себе тільки HTTP-трафік;

SOCKS-проксі-сервери. На відміну від HTTP-проксі-серверів, SOCKS передає всю інформацію, нічого не додаючи від себе;

окремо варто згадати CGI-проксі або «анонімайзери», які по суті становлять собою web-сервер з формою, де клієнт вводить адресу потрібного сайту. CGI-проксі, як і будь-який web-сервер може використовувати https для захисту каналу зв'язку між собою і клієнтом.

Проксі-сервера та VPN дають можливість змінити ip - адрес.

Комерційними провайдерами пропонуються такі протоколи VPN:

PPTP – використовується найбільш широко, швидкий, легко налаштовується, проте вважається «найменш захищеним» порівняно з іншими;

L2TP + IPSec. L2TP забезпечує транспорт, а IPSec відповідає за шифрування. Ця зв'язка має більш сильне шифрування, ніж PPTP, стійка до вразливостей PPTP, забезпечує також цілісність повідомлень і автентифікацію сторін;

OpenVPN – безпечний, відкритий, а отже, поширений, дозволяє обходити блокування, але вимагає окремого програмного клієнта;

SSTP – такий же безпечний, як і OpenVPN, окремого клієнта не вимагає, проте сильно обмежений у платформах: Vista SP1, Win7, Win8.

Окремо варто відзначити сервіси, що надають «DoubleVPN», коли перед тим, як вийти в Інтернет, трафік проходить 2 різних VPN-сервери в різних країнах, або навіть «QuadVPN», коли використовується 4 сервери, які користувач може вибрати сам і розташувати в довільному порядку.

Tor – це система маршрутизаторів, в якій клієнт з'єднується з Інтернетом через ланцюжок вузлів. Як правило, ланцюжок складається з трьох вузлів, кожному з них невідомі адреси клієнта і ресурсу одночасно. Крім того, Tor шифрує повідомлення окремо для кожного вузла, а відкритий трафік видно тільки вихідному роутеру.

Список використаних джерел:

1. Про інформацію: закон України від 02.10.1992; [із змінами і доповненнями на 16.06.2020]. Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 18.11.2021).

2. Практическое руководство по анонимности в онлайне // Хабр : сайт. 18.05.2021. URL: https://habr.com/ru/company/vdsina/blog/556914/(дата звернення: 19.11.2021).

3. VPN и приватность. Анонимность в интернете. Анонимайзеры. // URL: https://www.tadviser.ru/index.php/Статья:VPN_и_приватность_(анонимность,_анонимайзеры) (дата звернення: 21.11.2021).

УДК 004.932:351.741(477)

КІОР СЕРГІЙ СЕРГІЙОВИЧ

курсант навчальної групи Ф4-302

Харківського національного університету внутрішніх справ.

СОЛЯНИК ТЕТЯНА МИКОЛАЇВНА

кандидат технічних наук, доцент,

доцент кафедри протидії кіберзлочинності факультету № 4

Харківського національного університету внутрішніх справ

ЗАСТОСУВАННЯ НЕЙРОННИХ МЕРЕЖ ДЛЯ МОНІТОРИНГУ ДОРОЖНЬОГО ТРАФІКУ

Розвиток сучасних технологій поступово розширює можливості людства. Технічний прогрес полегшує роботу у багатьох сферах, у тому числі і в правоохоронній діяльності. Забезпечення правоохоронних органів різноманітними технічними засобами дає можливість більш ефективно використовувати людські ресурси і приносить плідні результати вже багато років. Прикладом є використання камер відеоспостереження для слідкування за дотриманням правил дорожнього руху (ПДР). На теперішній час вони встановленні майже скрізь: всі місця потенційного скупчення людей, вулиці, автомагістралі та навіть під'їзди будинків. З розвитком технологій нейронних мереж можливості таких камер значно розширились.

Використання нейронних мереж спрощує моніторинг дотримання ПДР у декілька десятків разів та дозволяє здійснювати його автоматично. Для цього достатньо один раз налаштувати систему та супроводжувати її роботу. Прикладом є використання системи КАСКАД (комплексна автоматизована система контролю автомобільних доріг). Незважаючи на обмежений

функціонал цієї системи (вона обробляє тільки факт перевищення швидкості) та відносно невелику кількість встановлених комплексів, за рік її роботи кількість ДТП у місцях встановлення камер знизилась на 65%, і це беззаперечно дуже позитивна динаміка. Проте в місцях, де таких комплексів немає, як і раніше за ситуацією на дорозі слідкують працівники правоохоронних органів. Автоматизація моніторингу дорожнього трафіку з використанням нейронних мереж дозволить збільшити ефективність використання камер відеоспостереження та зменшити навантаження на правоохоронців.

Аналіз існуючих підходів до вирішення цієї задачі показав, що існують два способи застосування нейронної мережі для моніторингу дорожнього трафіку. Перший – встановлювати цілі стаціонарні комплекси, які ведуть відеозапис та обробляють його. Недоліком такого рішення є велика вартість системи та складність в налаштуванні та обслуговуванні кожної одиниці (вартість системи КАСКАД – 683 тис. гривень). Іншим варіантом є використання звичайних відеокамер, які вже встановленні в багатьох місцях. Але при цьому виникає ряд вимог до технічних характеристик мережі відеоспостереження (камер), а саме:

1. Якість зображення, яка повинна бути достатньою для роботи штучного інтелекту.

2. Порівняно однакові можливості запису в будь-який період доби.

3. Камера повинна мати змогу охоплювати 3 та більше дорожніх смуг. Для цього потрібно визначитись з фокусною відстанню матриці камери та її відстані від дороги.

4. Система живлення використовуваних технічних засобів. Оптимально використовувати лінії електроживлення.

5. Утворення бездротової мережі з центром обробки даних.

Наступним є вирішення питання зі способом обробки даних. Це може здійснюватися безпосередньо на боці камери або віддалено. Перевагою віддаленої обробки є загальне налаштування та обслуговування системи для багатьох засобів відеофіксації. Інформація може оброблюватись у режимі реального часу або з носія після попереднього запису. Мінусом обробки у

режимі реального часу є необхідність у великих обчислювальних потужностях. Обробка запису потребує пам’яті для його збереження. Використання пам’яті можна оптимізувати автоматичним видаленням оброблених записів зі збереженням фрагментів, де було виявлено порушення. За умови, що обробка буде здійснюватися віддалено, треба визначити, як інформація буде передаватись до цього місця та як буде здійснюватися безпосередньо обробка. Та як саме нейронна мережа буде визначати, що сталось саме порушення ПДР?

Після отримання запису нейронна мережа оброблює його, визначаючи на ньому об’єкти та їх властивості. Це можуть бути колір, марка та номерний знак автомобіля. У більшості випадків для цього використовуються згорткові нейронні мережі. Це спеціальна багатошарова архітектура нейронної мережі, яка не має зворотного зв’язку між шарами та краще всього підходить для розпізнавання об’єктів.

Шляхом її навчання, завантажуючи зображення, на яких є транспорт, з вказанням типу цих об’єктів мережа оброблює їх та на основі отриманих даних згодом стає здатною сама виявляти такі об’єкти на інших записах. Якщо навчити мережу розпізнавати транспортний засіб, його номер та його крайні точки, мережа зможе порівнювати крайні точки транспорту з точками дорожнього покриття, визначаючи швидкість, перетин смуг та інші маневри. Створивши умови, за якими буде визначатись порушення, згідно ПДР та порівнюючи з ними поведінку об’єктів можна буде фіксувати відхилення від ПДР та класифікувати це як порушення.

Фіксація номерного знаку дозволить встановити власника транспортного засобу, а також перебування цього транспорту у розшуку, за допомогою офіційних відкритих розшукових обліків. Після того, як штучний інтелект розцінив поведінку як порушення ПДР, залишається вирішити, чи буде людина перевіряти вірність прийнятого рішення, і після цього виносити рішення про накладення стягнення.

Отже, використання штучного інтелекту для моніторингу дорожнього трафіку може значно спростити цю задачу. Це зменшить кількість ДТП у країні,

дозволить більш раціонально та ефективно використовувати матеріальні ресурси, технічні засоби та людський труд, що позитивно відобразиться на якості життя людей та умовах роботи працівників правоохоронних органів.

УДК 004.056.5

КОБЗЕВ ІГОР ВОЛОДИМІРОВИЧ

кандидат технічних наук, доцент,

доцент кафедри цифрових технологій та електронного урядування

Харківського національного університету ім. В.Н.Каразіна

ГОРЕЛОВ ЮРІЙ ПЕТРОВИЧ

кандидат технічних наук, доцент,

кафедри кібербезпеки та DATA-технологій факультету №6

Харківського національного університету внутрішніх справ

ІНФОРМАЦІЙНА БЕЗПЕКА В ТЕХНОЛОГІЯХ ДИСТАНЦІЙНОГО НАВЧАННЯ

Технології дистанційного навчання (ДН) є яскравим прикладом злиття освітніх та інформаційних технологій. Новітні інформаційні технології забезпечили можливість швидкого, досить дешевого поширення навчальної інформації, її адресної доставки на необмежену відстань у будь-який час та зумовили активізацію роботи багатьох закладів освіти з впровадження технологій ДН у навчальний процес. Особливого поширення використання ДН набуло під час епідемії COVID-19.

З'явилася велика кількість центрів дистанційного навчання, розроблений ряд систем ДН, серед яких найбільш популярні: Moodle, TrainingWare, Claroline LMS та ін.

Технології ДН дозволяють не тільки реалізувати швидкий та зручний доступ до навчального матеріалу, але й застосовувати технології спільної творчої діяльності (метод проектів), проблемні ролеві ігри, кейс-методи,

автоматизовані та відкриті форми контролю, як автоматизовані, так і відкриті види контролю та ін.

Але широке використання ДН особливо гостро ставить питання забезпечення інформаційної безпеки під час навчання.

Виділяють наступні загрози нормальному функціонуванню системи електронного навчання :

– неавторизований доступ до цифрового контенту;

– порушення цілісності і неадекватність навчальних ресурсів;

– порушення нормального функціонування служб і сервісів;

– порушення безпеки процедур тестування.

Безпеку електронного навчання необхідно забезпечувати в декількох взаємозалежних областях, які і впливають на якість електронного навчання. Перерахуємо деякі питання, що мають відношення до забезпечення інформаційної безпеки в ДН:

– чи самостійно слухач отримує знання, виконує завдання і роботи?;

– хто дійсно проходить процедури тестування, виходить в інтерактивний режим і навіть розмовляє з викладачем в режимі on-line?;

– чи буде слухач, що навчається за технологією дистанційного навчання мати навички публічних виступів, ведення диспутів і т. п.;

– як буде захищено авторське право викладача на курси, що розробляються їм, тести і інший методичний матеріал, що публікується в Інтернеті або розсилається по електронній пошті?;

– наскільки обґрунтованими можуть бути посилання студента на відмову в обслуговуванні, хакерські атаки, збої в роботі мережі. Організація взаємодії усіх учасників освітнього процесу для досягнення цілей навчання і рішення учбових завдань багато в чому залежить від тих педагогічних технологій, якими володіє педагог.

Однією з ключових умов забезпечення інформаційної безпеки ДН являється підготовка педагогічних кадрів, що володіють сучасними педагогічними і інформаційними технологіями організації учбового процесу з урахуванням особливостей дистанційного навчання.

Система підвищення кваліфікації і перепідготовки педагогічних працівників, професійна підготовка студентів вимагає включення в зміст навчання матеріалу з інформаційній безпеки, що відповідає критеріям професійної спрямованості.

УДК 343.1

КОРОСТЕЛЬОВА ЛІЛІЯ АНАТОЛІЇВНА

ад'юнктка Луганського державного університету

внутрішніх справ імені Е. О. Дідоренка

ІННОВАЦІЙНІ РОЗВІДКИ СОЦІАЛЬНИХ МЕРЕЖ У БОРОТЬБІ ІЗ ЗЛОЧИННІСТЮ

.Стрімкий розвиток за останні 10 років мережі Інтернет і розвиток соціальних мереж вражає.

Соціальні мережі стали найпопулярнішою складовою сучасного Інтернету, яким у світі користуються нині понад 2 млрд осіб. Більше 60 % з них є активними користувачами інтерактивних сервісів Web 2.0. Зі 100 найбільш відвідуваних сайтів у світі 20 – це класичні соціальні мережі, ще 60 – тією чи іншою мірою використовують Web 2.0, тобто є соціалізованими [1].

Активне спілкування, взаємне інформування та обговорення найгостріших проблем сучасності у найрізноманітніших життєвих сферах відбувається в соціальних мережах. Ця форма громадської активності стає однією з визначальних тенденцій стану розвитку суспільства. Соціальні мережі є невід'ємним елементом спілкування більшості учасників онлайн-комунікації. Через них користувачі здобувають альтернативні до традиційних медіа факти, коментують, інтерпретують і поширюють їх, стаючи таким чином співучасниками процесу [2].

Окрім позитивного направлення соціальних мереж є і негативне направлення, яке полягає у тому, що використовуються соціальні мережі злочинними угрупуваннями що займаються терористичною та екстремісткою

діяльністю, наркобізнесом, торгівлею людьми тощо. Через соціальні мережі також активно розповсюджується порнографічна продукція, пропагуються суспільно-небезпечні ідеї (насильство, національну та релігійну ворожнечу тощо).

Одним із напрямів дослідження соціальних мереж, який на разі використовують правоохоронні органи є оперативний кримінальний аналіз, який здійснюється за конкретними оперативно-розшуковими справами або кримінальними провадженнями для збору, оцінки, обробки й аналізу даних про осіб, групи осіб, організовані групи чи злочинні організації, знаряддя та засоби вчинення злочину, сліди злочину чи предмети, здобуті злочинним шляхом, та інших відомостей з метою встановлення події злочину, причетності конкретних осіб до його вчинення, також їх соціального й економічного статусу, структури та зв'язків злочинних груп, ролі їх окремих учасників тощо [3, с.125].

Використання сучасних програмних забезпечень надають нові напрями роботи кримінальному аналітику. Одним із таких спеціалізованих програмних забезпечень, які використовуються для аналізу соціальних мереж є *I2 Analysts Notebook.*

Аналітичні функції цієї програми дають змогу досліджувати групові структури та потоки інформації на схемі, фокусуючись на взаємозв'язках, які існують між об'єктами (саме цей тип аналізу називається аналізом соціальних мереж). Структура мережі може визначати:

– функціональність мережі загалом і її здатність досягати своїх ключових цілей;

– неочевидні характеристики мережі, наприклад, існування меншої підмережі, яка функціонує всередині мережі;

– взаємозв'язки між значущими особами, становище яких

допомагає найістотніше впливати на всю мережу;

– наскільки безпосередньо і швидко передається інформація між людьми в різних частинах мережі. [3, с.133].

Отже, використання сучасних інформаційних технологій кримінальними аналітиками із кожним роком все більше зростає. Для подальшої розвідки

даних із соціальних мереж у боротьбі із злочинністю необхідно створювати нові програмні продукти, які будуть ефективно взаємодіяти вже із існуючими спеціальними програмними забезпеченнями.

Список використаних джерел:

1. Проблеми суспільної безпеки в процесі розвитку соціальних мереж. URL:http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=1745 problemi-suspilnoji-bezpeki-v-protsesi-rozvitku-sotsialnikh merezh&catid=78&Itemid=412 (дата звернення: 10.11.2021).

