МВС України

Харківський національний університет внутрішніх справ

Факультет № 6

Кафедра кібербезпеки та DATA-технологій

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Матеріали

Круглого столу

м. Харків, 14 грудня 2022 року

Харків

2022

Застосування інформаційних технологій у правоохоронній діяльності: матеріали круглого столу, м. Харків, 14 грудня 2022 р. / МВС України, Харк. нац. ун-т внутр. справ. Харків. ХНУВС, 2022. 167 с.

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

УДК [351.74:004] (477)(08)

ББК 67.9(4УКР)301.163я43

Н34

ОРГКОМІТЕТ:

голова – ректор генерал поліції третього рангу Сокуренко В.В.;

заступник голови – перший проректор полковник поліції Моргунов О.А;

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 20 вересня 2022 року № 40

ЗМІСТ

СОКУРЕНКО В. В.
ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У КРИМІНАЛІСТИЦІ ……..... 8
МОРГУНОВ О.А.
МОДЕЛЮВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ІНФОРМАЦІЙНОЇ СИСТЕМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ 13
БУРДІН М.Ю.
ОЦІНКА ЕФЕКТИВНОСТІ ЗАСОБІВ ЗАХИСТУ ДАНИХ В ІНФОРМАЦІЙНИХ СИСТЕМАХ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ……..... 16
КРИКУН В.В.
КРИПТОГРАФІЧНІ ЗАСОБИ ЗАХИСТУ АКУСТИЧНОЇ ІНФОРМАЦІЇ…20
БРУСАКОВА О.В.
ПРОБЛЕМІ ВИКОРИСТАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ПРИ РОЗСЛІДУВАННІ ЗЛОЧИНІВ 26
БАЛТОВСЬКИЙ О.А.
МЕТОДИКА ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ ЧАСТКОВИХ АЛГОРИТМІВ УПРАВЛІННЯ ІНТЕГРОВАНОГО КОМПЛЕКСУ ……..30
ВАЙДА Т.С.
ОСОБЛИВОСТІ НАВЧАЛЬНОГО ПРОЦЕСУ У ЗАКЛАДІ ВИЩОЇ ОСВІТИ МВС УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ…….…32
ГОРЕЛОВ Ю.П., КОБЗЕВ І.В., ЄВСТРАТ Д.І.
ХМАРНІ СЕРВІСИ, ЯК ЗАСІБ ЗАХИСТУ ВІД АТАК ПІД ЧАС ВІЙНИ..40
ГУДІЛІН В.В., СТРУКОВ В.М., УЗЛОВ Д.Ю.
ПРОБЛЕМИ ШКІДЛИВОГО МАШИННОГО НАВЧАННЯ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ РОЗПІЗНАВАННЯ ОБРАЗІВ В ЗАДАЧАХ ПОЛІЦЕЙСЬКОЇ ІЯЛЬНОСТІ..……...44
КОВАЛЕНКО А.В.
ЦИФРОВІ ЧИ ЕЛЕКТРОННІ? ДО ПИТАННЯ ЙМЕНУВАННЯ НОВОЇ КАТЕГОРІЇ ДОКАЗІВ ТА СЛІДІВ КРИМІНАЛЬНОГО ПРАВОПОРУШЕННЯ……..47
КОЛІСНИК Т.П.
СИСТЕМА ОЦІНКИ SOCTA УКРАЇНА……50
МАНЖАЙ О.В., МАНЖАЙ І.А.
ОКРЕМІ АСПЕКТИ АВТОМАТИЗАЦІЇ АНАЛІЗУ САЙТІВ З ПРОТИПРАВНИМ КОНТЕНТОМ……..54
МОЖАЄВ О.О., МОЖАЄВ М.О., ПЕРЕСІЧАНСЬКИЙ В. М., РОГ В.Є.
РОЗПІЗНАВАННЯ РАДІОСИГНАЛІВ ЗА НЕЛІНІЙНИМ ВІДГУКОМ АКУСТООПТИЧНОГО СПЕКТРОАНАЛІЗАТОРА ДЛЯ ПОКРАЩЕННЯ ЗАХИЩЕНОСТІ МЕРЕЖ КРИТИЧНОГО ЗАСТОСУВАННЯ ……..56

НОСОВ В.В., БАННІКОВА М.А.
ДЕКЛАРАТИВНА ОЦІНКА ЕФЕКТИВНОСТІ ЗАСОБІВ БЛОКУВАННЯ ТРЕКЕРІВ ЗБОРУ ІНФОРМАЦІЇ З КОМП'ЮТЕРНОЇ СИСТЕМИ ПРИ КОРИСТУВАННІ ВЕБРЕСУРСАМИ…….62
НОСОВ В.В., ІВАХНЕНКО О.С.
ОЦІНКА ЕФЕКТИВНОСТІ ДЕЯКИХ ЗАСОБІВ МАСКУВАННЯ СИГНАТУРИ ШКІДЛИВОГО КОДУ…….65
НОСОВ В.В., УСЕНКО А.О.
ОЦІНКА ХАРАКТЕРИСТИК СЕРВІСІВ ДЕЯКИХ РОЗШИРЕНЬ БРАУЗЕРУ GOOGLE CHROME З ПРИХОВУВАННЯ IP АДРЕСИ СИСТЕМИ …….68
ОРЛОВ Р.Р., ОКУШКО А.В.
ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН У ДІЯЛЬНОСТІ ПРАВООХОРОНИХ ОРГАНІВ ТА ПРОТИДІЇ КІБЕРЗЛОЧИНАМ……..70
SAZANOVA L.S.
MODERN INFORMATION TECHNOLOGIES IN THE UNITED STATES POLICE……...…73
СТРУКОВ В.М., УЗЛОВ Д.Ю., ГНУСОВ Ю.В.
СТАН ТА ПЕРСПЕКТИВИ РЕАЛІЗАЦІЇ ПРЕДИКАТИВНОЇ МОДЕЛІ У ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ……..76

ТЕЗИ КУРСАНТІВ ТА СТУДЕНТІВ

ANISIMOV O.Y., OLENDRA N.B.
THE USE OF ILP ANALYTICS IN POLICING AND CRIME PREVENTION 79
БАННІКОВА М.А., ЛОГВИНЕНКО Є.С.
РОСІЙСЬКА ПРОПАГАНДА ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ.....82
БОЛОБАН Р.Ю., СВІТЛИЧНИЙ В.А.
ДЕЯКІ ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ.....85
ГЛУЩЕНКО І.О., СВІТЛИЧНИЙ В.А.
ОСОБЛИВОСТІ ПІДГОТОВКИ КАДРІВ ДЛЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ ПІДРОЗДІЛІВ НПУ.....89
ГРУБА В.В., СВІТЛИЧНИЙ В.А.
ЗАХИСТ ІНФОРМАЦІЙНОГО ПРОСТОРУ……91
ГУЩА А.А., ХОНДАК І.І.
ПОТЕНЦІАЛ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В УМОВАХ РОЗВИТКУ КРИМІНАЛІСТИЧНОЇ ТЕХНИКИ…….93

ЄЖОВ Д.М., СВІТЛИЧНИЙ В.А.
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ ПІД ЧАС ВІЙНИ……..…….96
ЄРЬОМЕНКО Я.С., ГЕЛЬДТ С.В., МАНЖАЙ О. В.
АСПЕКТИ ВИКОРИСТАННЯ ЧАТ-БОТУ «МВС РОЗШУК» У ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЇ УКРАЇНИ…….……98
КАЛАНЧА А.А., СВІТЛИЧНИЙ В.А.
ТЕХНОЛОГІЯ VPN, ЯК НАЙЛЕГШИЙ СПОСІБ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ У КІБЕРПРОСТОРІ……...101
KAPUSTIANSKYI V.D., KALCHENKO T.M.
FACIAL RECOGNITION TECHNOLOGY IN POLICE WORK……..104
КАРПЕЧЕНКОВ М.П., ТУЛУПОВ В.В.
КІБЕРБЕЗПЕКА В УМОВАХ ВІЙНИ: ЩО, ХТО, ЯК……106
КОБЗАР О.Б., БАСАРАБ О.К.
ШИФРУВАННЯ ПОВІДОМЛЕНЬ ПІД ЧАС ОБМІНУ СЛУЖБОВОЮ ІНФОРМАЦІЄЮ З ВИКОРИСТАННЯМ ВІДКРИТИХ МЕСЕНДЖЕРІВ……..110
КРИВОШЕЄВ Є.О., СВІТЛИЧНИЙ ВІТАЛІЙ АНАТОЛІЙОВИЧ
АКТУАЛЬНІ ПРОБЛЕМИ ПІДГОТОВКИ КАДРІВ ДЛЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ ПІДРОЗДІЛІВ НПУ…….112
КУЗОВКО В.О., СВІТЛИЧНИЙ В.А.
ІНФОРМАЦІЙНА СИСТЕМА ДЛЯ ЗАБЕЗПЕЧЕННЯ УКРАЇНСЬКИХ ЗАХИСНИКІВ АКТУАЛЬНИМИ ПЕРЕВІРЕНИМИ ДАНИМИ ПРО ВОРОГА ТА КООРДИНАЦІЇ СИЛ ОБОРОНИ……...115
МАЛЯРЕНКО Д.С., СВІТЛИЧНИЙ В.А.
ІНФОРМАЦІЙНИЙ ПОРТАЛ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ…117
МАТВІЙЧУК А.О., СВІТЛИЧНИЙ В.А.
ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ТА РОБОТЕХНІКИ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ……...120
НЕСТЕРОВ Д.С., СВІТЛИЧНИЙ В.А.
ЕТИЧНІ ПИТАННЯ В ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЯХ……...123
ПРОКОПЕЦЬ К.С., СИНИЦІНА Ю.П.
СУПУТНИКОВА СИСТЕМА STARLINK, ЇЇ ПЕРЕВАГИ ТА НЕДОЛІКИ……127
САЄНКО Д.О., СВІТЛИЧНИЙ В.А.
ШЛЯХИ ФОРМУВАННЯ СИСТЕМИ ПІДГОТОВКИ КАДРІВ У СФЕРІ КІБЕРБЕЗПЕКИ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ УКРАЇНИ В УМОВАХ РОЗВИТКУ ЦИФРОВОГО СУСПІЛЬСТВА УКРАЇНИ……130
SALOVA O.V., SAZANOVA L.S.
EFFECTIVE INNOVATIVE TECHNOIOGIES IN TEACHING FOREIGN LANGUAGES AT HIGH EDUCATION INSTITUTIONS OF THE MINISTRY OF INTERNAL AFFAIRS……..133
TALAN M.A., SAZANOVA L.S.

GOOGLE DORKS AS A RESOURSE FOR CRIME INVESTIGATION…..136
ТАРАНЕНКО А.Ю., БАСАРАБ О.К.
ЗАБЕЗПЕЧЕННЯ ЕЛЕКТРОЖИВЛЕННЯМ НАЗЕМНИХ КОМПЛЕКТІВ СУПУТНИКОВОГО ЗВ'ЯЗКУ STARLINK В ПОЛЬОВИХ УМОВАХ…138
ТОВСТИК В.О., СВІТЛИЧНИЙ В.А.
ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В КРИМІНАЛІСТИЦІ……140
ТОВСТИК В.О., СВІТЛИЧНИЙ В.А.
ВИКОРИСТАННЯ ДРОНІВ В РОБОТІ ПОЛІЦІЇ……143
УСЕНКО А.О., СВІТЛИЧНИЙ В.А.
КІБЕРБУЛІНГ ТА ПРОБЛЕМИ НЕЗАХИЩЕННОСТІ ДІТЕЙ У КІБЕРСФЕРІ……145
ЦИПАК І.Г., ОНИЩЕНКО Ю.М.
СМІШИНГ ЯК ВИД ШАХРАЙСТВА У КІБЕРПРОСТОРІ……...148
CHUKALOV K.E., OLENDRA N.B.
TECHNOLOGICAL INNOVATION IN POLICING AND CRIME PREVENTION……..151
ШЕВЧЕНКО М.В., СВІТЛИЧНИЙ В.А.
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ДЛЯ ПРОТИДІЇ ЗЛОЧИННОСТІ……..153
БОНДАРЕНКО Є.С., КЛІМУШИН П.С.
СИМЕТРИЧНА АВТЕНТИФІКАЦІЯ ІНТЕРНЕТ РЕЧЕЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПОЛІЦЕЙСЬКИХ ОХОРОННИХ СИСТЕМ ……...156
ДІДЕНКО О.В., КЛІМУШИН П.С.
МОБІЛЬНІ ЗАСОБИ УДОСКОНАЛЕННЯ ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ ……159
ЯКОВЛЄВ В.І., КЛІМУШИН П.С.
ПИТАННЯ ЗАХИСТУ ХМАРНИХ ІНФРАСТРУКТУР……162
ГРУЗІН Б.М., ГРИЩЕНКО Д.О.
БЛОКЧЕЙН – МАЙБУТНЄ ЦИФРОВОЇ БЕЗПЕКИ …….
ПАВЛЕНКО С.М., ГРИЩЕНКО Д.О.
ПРИНЦИП РОБОТИ CELLEBRITE UFED TOUCH ТА ВИКОРИСТАННЯ У ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ НПУ ……..164

УДК 343.43+004

СОКУРЕНКО ВАЛЕРІЙ ВАСИЛЬОВИЧ

доктор юридичних наук, професор,

член-кореспондент Національної академії правових наук України,

заслужений юрист України,

ректор Харківського національного університету внутрішніх справ

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У КРИМІНАЛІСТИЦІ

Постановка проблеми. Від часу виникнення криміналістики як окремої науки пройшло немало часу, в світі за цей час відбулось багато змін, особливо в сфері інформаційних технологій. Відповідно, це потребує введення інновацій, нових технологій в криміналістику для забезпечення максимальних результатів у розслідуванні злочинів. Ефективність роботи правоохоронних органів може бути підвищена завдяки розробленню й запровадженню в їх діяльність новітніх інформаційних технологій і науково-технічних засобів попередження злочинів. Використовувати технологічний підхід можна не лише в криміналістичній техніці, й у тактиці й методиці розслідування. Вивчення проблем теорії формування і практики застосування інформаційних технологій у криміналістиці, програмування й алгоритмізації на їх підставі діяльності правоохоронних органів дозволяло б долати проблеми кримінального процесу, криміналістики та організації правоохоронних органів, випереджаючи розвиток злочинності й запобігаючи її поширенню в умовах інформаційного суспільства, забезпечувало б стійку інформаційну перевагу правоохоронних і судових органів над організованою злочинністю.

Метою даної доповіді є проаналізувати стан впровадження інформаційних технологій в криміналістиці.

Інформатизація соціального середовища призвела до «технологізації» криміналістики, розробки і впровадження інформаційних, цифрових, телекомунікаційних технологій. Інформаційні технології - нова категорія криміналістики, що претендує на належне місце в її структурі. Використання

технологічного підходу можливе не лише в криміналістичній техніці, а й у криміналістичній тактиці і методиці (технології провадження окремих слідчих дій, слідчі або криміналістичні технології). Підвищення ефективності боротьби зі злочинністю вимагає всебічного наукового дослідження об'єктивно існуючих явищ та притаманних їм тенденцій і закономірностей.

Реалії життєдіяльності в Україні такі, що незважаючи на війну, вбивства українців, зруйновані мережі, відключення вітчизняних операторів на тимчасово захоплених територіях, міграція за кордон, кількість абонентів мобільного зв'язку на середину 2022 р. перевищила 55 млн при чисельності населення менше 31,5 млн осіб. При цьому структура продажів електронних засобів комунікації свідчить про стійку тенденцію до домінування смартфонів, що підтримують Інтернет-комунікації, над традиційними мобільними засобами зв'язку.

Глобальна інформатизація суспільства зумовлює те, що індивід фактично веде два життя, одне реальне, інше віртуальне. Усе частіше хронологія життя сучасної людини відображається в миттєвих sms-повідомленнях, змісті електронної пошти, записах в електронних адресних книгах і календарях, фотознімках і відеороликах, статусах на сторінках у соціальних Інтернет-мережах, блогах тощо, створюваних самою особою, а також у доріжках електронних слідів, що генеруються використовуваними людиною електронними пристроями незалежно від волі останньої. Характерна криміналістична особливість кіберпростору полягає в тому, що взаємодіючі в ньому об'єкти (файли даних і програм), які беруть участь у процесі створення слідів, що виникають при цьому, не мають зовнішньої будови. Відповідно весь арсенал засобів і методів роботи з матеріальними слідами, накопичений трасологією, у цьому випадку виявляється практично непридатним, що зумовлює актуальність криміналістичного дослідження електронних носіїв інформації.

Тобто, інформаційні технології настільки проникли в життя суспільства, що злочинці самі не помічають, як залишають сліди злочину у відкритому

доступі.

З метою забезпечення органів Національної поліції України інноваційним «продуктом», призначеним для своєчасного встановлення місця знаходження й ототожнення розшукуваних осіб (у тому числі дистанційно), перспективними напрямками розвитку криміналістики слід визнати:

– створення та пристосовування до виконання криміналістичних завдань широкого спектру інформаційних технологій (наприклад, технологій аналізування метаданих абонентів стільникового зв'язку й мережевого аналізу; автоматичного пошуку, розпізнавання та ідентифікації осіб за цифровими фото, відеозображеннями, розміщеними в мережі Інтернет);

– безконтактного автоматизованого розпізнавання емоцій за фотоеталонами (патернами) їх мімічних виразів; побудови картографічних геоінформаційних схем переміщення абонентів тощо, а також розроблення криміналістичних рекомендацій комплексного використання цих інформаційних технологій з урахуванням здобутого позитивного досвіду впровадження наукових розробок і використання відкритих online- джерел суб'єктами, які володіють ресурсами, для першочергового впровадження подібних інновацій (власниками найбільших соціальних Інтернет-мереж, провідними рекрутинговими агенціями, колекторськими компаніями, операторами ринку таргетованої реклами тощо). Використання потенціалу соціальних Інтернет-мереж вже сприяло розшуку органами Національної поліції України 23% зниклих без вісти дітей, а мобільного зв'язку - пошуку жертв техногенних катастроф;

– організація навчання та доведення до автоматизму навичок виявлення, попереднього дослідження, фіксації й вилучення слідчими не тільки традиційних матеріальних чи інтелектуальних, а й віртуальних слідів;

– самостійної роботи з електронними носіями інформації та електронними засобами фіксації, копіювання, зв'язку, контролю й забезпечення захисту осіб, радіоелектронними засобами, транспортними телекомунікаційними мережами та електронними інформаційними системами;

– проведення слідчих і спеціальних слідчих дій, зумовлених впровадженням у практику інформаційних і телекомунікаційних технологій, здійснення окремих процесуальних дій у дистанційних режимах відео та телефонних конференцій.

Технічна складова роботи слідчого також піддається вираженню досить простими алгоритмами. Складання документів можна автоматизувати, а нормативно-правову базу, якою користується слідчий, зосередити в єдиній базі даних. Це стосується й методичних рекомендацій щодо кваліфікації та методики розслідування злочинів тощо.

Сьогодні досягнення у сфері програмування дозволяють створювати локальні бази даних з широкими можливостями використання внесеної інформації. Принцип дії таких програм полягає в наступному. Слідчий вносить необхідні по кримінальному провадженню дані, на основі яких створюються документи та формуються звіти, при цьому витрати часу значно менші ніж при створенні документів без допомоги автоматизованого робочого місця. Така економія досить помітна під час створення багатьох документів щодо однієї особи, де частина анкети та особисті дані слідчого заповнюються автоматично.

Характерним для сучасної людини стало позиціонувати можливості електронних пошукових систем як продовження власного інтелекту, а електронні сховища інформації як розширення своєї власної пам'яті, довіряючи все більшу кількість аналітичних функцій штучному інтелекту, а конфіденційної інформації - електронним носіям. Виступаючи творцем і розповсюджувачем власного контенту та споживачем чужого, людина неминуче залишає в кіберпросторі віртуальні сліди своєї діяльності. За цими слідами можна встановити не тільки фізичні параметри часу та місця вчинення тієї чи іншої дії, а й з високим ступенем імовірності вирішити низку діагностичних завдань з формування психологічного профілю відображеного суб'єкта та прогнозування його майбутньої поведінки.

Висновки.

Постійний плин часу змушує розвиватися кожну галузь знань. Розвиток комп'ютерних технологій, науки, накопичення теоретичних рекомендацій дають змогу для створення нових методів роботи, підвищення професіоналізму та збільшення корисної дії кожного органу прокуратури, слідства й суду. Технічна складова роботи слідчого також піддається вираженню досить простими алгоритмами. Складання документів можна автоматизувати, а нормативно-правову базу, якою користується слідчий, зосередити в єдиній базі даних.

Проблемою є те, що більшість слідчих не володіє інноваційними методами отримання інформації, а це призводить до перешкод у розслідуванні тяжких, особливо тяжких і резонансних злочинів, а для підвищення ефективності діяльності слідчих необхідно вдосконалити наявну підготовку з функціонування інформаційних систем, локальних та глобальних мереж зв'язку, організації обробки інформаційних потоків. На основі криміналістичної інформації слідчий вимальовує картину вчинення злочину і вибудовує модель розслідування кримінального провадження. В цьому контексті важливо враховувати передовий досвід реформування правоохоронних органів, зокрема у Великобританії та США.

Тому дійсно можна вважати, що інформаційні технології є кроком в майбутнє, який дозволить розширити можливості криміналістики, як науки в цілому, та сприятимуть швидшому розкриттю, а іноді і попередженню злочинів.

УДК 004.7:538.56:519.25

МОРГУНОВ ОЛЕКСАНДР АНАТОЛІЙОВИЧ

доктор юридичних наук, професор,

заслужений тренер України,

перший проректор Харківського національного університету внутрішніх справ

МОДЕЛЮВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ІНФОРМАЦІЙНОЇ СИСТЕМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Інформаційна система Національної поліції України повинна забезпечить функціонування всієї системи Національної поліції і бути важливою частиною інформаційних систем державного управління, які забезпечують безпеку, незалежність та існування України. Інформаційне забезпечення правоохоронних органів має являти собою інформаційний процес, який визначається законодавцем як процес збирання, оброблення, накопичення, зберігання, пошуку й розповсюдження інформації, необхідної для вирішення різноманітних актуальних завдань.

Для обміну інформацією в інформаційних системах правоохоронних органів використовуються як локальні комп'ютерні мережі, наприклад, при здійсненні криміналістичної реєстрації, так і глобальна мережа Інтернет. У багатьох установ, як державних, так і недержавних, існують власні сайти, де можна отримати дуже корисну інформацію. У сучасній правоохоронній практиці комп'ютерні мережі (КМ) є невід'ємною частиною інструментального комплексу, тому забезпечення їх нормального функціонування стає надзвичайно важливим завданням. Це примушує користувачів ставити питання про ефективність систем контролю, захисту та передачі інформації.

До сучасних КМ пред'являються достатньо високі вимоги, але, нажаль, в умовах обмеженого фінансування та різноманіття галузевих програм інформатизації, що є характерним для сьогодення України, більшість КМ є гетерогенними, тобто складаються із різноманітних програмно-апаратних засобів під керуванням різних операційних систем і забезпечують споживачам

широкий спектр інформаційних послуг. Через велике зростання інформації, навантаження на комп'ютерну мережу істотно збільшується. Єдина помилка в комп'ютерній мережі може привести або до втрати інформації, або до зміни великої кількості даних, що може різко знизити якість і оперативність проведення експертизи. Нажаль, такі помилки можуть бути непомічені з багатьох причин: збій програмного й/або апаратного забезпечення, некоректне адміністрування та ін. Дуже небезпечними є помилки в програмному забезпеченні (переповнювання буфера, аварійні зупинки програми, перевантаження системи, отримання прав адміністратора). Отже, виникає необхідність в управлінні процесом передачі даних.

Завдання управління процесом передачі даних продиктоване необхідністю підтримувати в мережі трафік необхідного обсягу з певними вимогами якості обслуговування. Коли необхідний розмір смуги пропускання з'єднання перевищує доступний, може проявитися перевантаження. Для надійної передачі даних, утрачені пакети в подальшому повинні бути передані повторно, що призведе до збільшення завантаження мережі. Найчастіше перевантаження в мережі може підтримуватися повторними передачами навіть у той час, коли справжня причина цього перевантаження вже відсутня.

Можливими причинами, які породжують перевантаження, є такі: високошвидкісні сполуки з великим часом передачі пакетів; тимчасові перевантаження; неоптимальні топології та неузгоджені швидкості каналів; протоколи, що несуттєво знижують швидкість відправки пакетів у мережу при виникненні перевантаження.

Метою даної доповіді є аналіз різноманітних методів моделювання процесу передачі інформації в комп'ютерній мережі інформаційної системи Національної поліції України, використання яких дозволить забезпечити необхідні показники якості передачі інформації.

Засоби, які використовуються для вивчення пропускної здатності методів передачі даних, можна розділити на три категорії.

Експерименти. Дослідження реальних з’єднань (протоколом TCP) в мережі Інтернет або експериментальних мережах (в останньому випадку необхідна обов’язкова генерація фонового трафіку для емуляції трафіку реальних мереж).

Імітаційне моделювання. Моделювання всіх мереж і протоколу транспортного рівня проводиться програмним способом. Для вивчення протоколу TCP в даний час найбільшою мірою використовується The Network Simulator (NS-2). Це програмний пакет моделювання мережі, заснований на подіях, розроблений Lawrence Berkeley National Laboratory (США), що дозволяє проводити зі значною точністю як моделювання протоколу TCP, так й інших протоколів.

Математичне моделювання. Може ставитися як до протоколу, так і до мережі в цілому.

Ми будемо проводити дослідження пропускної здатності мережі, керованої протоколом TCP, за допомогою імітаційного моделювання на основі підходу, орієнтованого на вивчення структури мережі. Просторово-часовий вимірювач доступної смуги пропускання (STAB) можна розглядати як новий метод дослідження на основі електронної системи збирання даних, який дозволяє визначати місцезнаходження з’єднань з меншою доступною пропускною здатністю, ніж всі попередні з’єднання на досліджуваному маршруті.

Наш метод за рахунок використання безперервного зондування пакетами для визначення місцезнаходження вузьких місць допомагає оцінювати доступну смугу пропускання сегментів на наскрізних маршрутах мережі, що у свою чергу допомагає відшукати її вузькі місця. При передачі інформаційних пакетів одного за іншим використовується кілька пар близько розташованих пакетів; перший пакет у кожній парі є тривалим, але володіє заголовком із невеликим часом життя (TTL), у той час як наступний пакет є коротким, але має велику область TTL. Оскільки кожен маршрутизатор на маршруті зменшує тривалість TTL пакета на одиницю і відкидає пакет, якщо значення TTL дорівнює нулю, перший пакет у

кожній парі, приймає значення нуль після зв'язку; другий пакет доходить до одержувача.

Отже, нами було наведено основні види моделей процесу передачі інформації в комп'ютерній мережі інформаційної системи Національної поліції України. Розглянуто основні переваги і недоліки цих моделей. У результаті проведених теоретичних досліджень та імітаційного моделювання встановлено, що запропонована система оцінювання параметрів мережі інформаційної системи Національної поліції України дозволяє визначати місце розташування ділянок телекомунікаційної мережі з обмеженою пропускною спроможністю.

Застосування STAB дозволяє досить точно оцінювати доступну смугу пропускання каналу за рахунок її обчислень до *m*-го з'єднання в будь-який момент часу. Отже, можливим стає побудова альтернативних віртуальних маршрутів, що дозволить істотно знизити число втрачених пакетів і, у підсумку, підвищити якість передачі інформації в комп'ютерній мережі інформаційної системи Національної поліції України.

УДК 343.982

БУРДІН МИХАЙЛО ЮРІЙОВИЧ

доктор юридичних наук, професор,

проректор Харківського національного університету внутрішніх справ

http://orcid.org/0000-0002-6748-3321

ОЦІНКА ЕФЕКТИВНОСТІ ЗАСОБІВ ЗАХИСТУ ДАНИХ В ІНФОРМАЦІЙНИХ СИСТЕМАХ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Забезпечення належних показників ефективності засобів захисту даних в інформаційних системах критичного застосування є безумовно важливою та актуальною проблемою, для вирішення якої використовуються різноманітні підходи. Особливо ця проблема важлива в умовах війни та енергетичного тероризму з боку Росії.

Однією з інформаційних систем (ІС) критичного застосування є інформаційна система Національної поліції України, яка забезпечує значну

частину інформаційної системи України та сприяє існуванню правового простору на території держави. Тому оцінка ефективності засобів захисту даних в інформаційній системі Національної поліції України є безумовно важливою проблемою.

Метою даної доповіді є аналіз можливості забезпечення належних показників ефективності засобів захисту даних в інформаційній системі Національної поліції України на етапі розробки, проектування та удосконалення цієї системи.

Одним з найбільш важливих етапів розробки методів та засобів розподілу доступу та захисту даних у ІС критичного застосування є імітаційне моделювання та експериментальне дослідження. При цьому їх метою має бути вирішення таких приватних завдань:

– перевірка адекватності розроблених моделей та методів розподілу доступу та захисту даних у ІС критичного застосування;

– аналіз достовірності отриманих результатів у ході вирішення оптимізаційних завдань налаштування параметрів розподілу доступу до ІС критичного застосування;

– обґрунтований вибір показників та оцінка за ними ефективності розроблених моделей та методів;

– розробка науково-практичних рекомендацій щодо їх використання у сучасних та перспективних ІС критичного застосування.

Відомо, що в ході вирішення цих завдань на підставі проведених досліджень та досвіду практичної експлуатації ІС критичного застосування, у тому числі Національної поліції України, необхідно приймати рішення щодо способів можливого використання аналітичного та імітаційного моделювання, а також можливого лабораторного експерименту. Традиційно за допомогою математичного моделювання можна отримати за різних вихідних даних досить широкий спектр результатів, що вимагають уточнення під час імітаційного моделювання та експерименту. Тобто, засоби математичного моделювання

повинні органічно доповнюватися можливостями імітаційної моделі та лабораторної бази.

Для обґрунтування достовірності одержаних результатів та оцінки ефективності методів розподілу доступу та захисту даних у ІС Національної поліції України було проведено імітаційне моделювання систем ідентифікації стану та адаптивного управління безпекою у ІС Національної поліції України. Узагальнена структурна схема розробленої імітаційної моделі систем ідентифікації стану та адаптивного управління безпекою в ІС Національної поліції України складається з таких підсистем:

- підсистема збирання статичної інформації;
- підсистема реєстрації поточного стану ІС;
- аналізатор трафіку;
- підсистема структурної ідентифікації ІС;
- підсистема адаптивного управління безпекою ІС.

Збір вихідної інформації про стан ІС критичного застосування здійснювався за допомогою спеціально розробленого програмного комплексу та стандартного програмного аналізатора трафіку (наприклад, Wireshark).

Структура програмного комплексу збору вхідної інформації наведено на рис. 1. Як видно із рис. 1. основними елементами збирання статистичної інформації є відповідні сенсори. Під сенсором розуміється програмний засіб, призначений для отримання інформації про одну або декілька характеристик елементів.

Проведені дослідження показали, що при розробці архітектури в процесі проектування та особливо впровадження розроблених методів та засобів розподілу доступу та захисту даних слід використовувати низку рекомендацій, які допоможуть уникнути звичайних проблем у кожній із досліджених областей захисту даних:

- аутентифікація;
- авторизація;
- управління конфігурацією;

– управління винятками;
– протоколювання та інструментування;
– управління станом.

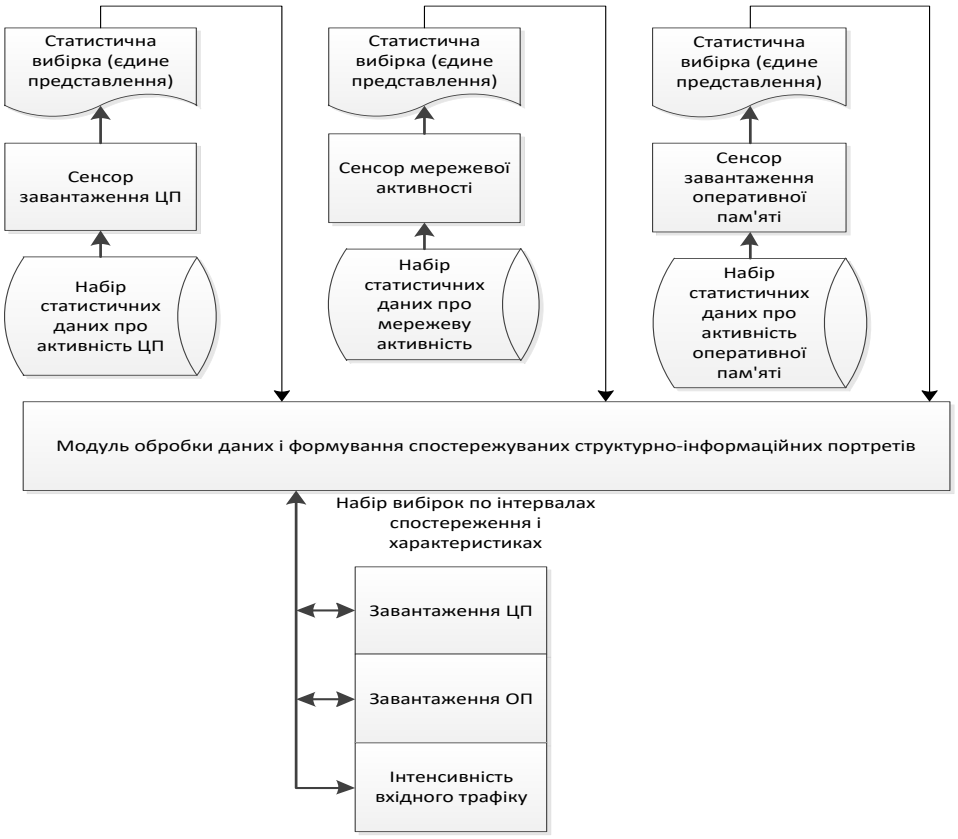


Рис. 1. Структура програмного комплексу збору вхідної інформації структурно-інформаційних портретів ІС Національної поліції України

Проектування ефективної стратегії аутентифікації має велике значення з точки зору забезпечення безпеки та надійності програми, інакше воно буде вразливим для атак з підробкою пакетів, атак перебором за словником, перехопленням сеансів та інших типів атак. При проектуванні стратегії аутентифікації необхідно керуватися такими рекомендаціями:

- Визначте межі довіри та проводьте автентифікацію користувачів та викликів на межі довіри. Врахуйте, що може знадобитися виклики аутентифікації як клієнта, так і сервера (взаємна аутентифікація).

- Забезпечте використання надійних паролів чи парольних фраз.

- За наявності множини систем у рамках програми, або якщо користувачі повинні мати можливість доступу до багатьох додатків, використовуючи одні й ті самі облікові дані, використовуйте стратегію єдиної реєстрації.

- Не передавайте паролі по мережі та не зберігайте їх у базі даних або сховищі даних у відкритому вигляді. Зберігайте пароль хеш.

Таким чином, розроблена імітаційна модель систем ідентифікації стану та адаптивного управління безпекою ІС критичного застосування здійснює збір та статистичну оцінку даних про стан КВВС критичного застосування, а також вхідного інформаційного потоку, ідентифікує стан ІС критичного застосування, виявляє аномалії в її поведінці та здійснює перерозподіл доступу до ресурсів КІУС критичного застосування на основі даних про стан системи. Результати імітаційного моделювання дозволять оцінити ефективність методів та засобів розподілу доступу та захисту даних у ІС критичного застосування.

Використання розроблених методів та засобів розподілу доступу та захисту даних у ІС критичного застосування дозволяє виконати вимоги гарантованого рівня безпеки в умовах, коли інтенсивність перевищує інтенсивність санкціонованого доступу до 5 разів, у той же час коли інші методи (мандатного та рольового доступу) можуть забезпечити дані вимоги лише за менших значень інтенсивностей шкідливих впливів.

УДК 004.451+004.056.55

КРИКУН ВЯЧЕСЛАВ ВІТАЛІЙОВИЧ

доктор юридичних наук, доцент,

проректор Одеського державного університету внутрішніх справ

ORCID ID: https://orcid.org/0000-0003-1089-555X

КРИПТОГРАФІЧНІ ЗАСОБИ ЗАХИСТУ АКУСТИЧНОЇ ІНФОРМАЦІЇ

Розрізняють два основні різновиди нейтралізації просочування акустичної (мовної) інформації з каналів зв'язку:

– засоби фізичного захисту акустичної інформації, які включають

постановники загороджувальних перешкод, фільтри і засоби пошуку каналів витоку аудіоінформації;

– засоби смислового захисту акустичної інформації в каналах мовного зв'язку.

Відомо, що засоби запобігання просочуванню акустичної інформації з першої групи мають низку слабких місць і обмежень на їх використання в тій або іншій практичній ситуації. Звісно, що засоби фізичного захисту акустичної інформації залежать від типу лінії зв'язку, її крайового устаткування, технічної кваліфікації персоналу і інших чинників. Тому в сучасних акустичних системах все більше уваги приділяється засобам смислового захисту.

