МВС УКРАЇНИ

Харківський національний університет внутрішніх справ

Кафедра інформаційних технологій та кібербезпеки

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Матеріали
науково-практичного семінару

м. Харків, 18 грудня 2019 року

Харків
2019

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

ОРГКОМІТЕТ:

голова – ректор полковник поліції Швець Д. В.;
заступник голови – проректор Бурдін М. Ю.;
секретар – доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Клімушин П. С.;
члени оргкомітету:

- декан факультету № 4 підполковник поліції Марков В. В.;
- завідувач кафедри інформаційних технологій та кібербезпеки факультету № 4 Гнусов Ю. В.;
- начальник редакційно-видавничого відділу підполковник поліції Білоус П. О.;
- начальник інформаційно-технічного відділу Полховський О. М.;
- начальник відділу зв'язків з громадськістю Щербакова І. В.;
- директор загальної бібліотеки Процких Т. О.;
- т.в.о. начальника відділу організації наукової роботи Чумак В. В.;
- заступник начальника відділу організації служби Тарасенко В. М.

Друкується за рішенням оргкомітету відповідно до доручення Харківського національного університету внутрішніх справ від 29 жовтня 2019 року

З-36 **Застосування інформаційних технологій у діяльності правоохоронних** органів : матеріали наук.-практ. семінару, м. Харків, 18 грудня 2019 р. / МВС України, Харк. нац. ун-т внутр. справ. Харків. ХНУВС, 2019. 87 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)

ЗМІСТ

УДК 351.741:004.89 (477)
ВАЛЕРІЙ ВАСИЛЬОВИЧ СОКУРЕНКО
Начальник Головного управління Національної поліції України в Харківській області, доктор юридичних наук, професор, генерал-поліції третього рангу

АНАЛІЗ СТАНУ ПОЛІЦЕЙСЬКОЇ ДІЯЛЬНОСТІ НА ОСНОВІ ОПЕРАТИВНИХ ДАНИХ ТА ІНФОРМАЦІЇ (ILP) В УКРАЇНІ

Поліцейська діяльність на основі оперативних даних і інформації (ILP) – це сучасна модель правоохоронної діяльності. ILP з'явилася в Сполученому Королівстві в 1990-х роках і використовувалася в основному для боротьби з серйозною і організованою злочинністю.

Двома основними проблемами сьогоднішнього правозастосування є транснаціональний і все більш складний характер злочинності, а також зростання суспільного попиту на фінансову ефективність, тобто «Робити більше меншою ціною». Модель ILP вирішує ці проблеми, підкреслюючи важливість і обґрунтовуючи необхідність ранжирування пріоритетів на основі оперативних даних, на підставі чого далі проводиться постановка завдань і виділення доступних засобів. фактичними даними.

Аналіз оперативних даних має більше значення в ILP I, ніж в інших сучасних моделях поліцейської діяльності. Це вимагає вдосконалених, а іноді і нових аналітичних знань і навичок в правоохоронних органах. Випереджаючого і перспективний метод ILP також спирається на знання керівників правоохоронних органів специфіки роботи з експертами-аналітиками і використання аналітичних матеріалів в процесі прийняття рішень та планування. Таким чином, при прийнятті та здійсненні ILP I необхідно приділяти особливу увагу підготовці та навчанню керівних і управлінських кадрів вищої та середньої ланки в правоохоронних органах. Необхідно відзначити, що всі проблеми і методи їх вирішення в практиці правоохоронної діяльності в Україні також вимагають комплексного підходу, що забезпечує необхідність ретельного вивчення моделі ILP і розробки рекомендацій щодо її використання в НПУ.

Метою даної доповіді є детальний аналіз ILP і розробка механізмів застосування цієї моделі в діяльності НПУ.

Що стосується методології правоохоронної діяльності, то дослідники і автори літератури зазвичай виділяють п'ять основних моделей правоохоронної діяльності: традиційна поліцейська діяльність, поліцейська діяльність, заснована на взаємодії з населенням, проблемно-орієнтована поліцейська діяльність, комп'ютерна система криміналістичного аналізу і статистики, і ILP. Кожна з цих моделей має різні стратегічні цілі, має свої сильні і слабкі сторони, і при одночасному використанні вони можуть доповнювати один одного. Наприклад, ILP все частіше застосовується для забезпечення більш тісного зв'язку між поліцейської діяльністю і місцевим населенням, оскільки ця модель пропонує чіткі процеси, процедури комунікації і структури управління для збору, аналізу та поширення даних та

інформації. Інший приклад – це коли традиційна модель правоохоронної діяльності, в основі якої лежить реагування, є переважаючою, а ILP застосовується тільки для протидії серйозної та організованої злочинності. Загальним фактором перших чотирьох вищезазначених моделей, який часто вважається слабкою ланкою в діяльності сучасних правоохоронних органів, є орієнтація на місцеві регіони і загрози.