2. Гіда О.Ф. Соціальні мережі як засіб деструктивних впливів через інформаційний простір. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*.Київ.2013. №3 (31). С.268-278.

3. Федчак І.В. Основи кримінального аналізу : навчальний посібник. Львів : Львівський державний університет внутрішніх справ, 2021. 288 с.

УДК 004.056

КУЗОВКО ВЛАДИСЛАВ ОЛЕКСАНДРОВИЧ

курсант 3 курсу факультету №4

Харківського національного університету внутрішніх справ

КАЛЯКІН СЕРГІЙ ВОЛОДИМИРОВИЧ

викладач кафедри протидії кіберзлочинності факультету №4 Харківського національного університету внутрішніх справ

ROOTKIT ЯК КОМПОНЕНТ МАСКУВАННЯ КІБЕРЗЛОЧИНІВ

Термін «rootkit» спочатку відбувається світу операційних систем Unix, де слово «root» використовується для опису користувача з максимально можливим рівнем прав доступу, аналогічно «Адміністратора» в Windows. Слово «kit» відноситься до програмного забезпечення, яке надає доступ до кореневої папки машини. Тепер з'єднаємо їх разом, і вуаля - виходить «руткіт», програма, яка дозволяє сторонньому користувача, незалежно від його намірів, отримати привілейований доступ до комп'ютера [1].

В останні роки особливо загострилася потреба використання кіберзлочинцями Rootkit, тому що він надає вносити зміни на фундаментальному рівні ОС що дозволяє переслідуючи мету несанкціонованого отримання інформації з метою отримання приватної, економічної, стратегічної переваги, використовуючи віддалений доступ до скомпрометованих вузлів, перехоплення мережевого трафіку, шпигування за користувачами, відслідковування натискання клавіш(так званий кейлоггер), викрадання даних для доступу або використання технічних засобів потерпілих для майнінгу криптовалюти, а також участь цих технічних засобів у DDOS атаках.

Руткити зустрічають в переліку шкідливого програмного забезпечення зловмисників не так часто, як інші різновиди. Наприклад, згідно з статистики компанією Bitdefender [2], руткити становлять менше 1% від загального списку шкідливих програм, що виявляються. Однак усі епізоди виявлення пов’язані з гучними атаками. Серед них, наприклад шпигунська компанія APT-груп «Strider» (вони ж ProjectSauron, або G0041), поширювали руткит Remsec (кейлоггер). Угруповання накопичувала інформацію про використовувані способи шифрування: в атаках на держустанови зловмисники крали ключі шифрування, файли конфігурації, збирали IP-адреси серверів інфраструєтури шифрування. Кіберзлочинці були націлені на організації на території Росії, Бельгії, Китаю, Ірану, Швеції та Руанди [3].

Хоча через високу складність розробки руткити використовуються не часто, вони несуть у собі загрозу, оскільки маскують шкідливу активність на пристроях і перешкоджають своєчасному виявленню факту компрометації. Руткити все ще успішно використовуються в атаках, незважаючи на впровадження засобів захисту від них в сучасних операційних системах.

В цілому RootKit це клас malware, які часто йдуть у парі з троянськими або іншими видами шкідливих програм. Сам по собі Rootkit нічого поганого не робить - його основне завдання приховати від сторонніх очей присутність в системі певних шкідливих програм. Найчастіше RootKit може бути виконаний як спеціальним чином модифікована системна програма (системний файл). Бувають

випадки, що якийсь із важливих системних файлів, після модифікації в ньому всього декількох байт стає RootKit-компонентом, дозволяючи іншому шкідливому програмному забезпеченню тривалий час успішно ховатися в системі. За наявності активного руткіта дуже важко знайти приховуваний ним файл «вірусу». Наприклад, RootKit може перехоплювати запити на пошук файла і не показувати його в результатах, таким чином навіть при фізичної наявності файлу його не можливо буде знайти [4].

Перший руткіт для Windows було написано в далекому 1999 році експертом в сфері безпеки Хоглундом і названо NT Rootkit. Він приховував всі файли і процеси, в імені яких зустрічалося сполучення root, перехоплював інформацію з клавіатури тощо.

Одним з найбільш відомих на сьогодні руткітів є Hacker Defender, який працює на користувацькому рівні. У 2005 році в системі захисту від копіювання фірми Sony було виявлено руткіт XCP, який блокував відключення даної програми. Після донесення цієї інформації до широкого загалу через деякий час почали з’являтися шкідливі програми, які до свого складу включали вище згаданий руткіт. Актуальним для сучасного користувача є існування таких відомих руткітів, як TDDS, ZeroAccess, Alureon і Necurs.

На рахунку TDDS більше 3 мільйонів інфікованих комп’ютерів. Розробники засобів безпеки не зупиняють свої зусилля у спробі зупинити поширення цього руткіту і продовжують удосконалювати програми з його виявлення і нейтралізації.

Боротьбою з ZeroAccess зайнялися фахівці з Microsoft разом з представниками ФБР і Європолу, і вже на першому етапі було виявлено більше 2 мільйонів ПК, скомпрометованих наявністю шкідливого кода. Alureon знаходять у 74% заражених комп’ютерів. Цей руткит й досі утримує одну із лідируючих позицій.

Найближчим часом руткіти не пропадуть із інструментів кіберзлочинців. Фахівці PT ESC відзначають появу нових версій руткітів, чий механізм роботи відрізняється від уже відомих шкідливих даних, і це свідчить про те, що зловмисники не стоять на місці і вигадують нові техніки обходу захисту.

Переваги, які дає використання руткітів - виконання коду в привілейованому режимі, можливість ховатися від засобів захисту та непомітно перебувати в мережі тривалий час - надто важливі для злочинців, щоб відмовитися від такого інструменту [4].

Список використаних джерел:

1. Що за звір rootkit? [Електронний ресурс]. – Режим доступу : https://ua.softlist.com.ua/articles/chto-za-zver-rootkit/

2. Антивірус Битдефендр [Електронний ресурс]. – Режим доступу: https://bitdefender.ru/

3. Руткіти: еволюція та способи виявлення [Електронний ресурс]. – Режим доступу: https://www.ptsecurity.com/ru-ru/research/analytics/rootkits-evolution-and-detection-methods/#id2

4. Руткіт: експерт з маскування шкідливого ПЗ [Електронний ресурс]. – Режим доступ: https://zillya.ua/rutkit-ekspert-z-maskuvannya-shkidlivogo-pz

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

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 пійматись на даний проект, треба бути скептично налаштованим. На справжніх проектах з виплати коштів, не треба вносити свої гроші, тому що на всі грошові операції використовуються посередні кошти з виплат.

HYIP проекти (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 проектів тим, що у них нема реальної діяльності проекта. 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 проекту 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 проектах, 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 проект, 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.

УДК 343.1 + 004

МАНЖАЙ ОЛЕКСАНДР ВОЛОДИМИРОВИЧ

кандидат юридичних наук, доцент,

завідувач кафедри протидії кіберзлочинності факультету № 4

Харківського національного університету внутрішніх справ

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ОРГАНАМИ ТА ПІДРОЗДІЛАМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Згідно з Інструкцією із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису, затвердженої наказом МВС України від 18.12.2018 р. № 1026 безпілотний літальний апарат (БпЛА) – це повітряне судно, призначене для виконання польоту без пілота на борту, керування польотом якого і контроль за яким здійснюються за допомогою спеціальної станції керування, що розташована поза повітряним судном. БпЛА можуть бути обладнані системами (однією або декількома) фото- і відеозапису

залежно від технічних характеристик повітряного судна. Кількість відеокамер та порядок їх використання на БпЛА (умови польотів, погодні умови, час доби тощо) визначаються згідно з керівництвом з льотної експлуатації БпЛА та/або згідно з інструкцією виробника. Підготовка та розробка польотного завдання, у якому визначається початок та кінець роботи систем фото- і відеозапису, розміщених на БпЛА, здійснюються у порядку, визначеному законодавством, із дотриманням відповідних вимог, польотне завдання затверджує керівник органу підрозділу поліції. Після виконання польотного завдання інформація з карти пам'яті або флеш-карти БпЛА експортується (переноситься) на носій інформації (карту пам'яті або флеш-карту) працівника поліції, який ставив завдання, про що робиться відмітка в польотному завданні.

Головними напрямами використання БпЛА в Національній поліції України можна назвати:

- картографування місцевості, результати чого у подальшому можна використовувати у розслідуваннях та забезпеченні публічної безпеки та порядку;

- висвітлення подій, які відбуваються на певній території;

- реагування на масові заходи та їх фіксація, у тому числі шляхом подачі звукових та світлових сигналів з БпЛА;

- допомога у розвитку та підтримці різноманітної діяльності населення;

- моніторинг вуличного трафіку;

- спостереження з оперативною метою;

- переслідування правопорушників;

- здійснення оголошень у важкодоступних місцях;

- виявлення місць вчинення правопорушень;

- криміналістичне дослідження місця злочину;

- дистанційне обстеження предметів;

- реконструкція подій;

- інспектування та моніторинг об'єктів, що становлять небезпеку для життя та/або здоров'я людини;

- виявлення та вилучення незаконних та незареєстрованих БпЛА;

- пошук підземних сховищ тощо.

Водночас потрібно розуміти, що головну цінність становлять не самі БпЛА, а дані, які одержують за їх допомогою: зображення, великі дані, дані сенсорів, логістичні дані тощо. Лише один БпЛА здатен накопичувати терабайти даних щодня. І ці дані потрібно накопичити та проаналізувати перед тим, як передати кінцевому споживачеві [1, с. 33]. Саме тому слід опрацювати питання:

- накопичення, зберігання та аналізу інформації з камер відеоспостереження дронів у взаємодії з державними та приватними підприємствами, установами, організаціями, що їх експлуатують;

- у межах системи безпечного міста реалізувати цілодобове патрулювання засобами БпЛА територій зі складною оперативною обстановкою. З цією метою слід проводити щосекундну панорамну зйомку з камер з великою роздільною здатністю (не менше 0,5 м на піксель). Ці дані слід зберігати на сервері та за необхідності відслідковувати ретроспективні події на певній території, аналізуючи матеріали зйомки. Вказана система здатна суттєво знизити рівень злочинності в місті. Описану систему вже було успішно випробувано у м. Балтімор США.

- поєднання технологій безпілотного пілотування та розпізнавання (номерів, обличь тощо);

- посилення прогностичної складової під час запровадження програмних рішень аналітичної обробки інформації з систем фіксації БпЛА. Це пов’язано з тим, що прогностична модель стримування злочинності поступово інтегрується з моделлю Intelligence-Led Policing – організації діяльності поліції на основі розвідувальних відомостей.

Список використаних джерел:

1. Jenkins D., Visagh B. Drone Economic$: Succeeding with the World’s Newest Form of Transportation, LLC, 2021. 400 p.

УДК 004.056.5, 004.7

МАСНИЙ ПАВЛО ІГОРЕВИЧ

курсант 1 курсу факультету №4

Харківського національного університету внутрішніх справ

СВІТЛИЧНИЙ ВІТАЛІЙ АНАТОЛІЙОВИЧ

кандидат технічних наук, доцент,

доцент кафедри протидії кіберзлочинності факультету №4

Харківського національного університету внутрішніх справ

ОГЛЯД ПРОГРАМ АНАЛІЗУ І МОНІТОРИНГУ МЕРЕЖЕВОГО ТРАФІКА

Вступ. Моніторинг трафіку життєво важливий для управління мережею. Він є джерелом інформації про функціонування корпоративних додатків, яка враховується при розподілі коштів, плануванні обчислювальних потужностей, визначенні та локалізації відмов, вирішенні питань безпеки.

Основна мета виступу. Однією з актуальних наукових завдань на даний час є аналіз (і подальше прогнозування) самоподібної структури трафіку у сучасних мультисервісних мережах. Для вирішення цього завдання необхідний збір та подальший аналіз різноманітної статистики (швидкість, обсяги переданих даних тощо) у діючих мережах. Збір такої статистики у тому чи іншому вигляді можливий різними програмними засобами. Однак існує набір додаткових параметрів та налаштувань, які виявляються дуже важливими при практичному використанні різних засобів.

Виклад основного матеріалу.

Нині можна нарахувати не один десяток програмних продуктів, призначених для аналізу та моніторингу мережевого трафіку, кожен з яких має свої переваги та недоліки. За результатом дослідження, було розглянуто близько десяти програм-аналізаторів трафіку (сніфери) та більше десятка програм для моніторингу мережевого трафіку, з яких було відібрано найцікавіші [1].

BMExtreme

Це нова назва добре відомої багатьом програми Bandwidth Monitor. Раніше програма поширювалася безкоштовно, тепер вона має три версії, і безкоштовною є лише базова. У цій версії не передбачено жодних можливостей, крім власне моніторингу трафіку, тому навряд можна вважати її конкурентом інших програм. За стандартом BMExtreme стежить як за Інтернет-трафіком, так і за трафіком у локальній мережі, проте моніторинг у LAN за бажання можна вимкнути.

BWMeter

Ця програма має не одне, а два вікна стеження за трафіком: в одному відображається активність в Інтернеті, а в іншому – у локальній мережі.

Програма має гнучкі налаштування для моніторингу трафіку. З її допомогою можна визначити, чи потрібно стежити за прийомом та передачею даних в Інтернет тільки з цього комп'ютера або з усіх комп'ютерів, підключених до локальної мережі, встановити діапазон IP-адрес, порти та протоколи, для яких буде або не проводитиметься моніторинг. Крім цього, можна вимкнути стеження за трафіком у певні години чи дні. Системні адміністратори, напевно, оцінять можливість розподілу трафіку між комп'ютерами в локальній мережі. Так, для кожного ПК можна задати максимальну швидкість прийому та передачі даних, а також одним клацанням миші заборонити мережну активність.

Observium

Додаток Observium, робота якого ґрунтується на використанні протоколу SNMP, дозволяє не лише досліджувати стан мережі будь-якого масштабу в режимі реального часу, а й аналізувати рівень її продуктивності. Це рішення інтегрується з обладнанням від Cisco, Windows, Linux, HP, Juniper, Dell, FreeBSD, Brocade, Netscaler, NetApp та інших вендорів.

Завдяки ідеально опрацьованому графічному інтерфейсу, дане ПЗ надає системним адміністраторам безліч варіантів для налаштування – починаючи від діапазонів для автовиявлення і закінчуючи даними протоколу SNMP, необхідними для збору інформації про мережу.

Bandwidth Monitor Pro

Її розробники дуже багато уваги приділили налаштуванню вікна моніторингу трафіку. По-перше, можна визначити, яку саме інформацію програма постійно показуватиме на екрані. Це може бути кількість отриманих та переданих даних (як окремо, так і в сумі) за сьогодні та за будь-який зазначений проміжок часу, середню, поточну та максимальну швидкість з'єднання. Якщо у вас встановлено кілька адаптерів, ви можете стежити за статистикою для кожного з них окремо [2]. При цьому потрібна інформація для кожної мережної картки також може відображатися у вікні моніторингу.

Nagios

Додаток Nagios – це поліпшене рішення для моніторингу, керування яким ґрунтується на веб-інтерфейсі. Він аж ніяк не простий в опануванні, проте, завдяки своїй досить великій інтернет-спільноті та добре опрацьованій документації, може бути опанований за кілька тижнів.