Смисловий захист акустичної інформації за допомогою криптографічних методів до недавніх пір розглядався фахівцями як єдина можливість гарантованого або високонадійного захисту різних каналів мовного зв'язку незалежно від умов ведення переговорів, технічних характеристик зв'язної апаратури і інших чинників.

Прийнято виділяти три типи пристроїв, що забезпечують криптографічний захист мовної інформації: маскіратори, скремблери і пристрої з передачею шифрованої мови в цифровому вигляді.

Маскіратори і скремблери.

Маскіратори і скремблери відносяться до апаратури часової стійкості, і не завжди забезпечують необхідний рівень безпеки мовної інформації. Проте через ряд позитивних чинників (простота і порівняно невисока вартість) ці засоби дотепер мають попит у ряді фірм і компаній.

Маскіратори мови.

Іноді для забезпечення безпеки мовної інформації достатньо, щоб ваш голос в телефонній трубці був невпізнанний. Для цих цілей використовується спеціальний прилад – маскіратор мови, який по всьому каналу зв'язку створює спеціальний шум і перешкоди, що не дозволяють зловмиснику чітко чути вашу мову. В той же час на іншому кінці зв'язку ваш абонент чудово вас чує, оскільки спеціальні фільтри відсівають створені шуми. Спочатку маскіратори мови

розроблялися для стаціонарного зв'язку, тобто історія їх появи і розвитку налічує не один десяток років. При появі стільникових телефонів змінник голосу знайшов широке застосування і в цій ніші. Розглянемо більш детально можливості захисту акустичної інформації за допомогою маскіраторів. Слід відмітити, що деякі основні послуги безпеки акустичної забезпечуються з використанням активних методів маскування:

– синфазної маскувальної низькочастотної перешкоди;

– маскувальної високочастотної перешкоди;

– маскувальної “ультразвукової” перешкоди;

– підвищення напруги;

– “обнуління”;

– низькочастотної маскувальної перешкоди;

– компенсаційного;

– “випалювання”.

Аналогові скремблери.

Під аналоговим скремблюванням мається на увазі перетворення початкового мовного сигналу з метою мінімізації ознак мовного повідомлення, в результаті якого цей сигнал стає нерозбірливим і невпізнанним. При цьому він займає таку ж смугу частот спектру, як і початковий сигнал. Необхідною властивістю такого перетворення є можливість зворотного перетворення для відновлення мовного сигналу на приймальній стороні.

Технічні засоби, що забезпечують захист інформації аналоговими методами, називаються скремблерами. Іноді їх називають також маскіраторамі мови. Як правило, в сигналі, закритому за допомогою аналогового скремблеру, все-таки зберігаються окремі ознаки відкритого мовного повідомлення.

В цілому, аналогові методи захисту інформації забезпечують менший ступінь закриття мовних сигналів в порівнянні з цифровими, проте при практичній реалізації вони, як правило, простіші, дешевші, а також характеризуються достатньо високою якістю відновленого мовного сигналу.

При скремблюванні можливо перетворення мовного сигналу по трьох параметрах: амплітуді, частоті і часу. Проте в системах рухомого радіозв'язку практичне застосування знайшли в основному частотні і часові перетворення сигналу, а також їх комбінації.

Комбіновані методи перетворення сигналу припускають використання одночасно декількох різних способів скремблювання (як частотних, так і часових), число яких обмежується, як правило, можливостями технічної реалізації аналогових скремблерів.

Основні характеристики. Основними технічними характеристиками аналогових скремблерів є рівень закриття інформації, залишкова розбірливість і якість відновлення сигналу.

Найбільш важливою характеристикою скремблеру для користувача, охочого забезпечити захист інформації в своїх каналах зв'язку, є рівень закриття інформації. Слід зазначити, що, якщо для складних цифрових систем передачі мови і даних поняття рівня закриття строго регламентується і визначається криптографічною стійкістю інформації, то для аналогових скремблерів (особливо в системах рухомого радіозв'язку) дане поняття носить умовний характер, оскільки до теперішнього часу із цього приводу не вироблено чітких стандартів або правил.

У ряді випадків як критерії рівня закриття інформації при порівнянні різних засобів рухомого радіозв'язку з аналоговим скремблюванням можна використовувати кількість ключових параметрів і кількість можливих ключів скремблеру.

Порівняльний аналіз аналогових скремблерів.

Звичайно користувача найбільше цікавить питання, який скремблер забезпечить найбільший захист інформації. Слід відмітити, що представлені аналогові скремблери не можуть забезпечити гарантовану стійкість інформації, тому їх не можна розглядати як засоби криптографічного захисту інформації.

Може йтися тільки про утруднення прослуховування конкурентом або зловмисником переговорів, що ведуться за допомогою радіозасобів, оснащених

скремблерами, в реальному масштабі часу. Як вже було сказано, деяке уявлення про ступінь закриття інформації може дати кількість ключових параметрів і кількість ключів. Причому слід розглядати ці параметри в сукупності, при рівній кількості ключів перевагу мають скремблери з більшою кількістю ключових параметрів. У смугових скремблерах ключовими параметрами системи є число частотних смуг і кодова комбінація їх перестановки.

Необхідність подальшого збільшення швидкості зміни параметру перетворення викликає деякі сумніви. Перехоплення повідомлень в реальному масштабі часу в каналах зв'язку, захищених за допомогою скремблерів з параметрами перетворення, змінними в часі, можливе при застосуванні спеціальних технічних засобів, що дозволяють спочатку визначити ключову послідовність (тобто правила зміни параметрів перетворення сигналу), а потім підстроїтися під знайдену ключову послідовність. Разом з тим, це устаткування повинне бути значно складніше в порівнянні із засобами перехоплення переговорів абонентів, радіостанції якихоснащені скремблерами з фіксованими параметрами.

Взагалі, провести строге обґрунтування ступеня захищеності скремблерів украй складно. Для гарантованого захисту телефонних переговорів бажано використовувати апаратуру, що побудована на принципах цифрової передачі мови і забезпечує криптографічний захист на всіх етапах передачі.

Цифрові скремблери.

У системах цифрового захисту мови, на відміну від розглянутих скремблерів, після кодування початкового сигналу по одному з криптографічних алгоритмів не відбувається перетворення закодованого сигналу в аналогову форму, а відбувається передача цифрової інформації через модем на канали зв'язку інформації При цьому можливі два варіанти передачі інформації:

– приховування мови відбувається в шифраторах до надходження для передачі на модем;

– приховування мови відбувається в так званих модемах, що засекречують.

Основною метою при розробці пристроїв цифрового приховування мови є збереження тих її характеристик, які найбільш важливі для сприйняття слухачем. Одним з шляхів є збереження форми мовного сигналу. Цей напрям застосовується в широкосмугових цифрових системах приховування мови. В той же час не можна забувати і про можливість використання властивостей надмірності інформації, що міститься в людській мові. Цей напрям розробляється у вузькосмугових цифрових системах приховування мови.

Ширину спектру мовного сигналу можна вважати приблизно рівною 3,3кГц, а для досягнення хорошої якості сприйняття необхідне співвідношення сигнал/шум повинне складати 30 дБ. Отже, мінімальна швидкість передачі основної технічної інформації мови не нижче 60-70 біт/с. Збереження форми сигналу вимагає високої швидкості передачі і, відповідно, використання широкосмугових каналів зв'язку. Наприклад, при імпульсно-кодовій модуляції, що використовується в більшості телефонних мереж, необхідна швидкість передачі, рівна 64 кбіт/с. У разі застосування адаптивної диференціальної імпульсно-кодовій модуляції вона знижується до 32 кбіт/с і нижче. Для вузькосмугових каналів, що не забезпечують такі швидкості передачі, потрібні пристрої, що виключають надмірність мови до її передачі.

Зниження інформаційної надмірності мови досягається параметризацією мовного сигналу, при якій характеристики мови, істотні для сприйняття, зберігаються.

Таким чином, правильне застосування методів цифрової передачі мови з високою інформаційною ефективністю є украй важливим напрямом розробок пристроїв цифрового закриття мовних сигналів. У таких системах пристрій кодування мови (вокодер), аналізуючи форму мовного сигналу, проводить оцінку параметрів змінних компонент моделі генерації мови і передає ці параметри в цифровій формі по каналу зв'язку на синтезатор, де згідно цієї моделі по прийнятих параметрах синтезується мовне повідомлення.

У таких моделях мовний сигнал представляється у вигляді нестаціонарного процесу з обмеженою швидкістю зміни параметрів із-за

механічної інерції голосових органів людини. На малих інтервалах часу (до 30 мс) параметри сигналу можуть розглядатися як постійні. Чим коротший інтервал аналізу, тим більш точно може бути представлена динаміка мови, але при цьому потрібна вища швидкість передачі даних. У більшості практичних випадків використовуються інтервали двадцять мілісекунд і досягається швидкість передачі даних 2400 біт/с.

УДК 343.982

БРУСАКОВА ОКСАНА ВАЛЕРІЇВНА

доктор юридичних наук, доцент,

декан факультету № 6

Харківського національного університету внутрішніх справ

ПРОБЛЕМІ ВИКОРИСТАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ПРИ РОЗСЛІДУВАННІ ЗЛОЧИН

У сучасних криміналістичних дослідженнях велике значення приділяється використанню різноманітних високотехнологічних методів та засобів. Одним із таких засобів є безпілотні літальні апарати (БПЛА)

БПЛА – один із багатьох елементів, що характеризують напрями та темпи розвитку сучасної науки та техніки. Сьогодні БПЛА активно використовуються в різних областях діяльності людини, включаючи моніторинг екологічної та протипожежної обстановки територій і лісових масивів, контроль транспортних магістралей та шляхопроводів, виконання завдань в оборонній сфері, отримання відео сюжетів для засобів масової інформації та багато іншого.

Сучасні БПЛА мають ряд вигідних якостей, що дозволяють їх застосовувати без підготовки спеціальних майданчиків та злітно-посадкових смуг: мобільність у доставці до місця застосування, швидка підготовка до зльоту та прокладання заданого маршруту польоту, значна дальність, висота та час польоту, простота в управлінні польотом, висока одержуваних відеоматеріалів. Можливість використання безпілотних літальних апаратів у діяльності органів

внутрішніх справ також може стати актуальною та корисною, наприклад, для досягнення результатів такої слідчої дії, як огляд місця події (ОМП).

Метою даної доповіді є аналіз проблем, що виникають при використанні БПЛА у практичної діяльності правоохоронних органів, у тому числі і Національної поліції України.

В рамках діяльності органів внутрішніх справ БПЛА можна використовувати при проведенні оглядів місць пригод за різними видами злочинів на ділянках місцевості великої площі, межі огляду якої визначені слідчим або обмежені висотою та дальністю польоту безпілотника, що використовується, а також у важкодоступній місцевості. До останньої можна віднести болотисті місцевості, високогірні ділянки, лісові чагарники, а також складні ділянки доріг.

Основними технічними параметрами, які оцінюються при використанні БПЛА з криміналістичною метою, є:

– сам матеріал, з якого виготовлено апарат (вуглецеве волокно, легкосплавний, дюралюмінієвий та ін);

– можливість роздільного управління польотом БПЛА та камерою;

– модифікація акумуляторів великої місткості та час польоту;

– наявність додаткових знімних конструкцій: наприклад, кілька фото- та відеокамер, джерела освітлення, радіостанції, що діють як повітряний ретранслятор, інша апаратура для збору інформації та радіоелектронної боротьби, різні датчики та лазерні локатори, кріплення для транспортування;

– обсяг корисного навантаження від 2 до 400 кг;

– кількість та характеристика двигунів (наприклад, 8 безколекторних двигунів з 15 карбоновими пропелерами; модифікація гіроскопа, що є основним вузлом, що відповідає за просторову орієнтацію дрона);

– наявність можливості онлайн-трансляції відео у форматі HD;

– можливість відстежувати з GPS траєкторію польоту, утримуючи позиції, повертаючись у точку старту або здійснюючи політ по точках;

– наявність функції обриву зв'язку з оператором (при втраті зв'язку перехід в автоматичний режим роботи з заздалегідь визначеною траєкторією польоту);

– наявність додаткового (захищеного) шифрування між модулем контролю БПЛА і пристроєм управління.

Водночас використання БПЛА у процесі розслідування злочинів має й низку негативних моментів. Усі вони можуть бути структуровані за такими напрямами.

1. Організаційний характер:

- відсутність чіткого алгоритму дій співробітника, що застосовує БПЛА в рамках провадження слідчої дії (з яких точок, висоти, ракурсу проводити фотозйомку, як правильно орієнтувати місце розташування і т. д.), та вимог, що пред'являються до ілюстративного матеріалу, що отримується.

2. Технічний характер:

– отримані за допомогою БПЛА орієнтуючі та оглядові фотознімки не мають принципових інформаційних відмінностей від своїх аналогів, виконаних методом панорамування з верхньої точки зйомки під час використання стандартної фотоапаратури.

3. Тактичний характер:

– дані фотознімки виготовляються фахівцем, який не вивчає отриманий матеріал у процесі експертних досліджень, реконструкцій початкової обстановки місця події тощо, у зв'язку з чим не виділяються інформаційні вузли, що містять ключові елементи майбутніх об'єктів досліджень.

У зв'язку з цим ми пропонуємо низку рекомендацій щодо організації та проведення слідчих дій з використанням БПЛА.

До виїзду на огляд місця події, під час якого планується застосування БПЛА, слідує:

– перевірити наявність всіх комплектуючих, необхідних для підготовки апарату та його експлуатації з метою огляду місця події, у тому числі впевнитись у працездатності програмного забезпечення;

– переконатися у повному заряді батарей технічного засобу, його пульта керування, планшетного комп'ютера, іншого комплектуючого обладнання;

– зібрати інформацію про політ інших літальних апаратів у повітряному просторі над місцем пригоди.

Після прибуття на місце слідчої дії потрібно встановити зв'язок БПЛА з пристроєм (планшетним комп'ютером або смартфоном), провести його калібрування. Потрібно зорієнтуватися біля за допомогою навігатора системи глобального позиціонування і співвідносити отримані інформацію з картографічними даними. У процесі підготовки апарату до експлуатації навколишня обстановка оцінюється щодо виявлення перешкод для зльоту та її подальшої роботи (будівлі, будівлі, дерева, лінії електропередачі). Потім вибирається місце для зльоту БПЛА – рівний майданчик діаметром не менше 10 м з твердим покриттям, проводиться загальний огляд місця огляду (оглядовий політ) з метою визначення меж території, де здійснюватиметься слідча дія. Загальний огляд ефективно проводити за допомогою дрона, тому що може охоплюватися велика площа території, а також виключається пересування по території, що дозволяє зберегти сліди. На робочому етапі за допомогою дрона можна зробити фотографії з повітря, які можуть бути доказами у справі і вдало доповнити фото таблицю. Камера, яка оснащена БПЛА, дає можливість розпізнавати особи учасників правопорушень, здійснювати їх відео-, фотозйомку, передавати матеріали в режимі реального часу на пульт оператора. При цьому БПЛА може бути оснащений приладом нічного бачення, тепловізором, супутниковою навігацією, що дозволяє виконувати спостереження (стеження) в різних умовах. Якщо огляд здійснюється в умовах міста, рекомендується виконувати роботу з квадрокоптером удвох. Один із співробітників повинен безпосередньо керувати апаратом та візуально контролювати його поведінку в повітрі. Другий же спостерігатиме за польотом через екран планшетного комп'ютера або смартфона, а також при необхідності давати рекомендації з управління та проводити фото- та відео фіксацію.

Таким чином, розумно використовуючи можливості БПЛА при провадженні окремих слідчих дій, можна в найкоротші терміни зробити якісну фото- та/або відео зйомку на будь-якій місцевості, незалежно від її масштабів, рельєфу та рослинного покриття, а також труднодоступності об'єкта, що підлягає фото-, відео зйомці, що суттєво підвищує ефективність процесу розслідування.

УДК 338.24

БАЛТОВСЬКИЙ ОЛЕКСІЙ АНАТОЛІЙОВИЧ

доктор технічних наук, доцент,

професор кафедри кібербезпеки та інформаційного забезпечення

Одеського державного університету внутрішніх справ

МЕТОДИКА ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ ЧАСТКОВИХ АЛГОРИТМІВ УПРАВЛІННЯ ІНТЕГРОВАНОГО КОМПЛЕКСУ

Широке впровадження в сучасне виробництво інтегрованих комплексів САПР–АСУТП–АСУ ставить перед проектувальниками цих систем питання коректної оцінки придатності тих і інших алгоритмів з використанням імітаційного моделювання [1, с.29]. Оцінка та адаптація нових часткових алгоритмів (ЧА) інтегрованих комплексів. Формалізованим завданням часткового алгоритму P^{μ}, $\mu = \overline{1, n_A}$ є вектор алгоритмічних характеристик:

$$X\left(P^{\mu}\right) = \left(\theta^{\mu}, T^{\mu}, m^{\mu}, n^{\mu}, \eta^{\eta}, d^{\mu}, \sigma^{\mu}\right),$$

де θ^{μ} - тип ЧА (формування сигналів управління); T^{μ} - час реалізації P^{μ}; m^{μ} - число процесорів, що використовуються при реалізації P^{μ}; n^{μ} - число підпроцесорів в межах одного процесора, що використовується при виконанні P^{μ}; η^{μ} - ознака перевивчаємості ЧА P^{μ}; d^{μ} - директивний термін завершення P^{μ}; σ^{μ} - пріоритет P^{μ}. Множина пов’язаних ЧА обслуговуючих об’єкти заданих типів, що використовується з однаковою частотою повтору утворюють групу

ЧА. Склад ЧА групи та їх зв'язки приставляються графом $\Gamma^g\left|P^{(g)},U^{(g)}\right|$, де P^g - множина вершин, кожна з яких відповідає конкретному ЧА; U^g - множина дуг, відображуючих зв'язки між ЧА групи [2, с.98].

Характеристика групи ЧА задається характеристичним вектором

$$X\left[P^{(g)}\right]=\left(\Pi^g,\tau^g,\theta^g,E^g,D^g,V^g\right),$$

де Π^g - пріоритет групи; τ^g - період виконання; θ^g - тип групи (формування сигналів управління); X^g - множина векторів алгоритмічних характеристик ЧА групи; E^g - директивний термін завершення реалізації групи; D^g - дисципліна обслуговування ЧА групи; V^g - вектор спеціальних характеристик групи. Формалізованим завданням характеристик кожної підмножини однотипних об'єктів, що обслуговуються системою є вектор характеристик об'єктів θ_ℓ-го типу $\left(\theta_\ell\in\theta_0\right)$.

$$I_0(\theta_\ell)=\left[N(\theta_\ell),\hat{P}(\theta_\ell),F_\ell,\delta(\theta_\ell),\theta_\ell\right],$$

де $N(\theta_\ell)$- кількість об'єктів типу θ_ℓ на інтервалі моделювання; $P(\theta_\ell)$- пріоритет об'єктів типу θ_ℓ; F_ℓ- частота запуску алгоритмів обслуговування об'єктів θ_ℓ- го типу; $\delta(\theta_\ell)$- номер групи (графа) алгоритмів обслуговування об'єктів типу θ_ℓ, $\ell=1,2,...,\left|\theta_0\right|$. Для установлення взаємооднозначної відповідності між номерами ε об'єктів та обслуговуючих їх ЧА, множину $P^{(g)}$ ЧА групи доцільно подати в індексному виді

$$P^{(g)}=\bigcup_{\varepsilon-1}^{Kg}P_\varepsilon^{(g)},$$

де $P_\varepsilon^{(g)}$- підмножина ЧА групи, обслуговуючих ε-й об'єктів.

Список використаних джерел:

1. Сучасні підходи щодо адаптивного автоматизованого управління складними системами в умовах невизначеності: монографія / Кокошко В.С., Ісмайлов К.Ю., Балтовський А.О., Сіфоров О.І., Пядишев В.Г., Форос Г.В. та ін. Одеса: ОДУВС, 2019. 340 с.

2. Ісмайлов К.Ю., Балтовський О.А., Сіфоров О.І. Основні підходи щодо вирішення завдання оптимального календарного планування з використанням спеціалізованих алгоритмів. *Електронне наукове видання «Порівняльно аналітичне право».* 2019. №2. С. 98 - 101.

УДК 35.088.6+37.018.43/351.74

ВАЙДА ТАРАС СТЕПАНОВИЧ

кандидат педагогічних наук, доцент,

доцент кафедри спеціальної фізичної та вогневої підготовки

Херсонського факультету,

Одеський державний університет внутрішніх справ

ОСОБЛИВОСТІ НАВЧАЛЬНОГО ПРОЦЕСУ У ЗАКЛАДІ ВИЩОЇ ОСВІТИ МВС УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

Актуальність проблеми. Заклади вищої освіти Міністерства внутрішніх справ України (*далі* – ЗВО МВС) в умовах воєнного стану оперативно здійснюють організаційні заходи щодо модернізації та оптимізації освітнього процесу з метою забезпечення подальшої належної підготовки фахівців для органів та підрозділів Національної поліції України (*далі* – НПУ) у відповідності до сучасних вимог суспільства та визначених стандартів [1]. Масштабні зміни, які торкнулися відомчих ЗВО МВС України внаслідок тимчасової окупації державою-агресором окремих регіонів України, зумовили ряд організаційних заходів: 1) евакуацію їх особового складу (постійного та перемінного) з місця постійної дислокації; 2) спричинили вимушене значне зростання ролі інформаційних технологій на початковому етапі при застосуванні дистанційного навчання здобувачів вищої освіти; 3) продовження дистанційного навчання

студентів денної та слухачів заочної форми навчання, підготовка котрих здійснюється за кошти фізичних та юридичних осіб; 4) потребу переосмислення та упорядкування обсягу засвоєння чинних фахових знань. Всі ці ТА ІНШІ аспекти фахової підготовки поліцейських (юристів) стали вирішуватися науково-педагогічним складом завдяки комунікативним процесам на основі використання можливостей сучасних інформаційних технологій.

До роботи в таких екстремальних умовах (на прикладі воєнного стану 2022 року, а саме – вимушеної тимчасової ізоляції учасників освітнього процесу (науково-педагогічного та перемінного складу ЗВО МВС України) на окупованих територіях України, зміна місця постійної дислокації закладу освіти тощо) повинна бути готовою відомча система освіти, яка має вчасно та адекватно реагувати на ці виклики, продовжувати якісно забезпечувати освітній процес з використанням (хоча й тимчасово) дистанційної форми навчання, яка передбачена статтею 49 Закону України «Про вищу освіту» [2].

На основі аналізу спеціальної літератури з піднятої нами проблеми організації дистанційного навчання зроблено висновок, що в умовах воєнного стану належне наукове обґрунтування та методичне забезпечення освітнього процесу є важливим базовим і необхідним компонентом для ефективної організації (зміни виду) діяльності у вишах зі специфічними умовами навчання. Розгляд проблем запровадження ДН і пошук шляхів їх вирішення досліджувала низка вітчизняних вчених, зокрема В. Биков, Т. Вайда, Ю. Жук, І. Зязюн, В. Кремень, Т. Левицький, Н. Ничкало та ін.

Дистанційне навчання (ДН) − форма організації і реалізації освітнього процесу, за якою його учасники (об’єкт і суб’єкт навчання) здійснюють навчальну взаємодію принципово й переважно екстериторіально (на відстані, яка не дозволяє і не передбачає безпосередньої навчальної взаємодії учасників віч-на-віч, коли учасники перебувають за межами можливої безпосередньої навчальної взаємодії, у процесі навчання їх особиста присутність у певних навчальних приміщеннях навчального закладу не є обов’язковою) [3, с. 191].

Залежно від характеру організації навчальної комунікації між учасниками освітнього процесу та організаторами освіти і способу побудови комунікаційного каналу навчального середовища розрізняють традиційне ДН (заочна форма навчання) і електронне дистанційне навчання (е-ДН). Е-ДН – це різновид ДН, за яким учасники і організатори освітнього процесу здійснюють переважно індивідуалізовану взаємодію як асинхронно, так і синхронно у часі, використовуючи електронні системи доставки дидактичних засобів навчання та інших інформаційних об’єктів, комп’ютерні мережі інтернет, медіа навчальні засоби та інформаційно-комунікативні технології (*далі* – ІКТ) [3, с. 191].

Спираючись на визначені В.Ю. Биковим характерні риси і принципи побудови е-ДН [3, с. 191-192], конкретизуємо його деякі специфічні якісні властивості: 1) гнучкість і адаптивність освітнього процесу до потреб і можливостей курсантів (студентів, слухачів) [4, с. 12-19]; 2) модульність побудови навчальних програм; 3) специфічна роль викладача (деякі відомі функції стають домінуючими – координація навчально-пізнавального процесу; коригування змісту дисципліни; керівництво навчальними завданнями та їх поточна перевірка тощо), а деякі виникають як нові (дистанційне консультування, управління навчальними групами, допомога у професійному самовизначенні тощо) [5, с. 202-212]; 4) спеціалізовані дистанційні форми контролю якості навчальних досягнень здобувачів (співбесіди на базі платформи Zoom, Skype; практичні/модульні контрольні/самостійні роботи; використання можливостей середовища комп’ютерних інтелектуальних тестових систем тощо); 5) використання базової і спеціалізованих комунікативних технологій підтримки взаємодії суб’єктів процесу е-ДН (технології телекомунікацій, їх транспортна основа); 6) залучення спеціалізованих засобів навчання (мобільні телефони, зв’язок 4-5 G-покоління, швидкісний оптичний інтернет); 7) використання спеціалізованого програмного забезпечення організаційної підтримки е-ДН (спеціалізовані програмні засоби − інформаційних систем е-ДН: наприклад, платформи Googleclassroom, Moodle, Mia.Osvita, АСУ ОДУВС та інших); 8) використання спеціалізованих форм організації освітньої діяльності

та дистанційно орієнтованих педагогічних технологій та ін., які є ефективними за великої кількості курсантів (студентів, слухачів) [4, с. 12-19].

Науково-педагогічний та перемінний склад ХФ ОДУВС мають певний досвід використання окремих інтернет-технологій в освітньому процесі. Насамперед, це автоматична система управління освітнім процесом АСУ ОДУВС (http://asu.oduvs.edu.ua), Mia.Osvita, які надають можливості на основі навчальних планів з підготовки фахівців із певної спеціальності та визначених обсягів педагогічного навантаження, його розподілу між викладачами складати методистом навчально-методичного відділення дистанційно розклад занять, а також віддалено цілодобово користуватися ним науково-педагогічному складу та здобувачами вищої освіти (розміщується на сайті ОДУВС).

У свою чергу здобувачі вищої освіти, керівники курсів, куратори та адміністративно-управлінський склад ХФ ОДУВС можуть цілодобово слідкувати за індивідуальною успішністю та якістю знань кожної особи з мобільного телефону чи стаціонарного комп’ютера. Також АСУ освітнім процесом ОДУВС полегшує роботу викладача з обчислення підсумкового результату навчання кожного курсанта чи студента (отримані оцінки за аудиторну та самостійну роботу, модульні контрольні роботи, залік / екзамен) за 100-бальною системою оцінювання знань ECTS. Для курсантів і студентів це дає можливість прогнозувати результати свого навчання та здійснювати їх корегування за необхідності завчасно, виконуючи додаткові завдання та відвідуючи консультації викладачів.

Через популярні інтернет-ресурси викладачі на період воєнного стану забезпечують курсантів (студентів, слухачів) всіма необхідними дидактичними матеріалами для самостійного вивчення закріплених дисциплін (методичними рекомендаціями, матеріалами для лекційних, практичних і семінарських занять, тестовими завданнями тощо). Звіти щодо виконаних завдань із практичних і семінарських занять, контроль самостійної роботи, їх оцінювання, а також консультації проводяться через такі сучасні відеоінструменти як Zoom та Skype,

месенджери[1] Viber, WatsApp, Telegram, Facebook, електронну пошту ukr.net; платформи е-ДН Moodle та Naurok, чати соціальних мереж (в закритих групах) Facebook, Viber та інших.

Варто зазначити, що запровадження режимів карантину (2020-2021 рр) та воєнного стан 2022 року прискорило поступовий перехід ОДУВС і його структурних підрозділів, зокрема Херсонського факультету, на єдину платформу для навчання курсантів і студентів Moodle (сторінка дистанційного навчання в будь-якому браузері − http://dist.oduvs.edu.ua/), а згодом і на Mia.Osvita, що сприяло оперативному створенню зручного комплексу навчально-методичного забезпечення дисциплін, а також доступному поширенню дидактичних матеріалів і завдань серед здобувачів вищої освіти для організації дистанційного освітнього процесу.

Викладачами кафедр ХФ ОДУВС створено та розміщено на цих платформах електронні варіанти методичного забезпечення (навчальні та робочі програми, тексти лекцій, методрозробки для проведення практичних і семінарських занять, тестові завдання), а також безпосередньо проводяться заняття з курсантами та студентами на цьому освітньому порталі ОДУВС (Mia.Osvita). Ця платформа дає також можливість застосовувати для організації вивчення кожної теми різні види ресурсів − скановані тексти в pdf-форматі, відеоматеріали в форматі mp4, використовувати гіперпосилання на публікації у Вікіпедії чи інші інтернет-ресурси, застосовувати для контролю знань тестові методики тощо. Розміщення викладачем на початку курсу завдання для організації самостійної роботи з навчальної дисципліни дає змогу здобувачеві вищої освіти розрахувати свої сили та планувати час протягом семестру для підготовки та своєчасного надання на кафедру якісно виконаної роботи.

На нашу думку, платформу Zoom доцільно використовувати для проведення дистанційних консультацій, а також онлайн-занять для осіб, які

[1] Миттєві повідомлення, або система обміну миттєвими повідомленнями (англ. Instant messaging, скорочено IM) − телекомунікаційна служба для обміну текстовими повідомленнями між комп’ютерами або іншими пристроями користувачів через комп’ютерні мережі (здебільшого через інтернет).

хворіють або перебувають у режимі самоізоляції. Відеоінструмент Zoom відмінно підходить для індивідуальних і групових занять. Курсанти можуть заходити в програму як з комп'ютера, так і з планшета чи мобільного телефону. До відеоконференції може підключитися кожен з учасників освітнього процесу, хто має посилання або ідентифікатор конференції. Освітній чи науковий захід можна запланувати заздалегідь (здобувач має час і можливість завчасно звільнитися від своїх побутових обов'язків), а також зробити посилання для постійних занять у певний час доби (наприклад, за розкладом занять), можна зробити одне і те ж посилання для входу. Zoom також має можливість запису всієї відеоконференції з подальшим переглядом та аналізом незрозумілого/проблемного питання.

У процесі проведення заняття з допомогою Zoom курсантам/студентам цікаво спілкуватися між собою та з викладачем (особливо в умовах самоізоляції кожному бракує живого емоційного обміну з товаришами свого навчального взводу (групи), вони можуть бачити один одного). Таким чином здобувачі освіти не лише вчаться і отримують нові професійні знання, а й паралельно діляться своїми позитивними враженнями на сторінках соціальних мереж.

Подібні можливості має також і платформа Skype, але часто від користувачів можна почути окремі нарікання на якість роботи цього відеоінструменту: загальмовування (дискретність) звуку, супровід мовлення різними сторонніми шумами; короткочасне «залипання» відеозображення; несинхронна передача відеозображення та аудіосупроводу до нього тощо.

У дистанційній формі навчання викладачами та здобувачами вищої освіти широко застосовуються меседжери, наприклад Viber, Telegram, а також електронна пошта. Цей сервіс (мобільний чи комп'ютерний варіант) об'єднує в собі можливості щодо створення і обміну завданнями для групи чи індивідуально, написання текстів (відповідей) і їх адресне надсилання викладачеві, письмове спілкування (обмін повідомленнями), ознайомлення курсантів (студентів, слухачів) із результатами оцінювання свого навчання тощо.

Інтерфейс Viber є зручним і простим для використання викладачами та курсантами (студентами), дозволяє організувати процес навчання як із персонального комп'ютера, так і з мобільних пристроїв (iOS, Android). До недоліків цього месенджера варто віднести: 1) деякі курсанти (студенти) зареєстровані під ніком[2], який не відображує його прізвище, або тільки за своїм іменем без прикріпленої фотографії, що ускладнює їх як ідентифікацію (особливо якщо фоторобота на паперовому носії не підписана), так і сортування (зберігання) роботи по навчальних групах; 2) встановлення автентичності самого виконавця та відправника роботи, хоча малоймовірною та малопоширеною є практика, коли хтось із членів сім'ї виконував і відправляв завдання за курсанта (студента); 3) залишається ризик технічних збоїв під час виконання окремими здобувачами вищої освіти наданого завдання чи при його відправленні (недостатнє мобільне покриття, раптове аварійне відключення електроенергії тощо). Тому викладачам доцільно застосовувати індивідуальний підхід і передбачати можливість повторного виконання завдання (самостійної, контрольної роботи тощо); 4) спостерігаються випадки списування, коли у курсанта, який першим розмістив свою роботу у групі, переписують варіанти відповідей інші особи.

Висновки. На основі опрацювання нормативно-правових актів та проведеного аналізу спеціальної педагогічної літератури з проблеми організації ДН курсантів (студентів, слухачів) ЗВО МВС України, з урахуванням систематизації напрацьованого досвіду використання цієї форми навчання під час карантинних заходів в умовах запровадження у 2020-2021 рр НС природного походження (протидія пандемії гострої респіраторної хвороби Covid-2019) та в умовах воєнного стану 2022 року можна зробити деякі узагальнення.

[2] Нік, нікнейм (*від англ*. nick, nickname; Міжнародний фонетичний алфавіт: [`niknem] − спочатку «кличка, прізвисько», від середньо-англійського an eke name − «інше ім'я», яке перейшло в «a nick name») − особисте, переважно вигадане ім'я, яким називають себе користувачі інтернету в різноманітних чатах, форумах, месенджерах, а також у Вікіпедії, на сайтах та вікісайтах.

Найбільш важливими поточними орієнтирами щодо застосування в освітньому процесі ДН у ЗВО МВС України можна визначити такі: 1) розробка адаптованого до потреб НПУ та обґрунтоване організаційне проектування цієї форми освітньої діяльності у практичній діяльності відомчих закладів; 2) створення якісних курсів дистанційного навчання та сучасних електронних середовищ, забезпечення інформаційної підтримки освітньої діяльності як на денній формі навчання (студенти), так і самостійного навчання здобувачів вищої освіти за всіма навчальними дисциплінами; 3) створення умов для відкритого доступу до інформаційних ресурсів навчального призначення для всіх категорій учасників освітнього процесу; 4) запровадження елементів педагогічних технологій ДН і сучасних інформаційно-комунікаційних засобів з метою забезпечення ефективної взаємодії суб'єктів освітнього процесу протягом всього навчального періоду; скорочення тривалості очних екзаменаційних сесій для осіб, які навчаються за заочною формою; 5) створення на основі використання сучасних освітніх платформ передумов для розбудови системи безперервної освіти поліцейських (підвищення кваліфікації та самостійного навчання працівників органів та підрозділів НПУ протягом всієї професійної кар'єри, зокрема й без відриву від несення служби); 6) при використанні е-ДН необхідно враховувати його суттєві переваги порівняно з традиційним навчанням.

Отже, досягнення освітньої мети – активне використання дистанційного навчання у ЗВО МВС України означає: 1) нормативно утвердити е-ДН як рівноправну форму здобуття правової освіти в сучасних умовах суспільного розвитку; 2) визнати пріоритетність цієї педагогічної форми в системі підготовки поліцейських для органів НПУ, яка забезпечує рівний доступ до якісної освіти широкого контингенту працівників органів та підрозділів правоохоронних органів; 3) створити необхідні умови для реалізації в освітніх системах принципів відкритості відомчої освіти МВС України.

Список використаних джерел:

1. Про правовий режим воєнного стану : Закон України від 12 травня 2015 року № 389-VIII (із змінами станом на 29.09.2022). URL: https://zakon.rada.gov.ua/laws/show/389-19#Text (дата звернення: 21.11.2022).

2. Про вищу освіту : Закон України від 1 липня 2014 року № 1556-VII. Дата оновлення: 18.03.2020. URL: https://zakon.rada.gov.ua/laws/show/1556-18.

3. Енциклопедія освіти / Акад. пед. наук України, головний ред. В.Г. Кремень. К. : Юрінком Інтер, 2008. 1040 с.

4. Вайда Т.С. Деякі проблемні питання розвитку дистанційного навчання в закладах вищої освіти МВС України // *Матеріали Міжнародної науково-практичної конференції «Реформування правоохоронних органів України у світлі змін євроінтеграційних процесів»* (20 березня 2020 року, ХФ ОДУВС). Херсон : Олді-плюс, 2020. С. 12-19.