Існують різні і навіть суперечливі трактування поняття ILP. Деякі вважають, що ILP відноситься до проведення оцінок загроз, в той час як інші стверджують, що ця модель спрямована на збір даних і інформації. Відмінності в підходах до ILP цілком зрозумілі, так як поліцейська діяльність на основі оперативних даних і інформації є відносно новою, що розвивається концепцією.

Але в даний час вже виробилося уявлення про те, що ILP означає структуру управління оперативною інформацією про злочинну діяльність і запланованої оперативною роботою, в якій оперативні дані є основою для визначення пріоритетів, стратегічних та оперативних цілей в галузі попередження і припинення злочинів та інших загроз безпеці. Вона також включає в себе прийняття відповідних рішень щодо оперативної діяльності та заходів, раціонального залучення наявних людських ресурсів і розподілу матеріальних і технічних засобів.

Той факт, що екстремісти, пов'язані з недавніми терористичними актами, включаючи терористів-одинаків, залишалися поза полем зору правоохоронних органів, обумовив необхідність вироблення попереджувального підходу і всебічного обміну і централізованого аналізу відповідних даних та інформації. Усвідомлення того, що робота за принципом реагування не забезпечить запобігання терористичних актів та раннє виявлення інших серйозних інцидентів, ставить ILP в центр уваги на міжнародній правоохоронній арені.

Виявлення та управління ризиками є невід'ємною частиною сучасної поліцейської діяльності. Належний підхід ILP до збору та аналізу даних і інформації дозволяє виявляти й оцінювати ризики, в тому числі в частині серйозних подій, географічних районів, видів злочинів, соціального збитку, небезпечних злочинців і кримінальних мереж.

Першим етапом ILP є збір інформації для проектів, пов'язаних з оперативною інформацією, є складним процесом. Хоча експерти-аналітики повинні забезпечити збір достатніх даних для охоплення всіх аспектів підлягає аналізу теми (або тим), вони повинні уникати надмірного обсягу даних і збору непотрібної або неадекватної інформації. Запорукою успіху цієї фази є поінформованість співробітників оперативних органів про існування, актуальності, доступності та надійності всіх джерел і установ, обраних для конкретного завдання зі збору оперативних даних, а також знання будь-яких юридичних обмежень і вимог в частині повноважень, які можна застосувати до використання різних типів джерел інформації . Знання і доступ до внутрішніх і зовнішніх джерел даних та інформації, а також обізнаність про

потенційні обмеження і вимоги є передумовами для ефективного збору і аналізу оперативної інформації.

На етапі обробки і систематизації вимагається наявності адекватної та послідовної системи роботи з інформацією. Ця фаза включає сортування, визначення пріоритетів і прив'язку зібраної інформації. Під час етапу систематизації аналітик організує і структурує зібрану інформацію, перетворюючи її в індексований і містить перехресні посилання формат, і переносить її в систему зберігання (тобто базу даних). Обробка інформації може бути настільки тісно пов'язана з аналітичної фазою, що часом складно провести чітку межу між ними.

Наступним кроком в застосуванні ILP буде аналіз оперативної інформації, який має різні класифікації. Найбільш поширеними класифікаціями аналізу є стратегічний аналіз, оперативний аналіз і тактичний аналіз. У доповіді тактичний і оперативний аналіз об'єднані під одним загальною назвою оперативний аналіз. Стратегічний аналіз використовується для підкріплення процесів прийняття рішень, розробки політики, планування та встановлення пріоритетів; розподілу ресурсів поліції; і визначає належний підхід до боротьби з певними видами злочинної діяльності. Оперативний аналіз допомагає в управлінні і оперативному впровадженні короткострокових завдань для досягнення оперативних цілей і підтримує поточні розслідування. Оперативний аналіз може включати особисту інформацію про підозрюваних.

Головним завданням органів МВС і НПУ є адаптація базової моделі ILP до національних правових рамок, що дозволяє здійснювати ILP відповідно до міжнародних правових стандартів. Серед них в першу чергу можна виділити такі:

– Національне законодавство повинно бути адаптовано до стандартів ОБСЄ – включати конкретні положення щодо реалізації ILP в діяльності правоохоронних органів;

– Збір, зберігання, обробка і обмін даними та інформацією повинні ґрунтуватися на національному законодавстві, строго відповідати міжнародним стандартам в галузі прав людини та захисту даних. Державам-учасницям ОБСЄ, в тому числі і Україні, пропонується запитувати технічну допомогу і консультації для оцінки відповідності цих законів міжнародним стандартам;

– Організацію реалізації шляхів впровадження концепції ILP в Україні доцільно здійснювати з урахуванням рекомендацій європейських експертів-аналітиків КМЄС, викладених в Листі Голови місії КМЄС в Україні Кястутіса Ланчінскаса від 20.01.2017 р. на ім’я міністра внутрішніх справ України Арсена Авакова.