За допомогою Nagios системні адміністратори здатні дистанційно регулювати кількість навантаження на користувача або вище обладнання в мережевій ієрархії (комутатори, маршрутизатори, сервери), стежити за ступенем навантаження запасів пам'яті в базах даних, стежити за фізичною працездатністю деталей мережевого обладнання (наприклад, температура материнської плати, спалювання якої є одним з найбільш частих поломок в цій області) і т.д.

Wireshark (раніше - Ethereal)

Програмне забезпечення для аналізатора трафіку для мереж Computer Ethernet та деяких інших. Має графічний інтерфейс користувача. Wireshark - це додаток, який «знає» структуру найрізноманітніших мережевих протоколів, а тому дозволяє проаналізувати мережевий пакет, відображаючи значення кожного поля протоколу будь-якого рівня. Оскільки PCAP використовується для захоплення пакетів, можна захопити дані лише з мереж, які підтримуються цією бібліотекою. Тим не менш, Wireshark здатний працювати з різними

форматами вхідних даних, відповідно, можна відкривати файли даних, захоплені іншими програмами, що розширює можливості захоплення.

Висновки. Загалом, можна сказати, що більшості домашніх користувачів буде достатньо функцій, які надає Bandwidth Monitor Pro. Якщо говорити про найбільш функціональну програму моніторингу мережевого трафіку, то це, безумовно, BWMeter. З-поміж розглянутих програм-аналізаторів мережевого трафіку хотілося б виділити Wireshark, яка має більшу кількість функціональних можливостей. Я вважаю, що цю тему можна розглядати ще велику кількість часу, але тут було виділено найголовніше (на мою думку).

Список використаних джерел:

1. Топ 10 найкращих програм для моніторингу мережі у 2021 році. Програми для моніторингу мережі [Електронний ресурс]. – Режим доступу : https://www.softinventive.ru/best-network-monitoring-tools/

2. Огляд програм аналізу і моніторингу мережевого трафіка. [Електронний ресурс]. – Режим доступу : http://pi.314159.ru/volotka/volotka1.htm

УДК 004.056.55:004.312.2

МОГІЛЕВСЬКИЙ ЛЕОНІД ВОЛОДИМИРОВИЧ

доктор юридичних наук, професор,

проректор Харківського національного університету внутрішніх справ

ІНФОРМАЦІЙНІ СИСТЕМИ ДЛЯ ПОКРАЩЕННЯ ЕФЕКТИВНОСТИ ЕКСПЕРТНИХ ДОСЛІДЖЕНЬ У ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

В даний час інформаційні системи підтримки прийняття рішень і керуючі інформаційні системи знаходять застосування в різноманітних сферах життя людського суспільства: промисловості, бізнесі, науці та освіті, фінансах і інфраструктурних проектах, будівництві та правоохоронної діяльності. Важливе місце такі інформаційні системи займають і в системі правоохоронній діяльності.

Різноманітна за формами і змістом правоохоронна діяльність неможлива без залучення інформаційних ресурсів, під якими законодавець розуміє окремі документи і окремі масиви документів, документи і масиви документів в інформаційних системах (бібліотеках, архівах, фондах, банках даних, інших інформаційних системах). Інформаційне забезпечення правоохоронної системи має являти собою процес, який визначається законодавцем як процес збору, обробки, накопичення, зберігання, пошуку і розповсюдження інформації. Таким чином, інформаційне забезпечення правоохоронної системи є необхідним для вирішення основних завдань правоохоронних органів. Вирішення таких задач неможливо без спеціалізованих експертних систем та установ.

За своєю сутністю експертне пізнання є різновид пізнання конкретного факту. Воно засноване на тих же принципах, що і будь-який інший вид пізнання в ході розслідування і розгляду справи. Разом з тим воно відрізняється не тільки своєю процесуальною формою, а й, що не менш важливо, засобами і методами.

Особливе місце серед них сьогодні зайняли інформаційні технології. Наслідком цього стали, з одного боку, певна трансформація експертного дослідження як процесу пізнання, з іншого - значне розширення його можливостей, а також підвищення наукової обґрунтованості одержуваних даних. І те й інше має свої об'єктивні передумови, визначається рядом закономірностей інформатизації експертних досліджень, вироблених як в теорії, так і в практиці.

Незважаючи на те що кожна з великого числа використовуваних нині методик експертного дослідження, заснована на використанні комп'ютерів, специфічна і орієнтована на вирішення конкретного завдання при дослідженні різних об'єктів, вони мають ряд загальних властивостей.

По-перше, в основі цих методик лежать такі кардинальні принципи правової інформатики, як принцип системної організованості об'єкта пізнання, кількісних визначень і використання математичного апарату, функціональний і алгоритмічний підхід до самого процесу пізнання і пізнаваного об'єкту.

По-друге, методологічною передумовою, ланкою, що передує формуванню і застосуванню будь-якої конкретної методики дослідження з використанням

комп'ютерів, є математичне моделювання об'єкта і розробка (або вибір) алгоритму процесу його пізнання. При цьому під математичним моделюванням в даному випадку мається на увазі більш широкий клас засобів пізнання, ніж клас засобів, використовуваних при вирішенні суто математичних задач. Тут моделювання передбачає не тільки побудова моделі вирішення певної задачі, а й створення моделі об'єкта аналізу, моделі порівняльного аналізу ознак та ін. А ці моделі в значній мірі є змістовними і будуються не математиками, а експертами-почеркознавцями, балістиками, трасологами і т. д., в залежності від виду експертного аналізу.

По-третє, незалежно від індивідуальних особливостей в структурі кожної з таких методик можна виокремити характерні для будь-якої з них елементи, зокрема, такі, як постановка задачі і визначення мети дослідження; розчленування спільної справи на приватні підзадачі; визначення конкретних засобів і прийомів їх реалізації; власне практична діяльність, що складається з певної сукупності трудових операцій; отримання результату і його оцінка; прийняття рішення.

По-четверте, жодна методика, заснована на використанні комп'ютерів, не охоплює всього процесу рішення експертної завдання. Їх використання, як правило, об'ективізує і автоматизує лише ту чи іншу операцію (або групу операцій), яка може ставитися як до самого процесу пізнання, так і до оцінки отриманих результатів. Тому використання комп'ютерних технологій ні в якому разі не виключає використання якісного підходу до об'єкту пізнання.

З урахуванням сказаного стає очевидним важливість проблеми: людина або машина. У більш ж широкої постановці, це проблеми визначення кордонів, завдань і умов використання комп'ютерів у сфері експертної діяльності, а також її суб'єктів, їх ролі і функцій в автоматизованих системах вирішення правових задач.

УДК 004.9 +343.1

НОСОВ ВІТАЛІЙ ВІКТОРОВИЧ

кандидат технічних наук, доцент,

професор кафедри протидії кіберзлочинності факультету № 4

Харківського національного університету внутрішніх справ

ДЕЯКІ АСПЕКТИ ВПРОВАДЖЕННЯ СТАНДАРТІВ ОБРОБКИ ЕЛЕКТРОННИХ ДОКАЗІВ ДЛЯ ОРГАНІВ МВС УКРАЇНИ

Комп'ютерні мережі інформаційно-телекомунікаційних систем (ІТС) органів Міністерства внутрішніх справ України оброблюють інформацію, яку можна у відповідності з [1, ст.1] віднести до державних інформаційних ресурсів. Згідно [2, ст.8] державні інформаційні ресурси та інформація з обмеженим доступом, крім державної таємниці, службової інформації та державних і єдиних реєстрів, створення та забезпечення функціонування яких визначено законами, можуть оброблятися в системі за умови підтвердження відповідності системи управління інформаційною безпекою (СУІБ) за результатами процедури з оцінки відповідності національним стандартам України щодо СУІБ.

На разі в Україні вже прийнята методом підтвердження ціла низка ДСТУ ISO/IEC серії 27xxx, які визначають вимоги із розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та постійного вдосконалення СУІБ. Для управління інформаційною безпекою у випадках реалізації ризиків, які призвели до виникнення інцидентів, з метою ефективного відновлення інформаційної безпеки, поширення інформації про події безпеки та слабкі місця (вразливості) згідно [3] необхідно впровадження підсистеми *управління інцидентами інформаційної безпеки та вдосконалення СУІБ*. У рамках цієї підсистеми потрібно визначити і при реагуванні на інциденти інформаційної безпеки використовувати *процедури для ідентифікації, збирання, отримання і зберігання інформації,* яку можна використовувати як *докази* для притягнення до юридичної відповідальності осіб, які вчинили правопорушення у сфері інформаційної безпеки. Ці докази за джерелами походження можна назвати *електронними (цифровими) доказами*.

Стандартизована методологія і процедури ідентифікації, збирання, отримання і зберігання електронних доказів мають очевидну цінність не тільки як складова СУІБ ІТС органів МВС України, а й як складова процесу розслідування підрозділами Національної поліції України кримінальних правопорушень у кіберсфері.

Аналіз ДСТУ ISO/IEC серії 27xxx дозволив визначити наступні стандарти, які доцільно впроваджувати у процесі досудового розслідування кримінальних правопорушень щодо електронних доказів:

- ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів;
- ДСТУ ISO/IEC 27040:2016 Інформаційні технології. Методи захисту. Безпека зберігання;
- ДСТУ ISO/IEC 27041:2016 Інформаційні технології. Методи захисту. Настанова щодо забезпечення прийнятності та адекватності методів розслідування;
- ДСТУ ISO/IEC 27042:2016 Інформаційні технології. Методи захисту. Настанови щодо аналізу та інтерпретації цифрового доказу;
- ДСТУ ISO/IEC 27043:2016 Інформаційні технології. Методи захисту. Принципи та процеси розслідування інцидентів;
- ДСТУ ISO/IEC 27050-1:2018 Інформаційні технології. Методи захисту. Електронне виявлення. Частина 1. Огляд та поняття;
- ДСТУ ISO/IEC 27050-3:2018 Інформаційні технології. Методи захисту. Електронне виявлення. Частина 3. Звід правил для електронного виявлення.

Впровадження зазначених стандартів через розроблення методик і настанов з урахуванням вимог КПК України для спеціалістів у кримінальному провадженні, які залучаються для надання безпосередньої технічної допомоги, консультацій та висновків щодо електронних доказів, дозволить значно підвищити ефективність кримінального провадження під час досудового розслідування та визнанням допустимості електронних доказів в інших юрисдикціях.

Список використаних джерел:

1. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 № 3475-IV // База даних «Законодавство України»/Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3475-15 (дата звернення: 23.11.2021).

2. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР // База даних «Законодавство України»/Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр (дата звернення: 23.11.2021).

3. ДСТУ ISO/IEC 27002:2015 (ISO/IEC 27002:2013; Cor 1:2014, IDT) / Поправка № 2:2019 (ISO/IEC 27002:2013/Cor 2:2015, IDT). Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки. Державне підприємство «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості». Київ, 2019. 22 с.

УДК 343.3

ОЛЕКСЮК ОЛЕКСАНДР ПЕТРОВИЧ

слухач магістратури групи Ф1-21-101м

Харківського національного університету внутрішніх справ

ЯНОВ ВАСИЛЬ ВІКТОРОВИЧ

кандидат технічних наук, доцент,

доцент кафедри протидії кіберзлочинності факультету № 4

Харківського національного університету внутрішніх справ

ДЕЯКІ АСПЕКТИ КОНТРОЛЮ ОБІГУ РИНКУ КРИПТОВАЛЮТ В УКРАЇНІ

В останнє десятиліття дуже стрімкими темпами розвивається галузь криптоіндустрії, зокрема ринок криптовалют. Так, станом на 18.11.2021 капіталізація електронних валют досягла вражаючої відмітки в 2,56 трлн. доларів США, і з кожним днем цей показник збільшується.

Для кращого розуміння об’ємів коштів, що циркулюють в даній галузі порівняємо об’єм торгів крипто валютами за 24 години та внутрішній валовий продукт України за 2020 рік, так циркуляція коштів за вищевказану добу становила 122,4 млрд. доларів США, а ВВП 155,6 млрд. доларів США. Україна заробляє шляхом виробництва товарів та наданням послуг за рік суму, яка циркулює в галузі крипто валют лише за 30 годин.

Згідно з дослідженням проведеного в 2021 році аналітиками платіжної платформи «Triple A» за 2020 рік Україна посіла перше місце за відсотком населення, яке володіє криптовалютою – 12,7% (у 5,6 млн. українців є криптовалюта).

Проблематика: Криптовалюти за своєю сутністю володіють високим рівнем анонімності, за рахунок чого ідеально підходять для незаконних операцій.

В Україні відсутня будь-яка нормативно-правова база, яка б регулювала використання крипто валют. Існує лише законопроект №3637 "Про віртуальні активи" від 09.06.2020, який був ухвалений 08.09.2021, але в подальшому повернений главою держави до парламенту зі поправками.

Відсутність правового регулювання електронних коштів зі сторони держави розв’язує руки злочинності, адже цифрові активи дають змогу для приховувати різні види злочинів, таких як: торгівля людьми чи наркотиками, фінансування тероризму, ухилення від сплати податків, відмивання коштів.

Особливе місце серед ряду цих злочинів посідає корупція, адже відсутність можливості відстежити шлях трансакції від відправника до адресата використовуючи технологію Cryptonote.

Під час декларування доходів, відповідно до пункту 6 частини першої статті 46 Закону України “Про запобігання корупції” у розділі 10 «Нематеріальні активи» у декларації слід зазначити криптовалюти, що належать суб’єкту декларування або члену його сім’ї на праві власності станом на останній день звітного періоду. Але процедура контролю за достовірністю інформації, яку надала особа, як така відсутня.

Нині криптовалюта набула такої популярності, що боротьба з нею, як інструментом фінансування злочинності є не доцільною. Шлях один – боротися проте не з монетами, а зі злочинністю та «чорними ринками».

Необхідно правове регулювання таких напрямів:

- реєстрація всіх придбаних та активованих гаманців;
- створення реєстру осіб, що являються власниками цифрових активів;
- оподаткування майнінгу криптовалют.

Список використаної джерел:

1. Законопроект №3637 "Про віртуальні активи" від 09.06.2020. Відомості Верховної Ради України (ВВР), 3637 від 11.06.2020. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69110 (дата звернення: 23.11.2021).

2. Валовий внутрішній продукт (ВВП) в Україні. // URL: https://index.minfin.com.ua/economy/gdp/ (дата звернення: 23.11.2021).

3. Перші в світі. 5,5 млн українців володіли криптовалютою за підсумками 2020 року. // URL: https://finance.liga.net/ua/cryptoeconomics/novosti/pervye-v-mire-55-mln-ukraintsev-vladeli-kriptovalyutoy-po-itogam-2020-goda (дата звернення: 23.11.2021).