5. Вайда Т.С. Педагогічні можливості деяких сучасних інформаційних технологій як засобів дистанційного навчання здобувачів вищої освіти у закладах МВС України. *Юридичний бюлетень* : наук. журнал. Одеса: ОДУВС, 2020. Випуск 12 (12). С. 202-212.

УДК 004.77

ГОРЕЛОВ ЮРІЙ ПЕТРОВИЧ,

кандидат технічних наук, доцент, доцент кафедри кібербезпеки та DATA-технологій Харківського національного університету внутрішніх справ

https://orcid.org/0000-0002-0330-5008

КОБЗЕВ ІГОР ВОЛОДИМИРОВИЧ

кандидат технічних наук, доцент,

доцент кафедри інформатики та комп'ютерної техніки

Харківського національного економічного університету ім. С. Кузнеця

https://orcid.org/0000-0002-7182-5814

ЄВСТРАТ ДМИТРО ІВАНОВИЧ

кандидат технічних наук, доцент,

доцент кафедри інформаційних систем

Харківського національного економічного університету ім. С. Кузнеця

https://orcid.org/0000-0001-8393-6063

ХМАРНІ СЕРВІСИ, ЯК ЗАСІБ ЗАХИСТУ ВІД АТАК ПІД ЧАС ВІЙНИ

З початку війни Україна стала ціллю чисельних кібератак, які охопили державні установи, приватні організації та громадян. Ті підприємства, які є частиною критичної інфраструктури, зокрема енергетичні, телекомунікаційні, медіа та фінансові компанії, також мають бути у режимі підвищеної готовності, оскільки саме ці галузі часто вважаються пріоритетними цілями у період війни.

Найбільш серйозним та руйнівним видом загроз для державних структур є DDoS-атака. DDoS-атака — це метод атаки, при якому хакери націлюються на сервери і перевантажують їх користувальницьким трафіком. Коли сервер не справляється з вхідними запитами, сайт, програма або додаток, розташовані на ньому, відключаються або працюють з низькою продуктивністю.

Наприклад, після початку повномасштабного вторгнення Росії в Україну Мінцифри створило добровільну кіберармію, яка здійснює DDoS-атаки на ресурси країни-окупанта. За короткий період IT ARMY of Ukraine поклала сайти російських пропагандистів, органів влади, компаній із держсектора, енергетики, банків, рітейлу, сервіси грошових переказів, бухгалтерської звітності та багато іншого [1].

Сьогодні в умовах війни з'явився різкий зростання запитів на хмарні технології. Організація резервних майданчиків для зберігання даних, резервного копіювання та кібербезпеки стали основними викликами для держави та бізнесу після вторгнення РФ на територію України.

Постановою Кабінету міністрів України від 12 березня 2022 року в умовах воєнного стану державні установи отримали дозвіл на розміщення державних інформаційних ресурсів та публічних електронних реєстрів на хмарних ресурсах та/або в центрах обробки даних, що розташовані за межами України. Це

розширило можливості використання хмар. Тепер державні організації можуть використовувати всі їхні переваги, щоб без перешкод працювати у складний воєнний період [2].

Державні установи всіх рівнів потребують перехід на хмарні інфраструктури. Це необхідно для швидкого надання населенню якісних послуг, гнучку, масштабну та економічну технологічну базу. Автоматизація процесів та їхнє перенесення у хмарне середовище дають можливість максимально прискорити процедуру надання послуг, а також забезпечити громадянам мінімальні витрати часу на отримання тієї чи іншої інформації. Першочергова загроза використання хмарних технологій у держсекторі – безпека зберігання даних. За кордоном із цією проблемою вирішили боротися шляхом використання приватних хмар, коли обладнання установи знаходиться безпосередньо всередині мережі держструктури. Традиційною проблемою використання публічних хмарних платформ державними структурами є специфічні вимоги до безпеки. Враховуючи, що держсектор є одним із найбільших ІТ-замовників у нашій країні, найлогічніше припустити, що він піде шляхом побудови «громадської хмари» — хмарної платформи, яка використовуватиметься іншими держструктурами зі схожими вимогами до безпеки.

Через масштабні бойові дії в Україні робота дата центрів під загрозою, оскільки територія країни знаходиться під постійними обстрілами армією РФ, тому навіть власники серверних не можуть дати гарантії, що дата центрів не постраждають.

Воєнний стан в Україні викликає занепокоєння також через нові виклики у забезпеченні безперебійної роботи критичних сервісів та систем, які можуть бути пошкоджені або виведені з ладу внаслідок бойових дій. Перенесення ІТ-інфраструктури в хмару або створення сайтів аварійного відновлення у глобальних хмарних ЦОД дозволить гарантувати необхідний рівень доступності.

Для цього потрібно обрати провайдера хмарних сервісів, враховуючи наявні компетенції ІТ-спеціалістів, визначити черговість та критичність перенесення тих чи інших елементів ІТ-архітектури в хмару; організувати

збереження резервних копій інформації в хмарі, організувати сайти аварійного відновлення в публічній хмарі в Європі або США. Наприклад компанія Microsoft вже надала безоплатні хмарні сервіси до кінця 2022 року і продовжила термін до 2023 року. Сьогодні значна частина критично важливої інформації перетворюється на цифровий вигляд за межі контрольованої зони. У зв'язку з цим ЦОД, які надають хмарні послуги, повинні взяти на себе цю роль і забезпечувати захист інформації шляхом запровадження внутрішніх сервісів, що обмежують доступ до інформації неавторизованим особам. Головний висновок із всього вищезазначеного — необхідно забезпечити свої корпоративні дані від наслідків війни можна, перемістивши їх на постійне або тимчасове зберігання у хмарне сховище

Список використаних джерел:

1. Що таке кібербезпека і як бізнесу захиститися від DDoS-атак. GigaCloud //URL: https://gigacloud.ua/blog/navchannja/scho-take-kiberbezpeka-i-jak-biznesu-zahistitisja-vid-ddos-atak

2. Підгайна Є. Тримаємо стрій: добірка корисних хмарних сервісів для відновлення роботи бізнесу в умовах війни / Євгенія Підгайна // Інтерфакс-Україна – URL: https://mind.ua/publications/20238662-trimaemo-strij-dobirka-korisnih-hmarnih-servisiv-dlya-vidnovlennya-roboti-biznesu-v-umovah-vijni.

УДК 004.8

ГУДІЛІН ВЛАДИСЛАВ ВЛАДИСЛАВОВИЧ

слухач магістратури факультету №5

Харківського національного університету внутрішніх справ

СТРУКОВ ВОЛОДИМИР МИХАЙЛОВИЧ

кандидат технічних наук, доцент,

професор кафедри кібербезпеки та DATA-технологій факультету №6

Харківського національного університету внутрішніх справ

ORCID ID: http://orcid.org/0000-0003-4722-3159;

УЗЛОВ ДМИТРО ЮРІЙОВИЧ

кандидат технічних наук,

доцент кафедри штучного інтелекту

Харківського національного університету радіоелектроніки

ORCID: https://orcid.org/0000-0003-3308-424X

ПРОБЛЕМИ ШКІДЛИВОГО МАШИННОГО НАВЧАННЯ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ РОЗПІЗНАВАННЯ ОБРАЗІВ В ЗАДАЧАХ ПОЛІЦЕЙСЬКОЇ ДІЯЛЬНОСТІ

На сьогоднішній день в Національній поліції України та правоохоронній діяльності загалом набирає популярності використання програмних або програмно-апаратних комплексів, заснованих на технології computer vision. Комп'ютерний зір (Computer Vision, CV) - це область штучного інтелекту, в якій розглядаються методи і моделі навчання комп'ютерних систем аналізувати, класифікувати або розпізнавати об'єкти на зображеннях і відео. В основі CV-систем зазвичай лежать алгоритми машинного навчання, за допомогою яких вони відрізняють одні об'єкти від інших, можуть знаходити патерни й закономірності.

Однією з задач, що постають перед такими системами в правоохоронній діяльності, є розпізнавання та порівняння обличь за банками даних, що знаходяться в їх розпорядженні. Це дозволяє швидко ідентифікувати особу та виявити місцезнаходження розшукуваного в загальнодоступному місці. Також технології комп'ютерного зору використовуються для розпізнавання реєстраційного номеру транспортного засобу, марки, кольору та типу

автомобіля, вироблення поведінкового профілю за історією фіксації технічними засобами, що мають функції фото- і відеозапису.

Нейронні мережі поки що не є настільки розумні, щоб мати здатність до повного протистояння злому наміру з боку людини. Метод машинного навчання, який спрямований на те, щоб обійти модель нейронної мережі, використовуючи вхідні дані, що вводять відповідну модель в оману, отримав назву «шкідливе машинне навчання» (adversarial machine learning). Він включає як генерацію, так і виявлення шкідливих вхідних даних (adversarial examples), спеціально створених для обходу класифікаторів, незважаючи на те, що вони нагадують дійсні вхідні дані для людини.

Сценарії атаки на моделі машинного навчання, як і багато інших, розділяють на атаки білої та чорної скриньки. Атака білої скриньки – це сценарій, у якому атакуючий має повний доступ до цільової моделі нейронної мережі, включаючи архітектуру моделі та її параметри. Атака чорної скриньки – це сценарій, у якому атакуючий не має доступу до моделі і має лише доступ до вихідних даних цільової моделі.

За типом серед найбільш поширених – атаки отруєння, атаки ухилення та крадіжка моделі. Атака отруєння – це атака, при якій, атакуючий впливає на навчальні дані або їх навчальні позначки (labels), щоб модель відпрацьовувала некоректно.

Атаки ухилення є найбільш поширеними та найбільш вивченими типами атак. Зловмисник маніпулює даними вже після розгортання застосунку, щоб обійти раніше навчені класифікатори.

Крадіжка моделі або вилучення моделі має на увазі дії зловмисника, що досліджує систему машинного навчання за сценарієм «чорна скринька», щоб або реконструювати модель, або витягти дані, на яких вона була навчена. Це особливо небезпечно, коли навчальні дані, або сама модель є конфіденційними.

В останні роки компанії, які активно інвестують у машинне навчання (Google, Amazon, Microsoft і Tesla), зіткнулися з певними атаками зловмисників.

Більше того, уряди починають впроваджувати стандарти безпеки для систем машинного навчання, а Європейський Союз навіть випустив повний контрольний список для оцінки надійності систем машинного навчання. Дослідницька фірма в сфері інформаційних технологій Gartner, повідомила, що розробники додатків повинні передбачати та підготуватися до збільшення потенційних ризиків пошкодження даних, крадіжки моделей та ворожих шкідливих вхідних даних.

Таким чином, із розвитком машинного навчання потреба захисту моделей державними органами стрімко зростає. Також слід зазначити, що наразі наголос щодо захисту систем Computer Vision, як і раніше, робиться на традиційну безпеку.

Для аналітичних підрозділів НПУ ця проблема вже зараз є актуальною у контексті переходу до предикативної моделі діяльності, оскільки ця модель в якості основних інструментів її реалізації передбачає застосування аналітичних систем, що базуються на застосуванні глибоких нейронних мереж.

Список використаних джерел:

1. Ian J. Goodfellow, Jonathon Shlens and Christian Szegedy. Explaining and harnessing adversarial examples, *California*, eprint arXiv:1412.6572v3, 2015. 11 p.

2. Cato Pauling, Michael Gimson and Basel Halak. A tutorial on adversarial learning attacks and countermeasures, eprint arXiv:1905.01051, 2022. 32 p.

3. Chawin Sitawarin, Arjun Nitin Bhagoji and Arsalan Mosenia. DARTS: Deceiving Autonomous Cars with Toxic Signs, eprint arXiv:1802.06430v3, *New Jersey*, 2018. 18 p.

УДК 343.98

КОВАЛЕНКО АРТЕМ ВОЛОДИМИРОВИЧ

кандидат юридичних наук

доцент кафедри кримінально-правових дисциплін
Луганський державний університет внутрішніх справ ім. Е.О. Дідоренка
м. Івано-Франківськ

ЦИФРОВІ ЧИ ЕЛЕКТРОННІ? ДО ПИТАННЯ ЙМЕНУВАННЯ НОВОЇ КАТЕГОРІЇ ДОКАЗІВ ТА СЛІДІВ КРИМІНАЛЬНОГО ПРАВОПОРУШЕННЯ

Кінець XX та початок XXI сторіччя характеризуються суцільною комп'ютеризацією усіх сфер суспільного життя. Електронно-обчислювальні машини різних типів та розмірів допомагають людині комфортно існувати, а іноді навіть успішно замінюють її при виконанні певних завдань. Але попри всі позитивні аспекти впровадження комп'ютерів у наше життя, ватро зазначити що такі прилади, як і інші новітні технології, беруться на озброєння особами, котрі вчиняють кримінальні правопорушення. Такі особи здатні обернути на свою користь практично будь-який електронно-обчислювальний пристрій: персональні комп'ютери та ноутбуки, смартфони, планшети, ігрові приставки, сервери, маршрутизатори й роутери, принтери та копіювальну техніку тощо.

Розкриття й розслідування кримінальних правопорушень, учинених з використанням комп'ютерної техніки, потребує з'ясування та фіксування операцій, здійснених правопорушником з подібними приладами. Дії користувача можливо відслідкувати за змінами, що утворюються у пам'яті електронно-обчислювальних пристроїв, котрі у свою чергу можна вважати специфічними слідами кримінального правопорушення. Подібні сліди вимагають новітніх підходів до їх виявлення, збирання та дослідження, а сформовані на основі їх опрацювання докази – своєрідного порядку їх використання у кримінальному провадженні.

У наукових колах відсутній єдиний підхід до найменування та визначення описаних видів слідів та доказів Учені-криміналісти називають зміни, що утворюються внаслідок взаємодії правопорушника з комп'ютерною технікою у її пам'яті, цифровими або електронними слідами (іноді використовується термін відображення, котрий на нашу думку є синонімічним слову слід). Відповідно

докази, що формуються сторонами провадження у результаті дослідження й процесуального закріплення даних слідів, аналогічно прийнято називати цифровими або електронними. Вважаємо за доцільне спробувати розібратися в етимології наведених термінів та запропонувати власний погляд на вирішення даної термінологічної колізії.

Терміни «цифровий слід» та «цифровий доказ» походять від англійського слова digital – цифровий (digit – цифра) та були запозичені у зарубіжних процесуалістів і криміналістів. Застосування категорії «цифровий» можна пояснити тим, що практично усі сучасні комп'ютери використовують математичні алгоритми й комбінації цифр (найчастіше – бінарний код, поєднання 0 та 1) як універсальний засіб кодування, збереження й передавання будь-якої інформації. Цифрову форму кодування прийнято протиставляти більш старій та менш розповсюдженій аналоговій, за якої дані передаються через коливання фізичних показників струму, світлового потоку, радіохвиль тощо. Відтак, у більшості випадків комп'ютерні дані (інформація), що мають значення для кримінального провадження, закодовані у цифровій формі та потребують інтерпретації (перетворення, декодування) для сприйняття людиною.

У свою чергу терміни «електронний слід» та «електронний доказ» походять від назви негативно зарядженої елементарної частинки – електрона, рух якої покладено в основу усіх електричних приладів. Більшість сучасних обчислювальних пристроїв (процесорів, логічних схем) та флеш-накопичувачів даних (SSD диски, USB-диски, вбудована пам'ять мобільних пристроїв) побудовані на базі транзисторів, а пристрої динамічної оперативної пам'яті (DRAM) працюють на базі конденсаторів. У максимально спрощеному вигляді принцип роботи наведених приладів можна описати так: дані кодуються, обробляються та передаються шляхом регулювання руху електронів через транзистори, а також накопичення певного електричного заряду конденсаторами. Відтак, комп'ютерні дані (інформація), що мають значення для кримінального провадження, безпосередньо пов'язані з рухом електронів у логічних елементах електронно-обчислювальної техніки.

Зауважимо що жоден з наведених підходів не є оптимальним з технічної точки зору: уже сьогодні існують системи кодування, що не побудовані на використанні цифр, а також обчислювальні пристрої й сучасні засоби передавання інформації, котрі не покладаються на рух електронів (квантові комп'ютери, передавання даних за допомогою оптичних сигналів тощо). Таким чином, для інформації що обробляється, передається чи зберігається описаними способами, використання термінів «цифрова» чи «електронна» буде технічно не вірним. Можна спрогнозувати що із розвитком науки і техніки поширення набудуть й інші комп'ютерні технології, котрі по суті не відповідатимуть розглядуваним термінам.

Проте у сучасних умовах, на нашу думку, категорії «цифровий» та «електронний» є рівнозначними та несуть однакове смислове навантаження. Обидві можуть застосовуватися для позначення комп'ютерних даних (інформації), що має значення для встановлення обставин кримінального правопорушення та використовується у доказуванні. Щодо йменування нового виду доказів, то спір між «цифровими» та «електронними» має вирішити законодавець шляхом закріплення такої категорії у КПК України. Видається що перевага має бути надана «електронним» доказам за аналогією з іншими галузями процесуального законодавства. Щодо йменування нової категорії слідів, то це питання лишається у віданні науковців та практиків. Можемо спрогнозувати що приживеться варіант аналогічний до закріпленої у КПК України назви нової категорії доказів.

УДК 004.77

КОЛІСНИК ТЕТЯНА ПЕТРІВНА

кандидат педагогічних наук, доцент,

доцент кафедри протидії кіберзлочинності факультету №4

Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-74428136

СИСТЕМА ОЦІНКИ SOCTA УКРАЇНА

З огляду на стан поширення організованої злочинності, складне безпекове середовище навколо України та криміногенну ситуацію всередині держави організація системної боротьби з організованою злочинністю повинна стати одним із пріоритетних завдань державної політики та потребує вжиття дієвих скоординованих міжвідомчих заходів і поглиблення міжнародного співробітництва.

З метою реалізації Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 р. № 287, Конвенції Організації Об'єднаних Націй проти транснаціональної організованої злочинності та зобов'язань, узятих Україною за Угодою про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, Україною вжити ряд кроків щодо імплементації циклу ЄС – EMPACT. Так, розпорядженням Кабінету Міністрів України від 16.09.2020 № 1126- р схвалено Стратегію боротьби з організованою злочинністю [1]. Ця Стратегія визначає напрями розвитку системи боротьби з організованою злочинністю та механізми реалізації державної політики у відповідній сфері в сучасних умовах. Було визначено три етапи реалізації Стратегії.

Крок 1: Оцінка загроз тяжких злочинів та організованої злочинності (SOCTA Україна).

Крок 2: Визначення стратегічних цілей згідно з висновками оцінки SOCTA Україна і розроблення комплексних планів заходів.

Крок 3: Виконання комплексних планів заходів.

Аналітичні висновки, зроблені за результатами проведення оцінки загроз тяжких злочинів та організованої злочинності (SOCTA Україна), формують політичні пріоритети, які трансформуються у стратегічні цілі. Затверджені стратегічні цілі є основою для розроблення комплексних планів заходів.

З метою реалізації першого етапу Стратегії – Постановою Кабінету Міністрів України від 26.01.2022 № 59 «Про деякі питання запровадження в діяльність центральних органів виконавчої влади системи оцінки SOCTA Україна» [2] затверджено Склад міжвідомчої робочої групи з координації запровадження в діяльність центральних органів виконавчої влади системи оцінки SOCTA Україна, Положення про міжвідомчу робочу групу з координації запровадження в діяльність центральних органів виконавчої влади системи оцінки SOCTA Україна та Порядок збирання і узагальнення інформації та здійснення оцінювання загроз організованої злочинності та тяжких злочинів відповідно до системи оцінки SOCTA Україна».

Система оцінки SOCTA Україна - сукупність розроблених за методологією Європейського поліцейського офісу механізмів збирання, узагальнення та аналізу інформації про загрози організованої злочинності та тяжких злочинів і визначення пріоритетів у протидії їм. Зібрана інформація повинна ґрунтуватися на здобутій оперативній інформації та матеріалах, отриманих під час проведення досудового розслідування, та матеріалах закритих кримінальних проваджень, які було розпочато 1 січня року, що є першим у визначеному періоді оцінювання, або пізніше. Згідно Порядку збирання і узагальнення інформації та здійснення оцінювання загроз організованої злочинності та тяжких злочинів відповідно до системи оцінки SOCTA Україна існує два види карток:

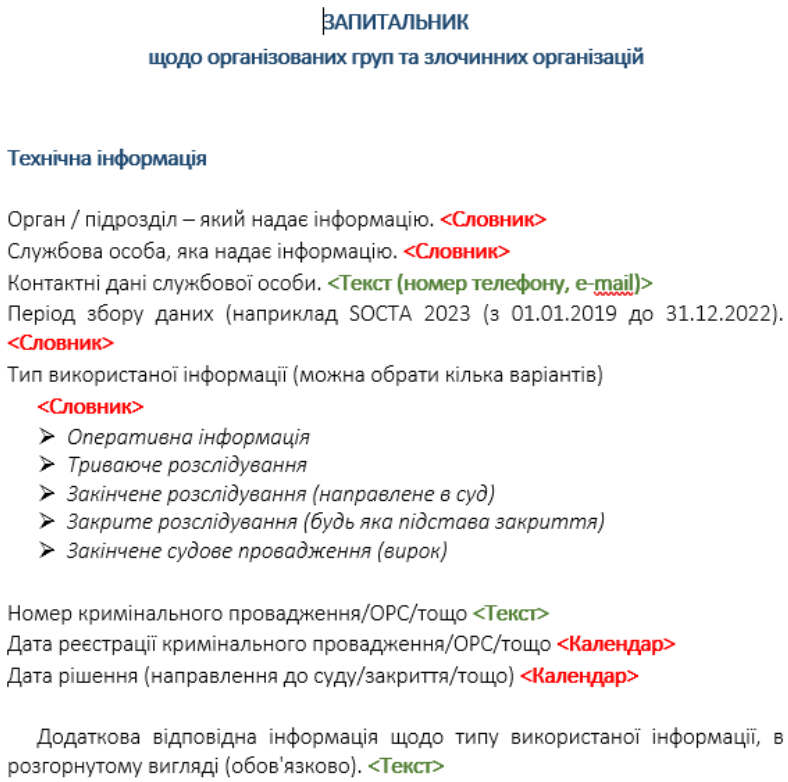
- облікова картка щодо організованої групи та/або злочинної організації;
- облікова картка щодо сфер злочинної діяльності.

Облікова картка щодо ОГ та ЗО заповнюється окремо на кожну організовану групу та/або злочинну організацію, злочинну спільноту. Облікова картка щодо сфер злочинної діяльності заповнюється окремо на кожну сферу злочинної діяльності, причому кожна сфера злочинної діяльності оцінюється за визначеним переліком індикаторів.

Відомості щодо організованої групи та/або злочинної організації, злочинної спільноти та сфер злочинної діяльності вносяться програмно-технічними засобами з використанням каналів зв’язку єдиної цифрової відомчої

телекомунікаційної мережі до єдиної інформаційної системи МВС у встановленому законодавством порядку.

02.11.2022 на першому засіданні міжвідомчої робочої групи, Національною поліцією було презентовано зразки карток (запитальників) щодо організованих груп і злочинних організацій та сфери злочинної діяльності (Рис.1).



ЗАПИТАЛЬНИК

щодо організованих груп та злочинних організацій

Технічна інформація

Орган / підрозділ – який надає інформацію. **<Словник>**
Службова особа, яка надає інформацію. **<Словник>**
Контактні дані службової особи. **<Текст (номер телефону, e-mail)>**
Період збору даних (наприклад SOCTA 2023 (з 01.01.2019 до 31.12.2022).
<Словник>
Тип використаної інформації (можна обрати кілька варіантів)
<Словник>

- *Оперативна інформація*
- *Триваюче розслідування*
- *Закінчене розслідування (направлене в суд)*
- *Закрите розслідування (будь яка підстава закриття)*
- *Закінчене судове провадження (вирок)*

Номер кримінального провадження/ОРС/тощо **<Текст>**
Дата реєстрації кримінального провадження/ОРС/тощо **<Календар>**
Дата рішення (направлення до суду/закриття/тощо) **<Календар>**

Додаткова відповідна інформація щодо типу використаної інформації, в розгорнутому вигляді (обов'язково). **<Текст>**

Рис. 1.

Методологія SOCTA використовує змішаний підхід, який складається з якісних та кількісних методів аналізу та набору чітко визначених показників, для виявлення та уточнення найбільш загрозливих кримінальних явищ.

Програмістами ДІАП спільно з ДКА НП України розробляється IT-рішення для виконання покладених на поліцію завдань у сфері збору даних для аналізу загроз SOCTA. Рішення запроваджується на базі Інформаційного Порталу Національної Поліції.

В автоматизованій інформаційній системі оперативного призначення єдиної інформаційної системи МВС (АІС ОП) створено відповідний облік

матеріалів з оцінювання загроз учинення тяжких злочинів та організованої злочинності (SOCTA). Зазначені матеріали можливо вносити до АІС ОП не тільки завдяки надсиланню відповідних матеріалів до підрозділів кримінального аналізу в областях та на рівні центрального органу управління поліції, але й безпосереднього самими оперативними підрозділами кримінальної поліції [3].

Список використаних джерел:

1. Про схвалення Стратегії боротьби з організованою злочинністю: Розпорядження КМУ від 16 вересня 2020 р. №1126-р // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1126-2020-р#Text (дата звернення: 19.11.2022).

2. Деякі питання запровадження в діяльність центральних органів виконавчої влади системи оцінки SOCTA Україна: Постанова КМУ від 26 січня 2022 р. № 59 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/59-2022-п#Text (дата звернення: 19.11.2022).

3. Про затвердження Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС: Наказ МВС України від 20.10.2017 № 870: [із змінами, внесеними згідно з Наказами Міністерства внутрішніх справ № 504 від 02.07.2020, № 441 від 19.07.2022] // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/z1433-17#Text (дата звернення: 19.11.2022).

УДК 65.012.8 + 004

МАНЖАЙ ОЛЕКСАНДР ВОЛОДИМИРОВИЧ

кандидат юридичних наук, доцент,

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

http://orcid.org/0000-0001-5435-5921

МАНЖАЙ ІРИНА АНДРІЇВНА

завідувач навчального відділу Харківського університету

ОКРЕМІ АСПЕКТИ АВТОМАТИЗАЦІЇ АНАЛІЗУ САЙТІВ З ПРОТИПРАВНИМ КОНТЕНТОМ

Під час виконання оперативно-службових завдань різним підрозділам поліції доводиться здійснювати моніторинг мережних ресурсів на предмет наявності протиправного контенту. Нерідко за результатами такого моніторингу накопичується великий масив даних, який потрібно дослідити та обрати серед знайдених ресурсів найбільш перспективні з точки зору подальшого документування. Правильний підхід до вивчення переліку знайдених ресурсів з протиправним контентом передбачає застосування різноманітних статистичних та аналітичних методів. У результаті матимемо орієнтуючу інформацію не тільки по пріоритетних сайтах, але й первинні дані про можливих володільців і адміністраторів таких ресурсів.

Один із методів, який дозволяє «грубо» виокремити ресурси зі спільним корінням є аналіз так званих фавіконів (favicons /favorite icons/) – значків веб-сайтів чи веб-сторінок. У випадку збігу унікальних використовуваних зображень можна припустити пов’язаність розробників та/або адміністраторів відповідних ресурсів.

Візуально представити набір використовуваних фавіконів можна у вигляді таблиці із завантаженням відповідного адресі (окремій сторінці) сайту фавікона у комірку Google- чи MS Excel-таблиці. Описану операцію можна виконати за допомогою формули та використання в ній функції IMAGE.

=IMAGE(TEXTJOIN("",ИСТИНА,"http://www.google.com/s2/favicons?domain="
,A1),3)

або

=IMAGE(TEXTJOIN("",ИСТИНА,A1,"/favicon.ico"),3),

де A1 – комірка з адресою досліджуваного Інтернет-ресурсу.

Функція IMAGE вже тривалий час доступна у Google-таблицях, а також стала доступною в пакеті Microsoft 365 з другої половини 2022 року.

Сама автоматизація порівняння фавіконов може бути виконана за допомогою спеціалізованих застосунків, як от FavFreak (https://github.com/devanshbatham/FavFreak). Ця утиліта розраховує унікальний ґеш для фавікону кожного сайту з переліку та порівнює їх. Перелік доменних імен для вивчення формується у вигляді окремого текстового файлу. У підсумку матимемо звіт із відповідними збігами та текстовими файлами, що міститимуть інформацію про ресурси з однаковими фавіконами (рис. 1).

```
~ [40]  : [1198047028]
~ [1]   : [702403635]
~ [1]   : [-1965981700]
~ [1]   : [-1131104052]
~ [1]   : [214280171]
~ [1]   : [-1819991364]
~ [1]   : [561456715]
~ [12]  : [-1170068949]
```

Рис. 1. Кількість ресурсів з однаковим фавіконом та його ґеш

Під час аналізу фавіконів слід враховувати, що їх може бути декілька в межах одного сайту, як от окремі значки для окремих вебсторінок. Тому під час порівняння бажано використовувати декілька способів завантаження відповідних значків. Після виокремлення потенційно пов’язаних мережних ресурсів результати можна представити у вигляді графу за допомогою відповідного програмного забезпечення, наприклад Gephi.

Описаний спосіб автоматизації дозволяє значно скоротити час на первинну обробку інформації та створити умови для подальшого більш ретельного вивчення накопичених даних.

УДК 621.37:621.39

МОЖАЄВ ОЛЕКСАНДР ОЛЕКСАНДРОВИЧ

доктор технічних наук, професор,

професор кафедри кібербезпеки та DATA-технологій факультету № 6

Харківського національного університету внутрішніх справ

МОЖАЄВ МИХАЙЛО ОЛЕКСАНДРОВИЧ

доктор технічних наук,

доцент кафедри кібербезпеки та DATA-технологій факультету № 6

ПЕРЕСІЧАНСЬКИЙ ВАЛЕРІЙ МИКОЛАЙОВИЧ

старший викладач кафедри кібербезпеки та DATA-технологій

факультету № 6

Харківського національного університету внутрішніх справ

РОГ ВІКТОРІЯ ЄВГЕНІЇВНА

старший викладач кафедри протидії кіберзлочинності факультету № 4

Харківського національного університету внутрішніх справ

РОЗПІЗНАВАННЯ РАДІОСИГНАЛІВ ЗА НЕЛІНІЙНИМ ВІДГУКОМ АКУСТООПТИЧНОГО СПЕКТРОАНАЛІЗАТОРА ДЛЯ ПОКРАЩЕННЯ ЗАХИЩЕНОСТІ МЕРЕЖ КРИТИЧНОГО ЗАСТОСУВАННЯ

Сучасний рівень розвитку систем моніторингу надзвичайних ситуацій, екологічної обстановки в Україні, а також досить складне економічне та енергетичне положення в країні, що визвано війною, вимагають створення і подальшого розвитку системи моніторингу України. Ця система повинна включати в себе підсистему збору первинної інформації в Україні (відповідні стаціонарні і мобільні пости, вузли і центри), підсистему передачі інформації як в рамках підсистеми збору інформації, а також оперативно-аналітичний центр, в який надходить найбільш важлива первинна інформація з локальних і регіональних центрів збору і обробки інформації [1,2].

Для підвищення ефективності використання мереж зв’язку необхідно проводити дослідження у двох напрямках – підвищення показників якості

самої мережі (пропускної здатності, значення затримки та ін.), а також зменшення кількості надлишкових даних, що передаються мережею, тобто використання якнайбільшого стиснення даних. Але, підвищення показників якості самої мережі (пропускної здатності, значення затримки та ін.), вимагає значних грошових витрат та модернізації усієї мережевої інфраструктури. Саме тому доцільно зменшувати кількість надлишкових даних, що передаються мережею.

Одною з основних проблем у сучасному стану системи передачі інформації є зменшення завадового впливу на якість функціонування системи. Для вирішення цієї проблеми використовуються багато різноманітних методів та засобів. Однім із шляхів вирішення є суттєве покращення частотних характеристик сигналів, що розповсюджуються в мережі. Для вирішення цього питання у системах передачі даних поширено використання акустооптичних аналізаторів спектру.

Акустооптичні спектроаналізатори, які реалізовують можливість проведення паралельної обробки сигналів в широкій смузі частот і практично в реальному масштабі часу, а також які виконують роль вимірювачів частоти, широко використовуються в сучасних радіотехнічних системах. Такий спектроаналізатор є аналогом багатоканального приймача, в якому частотне розділення каналів ґрунтується на принципах акустооптичної взаємодії.

Відомо, що характеристики виявлення радіоканалу визначаються енергією сигналу. Це твердження ґрунтується на тому, що складові частини акустооптичного спектроаналізатора, такі як лінзи, дзеркала, оптичні фільтри, модулятори, шар простору, діафрагми та ін. є лінійними, інваріантними відносно зрушень в координатній і частотній областях відповідно і характеризуються коефіцієнтом передачі, або коефіцієнтом пропускання.

Практичне використання акустооптичних аналізаторів спектру в радіотехнічних системах підтверджує це положення при виявленні сигналів малої енергії.

При цьому відгук на виході аналізатора відповідає сигналу на вході та однозначно характеризує частоту вхідного сигналу (тобто кожній частоті вхідного сигналу відповідає один осередок фотоприймача на приладах із зарядовим зв'язком).

У разі перевищення енергією радіосигналу певного порогу на виході спектроаналізатора формується складний сигнал, по якому важко визначити частоту вхідного радіосигналу. Це, можливо, обумовлено нелінійним характером залежності передатної функції радіоканалу і оптичних елементів від потужності радіосигналу, що приймається [3,4].

У існуючих спектроаналізаторах не реалізовані методи обробки сигналів, що дозволяють врахувати нелінійний характер акустооптичного перетворення [5-7].

Таким чином, облік впливу нелінійного характеру перетворень в акустооптичних аналізаторах спектру є актуальним науковим завданням.

Метою даної доповіді є облік особливостей розпізнавання вхідних радіосигналів за нелінійним відгуком акустооптичного спектроаналізатора.

Результати теоретичних досліджень

Можливі наступні підходи до рішення цієї задачі. Перший з них припускає строгий математичний опис проходження сигналу великої потужності через усі елементи радіотехнічної системи. Цей підхід дозволяє створити оптимальні алгоритми однозначного визначення частоти радіосигналу великої потужності по складному відгуку акустооптичного аналізатора спектру. Але цей підхід дуже громіздкий і трудомісткий в реалізації, тому він далі не розглядається.

В якості альтернативи аналітичному підходу можна запропонувати підхід, який ґрунтується на методах розпізнавання сигналів з використанням навчальної вибірки [1 – 4]. Сутність цього підходу полягає в наступному.

Вважатимемо, що на вхід системи поступають монохроматичні сигнали. За допомогою радіоканалу вимірюються тривалість імпульсу, період повторення імпульсів і інші параметри, окрім частоти. Вважаємо, що на вхід

акустооптичного спектроаналізатора поступає сигнал постійної частоти, проте у разі великої енергії сигналу на виході може бути сукупність імпульсів різних частот (рис. 1).

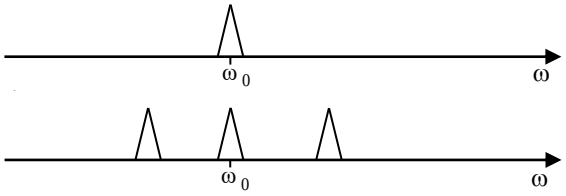


Рис. 1. Сигнал на вході (а) та на виході (б) спектроаналізатора

При зміні енергії змінюється кількість імпульсів і їх розташування на осі частот. Таким чином, для розпізнавання пред'являється сукупність імпульсів, яку можна записати у вигляді вектору $\mathbf{x} = (x_1, \ldots, x_n)^T$, де x_i – частота i-го імпульсу. Будемо вважати, що в залежності від розміру вхідного сигналу n може змінюватися від 1 до N, де N – кількість дозволених дискрет за частотою. Оскільки про розподіл вектору x інформації нема, доцільно отримати цю інформацію на етапі навчання, метою якого є побудова еталонних описів вихідних сукупностей сигналів (векторів x) залежно від двох параметрів вхідних сигналів – інтенсивності (I) та частоти (ω), які представимо вектором $\mathbf{B} = (I, \omega)^T$. Будемо також вважати, що кількість дозволених дискрет за інтенсивністю одно M.

Достовірність прийнятих рішень (ймовірності правильних рішень) про приналежність контрольної вибірки до класів 1 та 2 визначається відповідними ймовірностями $P_1 = 1 - \alpha$ та $P_2 = 1 - \beta$. У разі обраного нами критерію максимальної правдоподібності $\alpha = \beta$ та $P_1 = P_2 = P = F\left(\sqrt{d}/2\right)$. Залежності P та α від d наведені на рис. 2.