Таким чином, активне використання моделі ILP дозволить Україні зробити ще один крок до торжества європейських стандартів та забезпечити більш якісне функціонування правоохоронних органів.

УДК 65.012.8 + 004
ДМИТРО ВОЛОДИМИРОВИЧ ШВЕЦЬ
Ректор Харківського національного університету внутрішніх справ
кандидат педагогічних наук, доцент, полковник поліції

СИТУАЦІЙНІ ЦЕНТРИ НПУ, ЯК ОРГАНІЗАЦІЙНА ФОРМА ВЗАЄМОДІЇ ПІДРОЗДІЛІВ ПОЛІЦІЇ ПРИ РЕАГУВАННІ НА РЕЗОНАНСНІ ПРАВОПОРУШЕННЯ

Ефективність боротьби з правопорушеннями, і перш за все з кримінальними правопорушеннями, в значній мірі залежить від інформаційного забезпечення діяльності правоохоронних органів.

Співробітники правоохоронних органів у своїй роботі постійно використовують сучасні інформаційні технології. І прикладом впровадження таких технологій є створення ситуаційних центрів.

Тому дослідження впровадження новітніх інформаційних технологій у діяльність НПУ є досить актуальною задачею.

Метою даної доповіді є аналіз методів та засобів побудови та функціонування ситуаційних центрів НПУ.

Ситуаційний / диспетчерський центр – це приміщення (зал, кімната, кабінет), оснащене засобами комунікацій (відеоконференцзв'язок, конференц-зв'язок та іншими засобами інтерактивного представлення інформації), призначене для оперативного прийняття управлінських рішень, контролю і моніторингу об'єктів різної природи, ситуацій і інших функцій.

При цьому під центром розуміється не лише спеціально обладнане приміщення, але і відповідні інформаційні, телекомунікаційні, програмні та методичні засоби з метою вироблення відповідного управлінського рішення.

Таким чином, *ситуаційний центр* – це, передусім, сукупність спеціальних інформаційних технологій та апаратно-програмних комплексів, що реалізовують функції підготовки управлінських рішень з урахуванням оцінки їх наслідків, причому процес розробки і прийняття рішення відбувається в реальному часі по відношенню до тих подій, на які треба реагувати.

Основними завданнями ситуаційних / диспетчерських центрів є:

– моніторинг стану об'єкта управління з прогнозуванням розвитку ситуації на основі аналізу інформації, що надходить;

– моделювання наслідків управлінських рішень, на базі використання інформаційно-аналітичних систем;

– експертна оцінка прийнятих рішень і їх оптимізація;

– управління в кризовій ситуації.

Основними елементами технічного оснащення ситуаційного / диспетчерського центру є:

– комп’ютерна мережа, що дозволяє вводити, обробляти, зберігати і передавати інформацію за напрямком діяльності ситуаційного центру;

– екран колективного користування (відеостіна, проекційна установка) Екран колективного користування - це система мультіекранного відображення даних різного виду (відеозображення, електронні карти, графіки та діаграми, текстова документація в електронному вигляді). Завдяки модульній конструкції система може конфигурироваться індивідуально під конкретні приміщення і завдання. Ключовою властивістю екрану колективного користування є дозвіл і, відповідно, інформаційна ємність, що дозволяє представляти на одному екранному полі безліч «вікон», що містять повноцінні зображення від різних джерел;

– засоби відеоконференцзв'язку які грають одну з ключових ролей в ситуаційному центрі, забезпечуючи проведення колективних нарад між віддаленими учасниками обговорення. У разі виникнення надзвичайних ситуацій в ситуаційному центрі організовується безпосереднє мовлення з місця події. Дане рішення необхідно не тільки для міністерств з надзвичайних ситуацій, але для транспортних і видобувних компаній;

– система звукооснащення зазвичай включає конференц-систему, призначену для проведення групових обговорень. При цьому кожне робоче місце учасника нарад в ситуаційному / диспетчерському центрі оснащується окремим мікрофоном (мікрофонним пультом) для виступів. Система звукооснащення також включає системи посилення (мікшування) звуку і акустичні системи;

– допоміжне обладнання, яке включає в себе електронні засоби введення і відображення графічних даних, такі як документ-камери, інтерактивні дошки та ін.;

– інтегрована система управління ситуаційного / диспетчерського центру забезпечує взаємодію всіх елементів технічного оснащення. В силу високої складності система управління зазвичай вимагає постійної присутності обслуговуючого персоналу.

Ситуаційний центр, як правило, розміщується на базі окремого підрозділу, в якому є прямий доступ не тільки до різних джерел інформації, але і до всіх ключових співробітників, включаючи керівництво і конкретних виконавців.