УДК [004;343.6]

ОРЛОВ РОМАН РУСЛАНОВИЧ

курсант групи Ф-4-402 факультету № 4

Харківського національного університету внутрішніх справ

МАРКОВ В'ЯЧЕСЛАВ ВАЛЕРІЙОВИЧ

кандидат юридичних наук

помічник начальника ГУНП в Харківській області

ЗБУТ НАРКОТИЧНИХ РЕЧОВИН ЧЕРЕЗ МЕРЕЖУ ІНТЕРНЕТ ТА МЕСЕНДЖЕР «ТЕЛЕГРАМ» ТА МЕТОДОЛОГІЯ РОЗКРИТТЯ ТАКИХ ЗЛОЧИНІВ

Аналіз сучасної наркоситуації в Україні показує, що питома вага синтетичних наркотиків у загальній масі наркотичних засобів і психотропних речовин, що вилучаються, протягом останніх 10 років збільшилася в 13 разів і за підсумками 2021 року посідає друге місце після канабісних наркотиків (26,1%,

5,6 т)(1). Це з появою у світі нових видів «синтетики» (наприклад, похідних N-метилэфедрона).

Безконтактний спосіб поширення синтетичних наркотиків базується на широкому використанні мережі Інтернет, яка розглядається організаторами наркобізнесу не тільки як величезний рекламний та пропагандистський майданчик, але і як засіб комунікації, вербування продавців та кур'єрів, спосіб та місце збуту наркотиків. Аналогічні проблеми наголошуються і на доповідях Міжнародного комітету з контролю за наркотиками ООН.

У спеціалізованих мережевих спільнотах, так званих «наркофорумах», будь-хто охочий за певну плату може розмістити рекламу про продаж наркотичних засобів, їх види, ціни, способи придбання та посилання на свій інтернет-сайт. У тому числі на таких форумах будь-який із зареєстрованих там користувачів може брати участь в обговоренні тих чи інших видів наркотиків та оцінювання діяльності представлених інтернет-магазинів.

Існує два основних типи розповсюдження наркотичних засобів через мережу Інтернет:

1) через інтернет-сайти автоматичного продажу;

2) з використанням програм-месенджерів для миттєвого обміну повідомленнями.

Крім того, програми-месенджери використовуються для організації спам-розсилок з рекламою вказаних магазинів та способів обходу блокування. Для залучення нових та утримання постійних клієнтів проводяться спеціальні маркетингові акції, здійснюються безкоштовні доставки «пробників», надаються знижки тощо.

У цих системах простежується ступінчаста ієрархія, всі функції учасників злочинної діяльності чітко розподілені, дотримується жорстка дисципліна, продумана система безпеки, на яку щедро витрачаються отримані від наркобізнесу доходи. До таких злочинних структур зазвичай входять «заставники» різних рівнів, «вербувальники», «комірники», «кур'єри», «оператори», «фінансовий директор», програмісти, координатори, диспетчери,

фінансисти, касири, легалізатори, хіміки. Співробітник, що добре зарекомендував і проявив себе в роботі, перекладається на вищі посади зі збільшенням заробітної плати. Щодо «персоналу», який допустив порушення, застосовуються штрафні санкції. Кожен співробітник отримує розгорнуті інструкції, в яких докладно описано, як правильно фасувати, зберігати і перевозити наркотичні засоби, робити «закладки», спілкуватися зі споживачами наркотиків, як безпечно користуватися електронними рахунками та переводити в готівку кошти, як користуватися анонімними засобами передачі інформації через Інтернет та анонімними іноземними проксі-серверами при відвідуванні інтернет-сторінок та спілкуванні між собою, як вести себе у разі затримання співробітниками правоохоронних органів тощо. Ряди нижчих ланок постійно поповнюються за допомогою ведення грамотної «вербувальної» роботи в Інтернеті, обіцянням високого доходу за мінімальних тимчасових витрат.

Подібні схеми мережевого наркобізнесу значно ускладнюють встановлення особистостей наркоділків та формування доказової основи їх причетності до злочинної діяльності.

Проведений аналіз показує, що в Україні діє понад 10 тисяч інтернет-ресурсів (у тому числі автомагазини, канали в месенджері Telegram), за допомогою яких здійснюється незаконний збут наркотиків.

Правоохоронні органи, а саме Департамент боротьби з наркозлочинністю безпосередньо займаються розслідуванням та виявленням злочинів пов'язаних із незаконним збутом наркотичних речовин. Щорічно для співробітників вищезгаданого департаменту проводяться тренінги підвищення їх обізнаності та навичок використання інформаційних технологій для розкриття злочинів, пов'язаних із незаконним збутом наркотичних речовин у мережі Інтернет. Також на даний момент в Україні сприяють розкриттю таких злочинів створені боти в месенджері Телеграм: «Чат-Бот СтопНакркотик» (бот дозволяє блокувати наркомагазини в месенджері Телеграм), «StopDangerBot» (бот, що збирає від людей інформацію про наркозакладчиків, графітників та наркопритонів) інших менш відомих ботів, які надають допомогу в боротьбі з наркозлочинністю безпосередньо в інтернеті.

Також основною характерною особливістю розкриття злочинів пов'язаних із незаконним збутом наркотичних речовин у сфері комп'ютерних мереж є те, що цифрова інформація про всі дії в них завжди зберігається. Враховуючи це у практичній діяльності, співробітники Департаменту боротьби з наркозлочинністю для виявлення та встановлення учасників інтернет-магазинів застосовують систему інтернет-розвідки у відкритих джерелах - OSINT, що включає пошук, вибір та збір розвідувальної інформації, отриманої із загальнодоступних джерел, та її аналіз.

На підставі цього можна сказати, що зараз ведеться колосальна робота щодо боротьби з наркозлочинністю в Україні та з кожним днем правоохоронні органи стають все більш обізнаними у сфері інформаційних технологій, що є невід'ємною частиною боротьби зі злочинами, пов'язаними з незаконним збутом наркотичних речовин.

УДК 004.65: 004.451

ПЕРЕЦЬ ОЛЕКСІЙ В'ЯЧЕСЛАВОВИЧ

курсант 4 курсу факультету №4

Харківського національного університету внутрішніх справ.

КАЛЯКІН СЕРГІЙ ВОЛОДИМИРОВИЧ

викладач кафедри протидії кіберзлочинності факультету №4

Харківського національного університету внутрішніх справ

МОЖЛИВОСТІ ВИКОРІСТАННЯ OS ANDRAX У ДІЯЛЬНОСТІ КІБЕРПОЛІЦІЇ УКРАЇНИ

Операційна система (далі OS) Andrax є досить недооціненою операційною системою для діяльності в кіберсфері, та для розслідування кіберзлочинів, пошуку вразливостей, та захисту від них.

OS Andrax являє собою операційну систему для мобільних пристроїв на базі Android 5.0 та вище. Anrdax – це комплекс утиліт для проведення пошуку на вразливості пристроїв, систем та іншого технічного обладнання що може

допускати витоки інформації. В експлуатації Andrax знаходиться понад 200 утиліт для різноманітного застосування, середни них найбільш популярні: Metasploit Framework, Nmap, ARPSpoof, Hydra, Aircrack-NG Tools та ін.

OS Andrax дає змогу створити з мобільного телефону пристрій для проведення пентестінгу мереж та пристроїв. Дає можливість для взлому безпровідних систем (Bluetooth, Wi-Fi – в залежності від можливостей мобільного телефону), реалізації поставлених завдань на поліцейського, згідно відповідному чинному законодавству України.

Головною перевагою OS Andrax виступає візуальна непомітність для звичайних громадян, у людних місцях, де непомітність виконання певних оперативних дій є неможливою без ризику викриття своєї приналежності до правоохоронних органів, що може привести до провалу операції та компрометації своєї особи. В свою чергу OS Andrax встановлена на звичайний мобільний телефон не буде давати приводу стороннім особам або особі що знаходиться в оперативній розробці зайвий раз зловити себе на думці що за нею слідкує оперативний працівник.

Не менше вагомою перевагою з іншими мобільними операційними системами є автоматичне оновлення встановлених утиліт, завдяки чому, не буде зайвої необхідності перевірки оновлень використовуваних утиліт. Додатковим плюсом Andrax є встановлена середа для програмування, в якій оперативний працівник в цілях збору інформаціїї або ліквідації роботи системи зловмисника може в програмному середовищі написати вірус або скрипт що виконає поставлені на оперативного працівника завдання.

Окрім переваг є і недолік операційної системи. Він являє собою складність встановлення OS на певні моделі телефонів, правильність виконання алгоритмів встановлення. При порушенні алгоритму встановлення Andrax система буде працювати нестабільно або взагалі не працюватиме.

Враховуючи всі плюси та мінуси OS Andrax Національній поліції України є сенс на її реалізацію в практичних підрозділах кіберполіції.

УДК 621.34

РАЧИНСЬКИЙ ОЛЕКСІЙ ОЛЕКСАНДРОВИЧ

курсант 2 курсу факультету №1

Харківського національного університету внутрішніх справ

ЄВТУШОК ВОЛОДИМИР АНАТОЛІЙОВИЧ

старший викладач кафедри тактичної та спеціальної підготовки факультету № 2 Харківського національного університету внутрішніх справ

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ВИКОРИСТАННЯ 5G У ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Fifth generation (далі – 5G) – це п’яте покоління мобільної мережі, що в порівнянні з попереднім стандартом - 4G (LTE), дає змогу передавати дані зі значно більшою швидкістю, істотно знижує затримки та реалізує розрізання мережі на окремі простори для віртуалізації єдиної системи, за допомогою широкого спектру нових технічних функцій, яка дасть змогу створити повноцінну екосистему між пристроями.

Ефективність анти кримінальної та охоронної діяльності залежить від ступеня та якості інтеграції інноваційних технологій у роботу правоохоронних органів. 5G є засобом забезпечення найшвидшого зв’язку з майже відсутніми затримками, тому його ефективність застосування у критичних сферах, де необхідна якомога швидка передача даних: організація безпеки дорожнього руху, можливість створення стрімінгових платформ, які у режимі реального часу будуть вести трансляції з нагрудних камер поліцейських тощо. Також однією з головних переваг 5G є Internet of Things (далі – IoT). За допомогою технології розшарування мережі, IoT під’єднає пристрої до інтернету та надасть їм нові функції, після чого взаємопов'язані прилади виключать необхідність участі людини, за рахунок використання відповідного програмного забезпечення та обладнання. Наприклад, оснащення службових автомобілів автокеруванням, у випадках критичних ситуацій, де необхідно направити транспортний засіб з точки А у точку Б, без участі водія; проведення огляду

місця події спеціалістами-вибухотехніками НПУ, за відсутність можливості безпосереднього та фізичного контакту.

Незважаючи на всі позитивні аспекти переходу до 5G є ряд проблемних питань, які пов’язані з використанням систем законного перехоплення телекомунікацій (далі – СПТ) :

1. Неможливість опрацювання збільшеного об’єму даних. Як ми вже зазначили – мережі 5G передають дані зі швидкістю значно переважаючу минулий протокол зв’язку (швидкість LTE – 100 Мб/с, а вдосконалого LTE-Advanced - 1Гб/с, на відміну від 10-20 Гб/с, що надає 5G). Це майже унеможливлює проведення оперативно-розшукових заходів та негласних слідчих (розшукових) дій у телекомунікаційних мережах загального користування за допомогою стандартних методів СПТ, через технічну нездатність мережного комплекту і засобів управління системою перехоплення телекомунікацій (далі – ЗУСП) (сервери, станції, термінали та інші) опрацювати різко збільшений потік даних (збір, обробка, аналіз, зберігання тощо).

2. Хєндовер. Це процес передачі сесії зв’язку, що відбувається при переході користувача з однієї зони покриття в іншу. Явище виникає внаслідок неможливості повністю покрити країну однією інфраструктурою – покриттям 5G. Через це системи СПТ повинні опрацьовувати постійну фіксацію та контроль даних під час зміни мереж, які працюють на різних технологіях радіодоступу, що потребує технічного вдосконалення програмного забезпечення ЗУСП та СПТ в цілому.

3. Розгортання головної магістралі 5G Core. Мережа 5G Core дає змогу суміщати одночасну роботу 4G та 5G та має абсолютно нову архітектуру та механізми роботи. Головним нововведенням є підтримка криптографії протоколу захисту транспортного рівня (далі – TLS), яке дає можливість здійснювати зв’язок користувачам мережі, унеможливлюючи проведення дешифрування пакетів зв’язку та отримання доступу за допомогою СПТ, що є головною проблемою розгортання 5G.

Отже, з урахуванням вище викладеного матеріала ми можемо зробити такий висновок: мережа 5G має ряд інноваційних переваг над попереднім стандартом 4G(LTE), але через технічну недосконалість СПТ розгортання 5G ставить під загрозу проведення оперативно-розшукових заходів та негласних слідчих (розшукових) дій у телекомунікаційних мережах, що в свою чергу може призвести до погіршення криміногенного положення у країні та здійснення охоронних функцій правоохоронними органами.

УДК 004.056:351.741

РУДИЙ ТАРАС ВОЛОДИМИРОВИЧ

кандидат технічних наук, доцент,

доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів

Львівського державного університету внутрішніх справ

ЗАЧЕК ОЛЕГ ІГОРОВИЧ

кандидат технічних наук, доцент,

доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів

Львівського державного університету внутрішніх справ

ЗАХАРОВА ОЛЕКСАНДРА ВАСИЛІВНА

кандидат юридичних наук, доцент,

доцент кафедри кримінального процесу та криміналістики

Львівського державного університету внутрішніх справ

ДЕЯКІ АСПЕКТИ ОРГАНІЗАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ДЕРЖАВИ

Важливим завданням для України в найближчій перспективі є розроблення та негайне реалізування прийнятних організаційно-правових заходів у практиці протидії кіберзлочинності, наповнення уже прийнятих рамкових законів реальним змістом. До того ж, встановлені завдання суб’єктів

національної системи протидії кіберзлочинності не узгоджуються з базовими чинними законодавчими актами та забезпечення кібербезпеки.

З огляду на той факт, що чітких і зрозумілих нормативно-правових документів та організаційно-правових заходів щодо забезпечення національної системи кібербезпеки, захисту інформаційного простору держави нема, тому і розв'язання проблем політики держави у сфері безпеки цифрового простору (тобто без розгляду інформаційних відносин з пункту бачення об'єкта правового регулювання) є неможливим. Розглянемо основні проблеми та прогалини у організаційно-правовому забезпеченні протидії кіберзлочинності.

Кіберпростір України є дуже вразливим, бо не існує єдиної об'єднаної стратегії кіберзахисту. Основні завдання в сфері кіберзахисту, які повинні формуватися і реалізовуватися на державному рівні полягають у наступному: захист суверенітету кіберпростору та забезпечення базової кібербезпеки; захист об'єктів критичної інфраструктури; запровадження диджіталізації процесів державного управління; протидія кіберзлочинності, шпигунству і тероризму; розвиток кіберменеджменту; зміцнення міжнародного співробітництва шляхом імплементації у національне законодавство окремих норм нормативно-правових актів, прийнятих в країнах ЄС та НАТО, які на державному рівні визнаються усіма країнами.

Основним документом, на який варто звернути увагу і імплементувати його в національне законодавство, є Директива з мережевої та інформаційної безпеки, яка формує загальний підхід і правила ЄС у сфері кібербезпеки.

Регулятори в Україні явно запізнюються з розробленням правової бази для регулювання питань захищеності об'єктів критичної інфраструктури, а також з наповненням змістом та підзаконними актами рамкових законів щодо кібербезпеки [1].