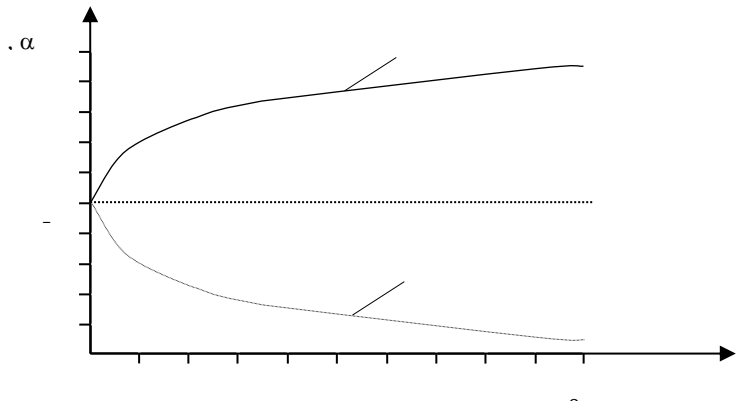


Рис. 2. Залежності P та α від d

З аналізу графіка випливає, що ймовірність правильного розпізнавання зростає із збільшенням величини, яку d можна трактувати як зважене помилками вимірювання відстань між класами

Зазначимо, що поведінка ймовірності α є дзеркальним відображенням поведінки P.

Таким чином, для побудови алгоритму розпізнавання необхідно за навчальними вибірками визначити характеристики. Далі знаходяться два класи, що мають найменшу середньозважену відстань між собою. По цій відстані знаходяться оцінки ймовірнісних характеристик алгоритму. Якщо вони не задовольняють заданим, то можна спробувати їх поліпшити шляхом накопичення та статистичної обробки прийнятих реалізацій сигналів (пачок сигналів).

Висновки.

В результаті проведених досліджень проведено аналіз особливостей розпізнавання вхідних радіосигналів за нелінійним відгуком акустооптичного спектроаналізатора.

В результаті аналізу встановлено, що нелінійні властивості акустооптичного аналізатору спектру дозволяє покращити правильне розпізнавання вхідних радіосигналів, які розповсюджуються у мережах передачі даних систем критичного застосування.

Це забезпечило правильне розпізнавання вхідних радіосигналів у випадку нелінійного відгуку акустооптичного спектроаналізатора.

Побудовано алгоритм розпізнавання вхідного радіосигналу, який базується на аналізу ймовірнісних характеристиках що залежать від енергетичних параметрів сигналу. Проведено оцінку параметрів розпізнавання вхідного радіосигналу та достовірності прийнятих рішень.

У подальших дослідженнях бажано провести оцінку зовнішнього впливу на достовірність прийнятого рішення про розпізнання радіосигналу.

Список використаних джерел:

1. M. Mozhaiev, N. Kuchuk, M. Usatenko. The method of jitter determining in the telecommunication network of a computer system on a special software platform. Innovate technologies and scientific solutions for industries. Kharkiv, 2019 - P. 134-140, DOI: doi.org/10.30837/2522-9818.2019.10.134.

2. Tanenbaum E., Van-Steen M. Distributed Systems. The principles and paradigms. SPb.: Peter, 2003. 877 p.

3. Rudnytsky, V., Mozhaiev, M. и Kuchuk, N. (2020) порушень мінхронізаціїМетод диагностики нарушений синхронизации телекоммуникационной сети компьютерной системы критического применения, (Method for the diagnostics of synchronization disturbances in the telecommunications network of a critical used computer system) *Современное состояние научных исследований и технологий в промышленности*, 2020 №1 (11), сс. 172-180. doi: 10.30837/2522-9818.2020.11.172.

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

5. Можаев М.А. , Буслов П.В. Метод повышение показателей качества распределенной информационной системы судебной экспертизы. Innovative Technologies and Scientific Solutions for Industries, No.4(14), P.57–65. DOI:https://doi.org/10.30837/2522-9818.2020.12.057. Современное состояние научных исследований и технологий в промышленности, 2020 №2 (14),

6. Kuchuk, G., Ruban, I., Davikoza, O. (2013), "Conceptual approach to synthesis of information and telecommunication network structure" ["Kontseptual′nyy pidkhid do syntezu struktury informatsiyno-telekomunikatsiynoyi merezhi"], *Systems of information processing: collection of scientific works*, No. 7 (114), P. 106–112.

7. Можаев М. О., Гомон В.О. Контроль якості функціонування телекомунікаційної мережі інформаційного порталу національної поліції/ Протидія кіберзагрозам та торгівлі людьми (27 травня. 2020 р., м. Харків) МВС України, Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2020. С. 75-76.

УДК 004.9 +343.1

НОСОВ ВІТАЛІЙ ВІКТОРОВИЧ

кандидат технічних наук, доцент,

професор кафедри протидії кіберзлочинності факультету № 4

Харківського національного університету внутрішніх справ

БАННІКОВА МАРІЯ АНДРІЇВНА

курсантка 4 курсу факультету № 4

Харківського національного університету внутрішніх справ

ДЕКЛАРАТИВНА ОЦІНКА ЕФЕКТИВНОСТІ ЗАСОБІВ БЛОКУВАННЯ ТРЕКЕРІВ ЗБОРУ ІНФОРМАЦІЇ З КОМП'ЮТЕРНОЇ СИСТЕМИ ПРИ КОРИСТУВАННІ ВЕБРЕСУРСАМИ

У процесі з'єднання веббраузеру з більшістю вебсайтів останні, як правило з маркетинговою метою, намагаються через спеціальні запити та запис в систему користувача так званих трекерів отримати унікальну інформацію про комп'ютерну систему (fingerprint). Отримані таким чином 99% «відбитків» є унікальними і належать до одної комп'ютерної системи [1].

У якості «відбитків» вебсайт здатен отримати при взаємодії із браузером інформацію про [2]:

- версію браузера та операційної системи;
- встановлену роздільну здатність монітору;

- деякі налаштування операційної системи;
- встановлені додатки або розширення браузеру (навіть якщо вони вимкнені);
- деякі параметри апаратного забезпечення системи;
- і інше.

Для забезпечення анонімності і приватності користувача комп'ютерної системи для браузерів Mozilla Firefox та Google Chrome розроблені аддони і розширення, які намагаються блокувати трекери і спеціальні запити від вебсайту, тим самим знижуючи унікальність системи користувача для вебсайту.

Аналіз репозиторіїв Mozilla Firefox та Google Chrome [3,4] дозволив виявити близько 100 аддонів і розширень блокування трекерів, які можна поділити на вузько- і багатофункціональні. Багатофункціональні також намагаються блокувати рекламний контент.

Для проведення декларативної оцінки ефективності засобів блокування трекерів і спеціальних запитів для браузерів Mozilla Firefox та Google Chrome було відібрано по 4 багатофункціональних аддони і розширення, які мали:

- найвищій рейтинг оцінки користувачів;
- декларативний звіт кількості заблокованих трекерів.

У якості вебсайту, який намагається отримати «відбитки» системи як для маркетингових, так і для безпекових цілей, було обраний ресурс olx.ua.

Відібрані аддони і розширення встановлювалися окремо один від одного у відповідні браузери, після чого здійснювалась спроба користування вебсайтом olx.ua і фіксувався звіт щодо кількості/видів заблокованих трекерів. Результати оцінки наведені у Табл. 1, 2.

Таблиця 1 – Декларативна оцінка ефективності розширень Google Google

Назва	Загальна кількість заблокованих трекерів	Кількість/Види заблокованих трекерів	Наявність платних функцій
Privacy Bagger	11	4 - аналітики	Ні

Trace	7	6 – HTML заголовків 1 – запит медіа контенту	Частково
UltraBlock	18	6 - рекламні 4 –аналітики 8 – невизначені	Ні
Disconnect	8	1 – рекламні 1 –аналітики 6 – невизначені	Частково

Таблиця 2 – Декларативна оцінка ефективності аддонів Mozilla Firefox

Назва	Загальна кількість заблокованих трекерів	Кількість/Види заблокованих трекерів	Наявність платних функцій
NoScript	6	5 –аналітики 1 – кліків мишкою	Ні
Ghostery	14	4 – невідомі 3 – аналітики 6 – рекламні 1 – HTML заголовків	Частково
AdBlocker Ultimate	10	----	Ні
ClearURLs	13	----	Частково

Декларативно більшу кількість заблокованих трекерів показали UltraBlock для Google Google і Ghostery для Mozilla Firefox, але для незалежного підтвердження їх ефективності потрібно провести дослідження відносно спеціально створеного вебсайту, на якому і фіксувати кількість отриманих/неотриманих відбитків комп’ютерної системи користувача із встановленими аддонами і розширеннями браузеру.

Список використаних джерел:

1. Antoine Vastel; Pierre Laperdrix; Walter Rudametkin; Romain Rouvoy. FP-STALKER: Tracking Browser Fingerprint Evolutions // DOI: 10.1109/SP.2018.00008 (дата звернення 09.11.2022).

2. The Beginner’s Guide to Browser Fingerprinting for Fraud Detection // URL: https://fingerprint.com/blog/what-is-browser-fingerprinting/ (дата звернення 09.11.2022).

3. Інтернет-магазин Ghrome // URL: https://chrome.google.com/webstore/ (дата звернення 09.11.2022).

4. Firefox Browser ADD-ONS // URL: https://addons.mozilla.org/ua /firefox/ (дата звернення 09.11.2022).

УДК 343.1 + 004

НОСОВ ВІТАЛІЙ ВІКТОРОВИЧ

кандидат технічних наук, доцент,

професор кафедри протидії кіберзлочинності факультету № 4

Харківського національного університету внутрішніх справ

ІВАХНЕНКО ОЛЕКСІЙ СЕРГІЙОВИЧ

курсант 4 курсу факультету № 4

Харківського національного університету внутрішніх справ

ОЦІНКА ЕФЕКТИВНОСТІ ДЕЯКИХ ЗАСОБІВ МАСКУВАННЯ СИГНАТУРИ ШКІДЛИВОГО КОДУ

Одним із способів маскування шкідливих програм є створення зловмисниками так званих троянів (Trojan), які виглядають як звичайні користувацькі файли і навіть зберігають свою функціональність, але додатково містять зловмисний код, що починає приховано виконуватися при запуску/відкриті такого файлу. Зокрема трояни із кодом для отримання віддаленого доступу до системи користувача (Remote Access Trojan, RAT) [1] зазвичай мають вигляд і функціональність файлів електронних документів (docx, xlsx, pdf, тощо). Відкриття користувачем такого електронного документу

приховано запускає в системі жертви сервер віддаленого доступу, який повідомляє клієнтській частині RAT зловмисника про готовність виконувати віддалені команди.

Зловмисник з клієнтської частин RAT має можливість віддалено:

- слідкувати за діями користувача;
- запускати довільні файли;
- відключати та зупиняти сервіси операційної системи;
- робити та зберігати знімки екрану;
- включати веб-камеру;
- сканувати локальну мережу користувача;
- завантажувати свої та модифікувати існуючі файли;
- відкривати та закривати логічні порти системи.

Сучасні антивірусні системи здатні виявляти шкідливий код відомих RAT через пошук відповідних сигнатур у файлах, що перевіряються. Для ускладнення виявлення RAT антивірусом зловмисники додатково модифікують код за допомогою засобів маскування, які застосовують: криптографічні перетворення, стиснення і/або штучну зміну сигнатури коду RAT без втрати функціональності (обфускація або затемнення). Загальна назва таких програм - обфускатори.

В рамках дослідження для оцінки ефективності деяких відомих програмних засобів маскування коду спочатку за допомогою фреймворка Msfvenom в ОС Kali Linux у вигляді документу Microsoft Word був створений RAT файл, який потім окремо був модифікований різними обфускаторами. Далі RAT файл без модифікації і всі модифіковані його версії було завантажено на вебсайт сервісу VirusTotal (https://www.virustotal.com), де здійснювалась сканування файлу різними антивірусними програмами на наявність шкідливого коду. Для дослідження було взято такі обфускатори:

- Shellter (https://github.com/ParrotSec/shellter);
- FuckThatPacker (https://github.com/Unknow101/FuckThatPacker);
- Chimera (https://github.com/tokyoneon/Chimera);

- HanzoInjection (https://github.com/P0cL4bs/hanzoInjection);
- Invoke-Obfuscation (https://github.com/danielbohannon/Invoke-Obfuscation).

У вихідному RAT файлі 51 антивірус сервісу VirusTotal з 71 виявив шкідливий код, результати сканування модифікованих різними обфускаторами файлу RAT наведений у Табл. 1.

Таблиця 1 – Результати виявлення антивірусами сервісу VirusTotal шкідливого обфускованого коду

Обфускатор коду	**Кількість антивірусів, що сканували обфускований код**	**Кількість антивірусів, що виявили шкідливий обфускований код**
Shellter	67	22 (33%)
FuckThatPacker	69	11 (16%)
Chimera	61	4 (7%)
HanzoInjection	60	0
Invoke-Obfuscation	71	9 (13%)

Загалом, усі обфускатори показали деяку ефективність у маскуванні сигнатури коду, але модифікований HanzoInjection шкідливий код не був виявлений жодним антивірусом сервісу VirusTotal, що підтверджує необхідність використання комплексних систем захисту, які враховують не тільки відомі сигнатури коду, а і інші чинники.

Список використаних джерел:

5. What is Remote Access Trojan (RAT)? URL: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-remote-access-trojan/ (дата звернення 21.11.2022).

УДК 004.9

НОСОВ ВІТАЛІЙ ВІКТОРОВИЧ

кандидат технічних наук, доцент,

професор кафедри протидії кіберзлочинності факультету № 4
Харківського національного університету внутрішніх справ
УСЕНКО АРІНА ОЛЕГІВНА
курсантка 3 курсу факультету № 4
Харківського національного університету внутрішніх справ

ОЦІНКА ХАРАКТЕРИСТИК СЕРВІСІВ ДЕЯКИХ РОЗШИРЕНЬ БРАУЗЕРУ GOOGLE CHROME З ПРИХОВУВАННЯ IP АДРЕСИ СИСТЕМИ

Одним із основних ідентифікаторів клієнта при з'єднанні з вебресурсом є IP адреса системи, за якою збирається інформація про можливого користувача або здійснюється обмеження доступу до вебресурсів. На сьогодні найбільш вживаним браузером для доступу до вебресурсів з часткою світового ринку 65,52% є Google Chrome [1], в якому можна встановити певний тип розширення (extension), що декларує приховування IP адреси системи при з'єднанні з вебресурсом.

Розробники таких розширень позначають їх як VPN або Proxy, але, строго кажучи, всі вони є тільки Proxy, оскільки спрямовують трафік до проміжного вузла мережі за прикладним (http/https) або сеансовим (SOCKS4/SOCKS5) протоколами. Для підключення до серверу VPN (віртуальної приватної мережі) потрібна або окрема клієнтська програма або вже наявні в операційній системі відповідні сервіси, які спрямовують увесь трафік системи до серверу VPN за протоколами мережевого/канального рівня (OpenVPN, L2TP/IPSec, і ін.).

Розширення Google Chrome доступні для встановлення у виділеному репозиторії chrome web store[3], де зазначений їх опис і характеристики. На сьогодні загальна кількість розширень у chrome web store близько 188620 [2], і серед них було виявлено 210 розширень Proxy, аналіз споживчих характеристик яких дозволив виділити чотири з найбільшою кількістю користувачів (табл. 1).

Таблиця 1 – Рейтинг розширень Proxy

[3] https://chrome.google.com/webstore/category/extensions

Назва	Кількість користувачів	Середня оцінка (макс. 5 балів)	Кількість оцінок
Touch VPN[4]	7000000+	4,6	77978
Hola VPN[5]	4000000+	4,9	355997
1clickVPN [6]	4000000+	4,8	32447
VeePN[7]	3000000+	4,7	7438

За середньою оцінкою користувачів і кількістю оцінок першим у рейтингу є розширення Hola VPN, а за кількістю користувачів - Touch VPN.

Також можна оцінити функціональність і доступність (безплатне використання) сервісів зазначених розширень (табл. 2).

Таблиця 2 – Функціональність і доступність сервісів розширень Proxy

Характеристика	Розширення			
	Touch VPN	Hola VPN	1clickVPN	VeePN
Платні функції	так	так	так	так
Додаткова анонімізація, блокування реклами	так	так	ні	так
Шифрування трафіку	так	ні	так	так
Блокування витоку IP адреси через WebRTC[8]	так	так (платно)	ні	так
Кількість безкоштовних/платних локацій проксі сервера	6/	200+/	1/9	6/89+

Найбільш доступними і функціональним є сервіси розширення Touch VPN і VeePN. Сервіс розширення Hola VPN має найбільшу кількість вибору безплатних локацій проксі, а 1clickVPN має найменшу кількість функцій.

[4] https://chrome.google.com/webstore/detail/touch-vpn-secure-and-unli/bihmplhobchoageeokmgbdihknkjbknd
[5] https://chrome.google.com/webstore/detail/hola-vpn-the-website-unbl/gkojfkhlekighikafcpjkiklfbnlmeio
[6] https://chrome.google.com/webstore/detail/1clickvpn-free-vpn-for-ch/fcfhplploccackoneaefokcmbjfbkenj
[7] https://chrome.google.com/webstore/detail/free-vpn-for-chrome-vpn-p/majdfhpaihoncoakbjgbdhglocklcgno
[8] https://proxy6.net/en/privacy

Варто зазначити, що кожний провайдер проксі сервісу декларує власну політику приватності щодо збору, зберігання і поширення унікальних даних користувачів.

Список використаних джерел:

1. MOST POPULAR WEB BROWSERS IN 2022. URL:https://www.oberlo.com/statistics/browser-market-share (дата звернення 26.11.2022).

2. Google Chrome Statistics. URL: https://truelist.co/blog/google-chrome-statistics/ (дата звернення 26.11.2022).

УДК 004.336

ОРЛОВ РОМАН РУСЛАНОВИЧ

магістр факультету № 5 за спеціальністю «Кібербезпека» Харківського національного університету внутрішніх справ, лейтенант поліції,

старший інспектор управління протидії кіберзлочинам в м. Києві Департаменту кіберполіції НПУ

ОКУШКО АНДРІЙ ВАСИЛЬОВИЧ

кандидат юридичних наук, полковник поліції,

заступник начальника Управління протидії кіберзлочинам в м. Києві Депараменту кіберполіції НП України

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН У ДІЯЛЬНОСТІ ПРАВООХОРОНИХ ОРГАНІВ ТА ПРОТИДІЇ КІБЕРЗЛОЧИНАМ

Безсумнівно, блокчейн — революційне явище, по значущості, яке можна порівняти з геніальним винаходом XX століття — Інтернетом. Це призвело до того, що технологія блокчейн створила платформу нового виду «Інтернету» та сприяла появі децентралізованих сервісів. На відміну від централізованого підходу, нові послуги базуються на децентралізованій розподіленій мережі, яка може використовуватися для різних цілей, включаючи кібербезпеку. На сьогоднішній день блокчейн найбільше затребуваний у фінансовому секторі (створення цифрових валют, здійснення транзакцій, обмін та зберігання

фінансової інформації). Він отримав прикладне використання і в інших сферах, таких як смарт-контракти, реєстрація публічних записів (реєстрація права власності на нерухоме майно, ліцензування, створення та ліквідація організацій тощо). Водночас блокчейн має свої слабкі місця. Зокрема, при зосередженні більш ніж 51 % вузлових точок (обчислювальних потужностей) в рамках одного замкнутого ланцюжка (пула) він набуває абсолютного контролю над процесом реєстрації угод у блокчейні, зводячи нанівець основну властивість блокчейну - децентралізацію реєстрів даних. Крім надання очевидних переваг та нової якості життя, тотальна цифровізація спричинила не лише масштабну залежність суспільства від інформаційних технологій, а й виникнення кіберзлочинності, а також найбільш руйнівних її форм — кібертероризму та кіберекстремізму. Інтернет реалізувався у створенні кіберпростору, в якому терористи та екстремісти можуть швидко та анонімно здійснювати широкий обмін інформацією, безперешкодно здійснювати комунікації та завдавати атаки на об'єкти, що становлять для них цінність. Сьогодні в мережі активно працюють такі терористичні групи, як ХАМАС, Хезболла, єгипетська Аль-Гамаа, а також сотні інших. Войовничі радикальні організації розглядають Інтернет, як ідеальну арену для незаконної діяльності через вкрай недостатнє законодавче регулювання відносин у кібермережі, безперешкодне поширення потоку безкоштовної інформації, легкий доступ в онлайн-простір практично з будь-якої точки світу. Відмінною особливістю кібертерористичних актів є те, що вони, як правило, націлені на критично важливі системи інфраструктури, які можуть зруйнувати великі міста, зірвати політичні вибори до органів влади, обвалити фінансову систему країни, викликати кризу громадської охорони здоров'я, викликати перебої з поставками продовольства, поставити під загрозу суспільну та державну безпеку, а також викликати масову паніку та загибель людей. Очевидно, що для запобігання терористичним загрозам і радикалізації в кіберпросторі правоохоронні органи повинні мати можливість бути в технологічному відношенні на крок попереду кіберкриміналу. Сприйнятливість і професіоналізм сучасних кібертерористів, а також їх фантастично зрослі

технологічні можливості вимагають від правоохоронних органів усього світу розробки адекватних механізмів протидії кібертероризму, стратегія боротьби з яким має бути спрямована на запобігання та мінімізацію загроз та ризиків, що породжуються глобальною цифровізацією. Кінцева мета такого підходу має полягати у виключенні будь-яких можливостей для дій терористів як у реальному світі, так і в кіберпросторі. Блокчейн відкриває нові ефективніші способи протистояння кібератакам у різний спосіб, одним з яких є надійний захист даних від злому, крадіжки або знищення цінної інформації. Якщо при зламі традиційної централізованої системи хакер за один вхід може отримати доступ до тисячі об'єктів, то при зламі децентралізованої блокчейн-системи кіберзлочинці можуть отримати доступ тільки до одного фрагменту, що робить їх дії більш трудомісткими, оскільки доведеться багаторазово зламувати базу, щоб отримати повну інформацію. У свою чергу, у правоохоронних органів з'являється додатковий час для виявлення джерела небезпеки та усунення загроз.

Крім захисту самих даних, блокчейн здатний захистити від кібератак та процес обміну інформацією. Наприклад, такі інструменти обміну миттєвими повідомленнями, як Facebook Messenger або WhatsApp, хоч і оснащені системами безпеки, але мають свої слабкі місця. Застосування технологій блокчейн та продуктів на її основі у протидії кібертероризму проводиться, як правило, комплексно з іншими технологіями. Так, блокчейн у поєднанні із штучним інтелектом використовується для фільтрації та ідентифікації важливої інформації, для пошуку у величезних масивах даних чим користуються технічні фахівці у правоохоронних органах.

Область застосування технології блокчейн у кібербезпеці безмежна завдяки таким його унікальним властивостям, як надійність, загальнодоступність, висока адаптивність, економічна ефективність та рентабельність. Використання блокчейну для боротьби з кіберзлочинністю може бути поширене на фінансові послуги, законодавство, транспортну галузь або будь-яку іншу галузь, яка потребує перевірки третьою стороною.

УДК 004.77

SAZANOVA LARYSA SERHIIVNA

senior lecturer of the department of foreign language of faculty No.4

Kharkiv National University of Internal Affairs

MODERN INFORMATION TECHNOLOGIES IN THE UNITED STATES POLICE

Police across the world are increasingly relying on emerging technologies to make their jobs more efficient. In their daily work, they are using drones, license plate readers, body cameras and gunshot detection systems to reduce injury and bodily harm. “From drones and body-worn cameras to facial recognition software and artificial intelligence, here’s a list of 12 of the most important technologies that are equipping law enforcement agencies with new capabilities to protect and serve” [1].

Police departments determine which technologies to adopt. Technologies can be a great tool for law enforcement agencies as they infiltrate every aspect of the lives. It is no wonder that solving crimes has become almost futuristic in its advances. Actual forensic technologies are advanced at helping to solve crimes. This field is one of the fastest growing in the United States. It is seen in the increased demand for forensic science technicians.

According to the Bureau of Labor Statistics (2021), there will be a 16 percent increase in jobs for forensic science technicians between 2020 and 2030. This growth is due to new forensic science techniques that have increased the availability and reliability of objective forensic information. Below there are some of forensic technologies.

DNA Phenotyping. Forensic scientists can sequence a DNA sample and provide investigators with identifying traits of the suspect (color of hair, eyes, complexion). Newer techniques can also predict age and biological background.

Biosensors for Fingerprint Analysis. Forensic scientists can use biosensors to analyze the minute traces of bodily fluids found in fingerprints to identify the suspect. Data that can be detected include age, medications, gender, and lifestyle. Biosensors can also be used on other bodily fluids found at a crime scene.

Immunochromatography. It is a method to test for diseases by dropping a small sample onto a prepared test strip. Results are relatively quick, and common tests that use this technique include COVID, HIV, and even pregnancy tests. In forensics, immunochromatography tests are used to detect substances in subjects' bodily fluids, such as drugs and medications. A smartphone-based sensor has even been developed to evaluate a saliva sample through immunochromatography without needing to be in a lab.

Geolocating a Suspect or Victim using Stable Isotopes of Water. Isotopes vary from atom to atom and can have a unique signature. Recent forensic developments have found that scientists can determine where the sample could have originated by isolating the isotopes in a water sample found on a suspect or victim. Isotope detection through other methods can also be used to determine the number of people present.

Forensic Palynology is a relatively new area for forensic scientists. Palynology is the study of pollen, spores, grains, and seeds and can be used in forensics to identify a subject's location. Pollen and spores are minute and can be deposited on skin and clothes largely undetected. Scientists have not developed techniques to gather and compare these trace materials and use them as evidence.

Blockchain-Based Solutions: Cloud Forensics. Over 50 percent of personal and corporate data is now stored in the cloud, meaning on remote servers. Digital forensic scientists have had to develop methods for collecting, analyzing, and evaluating data that has been collected from the cloud. Digital forensic scientists have begun to use blockchain technology as it is virtually impossible to tamper with.

Digital Vehicle Forensic. Investigators gather physical evidence (fingerprints, fluid samples, and trace materials like dirt). They can physically examine the car to determine how an accident, crash, or terrorist attack occurred. Scientists and investigators can gather data such as recent destinations, typical routes, personal data, and favorite locations.

Social Network Forensics. Over 3.6 billion people are on social networks, and this number is projected to increase to 4.5 by 2025. When social media first emerged, investigators and forensic scientists didn't have as much data to comb through.

Scientists have developed models for analyzing the information gleaned from social networks [2].

3D Technology to Determine Physical Fit. Forensic scientists often receive physical evidence that needs to be pieced back together. This is called physical fit and is a well-recognized method of determining that two pieces are from the same source. This evidence can be a variety of materials, and often they can be relatively fragile such as bones. A recent study at the University of Portsmouth used 3D imaging to map the exact dimensions of some burnt bones then replicated the pieces using a 3D printer. This enabled them to determine if pieces fit together or not without having to excessively handle the fragile evidence.

Drone Forensics. In August 2021, there were over 880,000 drones registered with the Federal Aviation Administration in the United States. Over 40 percent of those drones are registered for commercial use. The increased popularity of these unmanned aerial vehicles has given criminals a new tool to smuggle drugs, perform illegal surveillance, and attack victims. Forensic scientists are developing methods and models for gathering and analyzing data from drones, SD cards, and cell phones.

References

1. Erik Fritsvold 12 Innovative police technologies

URL: https://onlinedegrees.sandiegto.edu/10-innovative-police-technolo9gies/

2. 10 Modern Forensic Technologies Used Today

URL: https: www.forensicscolleges.com/blog/resources/10-modern-forensic-science-technologies

УДК 004.056.5

СТРУКОВ ВОЛОДИМИР МИХАЙЛОВИЧ

кандидат технічних наук, доцент,

професор кафедри кібербезпеки та DATA-технологій

факультету №6 Харківського національного університету внутрішніх справ

ORCID ID: http://orcid.org/0000-0003-4722-3159;

УЗЛОВ ДМИТРО ЮРІЙОВИЧ

кандидат технічних наук,
доцент кафедри штучного інтелекту Харківського національного університету радіоелектроніки;
ORCID: https://orcid.org/0000-0003-3308-424X

ГНУСОВ ЮРІЙ ВАЛЕРІЙОВИЧ

кандидат технічних наук, доцент,
завідувач кафедри кібербезпеки та DATA-технологій факультету №6 Харківського національного університету внутрішніх справ;
ORCID ID: http://orcid.org/0000-0002-9017-9635

СТАН ТА ПЕРСПЕКТИВИ РЕАЛІЗАЦІЇ ПРЕДИКАТИВНОЇ МОДЕЛІ У ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Міжнародною правоохоронною спільнотою на початку двохтисячних років після обговорення на чисельних національних і міжнародних науково-практичних заходах була обґрунтована і прийнята стратегія переходу від реактивного принципу діяльності до предикативного [1-3]. Реалізація цієї стратегії передбачає певні організаційні і науково-технічні заходи. В Україні імпульс руху в цьому напрямку був наданий в середині 2010-х років, коли групою експертів Європолу був створений і наданий керівництву МВС України документ – дорожня карта (пропозиції) щодо впровадження предикативної моделі діяльності, а саме - Intelligence Led Policing (ILP), в Україні. Слід відзначити, що в цьому напрямку вже пройдений значний шлях, а саме: створена організаційна інфраструктура – відповідні аналітичні підрозділи (Департамент кримінального аналізу, Департамент стратегічних розслідувань), нормативна база, у вищих навчальних закладах системи МВС (НАВС, ДДУВС, ОДУВС, НАДПСУ) здійснюється підготовка фахівців для підрозділів кримінального аналізу та стратегічних розслідувань; під егідою Консультативної Місії Європейського Союзу проведені тренінги з підготовки кримінальних аналітиків та ін. Разом з цим необхідно усвідомлювати, що повноцінна реалізація предикативної моделі у сучасних умовах **неможлива** без застосування відповідних інструментальних засобів – сучасних аналітичних систем на кшталт

Palantir, ePOOLICE. У роботах [4-6] проведений аналіз таких інструментальних засобів, в якому надана їх класифікація та сфери застосування. Зокрема, мова йде про дві групи інструментальних аналітичних засобів – 1) засоби, які забезпечують розв'язання оперативних завдань (I2, Maltego та ін.) та 2) засоби, які забезпечують розв'язання стратегічних завдань та завдань саме попередження злочинів (Palantir, ePOOLICE, PredPol). І якщо з інструментальними засобами першої групи більш менш все гаразд, то інструментальні засоби другої групи в наявності на даний момент відсутні. Можливі наступні шляхи отримання такого класу засобів: 1) закупівля відповідних інструментальних систем, 2) розробка власної платформи і 3) приєднання до консорціуму країн Євросоюзу – власників платформи ePOOLICE.

Список використаних джерел:

1. Common Competencies for State, Local, and Tribal Intelligence Analysts. United States Department of Justice, Jun, 2010.

2. Law Enforcement Analytic Standards. 2nd edition. United States Department of Justice, April, 2012.

3. OSCE Guidebook Intelligence-Led Policing. OSCE,Vienna, June 2017. 108 p.

4. Струков В.М., Узлов Д.Ю., Гнусов Ю.В. Інструментальні інтелектуальні платформи для кримінального аналізу. Харків, Право і безпека вип. 4(83), 2021, с. 64-79.

5. 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.

6. Узлов Д.Ю., Струков В.М., Власов О.В. Методологічний апарат аналітичної роботи в Національній поліції України // 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.64-66.

ТЕЗИ ДОПОВІДЕЙ КУРСАНТІВ ТА СТУДЕНТІВ

UDC 343:004.056

ANISIMOV OLEKSII YURIYOVYCH

a first-year cadet of faculty No.4

Kharkiv National University of Internal Affairs

OLENDRA NATALIIA BOHDANIVNA

scientific adviser

lecturer of the department of foreign

languages of faculty No.4

Kharkiv National University of Internal Affairs

THE USE OF ILP ANALYTICS IN POLICING AND CRIME PREVENTION

Analytical work is the selection of generalizations, analysis of accumulated information, its preparation for processing, submission of proposals, and the provision of conclusions.

It should be determined that the use of analytics by the authorized units of the National Police in crime prevention will contribute to a significant improvement in the effectiveness of the work of police officers, the identification and documentation of various types of crimes; reducing the level of crime, and improving the state of the criminogenic situation; preventive and timely implementation of operational and preventive measures within the regions and the state; making effective procedural and management decisions; But one of the key improvements is optimizing the process of collecting, storing, retrieving and using information.

The activities of the authorized units of the National Police in combating crime, at the time of 2022, guided by Intelligence Led Policing (ILP), is a model that was created to support institutional management and decisions of authorized persons through information analysis. An example of such activities are actions that are aimed

at identifying and accurately establishing the relationship between criminal information, persons, and other information related to a particular crime. Thus authorized units of the National Police, in accordance with the tasks assigned to them, analyze the level of crime, the criminogenic situation, and the factors on which it depends. After all the analytical work carried out (including the provision of proposals) on the information, the authorized units transfer it to the leadership of the National Police.

They also analyze the effectiveness of the use and optimization of forces and means in counteracting criminal offenses, and determine the tactics of intelligence activities, which in turn is associated with the detection of criminal offenses. On this basis, the authorized units form proposals to the leadership of the National Police to solve certain problems, as well as to increase the efficiency of operational and service activities.

That is why the need to introduce ILP model in the authorization of the National Police units is relevant today.

Analytical work is carried out in the following areas:

operational analysis (analysis of telephone traffic, transactions, and personal data of a particular person or object);

tactical analysis (analysis of the criminogenic situation in a particular territory, for a relatively short period of time, and for a certain type of crime);

strategic analysis (identification of patterns in certain crimes, and forecasting development over a long time).

In accordance with this division of divisions into areas, it is also necessary to divide workers according to skills and analytical skills. That is, it is necessary to standardize the skills, abilities and algorithm of actions of analysts and analytical products.

The main components of the development of the ILP model, which need to be introduced in the activities of the National Police units, should be: – information resources specially prepared for use in this analysis; – the system of their filling; – system of evaluation of information and sources of its receipt; – special software as a

tool; – integration of software with the information system; – specially trained employees (analysts).

To do this, you need to systematically conduct various types of trainings to acquire the necessary skills and improve the already acquired ones. It is also quite expedient to introduce training and advanced training.

The implementation of ILP analytics in combating crime will help to solve a number of problematic issues (risks) related to: the need to amend the legislation of Ukraine on the introduction of new positions of analysts, their monetary support, requirements for hiring (profile of professional competence), creation of new information subsystems, use of databases of other departments, etc.; bureaucratic procedure for approval in the process of preparing by-laws (orders, regulations, instructions, etc.); lack of a permanent source of funds for the implementation of the project; unwillingness of the heads of individual departments to manage changes, perform additional work, their lack of awareness of the need for change, fear of losing personal significance; inability to choose new, active forms of cooperation between various bodies and units of the National Police, as well as with external actors, in particular foreign partners; slowing down the process of recruitment and training; potential competition in the field of resources (human, material); untimely implementation or slowing down of the implementation of one or more stages of the introduction of criminal analysis and risk analysis systems; – expectation of quick results, which will lead to poor-quality implementation of the concept, amateur approach and inefficiency of the criminal analysis system. These threats can be minimized by: applying correct and systematic principles in organizing further actions; skillful management of human resources; rational use of financial resources; the use of a motivational system in relation to performers; dissemination of knowledge on criminal analysis and risk analysis, as well as conducting training courses, trainings, etc.

The model of the activities of the criminal analysis units of the National Police in combating crime provides coordination of the activities of regional criminal analysis departments, regulation of access to departmental information resources and other

resources of public authorities, coordination of the work of structural units during the development of identical subjects of crime (persons, groups, etc.).

УДК 342:[351.746.1:316.658.48](477+(470+571))

БАННІКОВА МАРІЯ АНДРІЇВНА

курсантка 4 курсу факультету № 4

Харківського національного університету внутрішніх справ

ЛОГВИНЕНКО ЄВГЕНІЯ СЕРГІЇВНА

науковий керівник

кандидат юридичних наук, доцент,

доцент кафедри конституційного і міжнародного права факультету № 4

Харківського національного університету внутрішніх справ

РОСІЙСЬКА ПРОПАГАНДА ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ

Згідно закону України «Про національну безпеку України» національна безпека – це захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз [1]. Політика в сфері національної безпеки регламентує діяльність у різних аспектах життя країни. Насамперед одною із основних напрямків діяльності є інформаційна область.

Невід'ємним документом, який регулює відношення в інформаційній сфері є Доктрина інформаційної безпеки. Згідно її положень «застосування російською федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства» [2].

Для успішного виконання завдань російська федерація проводить на території України не звичайну війну, у всіх її загальноприйнятих поняттях, а гібридну війну, що відрізняється тактикою ведення військових дій не тільки на місцевості, а й використанням інформаційного фронту. Основними принципами такої війни є використання:

1. Пропаганди.

2. Терористичних дій.
3. Злочинів проти людяності.
4. Порушення прав і свобод людини.
5. Узурпації влади.
6. Злочинних актів цензури.

Основою забезпечення успіху у такій війні є пропаганда. Вона, як метод не є новим, але через бурхливий розвиток інформаційних та телекомунікаційних технологій набула широкого застосування.