Ключовим компонентом СЦ має бути потужна багатофункціональна геоінформаційна система (ГІС).

Впроваджуючи геоінформаційні системи в роботу ситуаційних центрів, поліція отримує програмну платформу для реалізації ефективного управління та реагування в справі охорони громадського порядку. ГІС з самого початку створювалися для збору, аналізу і відображення даних в найбільш зрозумілому людині вигляді: шляхом нанесення на карту.

Подібні ГІС системи можуть інтегруватися з ситуаційними центрами загальнодержавного, обласного чи міського призначення, для підключення раніше недоступних або непридатних наборів даних. В результаті сумісних досліджень можна отримати більш повну картину злочинності, поліпшити тактику реагування та розслідування, значно спростити щоденні завдання. В результаті, процес прийняття рішень стає більш ефективним і виваженим.

УДК 65.012.8 + 004

СЕРГІЙ МИКОЛАЙОВИЧ БОРТНИК
Перший проректор Харківського національного університету внутрішніх справ, доктор юридичних наук, полковник поліції

ПРОБЛЕМИ ПІДГОТОВКИ КАДРІВ ДЛЯ ПІДРОЗДІЛІВ КІБЕРПОЛІЦІЇ УКРАЇНИ

Характерним і незворотним трендом епохи третьої і четвертої промислових революцій є стрімкий перехід матеріальних відносин у віртуальну сферу. Одним з негативних наслідків цього в цілому позитивного процесу є віртуалізація все більшої частки кримінальних правопорушень. Серед фахівців існує думка, що вже в найближчі 10 років зникнуть всі види злочинів, крім кіберзлочинів [1]. І це не популістська заява, а цілком обгрунтоване передбачення, засноване, в першу чергу, на таких двох факторах: а) можливість дистанційного отримання великих коштів незаконним шляхом, і б) відносна безпека і анонімність для виконавця.

Як проміжний етап реагування правоохоронних структур цивілізованого світу на цей виклик є створення підрозділів кіберполіції. В подальшому префікс кібер- можна буде відкинути, оскільки більшість підрозділів поліції будуть займатися профілактикою і розкриттям розгалужених різновидів кіберзлочинів.

Правоохоронці по всьому світу всерйоз готуються до появи підпільних синдикатів, що спеціалізуються на замовних високотехнологічних вбивствах, замаскованих під технічні інциденти різного роду. Беручи до уваги обсяг ринку замовних вбивств в Сполучених Штатах, що становить близько 2 млрд. дол. на рік, фахівці ФБР очікують появу такого мережевого синдикату, а швидше за все не одного, а декількох, в найближчі один-два роки. Враховуючі той факт, що така думка була висловлена 2 роки тому, є підстави вважати, що такий синдикат (синдикати) на поточний момент вже існують.

Головним інструментом подібних синдикатів можуть стати не хакерські програми самі по собі, а штучний інтелект.

Враховуючі вищезазначені обставини, не підлягає сумніву, що для виконання таких злочинів будуть а) залучені висококваліфіковані фахівці в галузі ІТ технологій і інтелектуальної обробки великих масивів даних з відповідно високим матеріальним заохоченням, б) залучене потужне високотехнологічне технічне і програмне забезпечення [1].

З цього незворотно випливає логічний висновок, що кваліфікація фахівців кіберполіції повинна бути як мінімум не гіршою ніж кіберзлочинців. Ситуація ускладнюється тим, що бурхливо розвивається як програмне так і технічне забезпечення комп'ютерів і комп'ютерних мереж, тобто змінюються їх можливості і, відповідно, правила їх застосування, що вимагає від фахівців у цій сфері постійно вивчати і засвоювати нові інструментальні засоби для того, щоб не тільки підтримувати свій кваліфікаційний рівень, а й

підвищувати його. Це ж стосується викладачів і тьюторів (тренерів), які здійснюють підготовку таких фахівців.

Відповідними темпами повинна оновлюватися матеріальна база як підрозділів кіберполіції так і закладів, де здійснюється їх підготовка і перепідготовка. В першу чергу, встигати за швидкими технологічними змінами повинні тренувальні комплекси, які є інструментальною основою системи підготовки. І це повинні бути сучасні високоефективні комплекси типу «Програмно-апаратний симулятор TnS для підготовки фахівців з реагування на кібер-інциденти та загрози», розроблений компанією CyberBit, Ізраіль. Навчально-тренувальний центр з підготовки фахівців для кіберполіції повинен мати сукупність таких інструментальних засобів для відпрацювання практичних навичок різних напрямів дій фахівців в умовах, максимально наближених до реальних. Використання таких засобів передбачає сучасний рівень технічного обладнання тренінгових центрів. Сучасні тренувальні багатофункціональні комплекси такого типу, як і комп'ютерні комплекси для їх функціонування, коштують немалих грошей, але альтернативою є лише суттєвє зниження рівня підготовки фахівців. Не слід також недооцінювати фактор матеріальної мотивації висококваліфікованих фахівців: заробітна платня фахівців поліцейських підрозділів не повинна кардинально (в менший бік) відрізнятися від заробітної плати у комерційних структурах, інакше рано чи пізно неминучий відтік висококваліфікованих кадрів.