Відсутній трансформаційний підхід до управління кібербезпекою з боку держави, що передбачає наявність органу, яка візьме на себе функції управління та контролю за впровадженням програми з кібербезпеки. Тобто, ці функції повинні належати неурядовій структурі. Очевидно, це має бути не

функція контролю (як зараз), а скоріше фасилітації (організація процесу колективного розв'язання проблем) і допомоги у розв’язанні проблем кібербезпеки державним і недержавним структурам [2].

На наше переконання, необхідно врахувати ще один вагомий чинник. Неможливість створення ефективного організаційно-правового забезпечення у сфері кібербезпеки на тривалий період обумовлена його високою динамічністю та мінливістю загроз. Тому, щонайменше, кожні два роки чинне законодавство у цій сфері потребуватиме корегування відповідно до нових загроз, а також змін у геополітичному безпековому середовищі.

Другим негативним сценарієм у цьому процесі може стати відсилання для сертифікування до процедур безнадійно застарілих комплексних систем захисту інформації (КСЗІ) [3].

Необхідно внести зміни до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" для прийняття сімейства стандартів систем менеджменту інформаційною безпекою (СМІБ) стосовно окремих категорій інформації, захист якої забезпечується законодавством України.

Для цього необхідно або адаптувати сучасні міжнародні стандарти систем захисту інформації (ЗІ), або розробляти та впроваджувати власні, якісно нові стандарти безпеки для державних органів та силових структур, що є неприйнятним з огляду на часові обмеження і матеріальні витрати.

Сертифікування за стандартами також вимагає проведення регулярних аудиторських перевірок з метою забезпечення відповідності виконання вимог та належного функціонування процесу управління кібербезпекою.

Як висновок, вважаємо, що існуюча нормативно-правова база у сфері кібербезпеки повинна бути істотно доповненою. Пропонуємо внести зміни до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" і на законодавчому рівні закріпити вимоги стандартів сімейства СМІБ для окремих категорій інформації, захист якої забезпечується законодавством України.

Список використаних джерел:

1. Юрій Котляров. Архітектура права сфери кібербезпеки в Україні. URL: https://www.asterslaw.com/ua/press_center/publications/architecture_of_the_cybersecurity_law_in_ukraine/ (дата звернення: 19.11.2021)

2. Живко З. Б., Рудий Т. В., Сеник В. В., Родченко С. С. Проблеми нормативно-правової бази забезпечення кібербезпеки в Україні: стан і перспективи / Соціально-правові студії : науково-аналітичний журнал / гол. ред. О. Балинська. Львів : ЛьвДУВС, 2020. Вип. 3 (9). С. 18-25.

3. Костенко О.В. Проблеми правового регулювання та розвиток кібернетичної безпеки України на сучасному етапі / Інформація і право. Науково-дослідний інститут інформатики і права Національної академії правових наук України. Київ. № 3(30)/2019. С. 96-104.

УДК 378:004

САЄНКО ДЕНИС ЛЕОНІДОВИЧ

курсант групи Ф4-402 факультету № 4

Харківського національного університету внутрішніх справ

ГРИЩЕНКО ДЕНИС ОЛЕКСАНДРОВИЧ

старший викладач

кафедри протидії кіберзлочинності факультету № 4

Харківського національного університету внутрішніх справ

ВИДИ КІБЕРЗЛОЧИННОСТІ ТА ЯК ЗАХИСТИТИСЯ ВІД НИХ

Зловмисна прив’язка до злому вперше була задокументована в 1970-х роках, коли ранні комп’ютеризовані телефони ставали мішенню. Підковані в техніці люди, відомі як "фрікери", знайшли спосіб оплати міжміських дзвінків за допомогою ряду кодів. Вони були першими хакерами,які навчились використовувати систему, модифікуючи апаратне та програмне забезпечення для крадіжки телефонного часу на великі відстані. Це змусило людей усвідомити, що

комп’ютерні системи вразливі до злочинної діяльності, і чим складніші системи ставали, тим більш сприйнятливими вони були до кіберзлочинності.

Також відомий випадок 1990 року, де був викритий великий проект під назвою «Операція Сандевіл» Агенти ФБР вилучили 42 комп'ютери та понад 20 000 дискет, які використовувались злочинцями для незаконного використання кредитних карток та телефонних послуг. У цій операції взяли участь понад 100 агентів ФБР, і знадобилося два роки, щоб розшукати лише кількох підозрюваних. Однак це було сприйнято як велике зусилля для зв’язків з громадськістю, оскільки це був спосіб показати хакерам, що за ними слідкуватимуть і будуть переслідуватися.

Інтернет — не безпечне місце. Кіберзлочинність зростає такими ж швидкими темпами, як і нові люди, які підключаються до цифрового світу. Подібно до того, як у реальному світі є хороші і погані люди, в Інтернеті ви знайдете людей, які використовують свої знання з кібербезпеки, щоб допомогти іншим (також відомі як білі капелюхи або етичні хакери). Є й ті, хто використовує свої цифрові навички для поширення страху та створення хаосу. Відомо, що ці не порушники здійснюють шахрайство, порушують конфіденційність і навіть викрадають вашу особу.

Кіберзлочинність в Інтернеті щорічно коштує організаціям, компаніям та урядам мільярди доларів. Навіть гірше, незаконна діяльність в Інтернеті не має ознак уповільнення. Насправді вірно все навпаки: кіберзлочинність дедалі більше зростає. І люди це усвідомлюють. Дослідження Gallup показує, що громадян більше турбує кіберзлочинність, аніж безпосередньо небезпечні для життя злочини, такі як вбивство чи тероризм.

Що таке кіберзлочинність? Якщо говорити просто, кіберзлочинність — це злочин, вчинений в Інтернеті, в локальних мережах або навіть проти ізольованих комп’ютерів. Це може впливати на будь-які ваші цифрові пристрої (включаючи ПК, ноутбуки, смарт-телевізори, планшети, смартфони, електронні системи тощо). Кіберзлочинність також стосується будь-якої діяльності, коли злочин вчиняється за допомогою будь-якої комп’ютерної системи. Кіберзлочинці

загальновідомі як хакери, хоча цей термін технічно неточний, правильний термін — «зломщик».

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

Кіберзлочинність проти фізичних осіб. Це той злочин, який безпосередньо впливає на будь-яку людину або її властивості. Приклади цього виду кіберзлочинності включають, але не обмежуючись ними: соціальна інженерія, фішинг, переслідування електронною поштою, кіберсталінг та розповсюдження незаконних матеріалів для дорослих.

Кіберзлочинність проти компаній (організацій). Це один із найпоширеніших видів кіберзлочинності сьогодні. Коли хакерство присутності компанії в Інтернеті або будь-якого з її продуктів стає серйозною проблемою, яка може спричинити велику кількість наслідків для компанії, а також її співробітників, партнерів та клієнтів. Приклади включають порушення даних, кібер-вимагання та розповсюдження warez(програма, яка розповсюджується незаконним шляхом з порушенням прав правовласника) тощо.

Кіберзлочинність проти суспільства. Це впливає на суспільство в цілому, наприклад: фінансові злочини проти громадських організацій, продаж нелегальної продукції, торгівля, азартні ігри в Інтернеті, підробка тощо.

Кіберзлочинність проти уряду. Це один з найгірших у світі видів кіберзлочинності і може призвести до переслідування з боку федеральної кібербезпеки та правоохоронних органів. Він також відомий як кібертероризм, і включає такі види діяльності, як проникнення в урядові системи та мережі, зневаження та закриття військових веб-сайтів та поширення пропаганди.

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

хмарних сховищах, таких як Dropbox або Google Drive. Справа в тому, чи є ви фізичною особою, малим бізнесом чи великою багатонаціональною компанією, ви щодня покладаєтесь на комп'ютерні системи. Поєднуйте це із зростанням хмарних сервісів, поганою безпекою хмарних сервісів, смартфонами та Інтернет ом речей (IoT), і ми маємо безліч загроз в мережі.

Здається, що в сучасну епоху технологій хакери заволодівають нашими системами, і ніхто не в безпеці. Середній час перебування, або час, необхідний компанії для виявлення кіберпроникнення, становить понад 200 днів. Більшість користувачів Інтернету не зупиняються на тому, що їх можуть зламати, і багато хто рідко змінюють свої облікові дані або оновлюють паролі. Це залишає багатьох людей сприйнятливими до кіберзлочинів, і важливо бути поінформованими. Навчіть себе та інших щодо профілактичних заходів, які ви можете вжити, щоб захистити себе як особистість чи бізнес тобто: станьте пильними під час перегляду веб-сайтів, ніколи не натискайте на незнайомі посилання чи оголошення, за можливості використовуйте VPN, перш ніж вводити облікові дані, переконайтесь, що веб-сайти в безпеці, оновлюйте антивірусні(прикладні) системи, використовуйте надійні паролі з 14+ символами.

УДК 004.4

СЕМЧУК АНДРІЙ ОЛЕГОВИЧ

курсант 2 курсу факультету №4

Харківського національного університету внутрішніх справ.

СВІТЛИЧНИЙ ВІТАЛІЙ АНАТОЛІЙОВИЧ

кандидат технічних наук, доцент,

доцент кафедри протидії кіберзлочинності факультету №4

Харківського національного університету внутрішніх справ

СПОСОБИ ВЗЛОМУ ЕЛЕКТРОННОЇ ПОШТИ

Сьогодні електронна пошта є одним із найпопулярніших та найдоступніших способів передачі інформації. Також, за допомогою

електронної пошти ми створюємо облікові записи в соціальних мережах, для адміністрування та зберігання електронних листів, тому важливо знати можливі загрози електронній пошті та як від них захиститись.

Троянський кінь. Одним із найпопулярніших способів отримання доступу до email є розсилка листів із влаштованими вірусами, якщо бути точнішим то вірус вбудовується не в сам лист, а лист містить лише посилання на нього. Зазвичай зміст листа повинен «зацікавити» користувача, і повинно бути таким, на яке він не зможе не відповісти. Після цього все просто: жертва переходить за посиланням і на його комп'ютер завантажується шкідливе програмне забезпечення [1]. Приклади таких троянів: SpyEye, Zeus, DarkComet RAT, Carpberp.

Взлом за номером телефону. Зловмисник, маючи номер телефону жертви(якщо він привязаний до електронної пошти) зі свого персонального комп'ютера на сервісі електронної пошти, виконує відновлення паролю до електронної пошти. Після чого жертві надходить SMS з кодом підтвердження відновлення паролю. Зловмисник відправляє друге SMS з вимогою вказати код для підтвердження з попереднього SMS. На сьогодні існує безліч сервісів для приховання свого номеру телефону при відправці повідомлень на інші номери телефону, або сервіси для оренди інших номерів телефону і подальшої відправки повідомлень [2].

Отримання доступу до пошти не є останнім пунктом в цьому способі. Для відвернення уваги жертви, після відновлення паролю, створюється тимчасовий і відправляється жертві. Даний спосіб є доволі старим але в руках професіоналів доволі ефективним. Авторство даного способу належить компанії Simantec [3].

Фізичний доступ до пристрою. Якщо є доступ до пристрою, з якого здійснюються сеанси в поштовий ящик, можна зчитувати інформацію кейлогерами. Суть кейлогера полягає в тому, що він представляє собою файл який зчитує все, що користувач вводить на клавіатурі. Перевагами для зловмисників є те, що кейлогери записують буквально всю інформацію, що вводиться, крім паролів записуються пошукові запити в інтернеті, все що

друкує жертва в особистій та діловій переписці з іншими користувачами. На щастя, сучасні антивіруси з легкістю визначають такі програми на пристрої. Також, проблемою отримати пароль буде якщо жертва використовує в поштовому клієнті функцію «запам'ятати пароль». Ще одним мінусом є те що не всі кейлогери передбачають в своєму функціоналі відправку зчитаної інформації зловмиснику, тому для нього виникне необхідність заново підходити до пристрою.

Соціальна інженерія. Більшості просунутим користувачам здається, що даний спосіб не є ефективним. Відносно недавно була зламана пошта екс-директора ЦРУ Джона Бреннана. Абсурдність полягає в тому, шо це зробив не досвідчений «хакер», а звичайний підліток. Він спочатку зв'язався з мобільним оператором, представившись співробітником технічної підтримки, уточнив деталі акаунту Бреннана, після чого скинув пароль.

Переваги способу в тому що для нього не потрібно мати спеціальні знання, успіх зловмисника залежить від його кмітливості.

Висновки. Отже, із зазначених методів атаки на поштову скриньку є різні методи захисту, наприклад:

– В першу чергу мати якісний антивірус, бажано останньої версії, аби мати можливість перевірити файли які надходять на пошту, та у випадку знаходження вірусу, знежкодити його.

– Для захисту від троянів необхідно не відкривати сумнівні листи, тим більше переходити за посиланнями в них, не запускати програми.

– Від взлому за номером телефону – уважно читати всі вхідні SMS-повідомлення, та пам'ятати про те, що почтові сервіси не вимагають відправки будь-яких кодів для відновлення доступу.

– Фізичний доступ – налаштувати блокування екрану(на смартфоні), або облікового запису користувача(на персональному комп'ютеру)

– Від шахраїв, які користуються методами соціальної інженерії, ніхто не застрахований, треба не втрачати пильності коли телефонують з невідомих номерів та намагаються випитати особисту інформацію

Список використаних джерел:

1. SpyEye Malware Mastermind Pleads Guilty [Електронний ресурс]. – Режим доступу : https://www.fbi.gov/news/stories/2014/january/spyeye-malware-mastermind-pleads-guilty/spyeye-malware-mastermind-pleads-guilty.

2. Ярошенко А. А. Хакинг на примерах. Уязвимости, взлом, защита / А. А. Ярошенко - СПБ.: Наука и техника, 2021; 50-52 с.

3. Password recovery scam tricks users into handing over email account access. [Електронний ресурс]. – Режим доступу : http://www.symantec.com/connect/ blogs/password-recovery-scam-tricks-users-handing-over-email-account-access

УДК 343.1:[351.74:161.111](100)

СТРУКОВ ВОЛОДИМИР МИХАЙЛОВИЧ

кандидат технічних наук, доцент,

професор кафедри кібербезпеки та DATA-технологій факультету № 6

Харківського національного університету внутрішніх справ;

УЗЛОВ ДМИТРО ЮРІЙОВИЧ

кандидат технічних наук,

доцент кафедри штучного інтелекту

Харківського національного університету радіоелектроніки;

ІНСТРУМЕНТАЛЬНІ ЗАСОБИ РЕАЛІЗАЦІЇ ПРЕДИКАТИВНОЇ МОДЕЛІ ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Правоохоронна сфера світових країн в останні роки все більше піддається впливу досягнень у сфері високих технологій, які успішно використовуються не тільки на благо людству, а й з деструктивними цілями. Найбільш характерними рисами сучасного етапу розвитку високих технологій є наступні:

1) «інформаційний вибух» не спадає, а навпаки, набирає обертів; драйвером цього явища є інтернет речей – IoT (Internet of Thingths), середовище «розумних» пристроїв, які постійно генерують телеметричну інформацію і взаємодіють між собою. Внаслідок цього інтернет-трафік все більше стає

перенасиченим даними, які автоматично генеруються різноманітними датчиками розумних речей і гаджетами. В той же час з усього океану інформації за оцінками фахівців менш 1% піддається аналізу. Це відбувається тому, що велика частка цієї інформації має неструктурований характер і важко піддається обробці (або не піддається) традиційними інструментами. Зокрема, це відноситься до відео- та медіа даних, що надходять до правоохоронних органів з різнотипних відеокамер спостереження, а також з інтернету; а на даний момент в арсеналі правоохоронних органів вкрай мало інструментальних систем, функціонал яких дозволяє ефективно обробляти дані такого типу і у відповідних обсягах[1-8].