Згідно визначення, пропаганда [3] – це поширення політичних, релігійних, філософських, наукових або інших поглядів шляхом донесення до народних мас різних аргументів, правдивих чи напівправдивих фактів, чуток або відвертої брехні з метою маніпуляції громадською свідомістю. За своєю суттю пропаганда є зрозумілою для кожної людини, бо вона використовує для маніпуляції прості та зрозумілі для людини речі.

Для розповсюдження такого методу маніпуляції думкою населення України використовуються [4]:

1) засоби аудіо та медіа: телебачення, радіо, кіно, фільми, новини, ток-шоу;
2) інтернет: веб-сайти, блоги, соц.медіа та соціальні мережі;
3) мистецтво та література: картини, плакати, комікси, журнали, газети;
4) виступи: мітинги, політичні події, концерти, заходи, виступи на площах.

Великий вплив на населення України пропаганда набула саме на території Луганської, Харківської та Донецької областей. Це обумовлюється певними історичними факторами. Пригнічення національної свідомості українського народу, репресії з боку Радянського Союзу та згубна політика СРСР були направлені для знищення українців як національності в цих регіонах. Апелюючи своєю спорідненістю, російська федерація проводить політику повної дезінформації. Саме історико-географічні та політичні причини впливають на таку масштабну роботу пропаганди на території Східної України.

Через певні історичні події, на території цих областей проживає переважна кількість людей російської національності [5]:

1) Луганська область – українці 57,96%, росіяни 39,05%;
2) Донецька область – українці 56%, росіяни 38%;
3) Харківська область – українці 70%, росіяни 25%.

Також одним із основних факторів, який мав великий вплив на розповсюдження пропаганди переважно в східних регіонах України – це мовний чинник. Велика кількість мешканців України саме в східних областях спілкуються (спілкувалися) у повсякденному житті російською мовою [6].

Через роботу механізму пропаганди російської федерації фактів виявлення колаборації стає все більше. Такі особи співпрацюють з окупаційною владою, виступають каналами інформування армії окупанта щодо позицій військових ЗСУ та шкодять національній безпеці власної держави. Згідно зі словами прокурора Харківщини Олександра Фільчакова: «Слідчими розслідується близько 800 кримінальних проваджень за такими категоріями як державна зрада, колабораційна діяльність та пособництво державі-агресору. Повідомлено про підозру 245 особам» [7].

Отже, пропаганда, як шкідливий фактор для національної безпеки Україні є досить дієвим методом. Через апелювання доволі простими речами вона може розповсюджуватися з миттєвою швидкістю. Завдання таких дій саме у затуманенні розуму населенню України для зміни їх точки зору на протилежну. Пропаганда російської федерації робить усе, щоб переманити населення нашої країни на свою сторону для проведення діяльності проти національної безпеки України.

Список використаних джерел:

1. Закон України «Про національну безпеку України» // URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення 18.11.2022)

2. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» // URL: https://www.president.gov.ua/documents/472017-21374 (дата звернення 18.11.2022)

3. Пропаганда – що це таке та хто такі пропагандисти // URL:https://termin.in.ua/propahanda/ (дата звернення 18.11.2022)

4. Identifying Types of Propaganda Lesson Plans by Kristy Littlehale // URL:https://www.storyboardthat.com/articles/e/propaganda (дата звернення 12.11.2022)

5. Росіяни в Україні // URL:http://surl.li/dtcey (дата звернення 18.11.2022)

6. Мови в Україні Wikipedia // URL: http://surl.li/drznz (дата звернення 11.11.2022)

7. Майже 800 кримінальних проваджень відкрили на Харківщині через ймовірну держзраду та колабораціонізм // URL: https://suspilne.media/299048-majze-800-kriminalnih-provadzen-vidkrili-na-harkivsini-cerez-jmovirnu-derzzradu-ta-kolaboracionizm/ (дата звернення 18.11.2022)

УДК 004.77

БОЛОБАН РУСЛАН ЮРІЙОВИЧ,

курсант 2 курсу факультету №4,

Харківського національного університету внутрішніх справ,

СВІТЛИЧНИЙ ВІТАЛІЙ АНАТОЛІЙОВИЧ

науковий керівник

кандидат технічних наук, доцент,

доцент кафедри протидії кіберзлочинності

Харківського національного університету внутрішніх справ,

ORCID http://orcid.org/0000–0003–3381–3350

ДЕЯКІ ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Необхідність впровадження цифрових технологій у сферу боротьби зі злочинністю зумовлена кількома очевидними факторами:

- Зростанням кількості правопорушень, при вчиненні яких використовуються сучасні технології (цифрові фінансові

інструменти, технологія блокчейн; вчинення масштабних злочинів за допомогою інформаційно-комунікаційних технологій тощо).

- Появою нових груп злочинців (хакерські угруповання, групи, що проповідують насильство в мережі тощо).
- Необхідністю удосконалення заходів кримінально-правового впливу та контролю за злочинністю на основі досліджень з використанням цифрових технологій:
  - в аналітичних цілях різних видів інформації в правоохоронній діяльності (технологія "великих даних" або BigData);
  - при виробництві слідчих дій, алгоритмізації слідчих і правоохоронних завдань (наприклад, комп'ютерне моделювання місця події);
  - при виробництві почеркознавчих експертиз (застосування технологій штучного інтелекту).

1. Технологія "великих даних" або BigData. Ця технологія відкриває нові можливості для аналітики різних видів інформації: аудіозаписів та відеозаписів з камер відеоспостереження, даних про трафік абонентів телекомунікаційних операторів, інформації з соціальних мереж та форумів, текстових документів. Також технології BigData дозволяють виявляти залежності з різних неструктурованих інформаційних баз даних [1]. Аналіз таких даних дає можливість прогнозувати вчинення злочинів у майбутньому, сприяє висуненню версій, плануванню розслідування кримінальної справи, розшуку підозрюваних та обвинувачених, які переховуються від слідства та суду. Наприклад, у Нью-Йорку, США, ще у 2007 році було прийнято рішення про створення централізованого оперативного центру громадської безпеки. Цей центр аналізує інформаційні потоки з понад 100 джерел (інформація з патрульних автомобілів, тисяч камер відеоспостереження, дзвінки від свідків тощо). Створення цієї системи дозволило знизити рівень злочинності в місті на 27%. Однією з реалізацій BigData є програма, яку використовує поліція Чикаго. Програма проаналізувала базу даних злочинців і змогла виявити список осіб,

яким загрожує вбивство. Дізнавшись їхні імена, поліція проводить з ними профілактичну роботу, що імовірно допомагає знизити ймовірність вчинення злочинів. Програма базується на десяти основних критеріях відбору. Серед них - ряд показників по історії приведення людини в поліцію. Алгоритм також враховує, чи затримувалася людина за незаконне зберігання вогнепальної зброї або за участь в організованих злочинних структурах. Алгоритм шукає людей, які відповідають усім або хоча б частині критеріїв відбору. Ті, хто має найбільше збігів за переліком критеріїв, потрапляють до групи підвищеного ризику. За даними поліції, новий алгоритм є досить ефективним. З 2,7 млн жителів Чикаго програма відібрала лише 1400 осіб з надзвичайно високою ймовірністю вбити або бути вбитими. Понад 70% людей з цього списку були застрелені протягом 2016 року. Кожен 4-й застрелений також перебував у списку чиказького департаменту поліції. За даними правоохоронців, 117 зі 140 осіб, заарештованих під час загальноміського рейду проти банд, також перебували у вищезазначеному списку і були в групі ризику.

2. Технології виробництва слідчих дій, алгоритми вирішення слідчих і правоохоронних завдань. Наприклад, комп'ютерне моделювання місця події. Впровадження в криміналістику технології віртуальної реальності дозволить моделювати місця злочинів, моделювання здійснюється за допомогою методу лазерного сканування. Використання цієї технології дасть можливість досліджувати об'єкти з довільної точки, виконувати вимірювання та розрахунки, автоматично формувати протоколи, необхідні для підготовки результатів експертиз [2]. А також при розгляді справи в суді дозволить віртуально побувати на місці вчинення злочину, змоделювати можливі сценарії дій осіб на місці події, а також чітко та аргументовано представити докази слідчим органам та суду. У перспективі 3D-моделювання має замінити систему криміналістичної фотографії та відеозапису.

У сучасному світі цифрові та комп'ютерні технології зайняли міцні позиції практично у всіх сферах людської діяльності, і як наслідок, цифрова криміналістика розвинулася як спеціалізована галузь судової експертизи.

Цифрова криміналістика має наступні цілі: виявлення, відновлення та криміналістичний аналіз даних, а також збір доказів з використанням цифрових технологій. Варто зазначити, що сфера поширення цифрової криміналістики є досить широкою, вона охоплює не тільки сучасні комп'ютерні технології, а й їх програмне забезпечення, електронні сховища даних, мобільний зв'язок тощо. У зв'язку з цим при розкритті злочинів необхідно докорінно змінювати систему використання нових технологій.

3. Штучний інтелект. Ця технологія здатна не тільки аналізувати значні обсяги інформації, але й робити певні "самостійні" висновки за результатами аналізу. Штучний інтелект використовується в різних сферах: медицині, промисловості, телекомунікаціях, науці, фінансах, кіноіндустрії та інших галузях [3]. Технології штучного інтелекту можуть бути успішно застосовані і в почеркознавчій експертизі. Почеркознавча експертиза проводиться, як правило, вручну висококваліфікованими експертами, тому результати можуть бути досить суб'єктивними і залежати від досвіду та професіоналізму експерта. Використання штучного інтелекту дозволяє мінімізувати людський фактор в процесі проведення експертизи. Крім того, штучний інтелект аналізує почерк набагато швидше, ніж експерт, і здатний розпізнавати закономірності в умовах сильних перешкод і спотворень. Технології штучного інтелекту мають надзвичайно важливу властивість - самонавчання, що підвищує якість отриманих результатів. На жаль, ця технологія має і суттєвий недолік: вона потребує великого обсягу вихідної інформації для навчання.

Висновки. Наведені вище технології тією чи іншою мірою впроваджуються в діяльність слідчих, оперативно-розшукових, кримінально-виконавчих та пенітенціарних органів України, і цей перелік далеко не повний. Розвиток сучасних інформаційних технологій дозволяє якісно підвищити ефективність виявлення, розслідування та попередження злочинів, а також їх своєчасного припинення. Міжнародний досвід може стати хорошим підґрунтям для розробки відповідних законодавчих ініціатив. Це дозволить максимально

ефективно використовувати сучасні технології як інструмент боротьби зі злочинністю.

Список використаних джерел:

1. 12 Innovative Police Technologies // вебсайт. URL: https://onlinedegrees.sandiego.edu/10-innovative-police-technologies/ (дата звернення: 18.11.2022).

2. Technological Advances Changing Law Enforcement. // вебсайт. URL: https://www.columbiasouthern.edu/blog/blog-articles/2020/february/technological-advances-in-law-enforcement (дата звернення: 19.11.2022).

3. The Growing Role Of Technology In The Criminal Justice Field. // вебсайт. URL: https://www.purdueglobal.edu/blog/criminal-justice/growing-role-technology-criminal-justice (дата звернення: 20.11.2022).

УДК 004.58

ГЛУЩЕНКО ІВАН ОЛЕКСАНДРОВИЧ

курсант 1 курсу факультету №4

Харківського національного університету внутрішніх справ,

СВІТЛИЧНИЙ ВІТАЛІЙ АНАТОЛІЙОВИЧ

науковий керівник

кандидат технічних наук, доцент,

доцент кафедри протидії кіберзлочинності

Харківського національного університету внутрішніх справ,

ORCID http://orcid.org/0000–0003–3381–3350

ОСОБЛИВОСТІ ПІДГОТОВКИ КАДРІВ ДЛЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ ПІДРОЗДІЛІВ НПУ

З 24 лютого 2022 року Україна потерпає від повномасштабної агресії з боку Російської федерації, що внесло зміни в побут всіх громадян, підприємств та державних установ України. В зв'язку з подіями в країні багато громадян виїхало за кордон, або мобілізувалося; це сильно повпливало на кількість охочих прийняти участь у відборі до лав національної поліції. Це з одного боку

зменшило конкурс на місце (в попередньому році, на спеціалізацію 125 "кібербезпека" було 16 абітурієнтів на місце, а в цьому 2,5), а з іншого боку, набагато менше людей бажають, або мають можливість, потрапити в лави Національної поліції. Зменшення конкуренції на місце дає більше шансів кожному з абітурієнтів для отримання вакантного місця, а з іншого боку, в НПУ потрапляють і ті люди, особові властивості яких не зовсім підходять для служби і які при нормальних умовах, ніколи не потрапили б до вузів МВС.

Основним завданням поліцейського є підтримання публічного порядку, шляхом забезпечення безпеки осіб, суспільства і держави [1]. Останнє під час війни є достатньо актуально, адже цей нелегкий час є розплідником для різного роду злочинців, через надання поліцейським додаткових обов’язків (наприклад кіберполіцейським підтримувати інформаційний фронт), що зменшує час на їх основну роботу. Такі зміни також несуть свої наслідки для вузів МВС. Набору кадрів також заважає репутація поліцейського, що закріпилася за ними ще з часів міліції, чи навіть раніше, це всі роки било по кількості охочих, а на момент війни всі проблеми, як воєнні, так і довоєнні, підсумовуються.

Також, однією з проблем є непридатність навчальних закладів МВС до навчання, через часткову або повну руйнацію, або окупацію останніх. в таких випадках робота з курсантами переноситься на дистанційне навчання, що значно зменшує якість навчання і також відлякує бажаючих навчатися; або університет частково, або повністю переноситься до інших міст (наприклад, ХНУВС), в такому випадку якість навчання також зменшується, адже деякі викладачі повинні переїжджати з однієї навчальної бази до іншої, що сильно обмежує час на викладення дисципліни. Розділення, або повна відсутність навчального приладдя також значно зменшує якість навчання, адже людина, яка вчилася "по картинках" буде гіршим спеціалістом, ніж та, яка навчалася на практиці.

Значно гальмує навчання та набір нових кадрів перебудова навчальних програм та життя університетів на воєнний лад, що потребує багато часу, та великих грошових вкладів (наприклад для побудови безпечних, та достатньо великих укриттів для перебування в них курсантів та особового складу

університету під час повітряної тривоги). На мою думку, війна з Росією дуже сильно впливає на набір кадрів до НПУ. Проте, за таких умов до лав національної поліції потраплять в більшій кількості справжні патріоти своєї держави, адже інші, в більшій кількості, втекли або вступили до інших навчальних закладів.

Список використаних джерел:

1. І. Дрок. Кадрова політика національної поліції України в умовах війни. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/258968 (дата звернення: 22.11.2022).

УДК 004.9

ГРУБА ВАЛЕРІЯ В'ЯЧЕСЛАВІВНА

курсантка 1 курсу факультету №4

Харківського національного університету внутрішніх справ,

СВІТЛИЧНИЙ ВІТАЛІЙ АНАТОЛІЙОВИЧ

науковий керівник

кандидат технічних наук, доцент,

доцент кафедри протидії кіберзлочинності

Харківського національного університету внутрішніх справ,

ORCID http://orcid.org/0000–0003–3381–3350

ЗАХИСТ ІНФОРМАЦІЙНОГО ПРОСТОРУ

З всеобіймаючим розвитком нашого суспільства для покращення та спрощення нашого життя, почався потужний розвиток інформаційно-технологічного напрямку. Нові побутові прилади, які приєднуються до всесвітньої мережі для того, щоб ви могли ними керувати на великих відстанях, перенесення ведення обліку сфер обслуговування в он-лайн режим – облегшує збереження великого обсягу інформації, тощо.

Усі перераховані вище факти розвитку нашої цивілізації дають можливість перенести всю інформацію про людину в базу де зберігається мільярди даних інших людей. Без сумніву, це може зацікавити злочинців, які розраховують отримати цю інформацію, безпосередньо від вас, за допомогою соціальної

інженерії чи за допомогою інформаційно-обчислювальних приладів, вони отримують доступ до вашої конфіденційної інформації, що дає можливість вкрасти ваші гроші, вчинити шахрайські діяння стосовного вашого майна і тому подібне.

Для запобігання, уникнення та усунення таких випадків неправомірного втручання у ваше життя та завдання шкоди вашому матеріальному становищу створюють групи в органах внутрішніх справ, які є спеціалістами у сфері інформаційної безпеки – кібербезпеки. Для вирішення поставлених перед ними задач з усунення можливостей виникнення подібних загроз, працівники здійснюють інформаційну підтримку в розкритті, розслідуванні, виявленні і попередженні злочинів, встановленні і розшуку злочинців, надавати багатоцільову статистичну, аналітичну і довідкову інформацію, служити інструментом багатьох експертно-криміналістичних програм [1]. Вони також можуть бути ефективним засобом розслідування, виявлення і попередження окремих видів злочинів [2], (особливо - злочинів у сфері інформаційних технологій, низки злочинів у сфері економіки і т.д.).

Подібні дії забезпечують не тільки розкриття кримінальних правопорушень у сфері інформаційних технологій, а й допомагають прискорити та покращити роботу усіх інших підрозділів.

Отже, органи кібербезпеки захищають ваш кордон інформаційного простору наступним чином: проводить профілактичні роботи з питань застереження використання електронно-обчислювальних приладів, користування соціальними мережами та інтернет мережею, а саме питання, які стосуються вашої конфіденціальної інформації та розкриття кримінальних правопорушень з використанням електронно-обчислювальної техніки.

Список використаних джерел:

1. Інформаційні технології в правоохоронній діяльності : НАВС. Головна сторінка :: НАВС. URL: https://www.naiau.kiev.ua/news/informacijni-tehnologiyi-v-pravoohoronnij-diyalnosti.html (дата звернення: 18.11.2022).

2. Використання нових інформаційних технологій у криміналістичному навчанні | Коментар. Мего-Інфо - Юридичний портал України №1, коментар ЦПК, КПК, КУПАП, ККУ, ЦК. URL: http://mego.info/матеріал/23-використання-нових-інформаційних-технологій-у-криміналістичному-навчанні (дата звернення: 18.11.2022).

УДК 004.83

ГУЩА АНАСТАСІЯ АНДРІЇВНА

студентка 1-го курсу рівня магістр

факультету інформаційних радіотехнологій

та технічного захисту інформації

Харківського національного університету радіоелектроніки

ХОНДАК ІННА ІВАНІВНА

старший викладач кафедри охорони праці

Харківського національного університету радіоелектроніки

ПОТЕНЦІАЛ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В УМОВАХ РОЗВИТКУ КРИМІНАЛІСТИЧНОЇ ТЕХНИКИ

Кримінальне судочинство, в тому числі його техніко-криміналістичне забезпечення, не залишається осторонь від високих технологій, активно застосовуючи системи швидкого переміщення, зберігання та аналізу великих обсягів інформації. Штучний інтелект (ШІ) – це один із атрибутів сучасної ефективної оперативно-розшукової та кримінально-процесуальної діяльності.

Дана робота ставить перед собою мету проаналізувати факт впливу штучного інтелекту на сферу криміналістики як невід’ємного чинника роботи, конкретизувати специфіку використання штучних нейронних мереж з метою оптимізації криміналістичних досліджень, дослідити технологічні наслідки введення інновацій на виробниче середовище компетентних спеціалістів.

Сьогодні система інтелектуального забезпечення кримінального процесу є синтезом наступних взаємодоповнюючих елементів:

– професійна підготовка суб'єктів виявлення, розкриття та

розслідування злочинів;

- законодавче забезпечення кримінального процесу;
- науково забезпечення кримінально-процесуальної діяльності;
- інформаційно-технічне забезпечення кримінального судочинства;
- забезпечення кримінального процесу системами ШІ.

Під штучним інтелектом традиційно розуміють комп'ютерні програми, програмні комплекси, здатні не просто діяти за заздалегідь заданим алгоритмом, а й реалізовувати такі іманентні людині творчі функції, як прогнозування, оцінка ризиків, робота з неповними даними. Натомість, робота штучної нейронної мережі заснована на інтелектуальному евристичному аналізі даних, який набагато ефективніший, ніж методи математичної статистики, що використовуються в більшості криміналістичних програмних комплексах [1].

Робоча штучна мережа може містити десятки і сотні шарів (рівнів оцінки і перевірки), що забезпечують комплексний розгляд будь-яких факторів, що дозволяє вирішувати вкрай складні завдання, в тому числі з розкриття і розслідування злочинів.

Відомо три етапи створення штучної нейронної мережі. На першому етапі відбуваються збір і узагальнення даних, які згодом будуть використані для навчання мережі. На другому етапі здійснюється вибір топології (внутрішньої архітектури) штучної нейронної мережі і підбір параметрів навчання; формується «прихований шар». На третьому, заключному, етапі підготовки штучної нейронної мережі відбувається безпосереднє тестування, за яким слідує перевірка його адекватності, тобто відповідності цілям створення мережі [2].

Основні напрямки в криміналістиці, де можуть бути використані штучні нейронні мережі:

1. Оцінка вихідної інформації у кримінальній справі з метою висунення простих і комплексних слідчих версій, визначення напрямків їх перевірки.

2. Моделювання події злочину та слідчої картини на основі неповних даних і попереднього «досвіду», що охоплює великий масив кримінальних справ.

3. Виявлення ознак серійності в умовах інформаційної недостатності та пропозиція варіантів дій слідчого щодо перевірки перспективних слідчих версій.

4. Збільшення ефективності почеркознавчих і габітоскопічних досліджень: до теперішнього часу найбільш перспективним напрямком розвитку штучних нейронних мереж вважається розпізнавання образів, що може дозволити, наприклад, автоматизацію виявлення ознак підроблення документів.

5. Пошук недоступних криміналістичному програмному забезпеченню комп'ютерних файлів, прихованих, наприклад, за допомогою стеганографії, встановлення первинного джерела інформації в мережі Інтернет.

Оптимізація робочих місць спеціалістів сфери криміналістики характеризуватиметься не тільки впровадженням програмного забезпечення, а й вдосконаленням взаємодії «Людина-машина-середовище». При використанні ШІ компетентний робітник матиме можливість вдосконалити робочий процес:

- структурувати великий обсяг даних;
- систематизувати оцифровані дані;
- зменшити часові витрати на опції обробки паперових документів;
- зменшити кількість вірогідних помилок людського фактору;
- підвищити загальну продуктивність праці.

Зменшити вплив таких психофізіологічних виробничих чинників як:

- монотонність праці під час диджиталізації інформації вручну;
- підвищеної розумової напруги та емоційного перенавантаження;
- підвищеного впливу на зорові аналізатори.

У найближчому майбутньому цілком можлива інтеграція застосування ШІ в криміналістичну практику, однак для цього потрібне подальше вивчення архітектури і можливостей штучних нейронних мереж, в тому числі вченими-криміналістами. Впровадження систем ШІ дозволить легко та швидко опрацювати великий масив даних, а також спрогнозувати можливі рішення суперечливих питань.

Список використаних джерел:

1. Криминалистика будущего. Какая она? / [Електронний ресурс]. – Режим доступу: https://ceur.ru/news/specproekty/item311872/ .

2. Использование методов искусственного интеллекта в изучении личности серийных убийц / [Електронний ресурс]. – Режим доступу: https://cyberleninka.ru/article/n/ispolzovanie-metodov-iskusstvennogo-intellekta-v-izuchenii-lichnosti-seriynyh-ubiyts

УДК 004.77

ЄЖОВ ДМИТРО МИХАЙЛОВИЧ,

курсант 1 курсу факультету №4,

Харківського національного університету внутрішніх справ,

СВІТЛИЧНИЙ ВІТАЛІЙ АНАТОЛІЙОВИЧ,

науковий керівник

доцент кафедри протидії кіберзлочинності факультету №4

Харківського національного університету внутрішніх справ,

кандидат технічних наук, доцент

ORCID ID http://orcid.org/0000-0003-3381-3350

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ ПІД ЧАС ВІЙНИ

Сучасний стан застосування інформаційних технологій у всіх галузях потребує розширення їх впровадження у діяльність правоохоронних органів. Так, в правоохоронних органах накопичений чималий досвід застосування сучасних інформаційних технологій при розкритті та розслідуванні злочинів, виконанні інших завдань боротьби зі злочинністю під час війни [1]. Насамперед, інформаційні технології під час війни застосовуються для запобігання дезінформації та протидії агресору.

Під час війни в правоохоронній діяльності інформаційні технології відіграють велику роль. На даний момент агресор широко застосовує новітні інформаційні технології проти нашої держави, тому основною задачею правоохоронних органів є запобігання цьому. Правоохоронні органи

застосовують масу інформаційних технологій у війні проти агресора, наприклад: мініатюрні безпілотники, потужні комп'ютерні системи, комп'ютерні віруси.

На сьогоднішній день найбільше застосовується правоохоронними органами супутникове стеження, комп'ютерні технології для стеження за переміщенням агресора та розповсюджувачів дезінформації. Але навіть при таких умовах розвиток інформаційних технологій недостатній.

Тому зараз потрібно більш ефективно розвивати інформаційні технології в правоохоронній діяльності, для цього потрібно насамперед створити більш масштабну підготовку спеціалістів у цьому напрямку.

Недоліки інформаційних технологій в правоохоронній діяльності теж існують. Наведу вам приклад з мого досвіду: недоліками є недостатнє технологічне забезпечення, нестабільне інтернет-з’єднання, недостача кадрового забезпечення, а під час війни проблеми з електрикою.

Підведу підсумок, що інформаційні технології в правоохоронній діяльності під час війни застосовують в усіх напрямках, тож потрібно розвивати цей напрямок, робити його більш масштабним та удосконалювати для більш ефективного застосування в боротьбі проти агресора.

Список використаних джерел:

1. «Сучасні інформаційні технології в діяльності Національної поліції України». Дніпропетровський державний університет внутрішніх справ. URL: https://dduvs.in.ua/2022/11/11/suchasni-informatsijni-tehnologiyi/ (дата звернення: 22.11.2022).

УДК 65.012.8 + 004

ЄРЬОМЕНКО ЯРОСЛАВ СЕРГІЙОВИЧ

курсант 3 курсу факультету №4

Харківського національного університету внутрішніх справ

ГЕЛЬДТ СТАНІСЛАВ ВОЛОДИМИРОВИЧ

курсант 3 курсу факультету №4

Харківського національного університету внутрішніх справ

МАНЖАЙ ОЛЕКСАНДР ВОЛОДИМИРОВИЧ

науковий керівник

завідувач кафедри протидії кіберзлочинності факультету № 4 Харківського національного університету внутрішніх справ, к.ю.н., доцент

АСПЕКТИ ВИКОРИСТАННЯ ЧАТ-БОТУ «МВС РОЗШУК» У ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЇ УКРАЇНИ

В сучасних. умовах Національна поліція України працює в посиленому режимі для забезпечення охорони прав і свобод українців, протидії злочинності, підтримання порядку та публічної безпеки на всій території України. З метою покращення інформаційно-аналітичного забезпечення відповідних підрозділів у 2017 році було затверджено положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України». Цей портал є сукупністю технічних і програмних засобів, призначених для обробки відомостей, що утворюються у процесі діяльності Національної поліції України та її інформаційно-аналітичного забезпечення [1]. Впровадження Інформаційного порталу Національної поліції України дозволило оптимізувати час і сили для пошуку інформації про людину, транспортний засіб, вогнепальну зброю тощо.

Паралельно з цим у відкритому доступі перебуває частина обліків МВС України (https://wanted.mvs.gov.ua), які також можуть стати в нагоді правоохоронцям, які не мають в конкретний момент часу доступу до відомчої мережі. З метою автоматизації пошуку відповідної інформації курсантами Харківського національного університету було розроблено чат-бот Telegram «МВС Розшук» (рис. 1). Він створений для полегшення пошуку безвісно зниклих осіб, вкрадених транспортних засобів, розшуку вогнепальної зброї, мобільних телефонів, осіб, які переховуються від органів влади, пошуку викрадених культурних цінностей чи пошук паспорту громадянина України серед втрачених чи викрадених. Загалом чат-бот може допомогти як звичайним громадянам України, так і працівникам Національної поліції чи інших відомчих структур.

Структура чат-боту доволі легка та інтуїтивно зрозуміла. Після його запуску з’являється повідомлення з проханням вибрати категорію розшуку.

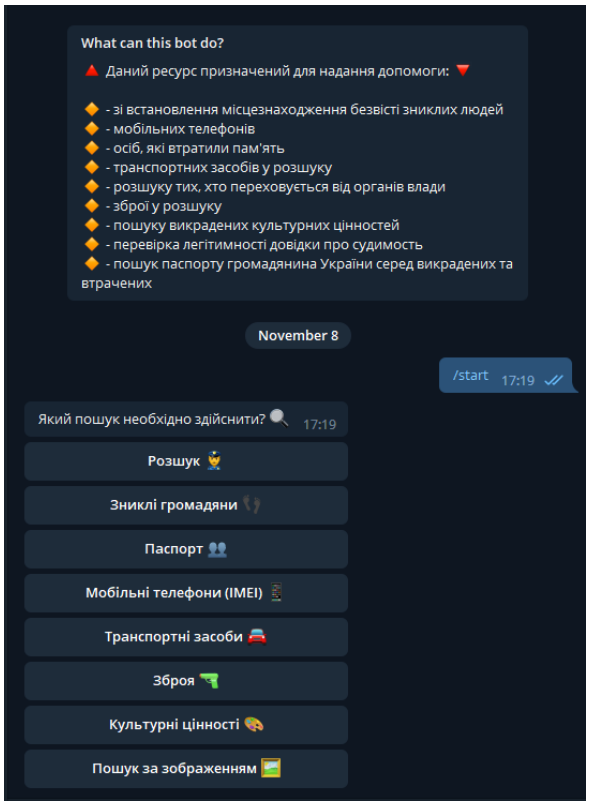


Рис. 1. Зовнішній вигляд чат-боту «МВС Розшук»

Серед доступних наразі такі:

- розшук;
- зниклі громадяни;
- паспорт;
- мобільні телефони;
- транспортні засоби;
- зброя;
- культурні цінності;
- пошук за зображенням.

Після вибору категорії «Розшук», можна побачити прохання ввести ПІБ, дату народження, стать та дату пропажі людини. Далі починається пошук осіб. Усі люди, які будуть підходити під опис з’являться на екрані з інформацією про орган МВС, що розшукує дану особу, запобіжний захід, що було застосовано, місце зникнення, причина розшуку та стаття, за якою звинувачують чи

підозрюють особу. Крім того, можна побачити фото злочинця, якщо воно є в базі. Інформація береться з офіційного сайту МВС - wanted.mvs.gov.ua, тому все, що з'являється в результатах пошуку не містить інформації з обмеженим доступом.

Цікавою категорією чат-бота «МВС Розшук» є «Пошук за зображенням». Після вибору цієї команди з'являється прохання надіслати фото розшукуваної людини. Коли фото надіслано, починається розпізнавання за фотографією серед даних розшукуваних осіб. У випадку позитивного результату пошуку в чат надсилається повна інформація про людину, яку розшукують. У результаті пошуку можна побачити ПІБ, дату народження, стать, орган МВС, який розшукує особу, категорію, місце зникнення, дату зникнення та статтю звинувачення.

Вказаний програмний продукт може стати у нагоді не тільки працівникам органів Національної поліції, а й звичайним громадянам України. На практиці чат-бот «МВС Розшук» можна застосовувати задля розшуку людей чи речей, що зникли чи вкрадені, та, звичайно ж, для буденних речей, наприклад, перевірки транспортного засобу при покупці по VIN-коду чи перевірки телефону при покупці по IMEI.

Список використаних джерел:

1. Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України»: веб сайт. URL: https://zakon.rada.gov.ua/laws/show/z1059-17#Text (дата звернення: 19.11.2022).

УДК 004.77

КАЛАНЧА АНДРІЙ АНДРІЙОВИЧ

курсант 2 курсу факультету №4

Харківського національного університету внутрішніх справ,

СВІТЛИЧНИЙ ВІТАЛІЙ АНАТОЛІЙОВИЧ

науковий керівник

кандидат технічних наук, доцент, доцент кафедри протидії кіберзлочинності Харківського національного університету внутрішніх справ

ORCID http://orcid.org/0000–0003–3381–3350

ТЕХНОЛОГІЯ VPN, ЯК НАЙЛЕГШИЙ СПОСІБ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ У КІБЕРПРОСТОРІ

Анонімність є основним способом, за яким особу неможливо ідентифікувати у мережі Інтернет. Необхідність цього терміну в глобальній мережі є досить великою, оскільки збір даних ведеться звідусіль: провайдер збирає ваші дані та надсилає до спеціальних служб, державних структур; великі корпорації, такі як Google, Microsoft, Apple та інші збирають інформацію користувача, для розповсюдження таргетованої реклами особам, що використовують цей пристрій (прикладом слугує – AdvertismentID, тобто технологія, яка слугує допомогою для рекламних служб за для персоналізації своїх пропозицій. Її можна знайти в операційний системі Windows, версії 10 та вище або у браузерах на ядрі Chromium, тобто, Google Chrome). Крім того, без анонімності не може існувати свобода слова. Тож *метою* роботи є ознайомлення із технологією VPN (Virtual Private Network), та її створення власноруч, оскільки готові варіанти, запропоновані в мережі Інтернет, не завжди гарантують 100% збереження вашого трафіку лише у межах цієї структури.

У першу чергу, розберемо два поняття, які досить часто плутають - «приватність» і «анонімність». Приватність ідентифікує особу, але не дії, які вона вчиняє, на противагу анонімності, під час якої неможливо зв’язати діяння користувача із самим користувачем, інформація про якого також невідома. Проте варто пам’ятати, що 100% анонімності не існує. Тож поговоримо про технологію, яка знаходиться на рівні стеку TCP/IP і здатна приховати запити та діяльність у мережі Інтернет.

VPN, або ж Virtual Private Network – це узагальнена назва технологій, метою якої є створення захищених віртуальних мереж поверх інших. Між двома вузлами створюється VPN-тунель, необхідний для з’єднання користувача із кінцевою точкою, що дозволить використовувати усі доступні функції в Мережі. При чому, цей тунель шифрує усі дані, що створює зашифрований канал між

точками моделі клієнт-сервер. При підключенні до VPN ваша реальна IP-адреса маскується, та замінюється на ту, яку пропонує сервер сервісу [0].

Типів VPN є дуже багато. SSL VPN, або Secure Sockets Layer VPN – VPN, що дозволяє організувати віддалений доступ до будь-якої внутрішньої мережі всередині організації. Достатньо на сайті компанії ввести логін-пароль користувача і все – з'єднання користувача захищене [2].

VPN типу "Site-to-site" — це, по суті, приватна мережа, призначена для приховування приватного інтранету і надання користувачам безпечної мережі для доступу до ресурсів один-одного.VPN типу "сайт-сайт" корисний, якщо у вашій компанії є кілька локацій, кожна з яких має власну локальну мережу, підключену до глобальної мережі. Site-to-site VPN в основному використовуються у великих компаніях. Їх складно реалізувати та вони не пропонують такої ж гнучкості, як SSL VPN. Однак вони є найефективнішим способом забезпечення зв'язку всередині та між великими відділами. Клієнт-сервер VPN. Замість того, щоб використовувати VPN для створення тунелю шифрування для маскування існуючого підключення до Інтернету, VPN може автоматично шифрувати дані, перш ніж вони стануть доступними для користувача. Це все більш поширена форма VPN, яка особливо корисна для постачальників незахищених публічних мереж. Це запобігає третім сторонам отримати доступу до мережевого з'єднання та шифрує дані на всьому шляху до постачальника. Він також запобігає доступу провайдерів до даних, які з будь-якої причини залишаються незашифрованими, і обходить будь-які обмеження на доступ користувача до Інтернету [3].

Для створення власного VPN необхідно визначитися із хостингом, тобто, віддаленою машиною, який буде обробляти запити особи, яка ним користується. Варто звернути увагу на те, які характеристики у серверу, на основі якого буде працювати віртуальна мережа. Оскільки сервер, це той же домашній комп'ютер, тільки зі своїми особливостями, як, наприклад, надлишкова потужність, необхідно встановити операційну систему, бажано на ядрі GNU/Linux, а потім налаштувати під використання VPN-серверу. Далі будь-яким зручним способом

для користувача підключаємося до піднятого власноруч VPN (напряму, чи за допомогою клієнтів, типу Wireguard) [4].

Таким чином, у роботі розглянуто технологію віртуальних приватних мереж, головною метою яких є перенаправлення усього трафіку особи через зашифрований тунель. VPN дозволяє приховати IP-адресу під час користування Інтернетом, роблячи її місцезнаходження невидимим для всіх. VPN-з'єднання також захищене від зовнішніх атак. Це тому, що лише ви можете отримати доступ до даних у зашифрованому тунелі – і ніхто інший не може, оскільки у них немає ключа. VPN дозволяє отримати доступ до регіонально обмеженого вмісту з будь-якої точки світу.