І якщо ці фактори не враховувати в навчальному процесі, це матиме негативний вплив на якість підготовки фахівців і, відповідно, на ефективність діяльності підрозділів кіберполіції у протистоянні кіберзлочинності.

Список використаних джерел:

1. Овчинский В. С. Криминология цифрового мира: учеб. М. : Норма ; ИНФРА–М, 2018. 352 с.

УДК 65.012.8 + 004

МИХАЙЛО ЮРІЙОВИЧ БУРДІН
Проректор Харківського національного університету внутрішніх справ,
доктор юридичних наук, професор

ІНСТРУМЕНТАЛЬНІ ЗАСОБИ КРИМІНАЛЬНОГО АНАЛІЗУ В РОЗСЛІДУВАННІ ЗЛОЧИНІВ

В навчальному посібнику, розробленому експертами-аналітиками різних держав в рамках співробітництва з Organization for Security and Co-operation in Europe (OSCE) [1] для , відзначено: «Той факт, що екстремісти, пов'язані з недавніми терористичними актами, включаючи терористів-одинаків, залишалися поза полем зору правоохоронних органів, обумовив

необхідність вироблення попереджувального підходу і всебічного обміну і централізованого аналізу відповідних даних та інформації. Усвідомлення того, що робота за принципом реагування не забезпечить запобігання терористичних актів та раннє виявлення інших серйозних інцидентів, ставить ILP в центр уваги на міжнародній правоохоронній арені.». В цьому реченні у дуже стислому вигляді сформульована необхідність і актуальність якнайшвидшого переходу діяльності правоохоронних органів європейських держав з традиційного принципу реагування на правопорушення на сучасний принцип профілактики і запобігання правопорушенням на основі оперативних даних та інформації – ILP. Передумовою і обгрунтуванням цієї концепції є бурхливий розвиток інформаційних технологій і супроводжуючий його інформаційний вибух. Якщо ще не так давно проблемою в процесі розслідування злочину був пошук і збір даних, то зараз проблемою частіше є виявлення в наявному величезному обсязі різнотипних даних з багатьох джерел корисної інформації у вигляді прихованих або неявних зв'язків типу «об'єкт-об'єкт», «об'єкт-подія», «подія-подія» для формування пропозицій для подальших управлінських рішень або гіпотез щодо розкриття злочину.

Ключовим і самим складним етапом технології ILP є Аналіз, в процесі якого здійснюється систематизація і аналітична обробка зібраних на попередніх етапах даних та інформації [1]. Причому на сучасному етапі кількість інформації, яка підлягає обробці і аналізу, досягає настільки великих обсягів, що людина вручну не в змозі їх опрацювати за реальний час. Тому ефективність виконання цього етапу визначається тими інструментальними засобами, які має в своєму розпорядженні аналітик. В першу чергу, наявністю сучасних програмних інструментальних засобів. В загальному випадку під інструментальними засобами аналітика будемо розуміти програмні системи або модулі і методики і методології опрацювання інформації.

Загальну класифікацію інструментальних засобів кримінального аналізу можна представити наступним чином:

1. Методології і методики аналізу.
2. Загальновикористовувані програмні засоби.
3. Традиційні інформаційно-пошукові системи.
4. Спеціалізовані інформаційно-аналітичні системи і комплекси кримінального аналізу.

До інструментів першої групи можна віднести, зокрема, такі часто використовувані методики як мережний аналіз, ANACAPA, SOCTA. Вони застосовуються як в ручному так і в автоматизованому режимі.

Мережний аналіз це загальна методологія аналізу, яка передбачає використання математичного апарату теорії графів для дослідження і виявлення зв'язків між об'єктами і подіями.

ANACAPA представляє собою методику розслідування злочинів і аналізу оперативної інформації, яка була розроблена в 1960-ті роки, після вбивства президента Кенеді. Методику названо на честь острова на західному

узбережжі Америки. Спочатку методика представляла собою систему структурування, візуалізації та аналізу інформації у паперовому виконанні. В подальшому фірмою Anacapa Sciences Inc. (США) були розроблені програмні продукти, які реалізують дану методику. Anacapa Sciences Inc. стояла у витоків розробки спеціальних аналітичних методик для сфери безпеки і ще на початку 1970-тих років почала проведення навчальних курсів з підготовки фахівців-аналітиків. На даний момент Anacapa Sciences Inc. пропонує наступні 4 базових курси:

1) аналіз інформації в ході проведення розслідувань Criminal Intelligence Analysis (CIA);

2) аналітичні методи розслідування Analytical Investigation Methods (AIM);

3) аналіз фінансових махінацій Financial Manipulation Analysis (FMA);

4) поглиблений аналіз з використанням комп'ютерних технологій Computer-Aided Analysis (CAA).