2) Темпи розвитку технологій, які є драйверами Четвертої промислової революції, характеризується зростаючою швидкістю; це означає, що завтра можливості, які сьогодні вважаються фантастикою, будуть буденним явищем.

3) Вартість високотехнологічних інструментів стрімко зменшується і вони стають доступними не тільки фінансово потужним державним і комерційним структурам, але і пересічним громадянам.

Внаслідок цих обставин правоохоронні структури вимушені переходити від реактивної до предикативної моделі діяльності, коли успіхом вважається не успішне розслідування скоєних злочинів, а їх виявлення та розкриття на етапі підготовки. Але такий перехід супроводжується складними проблемами правового та технічного характеру. Справа в тому, що, враховуючі вищенаведені обставини, одним з основних факторів реалізації такої моделі є використання високотехнологічних аналітичних інструментів вищеозначених типів даних. Складність і вартість розробки такого роду інструментів є дуже високою, як свідчить досвід США і Євросоюзу.

Зараз у світі існує досить невелика кількість високотехнологічних інструментальних аналітичних платформ, які використовують найсучасніші технології обробки даних – Data Mining, Web Mining, штучний інтелект та ін. До такого класу аналітичних інструментів можна віднести наступні:

- Palantir;

- ePOOLICE;
- PredPol;
- I2;
- Maltego;
- SmartCOP;
- RICAS.

Накопичений певний досвід їх застосування у прогнозуванні, профілактиці, запобіганні та розслідуванні злочинів. Цей досвід є вкрай цінним, оскільки ці платформи є першопроходьцями в цьому напрямі, і його вивчення дозволяє вірно зорієнтуватися при реалізації предикативної моделі діяльності поліції.

Список використаних джерел:

1. Dmytro Uzlov, Volodymyr Strukov, Oleksii Vlasov Using Data Mining for Intelligence-Led Policing and Crime Analysis. – IEEE 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), - p.499-502.

2. Volodymyr Strukov, Dmytro Uzlov Web-based Protected Geoinformation System of Criminal Analysis (RICAS) for Analytical Support for Crimes Investigation. - IEEE 2017 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), - p.508-511.

3. U. S. Department of Justice Office of Community Oriented Policing Services Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies Second Edition. – 2009.- 465p.

4. OSCE Guidebook. Intelligence-Led Policing. OSCE. Vienna, June 2017, 105 p.

5. Інформаційні технології у правоохоронній діяльності. Частина 1: Високотехноло гічні тренди у правоохоронній сфері зарубіжних країн: навч. посіб. [В.М. Струков, Д.Ю. Узлов, Ю.В. Гнусов та ін.] ; за заг. ред. канд. техн. наук, доц. В.М. Струкова / Харків. нац. ун-т внутр. справ. Х. : ТОВ «ДІСА ПЛЮС», 2020. 276 с.

6. Узлов Д.Ю., Струков В.М., А.Б. Григорович, А.И. Петрусенко, С.И. Доскаленко. Применение интеллектуальной системы криминального анализа в реальном времени (RICAS) для аналитического сопровождения оперативно-розыскной деятельности и досудебного расследования. Харків, Право і безпека вип. 2(57), 2015, с. 132-139.

7. Узлов Д.Ю., Струков В.М. Сучасні інструментальні засоби кримінального аналізу // Проблеми застосування інформаційних технологій правоохоронними структурами України та вищими навчальними закладами зі специфічними умовами навчання: збірник наукових статей за матеріалами доповідей Міжнародної науково.-практ. конф. (22 грудня 2017 р., Львів) МВС України, Львів. держ. ун-т внутр. справ: ЛДУВС, 2017. С.162-164.

8. Узлов Д.Ю., Струков В.М. Використання методів і технологій штучного інтелекту в кримінальному аналізі // Застосування інформаційних технологій в діяльності НПУ: матеріали наук.-практ. семінару(21 грудня 2018 р., Харків) МВС України, Харків. нац. ун-т внутр. справ: ХНУВС, 2017. С.17-19.

УДК 378.147:004.77

ТАЛАН МИКИТА АНДРІЙОВИЧ

курсант навчальної групи Ф4-302, Харківського національного університету внутрішніх справ.

СВІТЛИЧНИЙ ВІТАЛІЙ АНАТОЛІЙОВИЧ

кандидат технічних наук, доцент,

доцент кафедри протидії кіберзлочинності

Харківського національного університету внутрішніх справ

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ОРГАНІЗАЦІЇ ДИСТАНЦІЙНОГО НАВЧАННЯ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Постановка проблеми. Інформаційні технології нашого часу надають можливість вдосконалити ефективність освітнього процесу, та реалізуються за допомогою всесвітньої мережі Інтернет, що набагато розширює можливості в

навчанні. Та все ж таки, після аналізу різних джерел в мережі Інтернет, в яких знаходиться освітній матеріал, а також інформаційно-бібліотечного фонду в системах було виявлено, що створення систем управління освітою у освітній процес потребує подальшого покращення та удосконалення.

Основна мета виступу. Право на освіту [1] - право людини на здобуття певного обсягу знань, культурних навичок, професійної орієнтації, які необхідні для нормальної життєдіяльності в умовах сучасного суспільства. Але останнім часом, коли весь світ страждає від наслідків пандемії COVID-19, реалізувати своє право на освіту стає дедалі складнішим. Тому проблема потребує сучасного вирішення, в цьому випадку на допомогу приходять інформаційні технології. Дистанційне навчання – це технологія, що базується на принципах відкритого навчання, широко використовує комп'ютерні навчальні програми різного призначення та створює за допомогою сучасних телекомунікацій інформаційне освітнє середовище для постачання навчального матеріалу та спілкування. Створення сервісів, сайтів та систем дистанційного навчання не тільки надає можливість отримувати нові знання і реалізувати своє право на освіту для здобувачів вищої освіти, але і попередити розповсюдження хвороби, відповідальність за що несе кожен з нас.

Виклад основного матеріалу. Останнім часом, все більше і більше набувають великого розповсюдження системи управління навчанням для створення дистанційних навчальних курсів. Таким чином, реалізується процес навчання, аудиторна та позааудиторна роботи, організація доступу до інформаційно-бібліотечної бази, матеріалів курсів. Найефективнішим є те, що створюється безпосередня взаємодія здобувача із викладачем, можливість як очного так і заочного навчання.

Прикладом таких систем виступають Moodle, Canvas та інші. В них реалізовано мабуть все необхідне, для якісного та в повному обсязі отримання нових знань. Існує можливість управління навчальними курсами, проведення онлайн занять, реалізовано самостійна та контрольна роботи, тестування, забезпечено взаємодія викладача із здобувачами (оцінювання, перевірка,

контроль знань). Системи допомагають викладачам керувати процесом навчання, перевіряють, наскільки якісно засвоєно викладений матеріал. Великою перевагою є те, що завжди є доступ до нового, оновлюваного, корисного матеріалу, який надає викладач. Інформаційні технології дають змогу швидко обмінятися електронними листами з викладачем, знайти потрібні дані, підготувати реферат, підготувати звіт про виконану роботу та надати його для перевірки. [2]

Хмарні технології вказаних систем надають можливість нівелювати проблему у апаратно-технічному забезпеченні здобувачів вищої освіти та викладачів [3]. Обладнати робочі та навчальні місця можна невисоко продуктивними машинами, завдяки тільки необхідності забезпечення зв’язку с віртуальними машинами, які працюють у приватній хмарі. Звісно, існує потреба обладнання робочих місць високо продуктивними машинами, але деяку частину робочих станцій можна перенести в хмарну середу. Існує можливість розділення роботи на лекційні, лабораторні та практичні, що допомагає систематизувати освітній процес і організувати якісний контроль.

Щодо проведення практичних занять, викладач може здійснювати перевірку та контроль за допомогою тестів, паралельно вказуючи на помилки, які допускають здобувачі. Крім того, у разі виникнення проблем, які потребують роз’яснення викладача, можна використовувати різні форуми та мессенджери, такі як Facebook, Telegram, WhatsApp, де в додаток реалізована можливість створення спільних груп, що значно прискорює та вдосконалює освітній процес [3]. Студенти мають можливість вчитися не тільки на своїх помилках, але і помилках інших здобувачів освіти.

Реалізація лабораторних занять може відбуватися із залученням різних додаткових сервісів і завдань. Веб-квести, логічні та психологічні задачі, використання сервісів Google (Googel Docs, Google Tables), додавання тестових завдань є ефективним способом покращення освітнього процесу та взаємодії викладача із здобувачами. Захисти виконаних робот, проектів чи презентацій може відбуватися у вигляді веб-конференцій. [3]

Висновки. Отже, використання систем дистанційної освіти є високоефективним та систематизованим способом здобування вищої освіти. Завдяки цій системам, вдосконалюються практичні та теоретичні навички здобувачів, індивідуалізується процес навчання, організовується на високому рівні проведення лабораторних, практичних чи лекційних занять, реалізується якісний контроль знань, формуються професійні навички, загальні компетенції, вміння та навички роботи з різними інформаційними ресурсами. Таким чином використання дистанційної освіти надає можливість крім забезпечення засвоєння знань, формування навичок та умінь, мотивувати до навчання, в процесі здійснення інтерактивного навчання, тобто включати в себе мультимедійні фрагменти, зовнішні електронні ресурси, анімації, до яких здобувач може мати доступ. Важливе значення тут набуває розробка методик навчання, які використовують у дистанційної освіті, оскільки застосування сучасних знань потребує наявності чіткої структури навчання та належного інформаційного наповнення [3].

Особливо гостро питання дистанційних систем навчання стає в період пандемії COVID-19. Сервіси особливо корисні для здобувачів освіти, які знаходяться у віддалених малих населених пунктах та для людей з обмеженими можливостями, тому на сьогодні дуже важливо підтримувати та розвивати інформаційні технології у сфері освіти.

Список використаних джерел:

1. https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%B0%D0%B2%D0%BE_%D0%BD%D0%B0_%D0%BE%D1%81%D0%B2%D1%96%D1%82%D1%83

2. http://www.zhu.edu.ua/mk_school/mod/page/view.php?id=3370&lang=ru

3. Світличний В.А. Особливості застосування хмарних технологій CANVAS в освітньому процесі / В.А.Світличний // ІІІ Всеукраїнська науково-методична конференція «Забезпечення якості вищої освіти: підвищення ефективності використання інформаційних технологій у здійсненні освітнього процесу» (14–16 квітня 2021 року) м. Одеса / МОН України Одеська національна академія харчових технологій, м. Одеса, ОНАХТ, 2021. – С. 243-244.

УДК 351.741:004.89

ТКАЧУК КАТЕРИНА ВІТАЛІЇВНА

здобувач вищої освіти

Луганського державного університету внутрішніх справ імені Е. О. Дідоренка

КУЧМА ДАРИНА ГЕННАДІЇВНА

здобувач вищої освіти

Луганського державного університету внутрішніх справ імені Е. О. Дідоренка

ПІДГОТОВКА КАДРІВ ДЛЯ ПІДРОЗДІЛІВ КРИМІНАЛЬНОГО АНАЛІЗУ

Сучасний розвиток технологій і трансформація підрозділів Національної поліції України постійно потребує оновлення кадрів. Відносно новим напрямом роботи НПУ стало створення нового аналітичного підрозділу (Департаменту кримінального аналізу).

Департамент кримінального аналізу є уповноваженим структурним підрозділом Національної поліції України з проведення, організації та координації інформаційно-пошукової та аналітичної роботи, спрямованої на збір, оцінку та реалізацію інформації, у тому числі інформації з обмеженим доступом, шляхом надання її уповноваженим органам (підрозділам) для вжиття заходів відповідно до їх компетенції, оцінювання ризиків, а також використання її для забезпечення виконання функцій, покладених на поліцію [1].

Звертаючись до теорії, можна констатувати, що кримінальний аналіз є основою моделі *«Intelligence Led Policing»* (з англ. «поліцейська діяльність, керована аналітикою»), спрямованої на прийняття ефективних управлінських рішень на основі використання комплексу методів та технік збирання, обробки, оцінки, аналізу та реалізації інформації, а також обміну інформацією під час кримінального провадження, оперативно-розшукової діяльності та при розробленні тактичних і стратегічних заходів з протидії злочинності. Його суттєва і головна відмінність у тому, що підрозділи кримінального аналізу, маючи законний доступ до багатьох інформаційних баз, які діють на території нашої держави, а також володіючи навичками розвідувальної аналітики,

суттєво полегшили роботу оперативним працівникам. Кримінальні аналітики продемонстрували, що здатні відшукати найприхованіші закономірності в діяльності кримінальних елементів, побудувати системні зв'язки в ситуаціях неочевидності [2, с.39].

Важливим аспектом отримання якісних даних у підрозділах кримінального аналізу є саме організація фахової підготовки працівників поліції.

Сьогодні в Україні на жаль існують проблеми у підготовки кадрів для підрозділів кримінального аналізу. Наприклад, недостатнє забезпечення оперативних підрозділів Національної поліції України сучасною оргтехнікою, комп'ютерним програмним забезпеченням; відсутність системи навчання, підготовки та перепідготовки працівників відповідних аналітичних підрозділів відповідно до світової моделі поліцейської діяльності, керованої аналітикою ILP [3, с.240].

Отже, навчання і підвищення кваліфікації кримінального аналітика, відіграють важливу роль у протидії злочинності.

Нові технології та методи з'являються щороку, тож кримінальні аналітики повинні завжди бути в їх курсі, проходити навчальні тренінги з наступних тем: «MS Excel у кримінальному аналізі» та «Використання аналітичних програмних продуктів у кримінальному аналізі (Microsoft Excel, IBM i2 Analyst's Notebook, Power BI, ArcGIS)». Крім того, кримінальні аналітики самостійно повині опановувати значну кількість програмно-технічних компонентів, інструментів та методик, необхідних для здійснення кримінального аналізу.

Список використаних джерел:

1. Офіційний веб-сайт Національної поліції: https://www.npu.gov.ua/about/struktura/struktura/departament-kriminalnogo-analizu.html (дата звернення: 01.11.2021).

2. Білоус Р.В. Участь кримінальних аналітиків у розкритті злочинів. *Використання досягнень сучасної науки і техніки в розкритті злочинів:* тези доп. міжвідомчого науково-практичного круглого столу (м.Київ, 25 лют.2021 р.). Київ, 2021. С.38-41.

3. Шинкаренко І.Р. Проблеми запровадження кримінального аналізу в діяльність підрозділів кримінальної поліції: теоретико-історичне підґрунтя. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. Дніпро, 2017.№ 1.С.233-242.