Список використаних джерел:

1. Wikipedia. VPN. URL: https://uk.wikipedia.org/wiki/VPN (дата звернення: 20.11.2022)

2. Senetsy. SSL VPN. URL: https://senetsy.ru/materials/publications/posts/ssl-vpn/ (дата звернення: 20.11.2022)

3. Kaspersky. What is VPN? How it works, Types of VPN. URL: https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn (date of access: 20.11.2022)

4. Oleg Borisov. Создаём свой VPN-сервер. Пошаговая инструкция. URL: https://vc.ru/dev/66942-sozdaem-svoy-vpn-server-poshagovaya-instrukciya (дата звернення: 20.11.2022)

UDC 351.74:005.591.6

KAPUSTIANSKYI VLADYSLAV DMYTROVYCH

Cadet of group F4-201

Kharkiv National University of Internal Affair

KALCHENKO TETYANA MYKHAILIVNA

Teacher of the department of foreign languages

Kharkiv National University of Internal Affair

FACIAL RECOGNITION TECHNOLOGY IN POLICE WORK

Face recognition is a technology that allows you to automatically identify or verify a person in a photo, video or live. For recognition, neural networks are used that can read and analyze the unique features of the human face, and then check them against a database.

Interest in these systems is very high due to the wide range of tasks they solve. The essence of the technology lies in the use of servers with software or special cameras with built-in face recognition function to detect points on the face and measure the distances between them, which makes it possible to create a face map. Depending on the technology of the system, it is necessary to identify about 80 such points. After scanning the face search is carried out in the database to correlate the face with information that is available in the databases. The American video surveillance provider Clearview Al, has created huge databases containing more than 3 billion recognized faces by filtering social networking sites. The speed of this process takes less than one second, and the probability of error is minimal. Most developed countries have made great progress in the application of this technology in various industries. Most often face recognition is used to catch criminals. Identification can be carried out both with the help of cameras and with the help of smart glasses for the police.

For the police, this technology significantly improves the ability to monitor and search for suspects. A facial recognition system connected to a network of cameras can automatically track a person as he or she enters and leaves the area of coverage, even if no other information about him or her is available. A facial recognition system that works on the basis of a large database of information can enable the police to pinpoint the exact location of a person of interest on network cameras in the city. This greatly facilitates the work of the police in identifying suspects, searching for criminals and missing people. The advantage of this technology is that it would take weeks for a person to do this work, while a special computer application can reduce the time to a matter of seconds. Justice thus becomes fast, accurate and reduces costs.

But this technology also has concerns, including the problem of privacy and personal data protection. An important factor in guaranteeing the security of data introduction into the system is insurance against interception of this information by

intruders, the transfer of this data should be carried out using encryption technologies throughout the entire transfer process, and personal data should be anonymized.

In Ukraine, the development and implementation of face recognition technology is just at the beginning, but already now we can say that the technology has made a step towards the corporate sector and many companies are beginning to implement this technology.

УДК: 004.043

КАРПЕЧЕНКОВ МИКИТА ПАВЛОВИЧ

студент 3 курсу групи Ф6-Кбдср-20-2 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

КІБЕРБЕЗПЕКА В УМОВАХ ВІЙНИ: ЩО, ХТО, ЯК

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.

В умовах війни питання безпеки кіберпростору стає особливо важливим, тому як ворог перестає керуватися моральними принципами. Їх головна мета –

дестабілізація ситуації в країні, знищення "незручної" для них інформації, знищення або замороження техніки обробки та зберігання інформації.

Ворогом може бути не тільки зовнішній, а і внутрішній, вже непоодинокі випадки установи колаборантських контактів. Тому в умовах військового стану було оновлено основний юридичний склад злочину за ст. 361 Кримінального Кодексу України та створений новий закон - 2149-IX.

Мета нового закону полягає в наступному:

1. Оптимізація та посилення можливостей національної системи кібербезпеки для протидії загрозам, які надходять з кіберсфері.

2. Впровадження нових кримінально – правових механізмів протидії кіберзлочинності.

3. Забезпечення безпечного використання цифрових послуг державного значення.

Завдяки новому закону набула чинності і відредактоване формування ст. 361 Кримінального Кодексу України, а саме:

1. Змінено оцінку категорії шкоди. За новою редакцією шкода вважається значною, яка в триста і більше разів перевищує неоподатковуваний мінімум доходів громадянина – тобто була збільшена в 300 разів.

Завдана шкода тепер розуміється як несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж.

Важлива зміна, якщо раніше за шкоду розумівся факт витоку, зміни конфіденційної або секретної інформації, порушення праці державних установ або підприємств, то тепер можуть притягнути до відповідальності за сам факт установи втручання в роботу системи або причетності до витоку конфіденційної інформації.

2. Посилені санкції за кримінальні порушення – в середньому були оновлені або добавлені штрафи, які були підвищені на 500% або 1000%, також існуючі санкції у вигляді позбавлення волі підвищено від 30% до 80%.

Також були оновлені правила для білих хакерів так звані «білі капелюхи». Закон 2149-IX передбачає, що втручання в роботу інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж не вважатиметься несанкціонованим, якщо втручання було виконано відповідно до порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж. Проте, наразі умови для білих хакерів та людей, які виконують функцію Bug Bounty (пошук, виявлення та рекомендації по ліквідації вразливостей).

З вище наведеного можна виділити такий принцип: що каже закон і хто у зоні ризику, та як нам забезпечити особисту безпеку у кіберпросторі. В зоні ризику прибувають абсолютно всі користувачі ресурсів як правило Інтернет. Існує багато способів атак на персональні дані, розглянемо декілька із них.

Шкідливе ПЗ. Розрізняють два типи такого ПЗ – з використанням соціальної інженерії та вмонтоване в програму.

1. З використанням соціальної інженерії – як правило це спам, який пропонує потенційній жертві перейти за посиланням, після чого іде вмонтування шкідливого ПЗ в систему та втрачається анонімність персональних даних користувача. Тому слід для запобігання не нажимати на невідомі посилання, підозрілі будь які опитування, спам-листи, тощо.

2. Вмонтоване в програму ПЗ – даний тип зустрічається, тільки якщо користувач використовує неліцензійне або не перевірене ПЗ. Для уникання цього слід використовувати ліцензійні версії ПЗ, не користуватись неперевіреним ПЗ, завжди мати надійний антивірус, який може попередити або перевірити підозрілі файли тощо.

Соціальна інженерія – маніпуляція, завдяки якій злочинці змушують користувачів робити потенційно шкідливі дії наприклад: розголошувати якусь інформацію, пересилати файли, натискати посилання або переходити на ресурси, які користувач не мав наміру відвідувати. Чудовий порятунок від цього типу загроз – ніколи не робити у кіберпросторі того, що не збирався. Також для додаткового захисту можливе використання VPN.

Для захисту можливе використання спеціалізованих фільтрів, які покроково аналізують трафік для виявлення нестандартну мережеву активність та критичні помилки. Знаючи, що каже закон та хто знаходиться в зоні ризику можна вже розібратись, як можливо забезпечити захист собі, компанії або оточуючим.

Слід пам’ятати що у діловій сфері нашого життя самим небезпечним фактором у кіберсфері є людина. Регулярні консультації та тренінги створення надійної політики безпеки можуть виключити виток конфіденційної інформації через працівників. Тому, при створені політик інформаційних/кібербезпек під час війни слід дотримуватися таких простих організаційних або управлінських правил а саме:

1. Пересвідчитись, що співробітники мають доступ до надійних та перевірених джерел інформації щодо поточної ситуації і є обізнаними щодо ризиків фішингу та шахрайських вебсайтів з тематики війни в Україні;

2. Надавати поради з кібербезпеки для співробітників, що знаходяться в місцях потенційного ризику, працюють у правоохоронних органах або на державних посадах у секторі оборони. Надавати психологічну підтримку таким категоріям співробітників та їх сім’ям, включаючи проведення тренінгів або семінарів щодо дій в непередбачуваних або кризових ситуаціях у тому числі з кіберзахисту;

3. Подумати про термінову додаткову підтримку в управлінні звичайними функціями безпеки, аналізу збільшеного обсягу сповіщень безпеки та реалізації термінових покращень щодо безпеки.

В умовах військового стану, коли нам всім нелегко, ці рекомендації в якійсь частині допоможуть у розумінні деяких важливих питань що кіберзахисту, а втрата конфіденційності в кіберпросторі можуть привести до небажаних наслідків у життєвих сферах.

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-internetechistim-poisk-i-otklyuchaem-sbor-dannyh (дата звернення 18.11.2022)

2. Закон України про внесення змін до Кримінального Кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану: Закон України від 24.03.2022 № 2149-IX // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text. (дата звернення 18.11.2022)

3. Микола Єрема Боротьба з кіберзлочинністю в умовах дії воєнного стану Закон 2149-IX /Ліга: Закон: офіційний вебсайт. URL:https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix (дата звернення 20.11.2022)

УДК 004.056.55

КОБЗАР ОЛЕГ БОГДАНОВИЧ

курсант Національної академії Державної прикордонної служби України

БАСАРАБ ОЛЕКСАНДР КОРНІЙОВИЧ

кандидат технічних наук, доцент,

викладач кафедри телекомунікаційних та інформаційних систем

Національної академії Державної прикордонної служби України

ШИФРУВАННЯ ПОВІДОМЛЕНЬ ПІД ЧАС ОБМІНУ СЛУЖБОВОЮ ІНФОРМАЦІЄЮ З ВИКОРИСТАННЯМ ВІДКРИТИХ МЕСЕНДЖЕРІВ

Державна прикордонна служба України виконує завдання з охорони державного кордону, в основному, шляхом виставлення прикордонних нарядів на ділянці кордону. При цьому зв’язок в ланці прикордонний підрозділ – прикордонний наряд та між прикордонними нарядами організовано за

допомогою радіостанцій УКХ діапазону. Проте, зазначена організація зв'язку не в повній мірі забезпечує потреби прикордонних підрозділів в управлінні прикордонними нарядами – особливості рельєфу місцевості, природні умови, рослинність тощо не дозволяють встановити суцільне УКХ-покриття. У випадку наявності GSM-покриття національних операторів мобільного зв'язку військовослужбовці Державної прикордонної служби України можуть використовувати власні мобільні термінали для передачі голосових або текстових повідомлень за допомогою месенджерів типу Viber, Telegram або WhatsApp, але немає гарантії, що інформація не потрапить у руки третіх осіб, адже сервери цих месенджерів, знаходяться не в Україні.

Для забезпечення захисту службової інформації під час використання месенджерів нами розроблено додаток «BG – Cipher». Він розроблений на мові програмування високого рівня Python та є кросплатформенним, тобто, може використовуватися як на мобільних терміналах під керуванням операційної системи Android так і на пристроях під управлінням ОС сімейства Windows.

Розглянемо принцип роботи застосунку. Перша частина – шифратор, який використовує бібліотеку «pyAesCrypt». Ця бібліотека використовує шифр AES256–CBC із симетричним шифруванням. Принцип симетричного шифрування полягає у використанні одного і того самого ключа для шифрування та дешифрування. Суттєвою перевагою такого типу шифрування перед асиметричним типом є швидкість та менша обчислювальна потужність, що означає відсутність необхідності в потужних обчислювальних машинах та можливість застосування на більшості сучасних мобільних терміналах (смартфонах). Ключ в свою чергу згенерований модулем Fernet, що імпортується з бібліотеки «cryptography». Функція модуля Fernet «Fernet.generate_key()» використовує кодування base64 та створює 32 – байтовий ключ. Ця функція була обрана через її надійність. Адже ключ довжиною в 32 байти підібрати просто неможливо. Ключ формується щоразу унікальний, тому за допомогою «Fernet.generate_key()» підібрати його теж не вдасться. Після генерації за допомогою хеш-функції SHA-256 створюється хеш ключа. Хеш-функція

приймає групу символів (називається ключем) і відображає її на значення певної довжини (називається хеш-значенням або хешем). Значення хеша є репрезентативним для початкового рядка символів, але зазвичай менше, ніж оригінал.

Після створення хеша ключа додаток автоматично створює файл «password.txt» в корневій папці розташування самого додатку у всіх учасників обміну інформацією. В ньому зберігатиметься хеш. Під час дешифрування програма запросить у користувача ключ. Після того як користувач введе ключ програма створить його хеш та порівняє його з хешем, з яким було зашифровано інформацію. У разі ідентичності буде здійснено дешифрування. Бібліотека «pyAesCrypt» після шифрування створює файл з новим розширенням «.bg», яке жодна програма для роботи з текстовими документами та файлами не зможе відкрити. Тому цей спосіб шифрування досить надійний.

Принцип дешифрування полягає у тому, що програма за допомогою певних функцій мови Python знаходить усі файли із розширенням «.bg» та дешифрує їх. Механізм застосування ключа ідентичний з першою частиною.

Отже, нами розроблено додаток «BG – Cipher», за допомогою якого прикордонні наряди можуть отримувати та передавати захищені службові повідомлення використовуючи доступні месенджери та інтернет-покриття національних операторів мобільного зв’язку.

УДК 378:355

КРИВОШЕЄВ ЄВГЕН ОЛЕКСІЙОВИЧ

курсант 2 курсу факультету №4,

Харківського національного університету внутрішніх справ,

СВІТЛИЧНИЙ ВІТАЛІЙ АНАТОЛІЙОВИЧ

науковий керівник

кандидат технічних наук, доцент,

доцент кафедри протидії кіберзлочинності

Харківського національного університету внутрішніх справ,

ORCID http://orcid.org/0000–0003–3381–3350

АКТУАЛЬНІ ПРОБЛЕМИ ПІДГОТОВКИ КАДРІВ ДЛЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ ПІДРОЗДІЛІВ НПУ

У сучасному житті суспільства і держави навряд чи залишилася бодай одна сфера діяльності, на яку інформаційні (цифрові) технології не мали б істотного впливу. Ефективність, компетентність та обґрунтованість управління органами внутрішніх справ знаходяться у прямій залежності від якості інформаційно-аналітичного забезпечення.

Суттєві зміни відбуваються і в діяльності правоохоронних органів. На основі сучасних інформаційних технологій здійснюється впровадження потужних інформаційно-пошукових систем, удосконалюється і система управління та інформаційно-аналітичного забезпечення Національної поліції, розробляються ефективні методи збирання й аналізу інформації.

Складність організації протидії злочинності обмовлена низкою причин, серед яких небхідно відмітити: недостатню кількість досвідчених професіоналів в системі Національної поліції і необхідного правового, методичного та технічного забезпечення попередження, виявлення та припинення злочинів [1].

Головна кадрова проблема Національної поліції в сучасних умовах – це нагальна потреба фахівців, які на новому технологічному рівні були б спроможні убезпечити особу, суспільство та державу. Ефективно протидіяти злочинності можуть лише ті правоохоронці, які досконало володіють законодавчою базою, мають високий рівень професійної підготовки, досвід боротьби з сучасними видами злочинів [2]. Одна з важливих умов підвищення якості підготовки майбутніх фахівців у галузі інформаційних технологій – це формування високих моральних якостей, вироблення імунітету до скоєння правопорушень.

Підвищення значення аналітичної діяльності у процесі управління органами внутрішніх справ пов'язане з ускладненням завдань та зростанням ролі управління, збільшенням обсягу інформації та числа напрямків діяльності органів внутрішніх справ, що тягне за собою необхідність дедалі більшого впровадження в інформаційно-аналітичну практику наукових методів та

сучасних інформаційних технологій, що передбачають широке використання комп'ютерної техніки та інформаційно-обчислювальних мереж [3].

Водночас професійний рівень працівників оперативних підрозділів не завжди відповідає сучасним вимогам, недостатня увага приділяється і використанню новітніх інформаційних технологій. Все це негативно впливає на отримання оперативно-розшукової інформації.

Однією з актуальних проблем викладання дисциплін спеціалізації є недостатнє матеріальне забезпечення навчального процесу [4]. Для проведення практичних занять необхідна не лише сучасна комп’ютерна техніка, але й комплекси обробки мультимедійних даних, спеціалізовані програмні продукти, спеціальна техніка захисту інформації тощо.

Для підготовки кадрів для інформаційно-аналітичних підрозділів НПУ доцільно було б створити групи (з ретельним відбором кандидатів на навчання) з поглибленим вивчанням спеціальних технічних дисципліни у галузі інформаційних технологій; групи з поглибленим вивченням спеціальних юридичних дисциплін.

Оцінка результативності інформаційно-аналітичної діяльності будується на сукупності вимог повноти, достовірності, оперативності та цінності інформації, задіяної у процесі управління. Оцінювати ефективність необхідно з позиції цільових показників системи інформаційно-аналітичного забезпечення управління органами внутрішніх справ.

Підсумовуючи вищесказане, слід зазначити, що одним з основних завдань держави в рамках боротьби зі злочинами, скоєними з використанням інформаційних технологій, є підготовка та перепідготовка кадрів правоохоронних органів, які здатні ефективно попереджати, виявляти, документувати та розслідувати зазначені категорії злочинів. В рамках підготовки та перепідготовки таких кадрів необхідно дати здобувачам не тільки знання законодавства, виробити вміння та навички його застосування, а й розвинути здатність кожного співробітника органів внутрішніх справ до самостійного навчання, постійного вдосконалення своїх професійних знань,

навичок та умінь.

Список використаних джерел:

1. Хахановський В. Г. З досвіду підготовки кадрів для підрозділів кіберполіції. Всеукр. наук.-практ. конф. *Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС і навчальному процесі,* 2016. Львів, с. 304-306.

2. Мовчан А. В. Актуальні проблеми підготовки фахівців у галузі застосування сучасних інформаційних технологій. *Науковий вісник Національної академії внутрішніх справ*, 2012. № 1, с. 40- 46.

3. Федоренко О. Сучасні тенденції удосконалення професійної підготовки майбутніх офіцерів поліції. *Новий колегіум, 2016.* № 4, с. 42-52.

4. Кудінов В. А. Вирішення проблем добору та підготовки кадрів правоохоронців щодо протидії кіберзлочинності. *Кадровий вісник*, 2011. № 1, с. 51-68.

УДК 004.77

КУЗОВКО ВЛАДИСЛАВ ОЛЕКСАНДРОВИЧ

курсант 2 курсу факультету №4,

Харківського національного університету внутрішніх справ,

СВІТЛИЧНИЙ ВІТАЛІЙ АНАТОЛІЙОВИЧ

науковий керівник

кандидат технічних наук, доцент,

доцент кафедри протидії кіберзлочинності

Харківського національного університету внутрішніх справ,

ORCID http://orcid.org/0000–0003–3381–3350

ІНФОРМАЦІЙНА СИСТЕМА ДЛЯ ЗАБЕЗПЕЧЕННЯ УКРАЇНСЬКИХ ЗАХИСНИКІВ АКТУАЛЬНИМИ ПЕРЕВІРЕНИМИ ДАНИМИ ПРО ВОРОГА ТА КООРДИНАЦІЇ СИЛ ОБОРОНИ

Інформаційна система DELTA - це захищена мережа, що здатна стежити та обмінюватись в реальному часі розвідданими про ворожі угрупування, аж до

бойового порядку ворожого підрозділу, який перебуває в русі, та боєздатність окремого окупанта. Також вона в змозі планувати бойові завдання. Для зручності та більшої координації дій різних підрозділів Delta відображає інформацію в цифровій мапі.

Створена фахівцями з України та в партнерстві з країнами НАТО, для отримання переваги на полі бою під час війни з росією. Її можуть використовувати збройні сили, МВС, Нацгвардія, Територіальна оборона та мобільні оператори, завдяки чому українці діють набагато швидше за окупантів.

За допомогою інтегрованих телеграм ботів , «єВорог» та «STOP Russian War» навіть пересічний громадян, який пройшов автентифікацію, може повідомляти оперативну інформацію, яку може знати людина, яка перебуває безпосередньо поруч з позиціями бойовиків, не дивлячись чи це передові позиції чи тил зосередження військ.

Delta є хмарним рішенням і вже зараз впроваджує стандарти НАТО та останні тренди індустрії, такі як «cloud native environment», «zero trust security», «multi domain operations» [1].

Так як росія веде проти нашої країни запеклу війну не тільки на землі чи в небі, а й у кіберпросторі, орківські спецслужби кожного дня намагаються проникнути у систему, тому в Delta у кожного користувача є свій обмежений рівень доступу та даних, які він може бачити, відповідно до його посади. Це є превентивним захистом від людскої помилки, технічний захист засекречено.

Система застосовується від початку вторгнення, можно сказати, що вона брала активну участь при обороні Києва, та допомогла захисникам розбити 40 кілометрову колону окупаційної армії, яку виявили безпілотними літальними апаратами, а оборонці знайшли найкраще місце для більш ефективного перехоплення [2].

Також, в західних ЗМІ високо оцінюють вклад Delta у визволення Херсона. Географічне розташування міста обов’язково мало би ізолювати окупантів [3]. Склади та пункти управління активно "проганялися" через інформаційну систему, що негативно впливало на боєздатність ворогів.

Список використаних джерел:

1. Українську систему ситуаційної обізнаності презентували на щорічному заході НАТО. Про що йдеться?. *Громадське телебачення - Останні новини дня, всі надзвичайні новини в Україні*. URL: https://hromadske.ua/posts/ukrayinsku-sistemu-situacijnoyi-obiznanosti-prezentuvali-na-shorichnomu-zahodi-nato-pro-sho-jdetsya (дата звернення: 21.11.2022).

2. Унікальну українську систему ситуаційної обізнаності Delta презентували на щорічному заході НАТО • Mezha.Media. *Mezha.Media*. URL: https://mezha.media/2022/10/28/delta-for-nato/ (дата звернення: 20.11.2022).

3. Jakes L. For Western Weapons, the Ukraine War Is a Beta Test. *The New York Times*. URL: https://www.nytimes.com/2022/11/15/world/ europe/ukraine-weapons.html (дата звернення: 20.11.2022)

УДК 37.1174

МАЛЯРЕНКО ДМИТРО СЕРГІЙОВИЧ

курсант 2 курсу факультету №4,

Харківського національного університету внутрішніх справ,

СВІТЛИЧНИЙ ВІТАЛІЙ АНАТОЛІЙОВИЧ

науковий керівник

кандидат технічних наук, доцент,

доцент кафедри протидії кіберзлочинності

Харківського національного університету внутрішніх справ,

ORCID http://orcid.org/0000–0003–3381–3350

ІНФОРМАЦІЙНИЙ ПОРТАЛ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

З метою організації інформаційно-аналітичного забезпечення поліції було розроблено Положення про інформаційно-телекомунікаційна систему «Інформаційний портал Національної поліції України», який був затверджений Наказом Міністерства внутрішніх справ України 03.08.2017 №676. Інформаційний портал Національної поліції України» (далі - ІПНП) – це

сукупність технічних і програмних засобів, призначених для обробки відомостей, що утворюються у процесі діяльності Національної поліції України та її інформаційно-аналітичного забезпечення.

Призначення [1]:

1. Формування інформаційних ресурсів ЄІС МВС.
2. Обробка інформації, яка утворена в процесі діяльності поліції.
3. Аналітична обробка інформації, отриманої з автоматичної фото- і відеотехніки.
4. Надання безпосереднього оперативного доступу до інформаційних ресурсів ЄІС МВС.
5. Генерація інтерфейсів та функціонування вебсервісів для здійснення інформаційної взаємодії органів (підрозділів) поліції з іншими органами державної влади, органами правопорядку іноземних держав, міжнародними організаціями.
6. Здійснення пошукових та аналітичних функцій для використання інформації з інформаційних ресурсів (баз даних) поліції, МВС та інших органів державної влади в межах службової діяльності відповідно до рівня доступу і повноважень за запитом або регламентом.
7. Використання програмних компонентів геоінформаційних підсистем для візуалізації інформації у вигляді електронних карт, автоматичної зміни зображеного образу об'єкта в залежності від зміни його характеристик, зміни масштабу та деталізації картографічної інформації в інформаційних ресурсах.
8. Забезпечення автоматизації процесів управління силами та засобами поліції.
9. Забезпечення електронного документообігу в органах (підрозділах) поліції, обміну електронними документами з МВС.
10. Комплексний захист інформації та розмежування доступу до інформації, що зберігається в базах даних системи ІПНП.

Структура системи ІПНП.

Складовими системи є:

- центральний програмно-технічний комплекс;

- автоматизовані робочі місця користувачів;
- електронна комунікаційна мережа доступу;
- комплексна система захисту інформації.

Основна мета Інформаційного порталу [2]**:**

- об'єднання інформації щодо заяв і повідомлень про кримінальні правопорушення, що надійшли до органів поліції;
- забезпечення контролю за додержанням законності під час прийняття та реєстрації заяв і повідомлень;
- моніторинг стану оперативної обстановки в державі;
- забезпечення інформаційно-аналітичної підтримки діяльності поліції;
- встановлення зв'язків між даними, що мають значення для кримінального провадження та справ про адмін. правопорушення;
- формування статистичної звітності про результати роботи та дотримання законності органами (підрозділами) поліції.

Облік об'єктів ІП в "ЄО" ведеться за такими категоріями:

- заяви і повідомлення про кримінальні правопорушення та інші події;
- учасники кримінального правопорушення та іншої події;
- речі, документи та майно, пов'язані з учиненням правопорушення та іншою подією [3].

Висновок. Формування інформаційного порталу "Єдиний облік" здійснюється за допомогою програмно-технічних засобів системи "ІПНП", що забезпечує наповнення та підтримку в актуальному стані інформаційних ресурсів баз (банків) даних, що входять до ЄІС МВС, а також забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу, електронної взаємодії з МВС та іншими органами державної влади.

Список використаних джерел:

1. Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України». *Офіційний*

вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/z1059-17#Text (дата звернення: 22.11.2022).

2. ІПС ЛІГА:ЗАКОН - система пошуку, аналізу та моніторингу нормативно-правової бази. *LIGA:ZAKON*. URL: https://ips.ligazakon.net/document/RE33710?an=1 (дата звернення: 22.11.2022).

3. «Сучасні інформаційні технології в діяльності Національної поліції України». *Дніпропетровський державний університет внутрішніх справ*. URL: https://dduvs.in.ua/2022/11/11/suchasni-informatsijni-tehnologiyi/ (дата звернення: 22.11.2022).

УДК: 004.8; 004.9

МАТВІЙЧУК АНДРІЙ ОЛЕКСАНДРОВИЧ

курсант 1 курсу факультету №4,

Харківського національного університету внутрішніх справ,

СВІТЛИЧНИЙ ВІТАЛІЙ АНАТОЛІЙОВИЧ

науковий керівник

кандидат технічних наук, доцент,

доцент кафедри протидії кіберзлочинності

Харківського національного університету внутрішніх справ,

ORCID http://orcid.org/0000–0003–3381–3350

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ТА РОБОТЕХНІКИ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Сучасні технології пішли далеко вперед. Кожен рік робляться нові відкриття, провідний, на мою думку, є штучний інтелект, який постійно покращується і з кожним роком він становиться все більш розумний, тому використання його в правоохоронній системі є логічним розвитком.

Під штучним інтелектом (ШІ) розуміють комплекс технологічних рішень, що дозволяє імітувати когнітивні функції людини (включаючи самонавчання та пошук рішень без заздалегідь заданого алгоритму), і отримувати при виконанні

конкретних завдань результати, які можна порівняти як мінімум із результатами інтелектуальної діяльності [1].

Штучний інтелект є досить корисним і його використовують в багатьох системах, таких як: банківські системи, військові прилади, програмні забезпечення т.д., тому необхідно його впровадити і в криміналістику. Сучасність показує нам те, що більшість злочинів перейшло до мережі інтернет і використовує його для збагачення або здобуття інших цілей за допомогою інтернет мережі.

Прикладом найбільш простого використання ШІ є автоматизовані інформаційно-пошукові системи, які дають змогу отримувати інформацію о можливих напрямах розслідування кримінальних правопорушень.

Криміналістична реєстрація – науково розроблена система фіксації, накопичення та оброблення криміналістично-значущої інформації про злочини, осіб, які їх вчиняють, про засоби та способи їх дій.

Система криміналістичної реєстрації складається з низки підсистем (елементів), які називаються «обліками». Поняттям «облік» охоплюється і сама процедура обліку, тобто дії щодо збирання, накопичення, систематизації, оброблення, аналізу та надання співробітникам правоохоронних та інших державних органів криміналістичної значущої інформації або її матеріальних носіїв.

Також важливі програми: це ідентифікація автомобілів, які перебувають у розшуку за допомогою штучного інтелекту в відеокамерах; розпізнавання зловмисника за допомогою голосу.

Крім того, існують програми контент- та латентно-семантичного аналізу, які надають можливість розшифрувати текст, який написав зловмисник, з яким посиланням написаний даний текст та які емоції були у автора.

До того ж, використовуються штучний інтелект, який допомагає виявляти аномалії під час проведення фінансових транзакцій, під час укладання господарських договорів. Є спеціалізований софт розпізнавання незвичайних

коливань цін на активи, що вказують на інсайдерську торгівлю чи кримінальну поведінку на фінансових ринках [2].

У різних країнах світу під потреби правоохоронних органів адаптують ШІ (наприклад, безпілотних літальних апаратів, дронів, роботів тощо). Безпілотники використовують у якості спеціального техніко- криміналістичного засобу, зокрема для розвідки та фотографування ситуацій, які виникають у важкодоступних місцях.

Останнім часом у практиці криміналістів різних країн світу використовують роботів для проведення експертиз. Наприклад, робот здатний завдавати удари по одягу, нанесеному на манекен, у тому числі різними ножами, під різними кутами, з різною швидкістю. Криміналісти аналізують сліди, що залишаються при цьому в одязі та зразках тканин. Така система покликана допомогти криміналістам зрозуміти, як поводиться ніж при контакті з одягом і різними тканинами. Якщо удари по манекену буде завдавати людина, в імітаційний процес може вкрастися помилка.

Безумовно, все це допомагає вести більш ефективнішу боротьбу зі злочинністю. Всі приклади, що були наведені вище, використовуються правоохоронцями в усьому світі. Вони спрощують роботу поліцейських, криміналістів, захищають правоохоронців від нещасних випадків чи надмірної агресії злочинців, а також підвищують безпеку населення.

Список використаних джерел:

1. Автоматизированные информационно-поисковые системы. URL: https://scicenter.online/kriminalisticheskaya-tehnika-scicenter/avtomatizirovannyie-informatsionno-poiskovyie-158937.html (дата звернення: 20.11.2022).

2. Штучний інтелект і робототехніка на службі поліції. URL: https://matrix-info.com/shtuchnyj-intelekt-i-robototehnika-na-sluzhbi-politsiyi/ (дата звернення: 20.11.2022).

УДК 004.77

НЕСТЕРОВ ДМИТРО СЕРГІЙОВИЧ,

курсант 2 курсу факультету №4,

Харківського національного університету внутрішніх справ,

СВІТЛИЧНИЙ ВІТАЛІЙ АНАТОЛІЙОВИЧ

науковий керівник

кандидат технічних наук, доцент,

доцент кафедри протидії кіберзлочинності

Харківського національного університету внутрішніх справ,

ORCID http://orcid.org/0000–0003–3381–3350

ЕТИЧНІ ПИТАННЯ В ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЯХ

Інформаційні технології (ІТ) визначають компоненти, які використовуються для зберігання, отримання та маніпулювання інформацією на мінімальному рівні з сервером, що має операційну систему. Інформаційні технології мають широку сферу застосування в освіті, бізнесі, охороні здоров'я, промисловості, банківському секторі та наукових дослідженнях на великому рівні. З розвитком інформаційних технологій, необхідно володіти знаннями з питань безпеки, конфіденційності та основних негативних наслідків використання інформаційних технологій. Для вирішення цих питань в ІТ-суспільстві важливо з'ясувати етичні аспекти [1]. Нижче ми розберемо ці питання та проблеми.

Деякі з основних етичних проблем, з якими стикаються ІТ, є наступними:

– Особиста конфіденційність.

- Право доступу.
- Шкідливі дії.
- Патенти.
- Авторське право.
- Комерційна таємниця.
- Відповідальність.
- Піратство.

Нижче наведено пояснення їхнього впливу:

Особиста конфіденційність. Це важливий аспект етичних питань в інформаційних технологіях. ІТ полегшують користувачам, які мають власне обладнання, операційну систему та програмні засоби, доступ до серверів, які з'єднані один з одним та з користувачами мережею. Завдяки поширенню мережі у великих масштабах відбувається передача даних або інформації у великому обсязі, що призводить до прихованих шансів розкриття інформації та порушення приватності будь-яких осіб або групи осіб. Збереження конфіденційності та цілісності даних є основним викликом для ІТ-спільноти та організацій. Випадкове розкриття інформації невідповідним особам та положення щодо захисту точності даних, також входить в питання конфіденційності.

Право доступу. Другим аспектом етичних питань в інформаційних технологіях є право доступу. Право доступу стає пріоритетним питанням для ІТ та кіберпростору з великим розвитком технологій. Розвиток електронної комерції та електронних платіжних систем в Інтернеті загострив це питання для різних корпоративних організацій та урядових установ. Мережа в Інтернеті не може бути захищена від несанкціонованого доступу. Як правило, системи виявлення вторгнень використовуються для визначення того, чи є користувач зловмисником або належним користувачем [2].

Шкідливі дії. Під шкідливими діями в комп'ютерній етиці розуміють шкоду або негативні наслідки для ІТ, такі як втрата важливої інформації, втрата майна, втрата права власності, знищення майна та небажані суттєві впливи. Цей принцип етичної поведінки обмежує будь-яких сторонніх осіб від використання

інформаційних технологій у спосіб, що призводить до будь-яких втрат для користувачів, працівників, роботодавців та широкої громадськості. Як правило, такі дії полягають у навмисному знищенні або зміні файлів і програм, що призводить до серйозних втрат ресурсів. Для відновлення від шкідливих дій необхідні додаткові зусилля та час для видалення вірусів з комп'ютерних систем.

Патент. З патентом етичних проблем складніше мати справу. Патент може зберегти унікальний і секретний аспект ідеї. Отримання патенту є дуже складним у порівнянні з отриманням авторського права. У випадку з програмним забезпеченням потрібне ретельне розкриття інформації. Власник патенту повинен розкрити всі деталі програми досвідченому програмісту для створення програми.

Авторське право. Фахівці з інформаційної безпеки повинні бути знайомі з необхідною концепцією закону про авторське право. Закон про авторське право є дуже потужним правовим інструментом захисту комп'ютерного програмного забезпечення, як до порушення безпеки, так і, звичайно, після порушення безпеки. Таке порушення може полягати в неправильному поводженні з даними, комп'ютерними програмами, документацією та іншими подібними матеріалами, а також у їх неправомірному використанні. У багатьох країнах законодавство про авторське право змінюється або переглядається з метою забезпечення чітких законів для захисту комп'ютерних програм [0].

Комерційна таємниця також є важливою етичною проблемою в інформаційних технологіях. Комерційна таємниця захищає щось цінне і корисне. Цей закон захищає приватні аспекти ідей, які відомі лише першовідкривачу або його довіреним особам. Після розголошення комерційна таємниця втрачається як така і захищається лише законом про комерційну таємницю. Застосування закону про комерційну таємницю є дуже широким у комп'ютерній сфері, де навіть невелика перевага у розвитку програмного чи апаратного забезпечення може забезпечити значний конкурентний вплив [3].

Відповідальность. При прийнятті етичних рішень слід враховувати питання відповідальності. Розробник програмного забезпечення дає

користувачеві обіцянки та запевнення щодо характеру та якості продукту, які можуть бути обмежені як явна гарантія. Програмісти або роздрібні торговці мають законне право визначати явні гарантії. Таким чином, вони повинні бути практичними, коли вони визначають будь-які претензії та прогнози щодо можливостей, якості та характеру свого програмного чи апаратного забезпечення. Кожне слово, сказане ними про свій продукт, може мати таку ж юридичну силу, як і викладене в письмовій формі. Всі угоди повинні бути укладені в письмовій формі для захисту від відповідальності. Відмова від прямих гарантій може звільнити постачальника від відповідальності за неформальні, спекулятивні заяви або прогнози, зроблені на стадії укладання угоди.

Піратство - це діяльність, при якій створюється незаконна копія програмного забезпечення. Власник програмного забезпечення повністю вирішує, чи можуть користувачі створювати резервні копії свого програмного забезпечення. У міру того, як розвиваються закони, спрямовані на захист авторських прав, розглядається також законодавство, яке б зупинило несанкціоноване копіювання програмного забезпечення. Індустрія програмного забезпечення готова до боротьби з піратством. Суди розглядають все більшу кількість позовів щодо захисту програмного забезпечення [4].

Висновки: нами окреслені лише основні складники етичних питанньв інформаційних технологіях. Багатовимірність представлених досліджень дає змогу говорити про широке коло проблем, яке охоплює інформаційна етика як безпосередньо, так і опосередковано. Зважаючи на мінливість предмета досліджень, необхідним є схоплювання та адаптування останніх світових тенденцій в галузі поширення інформації, їх осмислення та відображення через призму інформаційної етики. В цілому питання етики у кіберпросторі вимагають подальшого дослідження та розробки ефективних механізмів впровадження їх у практику.