SOCTA (SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT) є методикою з оцінки ризиків щодо тяжких злочинів та організованої злочинності. SOCTA – ключовий стратегічно-аналітичний документ, присвячений боротьбі зі злочинністю, розроблений Європолом. Останній документ SOCTA опублікований Європолом у 2017 році – SOCTA 2017. Він готувався на протязі 2015-2017 років. В ході його підготовки був проведений безпрецедентний за масштабами аналіз серйозної і організованої злочинності, за результатами якого розроблені відповідні рекомендації.

До інструментів другої групи можна віднести комп’ютерні програми і системи загального призначення та проблемно-орієнтовані, які з успіхом використовуються для розв’язання задач кримінального аналізу з відносно невеликим обсягом даних. До числа таких інструментів можна віднести Microsoft Excel, MatCAD, MatLAB, StatGraph, Statistica та ін. Можливість ефективного застосування цих інструментів значною мірою визначається наявністю відповідних методик їх застосування для розв’язання конкретних задач кримінального аналізу, кваліфікацією і практичним досвідом фахівців. До інструментальних засобів цієї групи можна також віднести гео-інформаційні системи (ГІС), призначені для візуалізації об’єктів і подій на географічній мапі. Без застосування ГІС на сучасному етапі неможливо уявити аналітичну роботу як у правоохоронній так і у цивільній сфері. Вони є базовим інструментом візуалізації даних.

Типовими прикладами традиційних інформаційно-пошукових систем можна вважати Ліга-Закон і Google. Принципом роботи таких систем є опрацювання пошукового запиту, сформованого за певним шаблоном. Результатом роботи є перелік даних або документів, які відповідають пошуковому запиту. До систем такого типу належить і відомча інформаційно-пошукова система «Інформаційний портал Національної поліції України». Головною метою систем даного типу є пошук інформації. Вони, як правило, не мають інструментів аналітичної обробки великих і надвеликих обсягів інформації.

Найбільш ефективними інструментами кримінальних аналітиків є спеціалізовані інформаційно-аналітичні системи і комплекси кримінального аналізу. Системи цього класу мають потужний набір інструментів аналітика, які дозволяють проводити глибокий всебічний аналіз великих обсягів різнотипних даних і формувати гіпотези щодо аналізуємих подій і об'єктів. Найбільш відомими системами даного класу є I2, Palantir, HOLMS2, RICAS, Maltego.

Список використаних джерел:

1. Vol. 13 OSCE Guidebook Intelligence-Led Policing, TNTD/SPMU Publication Series Vol. 13, Vienna, June 2017.

УДК 343.9:159.9.075

ЛЕОНІД ВОЛОДИМИРОВИЧ МОГІЛЕВСЬКИЙ
Проректор Харківського національного університету внутрішніх справ,
доктор юридичних наук, професор

АРГУМЕНТАЦІЯ ЄДИНОГО ПІДХОДУ АРХІТЕКТУРИ БАЗ ДАНИХ ПРАВООХОРОННИХ АГЕНЦІЙ УКРАЇНИ

Згідно Рішення Колегії МВС України від 05.11.2018 р. № 18КМ, а також Наказу МВС України від 11.12.2018 р. № 1004 в МВС України з метою інтеграції інформаційних ресурсів МВС в національну систему електронної взаємодії державних інформаційних ресурсів в МВС розробляється і впроваджується Єдина Інформаційна Система органів внутрішніх справ України. В Концепції і Програмі реалізації цієї Концепції передбачено створення єдиної програмно-технічної платформи для інформаційної взаємодії всіх відомчих структур МВС України. Крім того, цими документами передбачено реалізація механізму міжвідомчої взаємодії ЄІС з інформаційними ресурсами інших відомств.

В рішенні колегії МВС України від 05.11.2018 р. № 18КМ також зазначено, що «існує нагальна потреба в забезпеченні автоматизованого доступу центральних органів виконавчої влади, у межах повноважень, до електронних інформаційних ресурсів МВС та ЦОВВ і в агрегації даних» оскільки МВС постійно здійснює активну інформаційну взаємодію з такими відомствами як Служба безпеки України, Національне антикорупційне бюро України, Генеральна прокуратура України, Міністерство юстиції, Національний банк України тощо. На поточний момент така взаємодія здійснюється «…за принципом формування запиту та відповіді безпосередньо користувачем, тоді як доцільно забезпечити автоматизований доступ у межах повноважень і агрегацію даних». Такий же принцип реалізований у взаємодії муж окремими відомствами всередині МВС оскільки інформаційні ресурси відомств як правило мають характер закритих корпоративних розподілених систем, які побудовані незалежно одне від

одного з відповідними наслідками. Вони, як правило, мають ієрархічну структуру і забезпечують доступ до центральної або розподіленої бази даних, і будуються на корпоративних SQL-серверах БД Oracle.