УДК: 004.043

ТУЛУПОВ ВОЛОДИМИР ВОЛОДИМИРОВИЧ

кандидат технічних наук, доцент,

доцент кафедри кібербезпеки та DATA-технологій факультету № 6 Харківського національного університету внутрішніх справ

ГОНЧАРОВ КИРИЛ ВІТАЛІЙОВИЧ

студент 3 курсу групи Ф6-Кбдср-19-1 факультету № 6

Харківського національного університету внутрішніх справ

ДЕЯКІ ОСОБЛИВОСТІ ВИДАЛЕННЯ ІНФОРМАЦІЇ ПРО ОСОБУ У КІБЕРПРОСТОРІ

На теперішній час у кіберпросторі існує думка, що видалити інформацію з глобальної мережі набагато складніше, ніж помістити її туди. Тому користувачеві потрібно запастись спеціальними знаннями, терпінням та ресурсами. Інформація, яку ми залишаємо про себе в мережі може бути використана також проти нас.

При видаленні цифрових слідів користувачі мережевих ресурсів найчастіше переслідують три основні цілі, а саме:

1. Захист онлайн - репутації. Інформацію про особу в Інтернеті може знайти будь-хто без проблем і застосування спеціальних сервісів, наприклад потенційний роботодавець, бізнес-партнер або просто новий знайомий.

2. Безпека. Ваша домашня адреса, разом з геоміткою про те, що зараз ви знаходитись, наприклад на відпочинку, можуть залучити потенційних грабіжників. Також доступ до персональної інформації робить вас легкою здобиччю сталкерів.

3. Небажання, щоб великі технологічні гіганти на кшталт Google та Facebook (Meta) знали про вас усе, а отже – керували тим, що ви бачите у мережі та заробляли на цьому [1].

Тому в ряді випадків переважно стоїть питання як знищити дані про себе або особу в Інтернеті. Багато заходів загалом зазвичай зводяться до чищення історії пошуку та відключенням збору даних.

Слід зазначити, що видаляти всю інформацію про себе в мережі – непросто, довго, дорого та невиправдано.

Розглянемо основні прості кроки, які допоможуть зменшити так званий "цифровий" слід, який залишає особа - користувач у мережі.

1. *Слід перевірити інформацію в пошуковій видачі*. Введіть своє прізвище та ім'я різними мовами, потім здійсніть пошук за адресами електронної пошти та номерами телефонів, якими ви користуєтеся. Так, ви отримаєте інформацію про сайти які мають доступ до ваших особистих даних і яка інформація до них прив'язана. Найчастіше така інформація про особу міститься на сайтах, які збирають свою базу відкритих державних реєстрів таких як https://data.gov.ua. (у даній базі наприклад, зібрано адреси українців, зареєстрованих як фізичні особи-підприємці).

Якщо наприклад хостер, реєстратор або власник цих сайтів не реагують на звернення, можна видалити інформацію з пошукової видачі в рамках DMCA.

Google та інші великі пошукові системи мають спеціальну форму скарг - DMCA report form. Наприклад, подати скаргу до Google можна через форму видалення вмісту з Google. Поскаржитися на матеріал можна через форму видалення матеріалів, що порушують авторські права. Якщо йдеться про фото, де чітко видно ваше обличчя, ймовірність успіху дуже велика.

2. *Подати запит на видалення особистих даних у Google.* До цієї категорії потрапляють матеріали інтимного характеру, фото неповнолітніх, ваші контактні дані, фінансова чи медична інформація, а також реквізити документів, що засвідчують особу. Також слід зауважити що, навіть якщо інформація зникне з пошуку Google, вона залишиться на тих же сайтах в Інтернеті.

Найпростішим способом видалення інформації з пошукової видачі є видалення фотографій та контенту через форму скарги. Ви можете написати власнику сайту, реєстратору доменного імені або хостинг-провайдеру. Через сервіси отримання реєстраційних даних про власників доменних імен напри приклад, WHOIS можна дізнатися контактні дані власника сайту, якщо на сайті ця інформація не розміщена.

Як правило, у всіх хостинг-провайдерів є e-mail, який приймає скарги, туди можна написати мовою реєстратора, коротко описавши суть проблеми та надавши посилання на конкретну сторінку, яка містить неприйнятний зміст. Реєстратор або хостинг-провайдер нададуть цю інформацію власнику домену або орендарю хостингу та дадуть час (як правило не більше 48 годин) для усунення проблеми. Іноді цю дію потрібно повторити кілька разів.

3. *Налаштувати оповіщення Google для вашого імені через сторінку www.google.com/alerts* (потрібно ввести там своє ім'я та прізвище або будь-які інші дані, про які ви хотіли б отримувати оповіщення).

4. *Вимкнути збір даних про себе в соцмережах та Google*. Для цього вам потрібно перейти до розділу My Google control. Тут можна керувати історією своєї активності. Компанія поділяє її на три категорії: Web та App Activity, Location History та Youtube history. Зазвичай усі ці дані компанія записує за умовчанням.

5. *Вимкнути збір інформації.* Наприклад, у Facebook через розділ "Настройки" пункт "Ваша информация в Facebook". У списку ви знайдете пункт "Действия вне Facebook". Там ви побачите, які компанії та організації надали соцмережі дані про вашу активність.

6. *Приховати данні свого об'єкта розташування із Google Maps.* Щоб "розмити" фотографії вашого будинку або автомобіля, вам потрібно відкрити Google maps або Street View Galery, ввести адресу та знайти фото, яке ви хочете "розмити". На ньому має бути ваше обличчя, будинок чи номерний знак автомобіля. Натисніть "Повідомити про проблему", заповніть форму та надішліть вашу заявку на розгляд.

7. *Згенерувати тимчасову пошту.* Для цього можна скористатися спеціальними сервісами. Наприклад, https://temp-mail.org або https://clipmails.com. Ви отримаєте e-mail, який дійсний протягом 10 хвилин, а потім зникне.

8. *Вимкнути збір даних на телефоні та комп'ютері.* Зайдіть до розділу "Налаштування" та уважно вивчіть параметри конфіденційності.

9. *Видалити данні у рамках GDPR* (Regulation (EU) 2016/679) - регламент у межах законодавства Європейського Союзу щодо захисту персональних даних усіх осіб у межах Європейського Союзу та Європейської економічної зони. Вона також стосується експорту персональних даних за межі ЄС і ЄЕЗ.

Висновки. Слід зазначити, що в деяких соціальних мережах сторінка видаляється не миттєво, адміністратори мереж залишають можливість логіну на відновлення на певний термін місяців після команди на знищення акаунту. Видалення сторінки наприклад, в Instagram, як і в Facebook, відбувається практично миттєво – користувачеві буде надано всього кілька днів на те, щоб передумати та відновити дані про себе.

Багато соціальних мереж відключають або «заморожують» сторінки користувачів на строк від декількох днів до кількох місяців перед їх остаточним видаленням. Це означає, що знайти людину або подивитися опублікований нею контент не вийде, проте всі фотографії та інші дані фізично ще зберігаються на серверах сервісів, прискорити їхнє знищення неможливо, але побачити їх ніхто не зможе (крім представників правоохоронних органів у передбачених законом випадках).

Список використаних джерел:

1. Як знищити дані про себе в Інтернеті / Ліга-Tech: веб-сайт. URL: https://tech.liga.net/technology/article/kak-unichtojit-dannye-o-sebe-v-internete-chistim-poisk-i-otklyuchaem-sbor-dannyh (дата звернення 12.11.2021)

2. Загальний регламент про захист даних / Вікіпедія. URL: https://uk.wikipedia.org/w/index.php?title=%D0%97%D0%B0%D0%B3%D0%B0%

D0%BB%D1%8C%D0%BD%D0%B8%D0%B9_%D1%80%D0%B5%D0%B3%D0%D0%BD%D0%B8%D1%85&oldid=22883078 (дата звернення 14.11.2021)

УДК 343.85:343.982.5

ФЕДОРЕНКО ОКСАНА АНАТОЛІЇВНА

науковий співробітник

наукової лабораторії з проблем

протидії злочинності ННІ №1

Національної академії внутрішніх справ

КОСМІЧНІ ЗНІМКИ ЯК ДЖЕРЕЛО ІНФОРМАЦІЇ ДЛЯ ПРАВООХОРОННИХ ОРГАНІВ У ПРОТИДІЇ ЗЛОЧИННОСТІ

Діяльність правоохоронних органів у сфері протидії злочинності в сучасних умовах (обумовлених у тому числі глобалізацією суспільних відносин як правової, так і кримінальної спрямованості) є важливою складовою динамічного соціально-економічного розвитку країни і вимагає безперервного вдосконалення. Правоохоронні органи покладаються на новітні технології у багатьох сферах своєї діяльності. На сьогодні розвиток інформаційно-комунікаційних технологій у поєднанні з сучасною космічною технікою надають широкі можливості *підвищення ефективності діяльності правоохоронних органів* у протидії злочинності.

За динамікою розвитку дистанційне зондування Землі посідає друге місце серед космічних інформаційних технологій після телекомунікаційного сектора. Україна має певні успіхи та науково-технічний потенціал у космічній галузі і зацікавлена у їх розвитку. Тому, актуальним є залучення в практичну діяльність правоохоронних органів методів і технологій дистанційного зондування землі (ДЗЗ) для створення ефективних загальноприйнятих варіантів обробки тематичної інформації та створення необхідної матеріально технічної бази (знімки, програмне забезпечення, комп'ютери) для підвищення ефективності виконання завдань та обов’язків які стоять перед Національною поліцією України [1].

Основними тенденціями у розвитку галузі ДЗЗ є: поява нових космічних апаратів (КА) ДЗЗ високої і надвисокої роздільної здатності з покращеними характеристиками оптико-електронної системи спостереження, підвищення просторової роздільної здатності і збільшення числа режимів зйомки.

Повний огляд поверхні Землі з висоти польоту супутника, висока швидкість руху супутникових датчиків і можливість реєструвати сигнали в декількох спектральних діапазонах дозволяють отримувати величезні обсяги даних.

Фотографії та інші зображення Землі, зроблені з космосу, показують багато про рельєф, рослинність та ресурси планети та їх зміни. Супутникові знімки, відомі як дистанційні знімки, дають змогу точно нанести на карту земний покрив і зробити ландшафтні риси зрозумілими в регіональному, континентальному та навіть глобальному масштабах. Перехідні явища, такі як сезонна активність рослинності та викиди забруднюючих речовин, порубка лісу, незаконний видобуток корисних копалин можна вивчати, порівнюючи зображення, отримані в різний час. Так як супутники можуть послідовно спостерігати всю земну кулю або визначену її частину протягом певного періоду часу [2].

Супутникові знімки високої роздільної здатності та дані ГІС (географічних інформаційних систем) дозволяють аналітикам визначати гарячі точки, а також інші тенденції та моделі для картування злочинності Тенденція використання супутникових знімків у діяльності правоохоронних органів має потенціал бути постійною частиною під час розслідування кримінальних проваджень та допомагати підтримувати забезпечення публічної безпеки і порядку, а також протидії злочинності.

Космічний знімок містить великий масив інформації, побачити та аналізувати яку можна через застосування низки інструментів спеціального програмного забезпечення (ПЗ) – ГІС (геоінформаційні системи).

Супутникові зображення можуть відображати важливу інформацію про злочинну діяльність, що відбувається в країні та в усьому світі. Додаткова

функціональність супутникових зображень і карт ГІС розширюють можливості боротьби зі злочинністю завдяки ефективності та швидкості аналізу. ГІС-карти та програми для картографування даних для картографування злочинності стали необхідним інструментом у правоохоронних органах. Картування злочинності є ключовим компонентом аналізу злочинності. Карти ГІС дозволяють аналітикам відображати на мапах реальні відомості, наприклад, такі як демографічні дані перепису, розташування магазинів, банків, шкіл тощо, щоб краще зрозуміти основні причини злочинності що допомагає правоохоронним органам розробити стратегії для вирішення проблеми. Та у прийнятті рішень. Застосування ГІС-технологій дає змогу накопичувати й аналізувати просторову інформацію, оперативно знаходити потрібні дані й відображати їх у зручному для використання вигляді, різко збільшувати оперативність та якість роботи порівняно з традиційними «паперовими» методами [3].

Дистанційне зондування Землі вже знайшло визнання провідних держав світу як один із способів забезпечення національної безпеки та підтримки міжнародної стабільності. Ця технологія визнана як основна для спостереження Землі та є одним з пріоритетних напрямків космічної діяльності України. Так, *Указом Президента України від 29.02.1992 р. № 177, було створено Національне космічне агентство України (із 2011 р. — Державне космічне агентство України), одним з основних пріоритетних завдань якого є розвиток національної системи спостереження Землі з космосу* [4]. Широкі можливості застосування матеріалів космічної зйомки для багатоаспектних цілей картографії, а саме: просторова роздільна здатність знімків з різних супутників зумовлює масштаби тематичних карт, розроблених на базі цих космічних знімків. Дані з космознімків високої просторової розрізненості є дуже корисними для контролю за незаконною вирубкою лісу; контроль та боротьба з нелегальними сміттєзвалищами; контроль і виявлення ймовірно незаконного будівництва , у містобудуванні і загального розвитку міста; та інше — все це може бути закартографовано за допомогою ГІС і технологій на основі космічних знімків. Без залучення цих матеріалів традиційні картографічні

документи, що відображають ситуацію на певну дату, застарівають досить швидко, оновлюються рідко і, фактично, цілісної актуальної картини сучасного стану та використання території міста звичайно не дають.

Список використаних джерел:

1. Дистанційне зондування Землі: аналіз космічних знімків у геоінформаційних системах : навч.-метод. посіб. / С. О. Довгий, С. М. Бабійчук, Т. Л. Кучма та ін. – Київ : Національний центр «Мала академія наук України», 2020. – 268 с.

2. Aerial Photographs and Satellite Images. URL: https://pubs.usgs.gov/gip/AerialPhotos_SatImages/aerial.html.

3. Application of Remote Sensing and GIS for Law Enforcement — Crime Mapping. URL: http://facegis.nuarsa.info/?id=638.

4. Указ Президента України від № 177/1992. 29.02.1992 р. «Про створення Національного космічного агентства України».

УДК 343.98:681.3

ХАХАНОВСЬКИЙ ВАЛЕРІЙ ГЕОРГІЙОВИЧ
доктор юридичних наук, професор,
професор кафедри інформаційних технологій та кібербезпеки
Національної академії внутрішніх справ;
ХАХАНОВСЬКИЙ АНДРІЙ ВАЛЕРІЙОВИЧ,
магістр права, адвокат

ДЕЯКІ ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ПРОЦЕСІ ВИКЛАДАННЯ СПЕЦІАЛЬНИХ ДИСЦИПЛІН

У свій час в Національній академії внутрішніх справ була впроваджена навчальна дисципліна «Криміналістична інформатика», специфіка якої полягає у тому, що її викладання потребує, крім навчально-методичного й технічного, відповідного програмного забезпечення (ПЗ). Останнє складається зі

стандартного та прикладного ПЗ, специфічного для криміналістичної діяльності.

На наш погляд, прикладне програмне забезпечення, використовуване під час викладання дисципліни, можна класифікувати таким чином:

- комп'ютерні програми, що застосовуються у практичній діяльності правоохоронних органів: бази та банки даних; криміналістичні обліки; автоматизовані робочі місця працівників галузевих підрозділів; інформаційно-аналітичні та експертні системи; системи підтримки прийняття рішень тощо;

- навчальні та контролюючі програми, що використовуються в процесі криміналістичної підготовки та підвищення кваліфікації;

- комп'ютерні імітаційні ділові ігри для відпрацювання тактичних та методичних навичок розкриття та розслідування злочинів.