Список використаних джерел:

1. Український інститут інтелектуальної власності // вебсайт. URL: https://ukrpatent.org/uk (дата звернення: 10.10.2022).

2. Право доступу //вебсайт. URL: https://www.wikiwand.com/uk/%D0%9F%D1%80%D0%B0%D0%B2%D0%BE_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D1%83 (дата звернення: 10.10.2022).

3. Комерційна таємниця // вебсайт. URL: https://pidru4niki.com/78148/pravo/komertsiyna_tayemnitsya (дата звернення: 10.10.2022).

4. Кримінальний кодекс стаття 446 Піратство // вебсайт. URL: https://urst.com.ua/ru/uku/st-446 (дата звернення: 10.10.2022).

УДК 378.147:004.34.08

ПРОКОПЕЦЬ КАРІНА СЕРГІЇВНА

курсантка І курсу

Навчально наукового інституту права та підготовки фахівців

для підрозділів Національної поліції

Дніпропетровського державного університету внутрішніх справ,

СИНИЦІНА ЮЛІЯ ПЕТРІВНА

науковий керівник,

кандидат технічних наук, доцент,

доцент кафедри економічної та інформаційної безпеки

Дніпропетровського державного університету внутрішніх справ

СУПУТНИКОВА СИСТЕМА STARLINK, ЇЇ ПЕРЕВАГИ ТА НЕДОЛІКИ

Наразі, сучасний етап розвитку суспільства характеризується переходом до всеохоплюючої інформатизації усіх інституцій і процесів, пов’язаних із формуванням інформаційних ресурсів та технологій. У діяльності Національної поліції все ширше використовуються спеціальні засоби, пошукова техніка, апаратура звуко- та відеозапису, фототехніка, електронно-обчислювальні машини та інші засоби на рівні останніх досягнень науки та техніки [1, с. 7]. Важлива роль розвитку інформаційного забезпечення у процесі здійснення

правоохоронної діяльності підтверджується у наукових працях видатних науковців таких, як Фролової О.Г., Катеринчук І.П. [2, с. 12], Калюжний Р.А. та Ткаченко В.М. та інші.

До основних актуальних питань у правоохоронній сфері можна віднести невідповідність інформаційних систем актуальним потребам правоохоронців та відсутність дієвої інтегрованої інформаційної системи. Саме тому впровадження сучасних інформаційних технологій є нагальною потребою.

Starlink це спутнікова система, головне завдання якої забезпечення високошвидкісного широкосмугового доступу до Internety у важкодоступних місцях. Проект Starlink створений у США компанією SpaceX під керівництвом Ілона Маска. Перший запуск тестових пристроїв відбувся у лютому 2018 року. А вже у травні 2019 року з допомогою ракети Falcon 9 на низьку навколоземну орбіту було виведено перші 60 супутників. Супутник Starlink - це пласка панель вагою 295 кілограмів із чотирма антенами та сонячною батареєю, датчиком орієнтування за зірками, а також із двигунами, що працюють на криптоні, за допомогою яких супутник може маневрувати та обирати іншу орбіту. На відміну від геостаціонарних супутників, Starlink не зависають над планетою, а мчать навколо неї з величезною швидкістю - приблизно 27 000 км/год. Супутники перебувають на низькій навколоземній орбіті, приблизно у 550 кілометрах над поверхнею Землі, тому затримка сигналу майже непомітна - до 20 мсекунд. Кожний користувальницький термінал оснащений GPS датчиком. Щоб знаходити супутники у небі, він має чітко визначити свої координати Землі. Тому SpaceX має технічну можливість обмежувати роботу абонентського обладнання. Якщо якась країна входить у зону покриття Starlink, але SpaceX ще не отримала дозвіл від місцевого державного регулятора, обладнання у цій країні може не працювати [3].

До основних переваг системи інтернету Starlink можна віднести: всеосяжність, а саме уся земна куля буде охоплена доступом до мережі. Наразі на сьогоднішній день половина з 3,8 мільярдів людей не мають доступу до мережі Інтернету через своє місцезнаходження. Це стосується віддалених сіл і

міських бідних районів; відносно низька цінова категорія системи інтернету Starlink, а саме на забезпечення відносно недорогого широкосмугового супутникового доступу до системи Інтернету; гарна швидкість, а саме згідно результатів досліджень швидкість інтернету може досягати 157 Мбіт/с. У цьому випадку швидкість повернення становить близько 27 Мбіт/с, а затримка становить близько 44 мс. Над на майбутнє прогнозована швидкість буде сягатиме рівня 1 Гбіт/с.

До основних недоліки системи інтернету Starlink можна віднести наступне: складність підключення до мережі, а саме не кожен смартфон може підключитися до мережі безпосередньо. Для повноцінного приєднання потрібні додаткове обладнання таке як потрібен трансивер, фазована антена й термінал для управління мережею. Вартість якої наразі складає близько 300 у.о.; обмежений доступ до системи інтернету, а саме, згідно розрахунків, Розрахунки показують, що якби в космосі було 12000 у космосі зможуть обслуговувати не більше 14,3 млн наземних терміналів супутників, а також й те, що супутники Starlink заважають і заважатимуть астрономам тому, що супутники дуже яскраві і заважають стежити за потенційно небезпечними для нашої планети Земля астероїдами та використовують майже аналогічні радіочастоти, що й астрономи.

Список використаних джерел:

1. Синиціна Ю.П., Прокопов С.О., Рижков Е.В. Спеціальна техніка в правоохоронній діяльності: навч. посібник. Дніпро: ДДУВС. 2021. 256 с.

2. Катеринчук І.П. Правові засади інформаційного забезпечення діяльності правоохоронних органів України: автореф. дис. на здобуття наук.ступеня д-ра юрид. наук : 12.00.07. Київ, 2015. 41 с.

3. Starlink: що це таке, як працює та хто зможе ним користуватися в Україні: веб-сайт. URL:https://ms.detector.media/it-kompanii/post/29166/2022-03-13-starlink-shcho-tse-take-yak-pratsyuie-ta-khto-zmozhe-nym-korystuvatysya -v-ukraini/ (дата звернення: 16.11.2022)

УДК 004.9, 004.3

САЄНКО ДМИТРО ОЛЕКСАНДРОВИЧ

курсант 2 курсу факультету №4

Харківського національного університету внутрішніх справ,

СВІТЛИЧНИЙ ВІТАЛІЙ АНАТОЛІЙОВИЧ

науковий керівник

кандидат технічних наук, доцент,

доцент кафедри протидії кіберзлочинності

Харківського національного університету внутрішніх справ,

ORCID http://orcid.org/0000–0003–3381–3350

ШЛЯХИ ФОРМУВАННЯ СИСТЕМИ ПІДГОТОВКИ КАДРІВ У СФЕРІ КІБЕРБЕЗПЕКИ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ УКРАЇНИ В УМОВАХ РОЗВИТКУ ЦИФРОВОГО СУСПІЛЬСТВА УКРАЇНИ

Попри динамічне зростання ІТ-сектору, українські державні та приватні ІТ-підрозділи постійно стикаються з браком кваліфікованих та досвідчених фахівців з інформаційної безпеки, в тому числі й кібербезпеки. Як свідчать роботодавці, випускникам цієї спеціальності часто бракує спеціалізації чи практичних навичок. У свою чергу експерти у сфері кібербезпеки зазначають про негайну потребу у перегляді наявних освітніх програм та запровадженні більш сучасних підходів в навчанні, як для працівників державної, так і приватної кібербезпеки. Крім того, потребує вдосконалення й система підвищення кваліфікації фахівців із кібербезпеки, яка вимагає їх успішну адаптацію до професійної діяльності, а також постійний освітній контакт з професійною спільнотою на всій території країни. У річному звіті Cisco за 2017 – 2018 роки з інформаційної безпеки вказується, що “миттєві атаки” стають усе складнішими, більш частими та тривалими. Більш третини кіберкомпаній, які були вражені хакерською атакою, понесли матеріальні збитки близько 20% прибутку. За даними спеціалістів протягом року 30,01% комп’ютерів Інтернет-користувачів у

світі хоча б один раз зазнавали веб-атаки класу Malware. Все це вказує на те, що потреба у фахівцях, які забезпечують захист інформаційних даних, буде зростати. Тому проблема підготовки справжніх професіоналів в області кібербезпеки є актуальною [1]. У цьому аспекті, надання послуг з навчання комп'ютерній грамотності, а також навчання щодо розроблення, модифікації, тестування та технічної підтримки програмного забезпечення можна забезпечити шляхом використання можливостей і потужностей віртуально-навчальних лабораторій, які на сьогодні активно впроваджуються "в життя" недержавними суб'єктами кібербезпеки, та введення яких у практичну площину стане дієвим розвитком всієї системи підготовки кадрів у сфері ІТ-технологій. Основним завданням віртуальної лабораторії інформаційних технологій є моделювання процесів обробки даних у сучасних інформаційних системах та мережах. Програмною основою віртуальної лабораторії є технології хмарних обчислень, які доступні, у тому числі, у режимі віддаленого доступу через канали глобальної зв'язку, наприклад Інтернету [2]. Як відомо системні вимоги щодо розгортання хмарної інфраструктури передбачають використання двох комп'ютерів, один з яких виконуватиме функції сервера управління та первинного сховища, а інший відповідатиме за роботу віртуальних машин (гіпервізор) та містить вторинне сховище. Широкий спектр можливостей спеціального програмного забезпечення для віртуалізації надає унікальні можливості при організації навчального процесу, що і підтверджує доцільність та можливість його широкого використання як основного засобу формування системи знань, умінь та навичок при вивченні загальних і професійних цифрових компетенцій, ІТ-технологій та знань у сфері кібербезпеки, а також при формуванні системи умінь в галузі інформаційних технологій. Серед переваг застосування віртуально-навчальної лабораторії для моделювання процесів у кібербезпеці для освітніх потреб державної і приватної кібербезпеки слід виділити:

– у загальноосвітньому аспекті:

• формування фахових компетенцій, які можуть бути безпосередньо перенесені в реальність;

• підвищення якості самостійної навчально-пізнавальної діяльності;

• зацікавленість у вивченні матеріалу, розвиток мотиваційної діяльності;

• доступність та автоматизацію операцій;

• постійне удосконалення програмних систем та технологій тощо;

– у організаційно-технічному аспекті:

• заощадження на придбанні апаратного забезпечення;

• доступ до комп'ютерів віртуально-навчальної лабораторії можна забезпечити із традиційних та мобільних платформ, використовуючи стандартні протоколи (RDP, SSH, VNC);

• можливість використання різноманітних операційних систем;

• можливість використання потенційно-небезпечного програмного забезпечення без загрози ушкодження реальних комп'ютерів;

• можливість створення необхідних апаратних конфігурацій;

• можливість об'єднання віртуальних машин у локальну мережу та доступ до них засобами поширених протоколів; високу мобільність працівників та кібертренерів (викладачів), що вирішує питання "прив'язаності" до певного місця, а також створює можливості для самостійної роботи фахівців у сфері кібербезпеки.

Основними недоліками віртуально-навчальної лабораторії та хмарних технологій в цілому є: безпека інформації, постійне з'єднання з мережею Інтернет та можливість втрати даних у "хмарі". Віртуальні освітні технології в світі тільки розпочали конкурувати з традиційними формами навчання, та в умовах сьогодення є безсумнівною підтримкою та стимулом до плідного навчання та цікавої наукової діяльності. Використання та подальше впровадження віртуально-навчальної лабораторії для моделювання процесів у кібербезпеці для потреб державної і приватної кібербезпеки стане ефективним інструментом навчання, який дозволить рухатися власною освітньою

траєкторією, та розширить коло навчальних задач і збагатить їх сучасним змістом.

Список використаних джерел:

1. Buriachok, V. L., Shevchenko, S. M., & Skladannyi, P. M. (2018). Віртуальна лабораторія для моделювання процесів в інформаційній та кібербезпеці як засіб формування практичних навичок студентів. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка;, 2(2), 98-104. https://doi.org/10.28925/2663-4023.2018.2.9810

2. Арсенович, Л. А. (2022). Подальший розвиток системи професійного навчання фахівців із кібербезпеки в умовах розвитку цифрових технологій. Таврійський науковий вісник. Серія: Публічне управління та адміністрування, (3), 3-13. https://doi.org/10.32851/tnv-pub.2022.3.1

UDK 372.881.111.1

SALOVA OKSANA VIKTORIVNA

a fourth-year cadet of faculty No.4

Kharkiv National University of Internal Affairs,

SAZANOVA LARYSA SERHIIVNA

scientific adviser

senior lecturer of the department of foreign languages

of faculty No.4

Kharkiv National University of Internal Affairs

EFFECTIVE INNOVATIVE TECHNOIOGIES IN TEACHING FOREIGN LANGUAGES AT HIGH EDUCATION INSTITUTIONS OF THE MINISTRY OF INTERNAL AFFAIRS

The era of the twenty-first century is often regarded as an era of technology. Technology, today, plays a very important role in our life. It is seen as a basis of growth of an economy. “An economy which is poor in technology can never grow in today’s scenario. This is because technology makes our work much easier and less time

consuming. The impact of technology can be felt in every possible field one such field is education" [1, p. 33].

Education is a purposeful cognitive people's activity to acquire knowledge, abilities and skills or to improve them. Modern education is the implementation of innovative technologies. The future of the civilization lies in the development of the intellectual and creative potential of its citizens.

The main direction of innovative technologies is the wide use and growth of new information and educational technologies, implementation of computer and network technologies.

Education with the use of innovative technologies qualitatively exceeds conventional education. It integrates processes that cannot be combined within the framework of conventional education: online learning, employment, work, career planning, continuous education. The most common innovative teaching methods are: developmental learning methods, interactive learning methods, project method, game methods of learning, and informational methods of learning.

"Nowadays it is very important that information andknowledge reach their destination as quickly andaccurately as possible. One of the most commonmethods for this is the e-learning" [2, p. 3].

Nowadays the use of the term "technology" in relation to the humanities and socio and economic sciences is the issue among the academics. This historical concept appeared with the connection of technical progress. It is most significant in the activities where technology is used as a set of knowledge about methods and means of processing materials.

The use of computer programs at foreign language classes at higher educational institutions means increasing motivation and desire to learn English; easier perception of the material in the classroom of at home (the cadets and students listen to audio and video recordings and get used to the pronunciation of various speakers and it makes the learning process easier); perception of new material, its primary and subsequent memorization; a means of increasing interactive and communicative activity; expanding knowledge on the main educational topic.

Training programs help to combine sensory, auditory and visual components of influence on the perception of the text.

The most frequently used method of memorizing foreign words is repetition. Learners repeat foreign words several times and memorize terms, phrases, and collocations.

When using this method, it is very important to make pauses or breaks at which new material is “recorded” by the brain in long-term memory.

An accessible and universal method of replenishing vocabulary is watching videos (films, cartoons, series, TV shows, news, etc.) in a foreign language.

At first the learners listen to a native speaker, then watch the video material that gives an opportunity to get acquainted with various phrases that occur in the language every day. The learners also watch the video, sometimes with subtitles and it makes the information more visual, accessible and interesting.

For successful learners’ vocabulary memorization at foreign language classes, it is important to develop a set of exercises based on a certain professionally oriented text. Using computer programs, one can immediately submit the key lexical units that students should know having studied this topic.

The technological conditions are the formation of information and communication environment by using computer and telecommunication networks in the system of foreign language teaching to master modern means of information and information technologies both by pedagogical staff and those who study.

The use of innovative technologies in teaching foreign languages at higher educational institutions allows creating a fundamentally new informational educational sphere that provides wide opportunities for educational activities, increases motivation, develops independence, ensures individualization and differentiation of the educational process, and supports the modernization of the traditional education system. A solution to this problem is possible if pedagogical methods are changed and innovative technologies are introduced.

References:

1. R. Raja, P. C. Nagasubramani Impact of modern technology in education

Journal of Applied and Advanced Research. Proceedings of the Conference on “Recent Trend of Teaching Methods in Education”. 2018: 3 (Suppl.1) 2018 Phoenix Research Publishers p. 33-35

URL: https://www.researchgate.net/publication/325086709

2. Jozsef Poor, Peter Sasvari, Zsigmond Szalay, Istvan Peto, Norbert Gyurian, Csilla Judit Suhajda, Ferenc Zsigri The implementation and management of e-learning in companies – the state of e-learning in Hungary based on empirical research Journal of engineering management and competitiveness (JEMC) vol. 10, No.1, 2020, 3-14

URL: https://www.academia.edu/79968618

УДК 004.77

TALAN MYKYTA ANDRIIOVYCH

a fourth-year cadet of faculty No.4

Kharkiv National University of Internal Affairs,

SAZANOVA LARYSA SERHIIVNA

scientific adviser

senior lecturer of the department of foreign language of faculty No.4

Kharkiv National University of Internal Affairs

GOOGLE DORKS AS A RESOURSE FOR CRIME INVESTIGATION

Nowadays, the question of finding criminals is very acute, especially if it's a cybercrime. Searching for criminals on the Internet is a very complex and difficult task. But every action done on the Internet leaves its mark. These marks can be used to find information that can help solve a crime. Within OSINT, we can use Google Dorks.

Google Dorks is an information search technique using Google operators (Advanced Search Operators). Google search operators are special characters and queries that extend the capabilities of plain text searches. With the help of Google Dorks, you can perform a variety of OSINT and cyber security tasks, identify potential vulnerabilities of sites and applications, find, and prevent data leaks, reveal hidden information that was indexed by robots and entered the Search Engine Result Page.

Google Dorks is actively used by Pentesters, reverse engineers, researchers and analysts of the IT sphere for the purpose of auditing and identifying security "holes" in systems and electronic resources [1].

Google Dorks allows you to collect quite large amounts of information: people search (names and surnames, nicknames), search for information in social networks, metadata and log files, e-mails, files, and documents (pdf, doc, txt, sql, mp3, jpeg, avi, etc.), web pages (URL), web services and servers, network Devices (IoT), administrative parts of electronic resources and applications (admin panels), vulnerabilities in electronic resources and systems.

Tasks that Google Dorks helps to solve: search for official, administrative, confidential, technically faulty web pages, login and authorization forms that are freely accessible and create security risks, search for vulnerable URLs to includes, injections, traversals, fuzzing, etc., search for official, confidential, user files and folders that are publicly accessible and create security risks, search for any information leaks, databases, usernames and accesses that are publicly available and compromise the system [2].

Google is a fast and effective way of collecting various information on the Internet, accumulating data/facts from open sources (OSINT). In fact, Google Dorks can act as a manual search scanner and parser for cybersecurity audits and OSINT investigations, which is very useful in law enforcement.

“Indeed, the right tool can determine whether you harvest the right information. It follows that the more tools you have in your portfolio, the more flexible your OSINT capabilities are likely to be” [3, p.1].

References

1. Useful Google Dorks for Open-Source Intelligence Investigations . URL: https://www.maltego.com

2. What is OSINT? URL: https://www.linkedin.com/pulse

3. Aleksandra Bielska, Noa Rebecca Kurz, Yves Baumgartner, Vytenis Benetis) Open-source intelligence tools and resources handbook 2020 URL: https://i-intelligence.eu/uploads/public-documents/OSINT_Handbook_2020.pdf

УДК 621.311.6

ТАРАНЕНКО АННА ЮРІЇВНА

курсант Національної академії Державної прикордонної служби України

БАСАРАБ ОЛЕКСАНДР КОРНІЙОВИЧ

кандидат технічних наук, доцент,

викладач кафедри телекомунікаційних та інформаційних систем

Національної академії Державної прикордонної служби України

ЗАБЕЗПЕЧЕННЯ ЕЛЕКТРОЖИВЛЕННЯМ НАЗЕМНИХ КОМПЛЕКТІВ СУПУТНИКОВОГО ЗВ'ЯЗКУ STARLINK В ПОЛЬОВИХ УМОВАХ

На сьогоднішній день глобальні інформаційні технології змінюють традиційні схеми спільної роботи і управління. Стрімко зростає потреба в телекомунікаціях, коли постійно потрібно бути на зв'язку і мати можливість доступу до даних. Тим більше важко переоцінити важливість зв'язку та передачі даних при управлінні військовими підрозділами та при здійсненні бойових дій. Органи та підрозділи Державної прикордонної служби України у взаємодії із Збройними силами України приймають безпосередню участь у відсічі повномасштабного вторгнення Російської Федерації на територію України та знаходяться в місцях безпосереднього зіткнення з ворогом. Зрозуміло, що в польових умовах основний вид зв'язку – це радіо- та супутниковий зв'язок.

На сьогоднішній день в світі існує чимало супутникових систем зв'язку, різних форм власності, з відмінними характеристиками та параметрами. Найбільш розповсюджені системи супутникового зв'язку: Iridium, Globalstar, Emsat, Inmarsat, Ka-Sat та Starlink. Вирішальну роль в прийнятті рішення на використання конкретної системи супутникового зв'язку відіграють наступні фактори – зона покриття, надійність та швидкість передачі даних, габарити та мобільність терміналів, країна-власник системи тощо.

Starlink – глобальна супутникова система, що розроблена компанією SpaceX (США) для забезпечення високошвидкісного широкосмугового

супутникового доступу в Інтернет у місцях, де він був ненадійним, дорогим або повністю недоступним. Супутниковий інтернет Starlink сьогодні відіграє важливу роль у боротьбі України проти російської агресії. Завдяки цій мережі космічних супутників, які роздають високошвидкісний бездротовий інтернет у місцях, де він недоступний, українська армія може завдавати точні удари по російських військах та керувати безпілотниками.

Система Starlink складається з трьох головних компонентів: супутників на низьких орбітах, наземних станцій, а також користувацьких терміналів. Супутник працює як посередник – він передає радіосигнал від наземної станції до користувача з терміналом і навпаки. Між самими наземними станціями та користувачами може бути відстань до тисячі кілометрів. Для доступу до супутникового інтернету необхідно мати спеціальний комплект обладнання – термінал, блок живлення та роутер. Комплект встановлює зв'язок із супутником та створює WI-FI мережу для локальних пристроїв. В Державній прикордонній службі України активно використовуються система супутникового зв’язку Starlink. Проте, є суттєвий недолік використання наземних комплектів Starlink у військових цілях – це залежність від електроживлення 220 В промислової мережі, яке в польових умовах, як правило, відсутнє.

Для забезпечення електроживленням у разі відсутності промислової електромережі можна використовувати резервні джерела електропостачання, а саме: бензо- або дизель-генератори, вітроелектростанції, сонячні панелі.

Бензогенератор та дизель-генератор є надійними джерелами електроенергії 220 В, проте, в бойових умовах використання генераторів не завжди є можливим, оскільки вони мають низку демаскуючих факторів – великий рівень шуму та інтенсивне випромінення в інфрачервоному спектрі як при роботі генератора так і тривалий час після вимкнення.

Використання енергії вітру має низку недоліків, які в бойових умовах можна віднести до критичних – непрогнозованість вітрового потоку, великі габарити обладнання – основні з них.

Сонячні енергетика – одне із найперспективніших і динамічних відновлюваних джерел енергії. Відносно невеликі габарити, доступна вартість, можливість нарощування панелей, простота використання та відсутність шуму при роботі є основними перевагами застосування зазначеного джерела живлення в польових умовах. Як недолік можна відмітити розробку додаткового пристрою – адаптера та застосування акумуляторної батареї для забезпечення стабільної роботи у випадках низької сонячної активності та вночі, яка б заряджалася під час інтенсивного сонячного випромінення.

Отже, виходячи з наведеного, для забезпечення стійкого та надійного зв’язку з використанням комплектів Starlink в польових умовах в якості джерела живлення пропонуємо застосовувати сонячні панелі та спеціально розроблений адаптер з акумуляторною системою.

УДК 004.9

ТОВСТИК ВАДИМ ОЛЕКСАНДРОВИЧ

курсант 1 курсу факультету №4

Харківського національного університету внутрішніх справ,

СВІТЛИЧНИЙ ВІТАЛІЙ АНАТОЛІЙОВИЧ

науковий керівник

кандидат технічних наук, доцент,

доцент кафедри протидії кіберзлочинності

Харківського національного університету внутрішніх справ,

ORCID http://orcid.org/0000–0003–3381–3350

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В КРИМІНАЛІСТИЦІ

В наш час дуже поширений розвиток засобів інформатизації (комп'ютерів, комп'ютерних комунікацій, всіляких електронних пристроїв), і через це, з’являються нові технологій обробки, передачі, одержання і збереження інформації. Це все дає нам змогу відкривати нові можливості їхнього застосування в навчальному процесі. Основна функція вузу – підготовити

здобувача освіти до повноцінної життєдіяльності. Щоб випускник знайшов своє місце в суспільстві, він повинен опанувати нові інформаційні технології, навички використання комп'ютера як інструмента професійної діяльності, в тому числі - інструмента, що допоможе в розслідуванні злочинів. Навчанням як використовувати такі технології у ХНУВС займаються кафедра протидії кіберзлочинності факультету № 4 і кафедра кібербезпеки та DATA-технологій факультету № 6. Вони враховують задачі криміналістичної підготовки слідчих, ці технології повинні бути повні предметним змістом у співвідношенні професійної діяльності і процесу навчання. Ці навички підвищують ефективність самостійної роботи учнів, дають нові можливості для освоєння і закріплення професійних навичок, дозволяють реалізувати нові форми і методи навчання. Розвиток інформаційних технологій також надає широкі можливості викладачам: дозволяють швидко поновлювати зміст навчальних програм разом з появою нових технологій і аналізувати поточний стан навчального процесу [1]. Навіть зараз, коли здається що перелік можливостей вже неабияк великий, дані технології продовжують активно розвиватися. Сьогодні в провідних країнах світу приділяється велика увага питанням інформатизації суспільства, тому сучасний етап розвитку суспільства в цих країнах характеризується переходом до повної інформатизації усіх соціальних інституцій і процесів, пов’язаних із формуванням ресурсів і передачею знань. В цих країнах боротьба зі злочинністю ведеться максимально ефективним «фронтом» за допомогою різних державних органів, громадських організацій, громадян. Особливо важлива роль правоохоронним органам, для котрих боротьба зі злочинністю є основною функцією. Зараз ефективність діяльності правоохоронних органів майже повністю залежить від технічного оснащення. Зокрема, в практичній діяльності органів Національної поліції України сьогодні широко впроваджується обчислювальна техніка, створюються локальні мережі, автоматизовані робочі місця, які обладнані сучасними потужними персональними комп’ютерами та базами даних. Це дозволяє максимально звільнити звичайних працівників від роботи над одноманітними операціями, допомагає знаходити оптимальні

рішення при розв’язанні різноманітних питань, дає можливість глибше вивчати процеси, деталізувати їх, забезпечує можливість одночасного розгляду значної кількості фактів у взаємозв’язку та залежності при одночасній обробці різноманітної інформації.

Отже, використання обчислювальної дає нове дихання як до постановки конкретних завдань, так і в виборі оптимальних методів їх вирішення. На підставі вище сказаного, можна зробити висновок, що в умовах прогресивної комп’ютеризації суспільства, у тому числі і правоохоронних органів, основною метою освітнього процесу є надання курсантам, студентам, слухачам вузів МВС України, працівникам правоохоронних органів держави знань, умінь та практичних навичок з інформаційної безпеки та обчислювальної техніки, інформаційного забезпечення правоохоронних органів, які би створили міцне підґрунтя для подальшого засвоєння і ефективного використання ними комп’ютерних технологій у своїй оперативно-службовій діяльності [2].

Список використаних джерел:

1. Інформаційні технології в правоохоронній діяльності : НАВС. Головна сторінка :: НАВС. URL: https://www.naiau.kiev.ua/news/informacijni-tehnologiyi-v-pravoohoronnij-diyalnosti.html (дата звернення: 18.11.2022).

2. Використання нових інформаційних технологій у криміналістичному навчанні | Коментар. Мего-Інфо - Юридичний портал України №1, коментар ЦПК, КПК, КУПАП, ККУ, ЦК. URL: http://mego.info/матеріал/23-використання-нових-інформаційних-технологій-у-криміналістичному-навчанні (дата звернення: 18.11.2022).

УДК 343.98

ТОВСТИК ВАДИМ ОЛЕКСАНДРОВИЧ

курсант 1 курсу факультету №4

Харківського національного університету внутрішніх справ,

СВІТЛИЧНИЙ ВІТАЛІЙ АНАТОЛІЙОВИЧ

науковий керівник

кандидат технічних наук, доцент,

доцент кафедри протидії кіберзлочинності

Харківського національного університету внутрішніх справ,

ORCID http://orcid.org/0000–0003–3381–3350

ВИКОРИСТАННЯ ДРОНІВ В РОБОТІ ПОЛІЦІЇ

В наш час арсенал поліції не обмежується спеціальними засобами відповідно до статті 45 Закону України «Про Національну поліцію», а стає з кожним днем все практичніше і сучасніше. Одним з прикладів модернізації є використання безпілотних дронів. Раніше дрони були лише в арсеналі Державної прикордонної служби, і використовувалися для патрулювання кордону. Але час йде, і технології розростаються й в інші структури МВС. Так, поліцейські почали отримувати дрони DJI Mavic 2, які давно стоять на «озброєнні» структур МВС. Вони дозволяють працівникам поліції України ефективно проводити повітряну рекогносцировку під час супроводження спеціальних операцій, забезпечення публічної безпеки та порядку, а також пошуку зниклих осіб [1]. В арсеналі також присутні дрони DJI Matrice серії 200 та DJI Mavic 2 Enterprise Dual, які можуть записувати відео в якості 4К з висоти до 6 км. Гарним прикладом використання дронів є пошук порушників карантину під час пандемії COVID-19. Поліція у Києві за допомогою безпілотних літальних апаратів шукала порушників карантину у важкодоступних для патрулів місцях. Також на техніку встановили гучномовці та закликали людей дотримуватися обмежень [2]. Під час війни з Російською Федерацією дрони є важливими через те, що можно дослідити територію на якій, можливо, знаходяться окупанти без ризику для свого життя. Поліцейські можуть за допомогою безпілотників побачити де знаходяться бази ворога і доповісти про це військовим, які в майбутньому використають цю інформацію для процесу деокупації. Також їх використовують для гуманітарних місій з евакуації цивільних. Деякі безпілотники обладнані тепловізорами, тому

вони можуть допомогти в пошуку людей після обстрілів. Ще дрони з тепловізорами можно використати для переслідування диверсійних груп, які переміщаються вночі. Безпілотники особливо потрібні на територіях, які заміновані або окопані, тому, що для їх використання не потрібно заходити в цю область. Для дослідження наслідків ракетних ударів, патрульна поліція використовує безпілотник "Сайконія". Цей український комплекс на базі літального апарата "Лелека-100" може 4 години перебувати у повітрі, долати відстань у 200 кілометрів, працювати і вдень, і в темряві.

Висновки. Повномасштабна війна росії проти України триває вже майже девять місяців. Попри складні економічні умови, Україна крокує в напрямі становлення верховенства права та демократії, розвитку інформаційно-просвітницької галузі, сфери освіти, культури тощо. У всіх цих сферах не обійтися без новітніх технологій. Через це все, в наш час безпілотники є невід'ємною частиною роботи правоохоронних органів, котра не тільки скорочує час роботи, а й значно оптимізує при фіксації кримінальних правопорушень, та слугуватиме джерелом інформації під час розслідування особливо тяжких злочинів.

Список використаних джерел:

1. Національна поліція отримала понад 30 нових БПЛА (фото) | Defense Express. Військовий портал Defense Express - все про військову справу. URL: https://defence-ua.com/news/natsionalna_politsija_otrimala_ponad_30_novih_bpla_foto-2537.html (дата звернення: 20.11.2022).

2. Поліцейські шукатимуть порушників карантину за допомогою дронів. У Києві вже почали так робити. Громадське телебачення - Останні новини дня, всі надзвичайні новини в Україні. URL: https://hromadske.ua/posts/policejski-shukatimut-porushnikiv-karantinu-za-dopomogoyu-droniv-u-kiyevi-vzhe-pochali-tak-robiti (дата звернення: 20.11.2022).

УДК 37.013:004

УСЕНКО АРІНА ОЛЕГІВНА

курсантка 3 курсу факультету №4

Харківського національного університету внутрішніх справ,

СВІТЛИЧНИЙ ВІТАЛІЙ АНАТОЛІЙОВИЧ

науковий керівник

кандидат технічних наук, доцент,

доцент кафедри протидії кіберзлочинності

Харківського національного університету внутрішніх справ,

ORCID http://orcid.org/0000–0003–3381–3350

КІБЕРБУЛІНГ ТА ПРОБЛЕМИ НЕЗАХИЩЕННОСТІ ДІТЕЙ У КІБЕРСФЕРІ

Кібербулінг — це один із видів булінгу, що описує неправомірні та жорстокі дії щодо особи, її приниження за допомогою сучасних електронних технологій: Інтернету та інших електронних засобів [1]. Цей термін з’явився зовсім нещодавно, але мав дуже швидке поширення серед користувачів мережі Інтернету. Загалом проявляється в поширенні брехні про когось або розміщення наклепницьких фотографій у соціальних мережах, надсиланні повідомлень або погроз через платформу обміну повідомленнями, які є образливими або можуть завдати шкоди будь-якій особі, у видаванні себе за іншу особу та надсиланні повідомлень іншій особі від його/її імені. Основною відмінністю від звичайного булінгу є використання Інтернет-середовища, а це в свою чергу може гарантувати анонімність, можливість підміни ідентичності, охоплення великої аудиторії одночасно, а також можливість тероризувати та тримати у напрузі жертву будь-де та будь-коли.

Найжорстокіша форма кібербулінгу трапляється серед дітей. “На жаль кожен третій підліток ставав жертвою онлайн-булінгу, а кожен п'ятий був змушений пропускати через це шкільні заняття. Під час пандемії COVID-19 вони почали ще більше часу проводити онлайн і стали ще більш вразливими для негативного впливу кібербулінгу”, — зазначають в ЮНІСЕФ Україна [2]. Вся жорстокість полягає в постійному натиску та знущанню над жертвою, що стає

причиною замкнутості та думок про смерть. Послаблена психіка дитини погано дається в знаки на навчанні, впевненості в собі, вмінню довіряти та самовиражатися, також впливає на фізичний, психологічний, психосоціальний та емоційний стан дитини. У багатьох випадках батьки навіть не здогадуються про проблеми власних дітей, а лише сварять за погане навчання, брудну одежу та пропуски в школах. Гостро стоїть і ситуація з безпекою підлітків, які зараховують себе до ЛГБТ - спільноти. Бо саме зараз на цю тему жорстокість людей на найвищому рівні, їх вважають “не такими”, тицяють пальцями, бояться, фізично принижують та не сприймають у соціумі.

Діти та підлітки найбільш незахищена категорія в мережі Інтернет. І хоч там почувають себе дорослими та безкарними через цікавість та відсутність деяких знань вони стають жертвами як і дорослих людей, так і своїх однолітків.

Тому велика відповідальність покладена на батьків та вчителів, щоб розпізнати та запобігти знущанню. Для цього навчіть дітей правил поведінки в Інтернеті, оскільки цифровий світ є частиною реального життя, існують і правила поведінки в Інтернеті.

На закінчення відзначимо, що важливо навчати юних користувачів правилам поведінки та спілкування в рамках цифрових медіа. На основі отриманих знань підлітки зможуть приймати правильні рішення, знаючи та розуміючи принципи, необхідні для безпеки в Інтернеті. Також можна розповісти про користь від використання мережі. Щоб захистити дітей від кібербулінгу та небажаного контенту в Інтернеті, батьки часто переходять межу та намагаються заборонити підліткам користуватися гаджетами. Однак у сучасних підлітків, які не уявляють життя без технологій, така поведінка може викликати негативну реакцію. Крім того, батьки не можуть контролювати доступ до Інтернету в будь-який час і в будь-якому місці, тому найкраще навчити маленьких користувачів правильно користуватися Інтернетом. Дуже важливо не забороняти гаджети, а показати, як їх використовувати для власної користі, особливо для отримання необхідної інформації, саморозвитку, навчання, спілкування та пошуку нових друзів. Ще одне вирішення ситуації це розповісти,

що скаржитися на кривдника — це нормально. У більшості випадків кібербулінгу підлітки знають, що інші залякуються, але вирішують не розповідати про це дорослим. Молоді користувачі часто бояться стати наступною жертвою або зіткнутися з покаранням дорослих. Крім розмови з батьками, про неприйнятну поведінку в Інтернеті можна і потрібно повідомляти на платформі. Майже в усіх соціальних мережах є можливість повідомляти про публікації, коментарі та навіть профілі, які поширюють небезпечний або образливий вміст. Дописи або профілі автоматично видаляються після отримання певної кількості таких скарг. Варто зазначити, що такі скарги абсолютно анонімні. А найголовніше заохочуйте відкритий діалог [3].