Розходження в ступені структурованості даних, доступних електронним способом, значні. З одного боку, дані, що зберігаються в традиційних реляційних і об'єктно-орієнтованих БД, мають цілком певну структуру. З іншого боку, існують як неструктуровані, так і напівструктуровані дані, частка яких останнім часом швидко зростає і ця тенденція в найближчому майбутньому буде тільки зростати. Аудіо- і відео зображення можна віднести до неструктурованих даних. Прикладом напівструктурованих даних може бути форматований текст, HTML- сторінки, дані в нетрадиційних форматах (наприклад, в ASNI), в форматі XML і ін.

При інтеграції даних з різнорідних джерел необхідно привести їх до загальної структурі, що при великій кількості джерел досить трудомісткий процес. При цьому узагальнена структура може бути дуже складною, а її використання неефективним. Тому найбільшу популярність придбали два підходи до вирішення цього завдання: застосування сховищ даних і віртуальних сховищ.

Процес інтеграції апаратних і програмних засобів такої сукупності корпоративних систем здійснюється шляхом вибору оптимального поєднання апаратних і програмних платформ, що в сукупності забезпечують реалізацію необхідного набору функцій і значень параметрів розподіленої БД, що задовольняють вимогам технічного завдання. При цьому повинні бути враховані:

– тип, архітектурно-структурна організація, функції та параметри системи управління розподіленою базою даних (СКБД), як якщо б вона була виконана за тією ж технологією, що і проектована БД, оскільки необхідні характеристик БД не можуть бути отримані без застосування відповідної СУБД і навпаки;

– тип, архітектурно-структурна організація та параметри комунікаційної мережі як фізичного середовище, в якому відбуваються затримки сигналів (наприклад, сигналів запиту до БД) і отриманих в результаті виконання запитів даних.

В загальному випадку можливі три підходи до побудови архітектури інформаційного середовища міжвідомчої інтегрованої інформаційної системи:

1) побудова нової єдиної архітектури інформаційного середовища з урахуванням сучасних технологічних вимог і приведенням існуючих архітектур до нової;

2) побудова інтерфейсної платформи, як єдиного інформаційного середовища з використанням конверторів між існуючими банками даних,

3) комбінований варіант – побудова двохярусної архітектури інформаційного середовища з центральним сегментом, побудованим на сучасних технологічних принципах, та з інтерфейсним модулем з

конверторами до існуючих корпоративних баз даних при частковій модернізації останніх.

Вибір конкретного варіанту реалізації залежить від трудомісткості його реалізації та фінансових витрат. При цьому слід мати на увазі, що розробка відповідного конвертора, його налаштування та подальший супровід може коштувати порівняно з витратами на розробку самої БД (як, наприклад, для системи I2).

УДК 004.94

ЮРІЙ ВАЛЕРІЙОВИЧ ГНУСОВ
кандидат технічних наук, доцент, завідувач кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ
СЕРГІЙ ВОЛОДИМИРОВИЧ КАЛЯКІН
викладач кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ПЕРСПЕКТИВИ РОЗВИТКУ КВАНТОВИХ ТЕХНОЛОГІЙ

У сучасному суспільстві основним технічним засобом технології переробки інформації служить персональний комп’ютер, який істотно вплинув як на концепцію побудови і використання технологічних процесів, так і на якість отриманої інформації.

Деякі задачі сучасної науки потребують для вирішення великої кількості комп’ютерного часу, тому Візнер і Фейнман висловили ідею побудови квантового комп'ютера.

Квантовий комп'ютер використовує для обчислення не звичайні (класичні) алгоритми, а процеси квантової природи, так звані квантові алгоритми. В основі квантового комп’ютеру лежить кубіт, який може перебувати одночасно в стані 0 і 1. При класичному вимірі 0 або 1 випадуть з певною ймовірністю, а наприклад, система з п'яти кубітів буває одночасно в 32 станах. Квантові обчислення маніпулюють усіма ними відразу, що призводить до значного підвищення швидкодії.

У 2017 році корпорація IBM відкрила власні хмарні сервери для всіх бажаючих попрацювати з квантовими алгоритмами. Спочатку це були пятикубітні системи, потім - шістнадцятикубітні. На цих системах вчені вирішують ресурсоємні завдання, потім перевіряють результати на звичайному комп'ютері. Звичайні комп’ютери поки ще дають точніші результати, хоча і витрачають на розрахунки значно більше часу.