Так, з теми «Експертні системи, проблеми їх використання для вирішення криміналістичних завдань» використовується програма «Пошук серійного вбивці». Комп'ютерна програма «Очевидець» призначена для відпрацювання навичок описання зовнішності людини.

Відомо, що в курсі криміналістики послідовно вивчаються основи тактики проведення окремих слідчих дій, згодом – методики розслідування окремих видів злочинів. На наш погляд, обсяг навчальних годин курсу криміналістики не дозволяє достатньо повно засвоїти всі криміналістичні поняття. Крім того, при традиційному вивченні криміналістики неможливо забезпечити надбання навичок використання отриманих знань в конкретній слідчій ситуації, вирішення якої потребує не тільки послідовності певних слідчих дій, але й значного обсягу дій і рішень, пов'язаних з виконанням організаційно-розпорядчих функцій, кримінально-правової, процесуальної та іншої оцінки сукупності інформації у справі.

Зважаючи на викладене вище, а також, як правило, обмеженість навчального часу, досить ефективним є використання так званих комп'ютерних криміналістичних ділових ігор.

Виявилося можливим виділення із сукупності простих тактичних прийомів стійких у різних слідчих ситуаціях елементів (криміналістичних

знань). Різні етапи розслідування містять слідчі дії, оперативні та організаційні заходи (допит, обшук, огляд, упізнання, очна ставка тощо), прийоми проведення яких досить типові, а отже можуть бути формалізовані у комп'ютерних системах.

Програмне забезпечення окреслених систем дозволяє вдосконалювати існуючі ігри, а також розробляти нові для засвоєння методик розслідування інших категорій злочинів. Крім того, практично всі такі імітаційні ділові ігри розроблені на базі реальних кримінальних справ.

Поєднуючи можливості сучасних комп'ютерних технологій та ігрових механізмів, комп'ютерні імітаційні ділові ігри забезпечують оптимізацію процесу навчання курсантів (слухачів, студентів) з огляду на індивідуальні особливості особи. Коли створюють такі програми, як правило, передбачають розвинуту систему підказок, простоту керування, вони мають бути захопливими (модельовані ситуації містять елементи новизни), забезпечувати вирішення практичних завдань, а також оцінювання дій.

З відомого сьогодні програмного забезпечення у сфері криміналістичної підготовки заслуговують на увагу такі комп'ютерні програми: «Розбій», «Слідчий», «Убивство», «Дізнання», «Мак»; «Пошук зниклого», «Крадіжка» тощо. Кожна з них має свої особливості.

Багаторічний досвід викладацької практики у Національній академії внутрішніх справ свідчить про значне підвищення ефективності навчального процесу при використанні таких програм.

Стрімкий розвиток комп'ютерних технологій, дозволяє забезпечити новий якісний стрибок у розробці ділових ігор. Зокрема, достатньо перспективним напрямом їх розвитку є використання підходів, які інтегрують можливості баз даних, баз знань, механізмів пошуку рішень, а також різних прийомів виявлення експертних знань. Крім того, достатньо перспективним напрямом розвитку імітаційних комп'ютерних ділових ігор для підготовки юристів є застосування так званих флеш-технологій, зокрема «Macromedia Flash MX».

Проте розробка аналогічних комп'ютерних програм, в яких, безумовно, зацікавлені фахівці, не має ніякої системності. Поодинокі спроби у цьому напрямі можна лише вітати, але вони не вирішують проблеми загалом. Тому у свій час ми висловлювали пропозиції щодо формування відповідної робочої групи з представників вищих юридичних навчальних закладів, що дозволило б створити єдиний державний банк комп'ютерного програмного забезпечення юридичної діяльності – як для вищих і середніх навчальних закладів, так і для практичних підрозділів правоохоронних органів.

УДК 004.4

ШЕВЧЕНКО НІКІТА МИХАЙЛОВИЧ

Курсант 2 курсу факультету №4

Харківського національного університету внутрішніх справ

СВІТЛИЧНИЙ ВІТАЛІЙ АНАТОЛІЙОВИЧ

кандидат технічних наук, доцент,

доцент кафедри протидії кіберзлочинності факультету №4

Харківського національного університету внутрішніх справ

ОСНОВНІ ВІДИ КІБЕРШАХРАЙСТВА

Як уберегти себе та близьких від фінансового шахрайства. Списання грошей з рахунку без відома власника, крадіжка паролів та ПІН-кодів, легкий заробіток в інтернеті та вклади під неймовірні відсотки, онлайн-казино – це види фінансового шахрайства. Злочинці спекулюватимуть на ваших почуттях, обіцятимуть золоті гори, маскуватимуться під співробітників банків або державні організації, щоб виманити гроші. Як розпізнати шахрая і що робити, якщо вас таки вдалося обдурити? Стати жертвою злочинців може кожен, і не має значення, використовує він банківську картку або вважає за краще розраховуватися готівкою. Шахраї вміють виманювати гроші онлайн, за допомогою дзвінків та СМС, у соціальних мережах та офісах. Як вони це роблять?

Шахрайство з банківськими картками. Щоб використовувати вашу карту в своїх цілях, шахраям потрібно дізнатися про її номер, ім'я власника, термін дії, номер CVC або CVV. Вони можуть встановити скіммер на банкомат (спеціальний пристрій, який накладають на приймач картки в банкоматі) та відеокамеру над клавіатурою. Достатньо один раз скористатися таким банкоматом і не прикрити рукою клавіатуру в момент набору ПІН коду — і ваші гроші можуть зняти, перевести на кілька рахунків і перевести в готівку. Вкрасти дані вашої картки можуть навіть у кафе чи магазині. Зловмисником може бути продавець, який отримає доступ до вашої карти хоча б на п'ять секунд. Сфотографувавши вашу картку, він зможе скористатися нею для розрахунків в інтернеті.

Як не дати себе обдурити: Перед зняттям грошей у банкоматі огляньте його. На картоприймачі не повинно бути сторонніх предметів, клавіатура не повинна хитатися. Набираючи PIN-код, прикривайте клавіатуру рукою. Робіть це навіть під час розрахунків карткою у кафе. Підключіть мобільний банк та СМС-повідомлення. Якщо робите покупки через інтернет, нікому не повідомляйте секретний код для підтвердження операцій, який приходить вам по СМС. Намагайтеся ніколи не втрачати на увазі вашу карту.

Кібершахрайство. Допустимо, ви завжди знімаєте гроші тільки в касі банку, а картою і зовсім не розраховуєтеся. Ви відчуваєте себе у безпеці. Раптом вам надходить СМС або лист нібито від банку з посиланням, проханням передзвонити за невідомим номером або з повідомленням про несподіваний великий виграш. Або дзвонять від імені банку та просять повідомити особисті дані, ПІН-код від картки або номер СМС-підтвердження. Або пишуть у соціальних мережах від імені родичів чи друзів, які раптово потрапили в біду (догодили в поліцію, збила машина, вкрали сумку) і просять переказати енну суму грошей на невідомий рахунок. У 99,9% випадків ви маєте справу із шахраями. За посиланнями, швидше за все, таяться віруси, на іншому кінці дроту — фахівці з обману, які всіма правдами та неправдами хочуть виманити

необхідні їм дані, а по той бік екрану — зловмисники, які грають на ваших бажаннях, почуттях та турботі про близьких.

Як не потрапити в халепу:

– Не переходьте за невідомими посиланнями, не передзвонюйте за сумнівними номерами. Навіть якщо посилання видається надійним, а телефон вірним, завжди звіряйте адреси з доменними іменами офіційних сайтів організацій, а номери перевіряйте в офіційних довідниках.

– Якщо вам надходить СМС про зарахування коштів (і повідомлення схоже на звичне повідомлення банку), а потім дзвонить нібито розтяпа, який помилково зарахував вам гроші і просить повернути, не поспішайте нічого повертати. Така ситуація більше схожа на шахрайську схему: швидше за все гроші не приходили, СМС — не від вашого банку, а дзвонив вам зловмисник. Перевірте стан вашого рахунку, замовте виписку в онлайн-банку або зателефонуйте до банку, перш ніж переказувати комусь гроші.

– Якщо вам надходить повідомлення «Підтвердіть покупку» та код, а потім лунає дзвінок знову ж таки від «розсіяної» людини, яка каже, що помилково вказав ваш телефонний номер, і просить продиктувати йому код, ні в якому разі не робіть цього. Шахраї намагаються виманити код, щоб списати з вашого рахунку гроші або підписати вас на непотрібний платний сервіс.

– Нікому не повідомляйте персональні дані, а тим більше паролі та коди. Співробітникам банку вони не потрібні, а шахраям відкриють доступ до ваших грошей.

– Не зберігайте дані карт на комп'ютері або смартфоні. Перевірте інформацію. Якщо вам кажуть, що ви щось виграли або з вашої карти випадково списали гроші і потрібно назвати свої дані, щоб зупинити операцію, закінчіть розмову і передзвоніть у банк за номером телефону, вказаним на звороті вашої картки.

– Якщо вам повідомляють, що у родичів чи друзів неприємності, спробуйте зв'язатися з ними безпосередньо.

– Встановіть на комп'ютер антивірус і собі, і родичам.

Поясніть старим родичам та підліткам ці прості правила.

Шахрайство на фінансових ринках. Ще один тип шахраїв – псевдопрофесійні учасники фінансового ринку, які активно рекламують свої послуги з організації торгівлі на ринку Форекс. Напевно ви чули історії, як прості люди «з вулиці» заробили статки, купуючи та продаючи валюту на ринку Форекс. Звучить привабливо, але не поспішайте ризикувати. Фізична особа з невеликим стартовим капіталом не має доступу на реальний ринок Форекс, де продають та купують валюту переважно великі банки. Щоб звичайній людині вийти на Форекс, потрібно укласти договір з посередником, форекс-дилером і торгувати через нього. Торгівля на ринку Форекс сама собою великий ризик, гарантій немає, більше шансів втратити все, ніж зірвати куш. Але небезпека криється і в посередниках: можна нарватися на шахраїв, які просто не повернуть гроші. Імовірний такий варіант: вам пропонують напрочуд низькі комісії, різні бонуси (сума на вашому рахунку, припустимо, подвоюється). Ви навіть можете укласти з дилером договір через інтернет за допомогою електронного документообігу і начебто виграти цілий мільйон! Але прибутку ви не отримаєте і вкладення втратите.

Не варто зв'язуватися із так званими бінарними опціонами. Реклама в інтернеті обіцяє вам нечуваний прибуток: відкрийте рахунок, робіть ставки на зростання чи падіння валют чи акцій за певний період. Якщо після закінчення заявленого часу ваш прогноз виявляється вірним, ви отримуєте значний відсоток прибутку, якщо ви не вгадали — втрачаєте гроші. Насправді сьогодні в інтернеті немає майданчиків, на яких можуть проводитися такі угоди, тому всі обіцянки про легке заробіток на бінарних опціонах — це шахрайство. Ви просто втратите свої гроші.

Як уберегтися від обману. Якщо ви все ж таки зважилися вийти на ринок Форекс, уважно вивчіть закон і «Базовий стандарт здійснення операцій на фінансовому ринку при здійсненні діяльності форекс-дилера». Перевірте форекс-дилера, з яким маєте намір працювати, — у нього обов'язково має бути ліцензія. Уточнити, чи вона є, можна в довіднику учасників фінансового ринку.

Якщо компанія зареєстрована в офшорних зонах, насторожіться: швидше за все перед вами шахраї. Попередьте літніх родичів, що агресивна реклама швидкого заробітку в інтернеті насправді обернеться не прибутком, а втратою грошей.

УДК 351.741(477)/355/519.688

ШЕВЧЕНКО ТИХІН ВІТАЛІЙОВИЧ

кандидат юридичних наук,

старший викладач кафедри тактичної

та спеціальної фізичної підготовки факультету № 3

Харківського національного університету внутрішніх справ

АКТУАЛЬНІ ПИТАННЯ ВПРОВАДЖЕННЯ ЛОГІСТИЧНОГО КОМПЛЕКСУ ЗАБЕЗПЕЧЕННЯ БОЄЗДАТНОСТІ ПРАВООХОРОНЦІВ

Розвиток науково-технічного прогресу не стоїть на місці, а його темпи с кожним днем зростають майже в геометричній прогресії. Сучасні електронні комплектуючі, процесори, датчики та модулі змагаються за вагу у декілька грамів, а їх доступність та ціна дає змогу масово застосовувати без значних матеріальних витрат.

У свою чергу, одним з найважливіших замовників та рушіїв науково-технічного прогресу є військово-промисловий комплекс, а новітні розробки успішно застосовуються у сучасних арміях світу.

Комплекси солдатів майбутнього успішно перейшли з екранів телевізора та сторінок фантастичної літератури до сучасного життя. ВПК сильніших економік світу успішно презентують свої системи під загальною названою «солдат майбутнього», такі як «FELIN», «FIST», «Land Warrior», «Ратник», «IVAS» та більш ніж 50 схожих за своїм призначенням систем.

Однак, слід зауважити, що подібні системи проектуються та використовуються для збройних сил та ведення бойових дій, з урахуванням їх цілей, мети та завдань та не можуть частково, а іноді у повній мірі використовуватись у правоохоронних органах.

З метою забезпечення інтегрування новітніх технологій до діяльності правоохоронних органів, забезпечення особистої безпеки правоохоронців, визначення стану боєздатності та боєготовності окремих поліцейських підрозділу в цілому, контролю за станом боєздатності та боєготовності, визначення критичних критеріїв реагування на екстремальні ситуації, опрацювання взаємодії між поліцейськими, у складі підрозділу та між підрозділами, спрощення порядку планування оперативних заходів та контролю за їх виконанням, оперативного коригування дій особового складу під час проведення оперативних заходів, підвищення ефективності виконання службово-бойових задач, покращення взаємодії особового складу в підрозділі, контролю за веденням вогневого контакту, підвищення його ефективності, підвищення ефективності забезпечення публічної безпеки та порядку, підвищення ефективності проведення пошукових заходів пропонується розробка та впровадження логістичного комплексу забезпечення боєздатності правоохоронців. Введення у експлуатацію Комплексу суттєво змінить систему професійної підготовки Національної поліції, а також, зокрема, внесе зміни у підготовку командирів та керівників усіх ланок.

Список використаних джерел.

1. Шевченко, Т. В. Концептуальні питання впровадження логістичного комплексу забезпечення боєздатності правоохоронців / Шевченко Т. В., Власенко І. В. // Підготовка поліцейських в умовах реформування системи МВС України : зб. наук. пр. [конф. (м. Харків, 28 трав. 2021 р.)] / МВС України, Харків. нац. ун-т внутр. справ, Каф. тактич. та спец.-фіз. підгот. ф-ту № 2. – Харків : ХНУВС, 2021. – С. 73-76.

Для нотаток

НАУКОВЕ ВИДАННЯ

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Матеріали

Круглого столу

м. Харків, 14 грудня 2021 року

ВИДАНО В АВТОСЬКІЙ РЕДАКЦІЇ

Відп. за випуск В.М. Струков

Формат 60х84/16. Папір офсетний. Гарнітура Times ET. Умов. друк. арк. 8,19.
Наклад 100 прим. Замов. № 1208/3-21.

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) 778-60-34, e-mail:bookfabrik@mail.ua