Список використаних джерел:

1. Справи Сімейні - Сімейний портал. *Справи Сімейні - Сімейний портал*. URL: https://familytimes.com.ua/ (дата звернення: 19.11.2022).

2. Кібербулінг – що це та як це зупинити?. *UNICEF*. URL: https://www.unicef.org/ukraine/cyberbulling (дата звернення: 19.11.2022).

3. Кібербулінг – як запобігти Інтернет-цькуванню, рекомендації ESET. *ESET - офіційний сайт. Антивірусні програми Ісет в Україні. | ESET*. URL: https://eset.ua/ua/blog/view/34/kak-predotvratit-kiberbulling-sovety-roditelyam (дата звернення: 19.11.2022).

УДК 343.985.5

ЦИПАК ІЛЛЯ ГЕННАДІЙОВИЧ

курсант групи Ф-4-301 факультету № 4

Харківського національного університету внутрішніх справ

ОНИЩЕНКО ЮРІЙ МИКОЛАЙОВИЧ

кандидат наук з державного управління, доцент,

доцент кафедри кібербезпеки та DATA-технологій факультету № 6

Харківського національного університету внутрішніх справ

СМІШИНГ ЯК ВИД ШАХРАЙСТВА У КІБЕРПРОСТОРІ

Шахраї не стоять на місці, і відколи у людей з'явилися мобільні телефони, вони майже миттєво почали вигадувати нові види обману. Вони дзвонять людям з метою виманити гроші, відправляють смс та займаються спамом. Пропонується розглянути такий вид шахрайства, як смішинг. Смішинг є телефонним шахрайством за допомогою смс повідомлень, який спрямований на недосвідчених користувачів та літню частину населення.

Смішинг – вид фішингу через смс повідомлення, який походить від слова "смс", тобто Smishing. Він не обов'язково реалізується через смс-повідомлення на телефон, а й проводиться за допомогою месенджерів, електронної пошти тощо. Смішинг-атаки зазвичай запрошують користувача перейти за посиланням, зателефонувати за номером або зв'язатися за електронною адресою, наданою зловмисником у повідомленні. Далі жертві пропонується надати свої приватні дані; часто це можуть бути дані інших сайтів або служб. Крім того, через природу мобільних браузерів, URL-адреси можуть відображатися не повністю; це може ускладнити ідентифікацію підробленої сторінки входу в систему. Оскільки ринок мобільних телефонів насичений смартфонами, які мають швидке підключення до інтернету, шкідливі посилання, надіслані в SMS, можуть мати той же результат, що й при надсиланні електронною поштою. Смішингові повідомлення можуть надходити з телефонних номерів у дивному або незрозумілому форматі.

Смішинг може бути як звичайним виманюванням грошей пересічних громадян через смс-повідомлення, так і виманюванням грошей у юридичних осіб, використовуючи людський фактор співробітників компаній, підприємств, установ, організацій тощо. Все залежить від навичок шахрая ввести в оману потенційну жертву.

Смішинг є шахрайством пов'язаним із соціальною інженерією, тобто для отримання своєї цілі шахрай не використовує спеціальні програми або навички хакінгу. Для цього зловмиснику лише потрібні навички спілкування та аналізу поведінки людей. Не виключено, що шахраєм може бути дипломований психолог, який знає людську натуру на найвищому рівні.

Методи соціальної інженерії дозволяють зловмисникам маніпулювати жертвою під час прийняття рішень. Якщо розглядати основні способи реалізації шахрайської схеми, то можна визначити такі критерії:

- **довіра**: шахраї можуть бути дуже розумні в сфері соціальної інженерії, можуть втертися в довіру настільки добре, що жертва відчуватимете в ньому споріднену душу і в змозі зовсім забути про кібербезпеку в мережі Інтернет;
- **контекст повідомлення**: шахраї використовують обставини та інформацію, яку вони дізналися з життя жертви, проти неї або розсилають спам про подію, що трапилася з близькою людиною жертви, наприклад аварія, травма, інцидент з поліцією тощо;
- **емоції**: посилюючи емоції жертви шляхом створення психологічного тиску, зловмисники можуть перекрити її критичне мислення та спонукати до швидких дій, моделюючи ситуацію, де нема часу на обміркування та неквапливе прийняття рішення.

Як захистити себе від Смішингу? Насамперед, це залежить від здатності цільового користувача ідентифікувати смішинг-атаку та проігнорувати повідомлення або повідомити про нього. Захист від смішинг-атак може здійснювати стороння особа/установа, наприклад, надсилаючи клієнту повідомлення у вигляді попередження від оператора мобільного зв’язку, банку тощо.

У шахрайських смс-повідомленнях можуть бути запити надіслати дані банківської карти. Ніколи не слід робити це, адже у будь-якого банку такі дані зберігаються у надійно захищеній базі даних. Шахрайські смс-повідомлення можуть містити пропозиції швидко забрати великий виграш із посиланням

унизу, що звичайно ж веде на сайт шахрая, або на завантажувач шкідливої програми, що може зчитувати особисті дані жертви. Не варто залишати в телефоні, у нотатках або іншому додатку свої особисті дані або дані свого банківського рахунку.

Чи можна зробити так, щоб ці повідомлення не потрапляли на телефон? На жаль, важко запобігти тому, щоб смішінг-повідомлення потрапляли на телефон. Відкритий характер обміну SMS-повідомленнями означає, що кожен може надіслати SMS на будь-який номер телефону. Єдине що може захистити користувача – це його розсудливість, обережність та відсутність панічних настроїв у нестандартних та критичних ситуаціях.

Не розповсюджуйте дані або номер телефону. Зазвичай номери телефонів потенційних жертв смішингу беруться з незахищених баз даних, які можуть зберігатися на сайтах купівлі/продажу або в опублікованих оголошеннях, зокрема комерційного характеру. Витрати часу на роздуми про автентичність потенційно небезпечного текстового повідомлення (надто привабливого змісту або навпаки такого, що вимагає швидкого прийняття рішення та дій щодо надання певної інформації) значно допоможе запобігти успішній атаці смішингу.

Отже, смішинг не є страшною та ефективною хакерською атакою. Це доволі примітивна шахрайська схема, розрахована на неуважних людей, і на неї важко потрапити, якщо витрачати більше часу на осмислення тексту повідомлення.

UDC 351.74:005.591.6

CHUKALOV KYRYLO EDUARDOVYCH

a first-year cadet of faculty No.4

Kharkiv National University of Internal Affairs

OLENDRA NATALIIA BOHDANIVNA

scientific adviser

lecturer of the department of foreign

languages of faculty No.4

Kharkiv National University of Internal Affairs

TECHNOLOGICAL INNOVATION IN POLICING AND CRIME PREVENTION

Technological advancement in the field of law enforcement is rapidly progressing. Governments all over the world are trying to incorporate state of the art technology in their law enforcement infrastructure to improve efficacy and ease of working.

Due to the rapid growth in the technology sector, the criminals are now committing crimes with the help of high tech devices. Most industries are becoming more and more tech-savvy and it seems the criminals have jumped aboard this bandwagon too. This has wreaked havoc for law enforcement officials.

Examples of technology used to commit crimes:

accessing your online information by sending you malware;

virtual kidnapping i.e making a ransom call pretending they have someone hostage when they don’t;

using apps that indicate the presence of police personnel to get away with crimes.

This means that to protect their communities, law enforcement now has to use innovative and advanced technology products as well.

Many patrol cars or police vehicles now have built-in cameras. These cameras are easy to install as it only consists of a control panel, a camera, and storage to record video. Some car cameras installed are so high tech that they automatically get triggered with the press of an emergency button by the police official. Other cameras need to be turned on physically. Car cameras increase transparency in the functioning of the police. The footage can be used to clear any confusion or suspicion involving the actions of the police. They can be used to record evidence.

Crime mapping is done by various algorithms to analyze in which areas, crimes are more likely to take place and who are the possible suspects. It does so by processing the data that has been fed into it concerning ex-convicts, dynamics of a neighbourhood,

and its previous criminal history. Based on this, some geographical locations are identified as hot spots. This means that there is a greater chance of criminal activity taking place there. In such a scenario, more resources and police personnel should be allotted to such hotspots. Here are the advantages of crime mapping:

it lessens the work burden and increases the efficiency of the police in solving crimes;

crimes can be prevented by having knowledge of potential risks. For example, Gang members/ Mafia members can be separated if they are in the same prison;

it creates a stronger working relationship between the police and the community.

Automatic License Plate Readers (ALPRs) are computer operated high-speed cameras that capture the photograph of the car. This includes the license plate and sometimes the driver or and the passengers.

Some key points about Automatic License Plate Readers:

these cameras are usually attached to street lights, freeway exits, and especially police patrol cars;

if the car is going over the speed limit or in the wrong direction, a photograph of the car is uploaded to a common server;

the license plate number then provides access to the driver's driving history, places frequented, traffic violations, criminal involvement if any, etc;

a copy of the challan or fine is sent to the driver and a penalty may be charged accordingly.

Also called unmanned aerial vehicles (UAVs), drones are increasingly being used by police to gain aerial vantage points for crime scene work, search and rescue efforts, accident reconstruction, crowd monitoring and more. Some of the more sophisticated models can be equipped with thermal imaging or 3D mapping software to offer GPS-enhanced precision to the areas being surveyed.

Many police drones and UAVs are also equipped with zoom cameras, making them incredibly valuable for delivering actionable, real-time intel in high-risk, "armed and dangerous" situations.

Technology is the greatest boon to mankind. The technology used by the police for criminal investigation has sped up the whole process and has provided people with an option of distress call to the police station at the time of emergency. This has also instilled confidence among people for faster and more accurate investigation.

With the advent of technology, the jobs of the police personnel have been made easier. Tools like predictive analytics and crime mapping have the potential to anticipate crimes and apprehend suspects, which is game-changing. The challenge however lies in the successful implementation of such technologies. However, an informed decision must be made before implementing a technological tool i.e the consequences of its use must be studied well.

УДК 004.9

ШЕВЧЕНКО МИКИТА ВІКТОРОВИЧ

курсант 2 курсу факультету №4

Харківського національного університету внутрішніх справ,

СВІТЛИЧНИЙ ВІТАЛІЙ АНАТОЛІЙОВИЧ

науковий керівник

кандидат технічних наук, доцент,

доцент кафедри протидії кіберзлочинності

Харківського національного університету внутрішніх справ,

ORCID http://orcid.org/0000–0003–3381–3350

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ДЛЯ ПРОТИДІЇ ЗЛОЧИННОСТІ

Інтернет є однією з найбільш швидкозростаючих сфер розвитку технічної інфраструктури. Сьогодні інформаційно-комунікаційні технології є всюдисущими, а тенденція до оцифрування зростає, попит на підключення до Інтернету призвів до інтеграції комп'ютерних технологій у продукти, які зазвичай функціонували на задвірках технологічного розвитку суспільства.

Злочинність. Злочин - це щось більше, ніж акт простої непокори закону. Це дія, яка одночасно заборонена законом і суперечить моральним принципам суспільства [0]. Тут знову ж таки треба бути обережним, оскільки моральні

почуття суспільства є гнучкими в різні часи і в різних місцях. Насправді кримінальні правопорушення є породженням політики сильних і проникливих людей, які захищають свої інтереси і безпеку. Злочин визначається як діяння, що карається законом як заборонене статутом або таке, що завдає шкоди суспільному добробуту. Це дуже широке визначення. Все, що завдає шкоди суспільному добробуту, є злочином. У сучасному складному суспільстві багато чого може бути проти суспільного добробуту.

Кіберзлочинність є новітньою і, можливо, найскладнішою проблемою в кібернетичному світі. про кіберзлочинність можна сказати, що це ті види злочинів, з яких основними є звичайні злочини, і де або комп'ютер є об'єктом, або суб'єктом діяння, що становить злочин.

Узагальнене визначення кіберзлочинності - протиправні дії, в яких комп'ютер є або інструментом, або ціллю, або і тим, і іншим. Перш ніж оцінювати концепцію кіберзлочинності, очевидно, що необхідно обговорити концепцію звичайної злочинності і визначити точки схожості і спільності між обома цими формами [2].

Інформаційні системи (мережеві пристрої, сервери, хости тощо) піддаються зловмисній активності на регулярній основі. На щастя, переважна більшість атак є невдалими. Інциденти в мережах і системах, як з внутрішніх, так і з зовнішніх джерел, будуть продовжуватимуть кидати виклик правоохоронцям і фахівцям з інформаційної безпеки. Виклики включають в себе те, як реагувати, які особи/компанії/місцеві або регіональні органи влади/державні органи влади/міжнародні органи влади або групи повідомляти, а також збереження "доказів". Інцидент, як правило, спричиняється аномальною подією в комп'ютерній мережі. Ця подія може бути викликана зловмисником, який отримує несанкціонований доступ до електронної пошти компанії серверу компанії або хакер, який спричиняє псування веб-обличчя корпорації-жертви. Коли виявлено інцидент, скоєний хакером або злочинцем, співробітники правоохоронних органів повинні реагувати таким чином, щоб цифрові докази не були скомпрометовані через неналежного поводження.

Виявлення кримінального правопорушення включає в себе:

1. Ідентифікація інциденту. Для того, щоб розслідувати інцидент, правоохоронці повинні усвідомлювати, що мала місце протиправна діяльність.
2. Категоризація інциденту. Інцидент повинен бути класифікований для проведення належного реагування.
3. Визначення пріоритетності інциденту.

Рекомендації щодо посилення боротьби з кіберзлочинністю включають додаткове навчання, покращення зв'язку та співпраці, розширені мережі для обміну інформацією, оновлену модель кіберзлочинності, розширені програми страхування для жертв кіберзлочинів, запити на збільшення фінансування та використання федеральних і державних програм і технології.

Все сказане дозволяє зробити висновок, що деякі з цих пропозицій можуть бути серйозною проблемою через брак часу та ресурсів, і вони можуть вимагати втручання політики та великих зусиль і співпраці. Проте місцеві правоохоронні органи перебувають на передовій більшості кримінальних і соціальних проблем; зміцнення їхньої спроможності та спроможності справлятися з виникаючими та значно шкідливими проблемами, такими як кіберзлочинність, має бути пріоритетним завданням, особливо під час воєнного стану [3].

Список використаних джерел:

1. *ОДУВС – Одеський державний університет внутрішніх справ*. URL: http://oduvs.edu.ua/wp-content/uploads/2016/09/l8.pdf (дата звернення: 09.11.2022).

2. Кіберзлочинність як загроза міжнародній безпеці. *Актуальні проблеми країнознавчої науки*. URL: https://internationalconference2014.wordpress.com/2015/12/29/кіберзлочинність-як-загроза-міжнаро/ (дата звернення: 09.11.2022).

3. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX | ЮРЛІГА. *ЮРЛІГА*. URL: https://jurliga.ligazakon.net/analitycs/210562_

borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix (дата звернення: 09.11.2022).

УДК 351.74+343.982.33

БОНДАРЕНКО ЄВГЕНІЙ СЕРГІЙОВИЧ

курсант четвертого курсу факультету № 4

Харківського національного університету внутрішніх справ

КЛІМУШИН ПЕТРО СЕРГІЙОВИЧ

науковий керівник,

кандидат технічних наук, доцент,

доцент кафедри протидії кіберзлочинності факультету № 4

Харківського національного університету внутрішніх справ

ORCID ID: https://orcid.org/0000-0002-1020-9399

СИМЕТРИЧНА АВТЕНТИФІКАЦІЯ ІНТЕРНЕТ РЕЧЕЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПОЛІЦЕЙСЬКИХ ОХОРОННИХ СИСТЕМ

Автентифікація є ключовою технологією для безпечного керування комп’ютерними ресурсами та мережами. Технологія автентифікації потрібно враховувати недолік обмежених ресурсів IoT. Як відомо, автентифікація пристрів IoT в мережі виконується з допомогою криптографічних перетворень - симетричним і асиметричним методами. Відмінності цих методів полягають в кількості та використанні криптографічних ключів. Автентифікація – симетрична, якщо використовується один криптографічний (сеансовий) ключ на хоста і клієнта для шифрування і дешифрування. При асиметричної автентифікації використовується два математично пов’язані ключа публічний та приватний, один служить для шифрування, а другий для дешифрування ідентифікаційних даних. о.

На практиці застосовуються комбінації симетричного та асиметричного підходів із їх плюсами - швидкістю роботи симетричного та безпекою асиметричного. Компанія Atmel випускає мікросхеми для обох типів автентифікації [1].

Ключовими особливостями мікросхем CryptoAuthentication компанії Atmel є безпечне зберігання ключів та апаратні блоки, що допомагають протистояти різним зовнішнім атакам, у тому числі агресивним. Ці пристрої, що мало споживають електроенергії, підтримують сучасні криптографічні протоколи, зокрема ECDSA для цифрового підпису та ECDH для генерації спільних сеансових ключів симетричного шифрування. Вони можуть працювати з будь-яким зовнішнім мікроконтролером, вимагають лише одну лінію вводу/виводу, діють у широкому діапазоні напруги живлення. Все це допомагає розробникам без особливих проблем додавати до своїх виробів сучасний, надійний рівень інформаційної безпеки за мінімальну вартість [2].

Особливістю процедури симетричної автентифікації відповідно до схеми "Запит - відповідь" із зберіганням таємного (сеансового) ключа в захищених пристроях хоста та клієнта є швидкодіюча процедура автентифікації, захищені криптографічні мікрочипи з обох сторін забезпечують безпечне зберігання таємних ключів. Однак, недоліком такої схеми є необхідність мати на стороні хоста захищену криптографічну мікросхему для зберігання таємних ключів.

Більш економічною є процедура симетричної автентифікації IoT, яка не припускає використання захищених криптографічних мікросхем на стороні хоста для зберігання таємних ключів. Такий підхід має назву «фіксований запит».

Особливістю автентифікації в схемі «фіксований запит» є також швидкодіюча процедура автентифікації та економія апаратного обладнання за рахунок відмови від випадкової складової в процедурі автентифікації і заміні цієї складової певною парою заздалегідь обчислених чисел (значення запитів і відповідні відповіді, що записуються в енергонезалежну пам'ять мікроконтролера на стороні хоста). Ця заміна, з одного боку, наводить к спрощенню схеми автентифікації, а з другого боку, веде до зниження її криптостійкості через заміну випадкових чисел на певні пари заздалегідь обчислених чисел, так як криптоаналітик може розгадати певну пару заздалегідь обчислених чисел з допомогою логічного аналізатора на інформаційної шині [3].

Висновки. Таким чином, багато розробників в даний час покладаються на спеціалізовані апаратні криптографічні засоби, включаючи закінчені пристрої та захищені інтегральні мікросхеми різного класу. В загальному разі такі засобі пропонують наступні рішення: сильний захист криптографічних ключів; належне використання режимів та протоколів для криптографічних операцій; високоякісні генератори випадкових чисел, які ґрунтуються на випадкових фізичних подіях та які досконально протестовані.

Апаратно захищені мікросхеми сімейства CryptoAuthentication компанії Atmel належать до таких спеціалізованих криптографічних засобів. Вони можуть застосовуватись у широкому діапазоні кінцевих додатків поліцейських охоронних систем.

Список використаних джерел:

1. Клімушин П.С., Спасібов Д.В. Симетрична автентифікація: потенційне застосування апаратно захищених мікросхем для забезпечення безпеки інтернет речей. Протидія кіберзлочинності та торгівлі людьми : зб. матеріалів міжнарод. наук.-практ. конф. (м. Харків, 27 травня 2022 р.). Харків : ХНУВС, 2022. С. 75-78.

2. Krivchenko I. Hardware-protected chips of the CryptoAuthentication family: potential applications of ATSHA204A. Components and technologies. 2015, no. 10, pp. 60–65.

Klimushin P., Solianyk T., Kolisnyk T., Mozhaev O. Potential application of hardware protected symmetric authentication microcircuitsto ensure the securityof internet of things. Advanced Information Systems. 2021. Vol.5, Харків : 2021, No.3, p. 103-111.

УДК 351.74+343.982.33

ДІДЕНКО ОЛЕКСІЙ ВОЛОДИМИРОВИЧ

курсант 2 курсу факультету № 4

Харківського національного університету внутрішніх справ

КЛІМУШИН ПЕТРО СЕРГІЙОВИЧ

науковий керівник,

кандидат технічних наук, доцент,
доцент кафедри протидії кіберзлочинності факультету № 4
Харківського національного університету внутрішніх справ
ORCID ID: https://orcid.org/0000-0002-1020-9399

МОБІЛЬНІ ЗАСОБИ УДОСКОНАЛЕННЯ ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Інформаційне суспільство - мета більшості сучасних країн світ. В першу чергу, це обумовлено стратегічною перевагою. Такі країни як США, Канада, Японія, члени європейського союзу, вже давно впроваджують інформаційні технології в повсякденні сфери життя.

В основному пов'язаний подальший розвиток інформаційних технологій, з появою нових технічних засобів обробки інформації, які визначають рівень розвитку інформаційних технологій. Покращення управління є найважливішим чинником підвищення ефективності. На основі досягнень ведеться робота з удосконаленням форм і методів управління науково-технічного прогресу, вивчення законів, способів накопичення, обробка та передача інформації.

Згідно з рейтингом міжнародного конкурсу - World Digital Competitiveness Ranking [1], Україна у 2021 році посіла 54 місце. Порівняно з 2020 роком показник покращився на чотири позиції. Підсумкова рейтингова система розраховується на основі трьох показників: якість освіти та науки; регуляторне середовище, фінансовий капітал у IT-галузі, стан інтернету та комунікаційних технологій; рівень готовності використання цифрової трансформації. На сьогоднішній день наша держава прагне розпочати новий етап формування інформаційного суспільства. Відбувається перехід від впровадження інформаційних технологій до комплексної побудови цифрової системи в масштабі країни.

Ефективність правоохоронної діяльності значною мірою залежить від якості інформаційного забезпечення, тому інформаційні технології широко використовуються в діяльності правоохоронних органів. Найдоступнішим та найпростішим джерелом інформаційних технологій є сучасний смартфон.

Фактично кожен поліцейський може лише за допомогою цього девайса бути на зв’язку з колегами, отримати доступ до онлайн-карт, усіх типів баз даних, навіть дізнатись особисті данні злочинця.

В свою чергу такий легкий доступ до мережі, надає можливість злочинцям порушувати закон, не виходячи з дому. Одним з найпопулярніших видів злочину за допомогою мобільних пристроїв є “онлайн-магазини наркотичних речовин”. Більшість з яких працюють через анонімний месенджер “telegram”. Такий спосіб збуту має певні переваги: продаж відбувається повністю анонімно, продавець та покупець не мають фізичного контакту [2].

Найпростішим способом боротьби з цим “феноменом” є сам месенджер , в якому є можливість поскаржитись на аккаунт чи канал, набираючи певну кількість скарг, вони блокуються. Існує телеграм бот “стоп наркотик” розроблений працівниками органів внутрішніх справ, який збирає такі канали та дає можливість кожному охочому поскаржитись маючи з собою лише мобільний пристрій, що значно спрощує цю процедуру. Завдяки цьому боту кожен день блокуються сотні аккаунтів.

Ще одним видом використання злочинцями мобільних пристроїв є телефонне шахрайство. Злочинець телефонує жертві представившись працівником банку чи інших установ, та починає запитувати персональні данні. Для запобігання подобних випадків слід дотримуватись наступних рекомендацій: встановити додаток для ідентифікації невідомих номерів, не залишати особисті данні на невідомих сайтах, надавати інформацію про шахраїв відповідним органам.

Висновки. Суспільство широко використовує новітні технології в повсякденному житті, найчастіше, мобільні пристрої. Це стало появою відповідного шахрайства. Органи внутрішніх справ в свою чергу активно використовують мобільні пристрої для протидії відповідній злочинності. Сучасні проблеми потребують сучасного рішення з допомогою засобів захисту інформації та обмеження доступу до персональних даних громадян.

Список використаних джерел:

1. World Digital Competitiveness Ranking. Report 2021. URL: https://www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/ (дата звернення 26.11.2022)

2. Пядишев В. Г., Монастирський М. В. Смартфони в руках населення як засіб удосконалення діяльності поліції: порівняння українського та зарубіжного досвіду. Південноукраїнський правничий часопис. 2022, 1-2’. С. 152-158.

УДК 351.74+343.982.33

ЯКОВЛЄВ ВЛАДИСЛАВ ІГОРОВИЧ

курсант 2 курсу факультету № 4

Харківського національного університету внутрішніх справ

КЛІМУШИН ПЕТРО СЕРГІЙОВИЧ

науковий керівник,

кандидат технічних наук, доцент,

доцент кафедри протидії кіберзлочинності факультету № 4

Харківського національного університету внутрішніх справ

ORCID ID: https://orcid.org/0000-0002-1020-9399

ПИТАННЯ ЗАХИСТУ ХМАРНИХ ІНФРАСТРУКТУР

Хмарні обчислення - це модель для забезпечення зручного мережевого доступу на вимогу до загального пулу конфігурованих обчислювальних ресурсів (наприклад, мереж, серверів, сховищ, додатків та послуг), які можуть бути швидко надані з мінімальними зусиллями щодо управління або взаємодії з постачальниками послуг.

Існує чотири основні моделі надання хмарних обчислень залежно від того, хто надає послуги хмар:

1) Приватна хмара, в якій хмарні послуги надаються виключно для організації та керуються організацією або третьою стороною.

2) Публічна хмара, в якій хмарні послуги доступні для громадськості і належать організації, що продає послуги хмар, наприклад, хмарний сервіс Amazon.

3) Урядова хмара, яка надає послуги одним або декількома агентствами для використання всіма чи більшістю державних установ.

4) Гібридна хмара, яка є композицією різних інфраструктур хмарних обчислень (публічних, приватних або урядових). Прикладом гібридної хмари можуть бути дані, що зберігаються в приватній хмарі туристичної агенції.

Існує безліч проблем безпеки для хмарних обчислень, оскільки вони охоплюють безліч технологій, включаючи мережі, бази даних, операційні системи, віртуалізацію, планування ресурсів, управління транзакціями, балансування навантаження, контроль паралелізму та управління пам'яттю. Забезпечення безпека даних включає шифрування даних, а також забезпечення дотримання відповідних політик для обміну даними. Крім того, алгоритми розподілу ресурсів та управління пам'яттю мають бути безпечними. Нарешті, виявлення шкідливих програм у хмарах можуть застосовуватися методи інтелектуального аналізу даних - підхід, який зазвичай використовують у системах виявлення вторгнень [1].

В даний час виробники жорстких дисків випускають диски, що самошифруються, в яких реалізовані стандарти зберігання даних групи довірених обчислень. Ці диски, що самошифруються, вбудовані в апаратні засоби шифрування, забезпечуючи автоматичне шифрування з мінімальними витратами або впливом на продуктивність. Механізми автентифікації та захисту цілісності гарантують, що дані потраплять лише туди, куди хоче клієнт. Надійна автентифікація є обов'язковою вимогою для будь-якого хмарного розгортання [2].

Однією з найбільш очевидних проблем хмарних обчислень є розподіл користувачів хмарного середовища, щоб уникнути випадкового або навмисного доступу до конфіденційної інформації. Як правило, для поділу клієнтів провайдер хмарних обчислень використовує віртуальні машини та гіпервізор. В даний час доступні технології, які можуть забезпечити значне підвищення безпеки віртуальних машин та поділ віртуальних мереж. Крім того, модуль

довіреної платформи може забезпечити апаратну перевірку цілісності та віртуальних машин і тим самим забезпечити надійний поділ мережі та безпеку.

У хмарних обчисленнях надзвичайно важливими є юридичні та нормативні питання, що впливають на безпеку. До питань, які необхідно розглянути у зв'язку, відносяться безпека та експорт даних, відповідність нормативним вимогам, аудит, зберігання та знищення даних, а також юридичне розкриття інформації. В області збереження та видалення даних ключову роль в обмеженні доступу до конфіденційних та критичних даних можуть відіграти методи довіреного зберігання та модульного доступу до довірених платформ.

Висновки. Незважаючи на гучні ділові та технічні переваги хмарних обчислень, багато потенційних користувачів хмар ще не приєдналися до них, а великі корпорації, які є користувачами хмар, здебільшого розміщують у хмарі лише менш конфіденційні дані. Відсутність контролю – прозорості при впровадженні хмари суперечить розвитку хмарних обчислень. Прозорість потрібна з нормативних причин і для того, щоб зменшити занепокоєння з приводу можливості витоку даних.

Список використаних джерел:

1. Cloud Security Issues & Challenges. URL: https://www.kaspersky.com/resource-center/preemptive-safety/cloud-security-issues-challenges (дата звернення: 22.11.2022).

2. Cloud computing security issues and challenges URL: https://www.businesstechweekly.com/cybersecurity/data-security/cloud-computing-security-issues-and-challenges/ (дата звернення: 22.11.2022).

УДК 336.743

ГРУЗІН БОГДАН МИХАЙЛОВИЧ

курсант 3 курсу факультету №4

Харківського національного університету внутрішніх справ

ГРИЩЕНКО ДЕНИС ОЛЕКСАНДРОВИЧ

науковий керівник

старший викладач кафедри протидії кіберзлочинності

Харківського національного університету внутрішніх справ

ORCID http://orcid.org/0000-0001-5066-7389

БЛОКЧЕЙН – МАЙБУТНЄ ЦИФРОВОЇ БЕЗПЕКИ

Цифрова трансформація вже давно вийшла за межі ІТ-індустрії та розповсюдилась в усі сфери нашого життя. За останні два роки, Україна зробила великий прорив у цифровізації. Завдяки програмі Президента «Держава у смартфоні» - ми стали першою країною, яка має паспорт у смартфоні, можливість змінити прописку або подати заявку на шлюб онлайн, та найшвидшу реєстрацію бізнесу, не виходячи з дому. Це маленький крок до великої мети - держава без корупції, бюрократії та черг. Але чим більш грандіозний проект, тим більше відповідальність та ризики. З'являються нові загрози витоку особистої та конфіденційної інформації, часткова або повна втрата майна, грошей, інтелектуальної власності, тощо. Левову частку можливих проблем може вирішити блокчейн технологія.

Блокчейн - це технологія обробки, зберігання інформації та ідентифікації клієнтів. Дослівно з англійської блокчейн (blockchain) перекладається, як «ланцюжок блоків», а сама технологія була запропонована в 2008 році Сатоши Накамато (псевдонім людини або групи людей). Роботу блокчейну можна зіставити з Torrent - функціонування системи відбувається в режимі P2P (peer to peer - комп'ютерна мережа, де всі учасники рівноправні). Коли ми завантажуємо фільм з трекеру, центральний сервер не використовується. Файл безпосередньо завантажується з комп'ютера такого ж учасника торрента, як і ви. Аналогічно і в blockchain. Усі транзакції проводяться між учасниками мережі безпосередньо.

А здійснюються вони за рахунок того, що їхні комп'ютери під'єднані до однієї мережі – блокчейн [1].

Технологія блокчейн може використовуватися для запобігання будь-якого типу витоку даних, крадіжки особистих даних, кібератак або нечесної гри в транзакціях. Це гарантує, що дані залишаться конфіденційними та безпечними. В IT-спільноті вже сформувалася стала думка про те, що блокчейн може добре допомогти людям з точки зору забезпечення безпеки даних. Можливість швидкого виявлення підробок, стійкість до DDoS, високий рівень захищеності інформації роблять блокчейн дуже привабливою технологією [2].

Ще одна важлива річ, яку слід відзначити щодо користувачів блокчейну, полягає в тому, що вони можуть зберігати всі дані у своїй мережі на своєму комп'ютері, якщо захочуть. Це призводить до двох речей. По-перше, вони можуть заробити на оренді свого «зайвого» складського приміщення, а по-друге, гарантують, що ланцюжок не впаде. Якщо, наприклад, хтось, хто є власником частини даних (скажімо, хакер), намагається підробити блок, вся система аналізує кожен окремий блок даних, щоб знайти той, який відрізняється від інших (чи інших). більшість). Якщо система знаходить блок такого типу, вона виключає його з ланцюжка, ідентифікуючи як помилковий [3].

Блокчейн – це прорив у кібербезпеці всього цифрового світу. Нова технологія забезпечить найвищий рівень конфіденційності, доступності та безпеки даних. Щоб знищити або експортувати блокчейн, хакеру доведеться знищити дані, які зберігаються на комп’ютері кожного користувача в глобальній мережі. Це можуть бути мільйони комп'ютерів, на кожному з яких збережеться копія деяких або всіх даних. Якщо хакер не зможе одночасно вивести зі ладу всю мережу (що практично неможливо), непошкоджені комп'ютери, а також відомі як «вузли», будуть продовжувати працювати, забезпечую бездоганну та безперервну безпеку особистих даних користувачів. Блокчейни дозволяють нам створювати надзвичайно надійні та надійні записи про події, що відбулися, що корисно для таких речей, як підписання документів, керування ідентифікацією та відстеження доступу. Крім того, вони можуть

розширити можливості обміну інформацією між підприємствами та кордонами, створеними для цієї мережі, які ніким не контролюються, але перевіряються і якими довіряють всі.

Список використаних джерел:

1. Що таке блокчейн? [Електронний ресурс] / Режим доступу до ресурсу: https://bankchart.com.ua/finansoviy_gid/investitsiyi/statti/scho_take_blokcheyn_#1 (дата звернення: 21.11.2022)

2. Майбутнє кібербезпеки: блокчейн [Електронний ресурс] / Режим доступу до ресурсу: https://habr.com/ru/company/cloud4y/blog/527946/ (дата звернення: 21.11.2022)

3. The Future of Cyber Security: BlockChain Technology [Електронний ресурс] / Режим доступу до ресурсу: https://www.linkedin.com/pulse/future-cyber-security-blockchain-technology-anurag-agrawal

УДК 336.743

ПАВЛЕНКО СТАНІСЛАВ МИХАЙЛОВИЧ

курсант 3 курсу факультету №4

Харківського національного університету внутрішніх справ

ГРИЩЕНКО ДЕНИС ОЛЕКСАНДРОВИЧ

Науковий керівник

старший викладач кафедри протидії кіберзлочинності

Харківського національного університету внутрішніх справ

ORCID http://orcid.org/0000-0001-5066-7389

ПРИНЦИП РОБОТИ Cellebrite UFED Touch ТА ВИКОРИСТАННЯ У ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ НПУ.

В сучасному світі новітні технології стали буденністю, їх використовують у всіх сферах життя людини. Вони полегшують наш побут, але водночас в них прихована велика небезпека, деякі люди можуть використовувати їх для своїх протиправних дій. Зловмисники не стоять на місці, вони постійно використовують новітнє обладнання, нові способи та методики,

для того щоб використати їх у злочинних цілях. Правоохоронні органи повинні покращувати свої навички та обладнання для протидії кіберзлочинцям.

Одним із таких пристроїв є UFED Touch 2 – комплекс для криміналістичних досліджень, що дає фахівцям за дослідженнями можливість отримувати, декодувати та аналізувати доказові дані, отримані з різних моделей мобільних пристроїв. Легкий у використані сенсорний інтерфейс екрана та вбудована батарея, забезпечують швидкість, зручність використання та перенесення як у лабораторних, так і польових умовах, що є безумовною перевагою даного пристрою [1]. UFED Touch є ліцензійним пристроєм, який має позитивні відгуки у багатьох країнах світу, а також використовується багатьма спеціальними службами у своїй діяльності. Величезною перевагою є те, що висновки та результати даного пристрою можна використовувати в суді, як докази.

Сама компанія Cellebrite є світовим лідером у галузі передових систем для криміналістичних досліджень мобільних пристроїв. Cellebrite розробляє гнучкі, перевірені в "бою" інноваційні кросплатформні комплекси для проведення досліджень у польових умовах та в лабораторії [1].

Принцип роботи UFED Touch полягає в тому, що він обходить логічний захист мобільного пристрою використовуючи вразливості кожної конкретної моделі, яка вказується під час роботи з приладом, швидкий dump інформації, аналіз та висновок і це все в одному пристрої. З особистого досвіду можу додати, що для роботи з даним пристроєм непотрібно мати особливих навичок, інструкція вбудована в систему, витративши 20 хвилин часу, можна вже працювати з ним.

Таким чином ми розглянули лінійку пристрої UFED Touch для кримінального аналізу, які на жаль ще не розповсюджені у правоохоронних органах нашої країни, через велику вартість, але я впевнений, що завдяки користі даного пристрою буду прийняте рішення щодо забезпечення підрозділів достатньою кількістю Cellebrite UFED Touch.

Список використаних джерел:

1. BAKOTECH.ua // uploads // product// files.
URL: https://bakotech.ua/uploads/product/278/files/554/file.pdf
(дата звернення: 22.11.2022)

НАУКОВЕ ВИДАННЯ

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Матеріали

Круглого столу

м. Харків, 14 грудня 2022 року

ВИДАНО В АВТОСЬКІЙ РЕДАКЦІЇ

Відп. за випуск В.М. Струков