У жовтні 2019 року наукова група Джона Мартінеса з Google заявила про досягнення квантової переваги на 53-кубітном прототипі квантового комп'ютера. Ця подія демонструє колосальний прогрес в технології квантових процесорів.

Квантова комп'ютерна система заснована на принципах суперпозиції і заплутаності. Теоретично вона здатна вирішувати за секунди завдання, на які звичайний цифровий комп'ютер витратить десятки тисяч років.

Підвищити швидкість обчислень допомагає також квантова заплутаність - коли неможливо точно дізнатися, який з пари або ланцюжка кубітів знаходиться в даному стані, вони всі знаходяться в ньому одночасно.

Основна проблема квантових обчислень полягає в тому, що потім результат цих обчислень потрібно перевести в класичний формат, на це і витрачається основний час.

Друга фундаментальна проблема - корекція помилок, які неминуче виникають при обчисленнях, зчитуванні й запису інформації в кубіти через руйнування їх квантового стану. Щоб мінімізувати або виключити їх вплив на обчислення, потрібно розробляти квантові коди, на що може піти не один десяток років. Тому поки на практиці намагаються створювати гібридні квантово-класичні процесори класу NISQ - noisy intermediate scale quantum computer, тобто зашумлений квантовий комп'ютер проміжного масштабу.

Квантові обчислювальні системи бувають двох типів. Ті, що вміють вирішувати одне-єдине завдання, називають квантовими симуляторами. Одна з перших таких систем з двох кубітів представляла собою модель молекули водню. На ній можна було тільки розрахувати її властивості. Квантові симулятори можуть працювати в звичайних комп'ютерах як співпроцесори, що вирішують конкретні і дуже затратні за часом задачі.

Універсальний квантовий комп'ютер здатний виконувати безліч різних завдань. Залежно від складності обчислень число кубітів в ньому нарощують. Недавнє досягнення Google - це демонстрація прототипу універсального квантового комп'ютера, але поки що без повної корекції помилок.

Експеримент по демонстрації квантового переваги є концептуальним доказом ефективності квантових комп'ютерів. І справа не в тому, наскільки швидше були проведені обчислення в порівнянні з класичним і навіть суперкомп'ютером, а в тому, що була продемонстрована принципова можливість проведення керованих обчислень на квантовому процесорі такого великого масштабу. До теперішнього моменту ряд теоретичних команд висловлювали і продовжують висловлювати припущення про неможливість функціонування великих штучних квантових систем в силу принципових фізичних обмежень. Результати, які отримала команда Google, експериментально спростовують ці твердження.

Перспективи розвитку квантової обчислювальної техніки сьогодні складно спрогнозувати навіть фахівцям, але вже зараз зрозуміло, що з появою квантового процесора впевненості в повному захисті даних, включаючи секрети державних органів, big data бізнес-структур, цивільного населення, може прийти кінець, хоча в той же час квантові технології можуть стати як найпотужнішою зброєю, так і найпотужнішим захистом.

Квантовий алгоритм Шора дає можливість обчислити прості множники великих чисел за практично прийнятний час і зламати шифри RSA криптосистем, тобто асиметрична криптографія опиниться під великим

ударом, як тільки буде запущений ефективний квантовий комп'ютер. Таким чином потрібна розробка нових квантово-криптографічних методів захисту інформації.

Інша загроза, якої можна уникнути, впроваджуючи квантово-криптографічні методи захисту інформації, це можливість переорієнтації великих обчислювальних потужностей, які вже обслуговують майнінг криптовалют, на переборні методи злому асиметричних (класичних) систем шифрування.

Квантові комп'ютери, коли їх можна буде використовувати масово, цілком змінять наш світ і стануть символом прогресу сучасних інформаційних систем.

УДК 343.9:159.9.075

ВОЛОДИМИР МИХАЛОВИЧ СТРУКОВ
кандидат технічних наук, доцент, професор кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ
ДМИТРО ЮРІЙОВИЧ УЗЛОВ
кандидат технічних наук, начальник Управління інформаційно-аналітичної підтримки ГУ НП в Харківській області, полковник поліції
ОЛЕКСІЙ ВЯЧЕСЛАВОВИЧ ВЛАСОВ
заступник начальника Управління інформаційного-аналітичної підтримки ГУНП в Харківській області, підполковник поліції

ПРОБЛЕМИ І ПЕРСПЕКТИВИ РОЗВИТКУ ТЕХНОЛОГІЙ ОБРОБКИ ДАНИХ В ПРАВООХОРОННІЙ СФЕРІ УКРАЇНИ

Дослідження, які щорічно проводяться в сфері обробки інформації, свідчать про те, що з моменту появи глобальних комп'ютерних мереж і, зокрема, Інтернету, лавиноподібне наростання кількості згенерованих і загальнодоступних даних є стійкою характерною тенденцією.

До 2020 р. прогнозується збільшення обсягу згенерованих доступних даних до 40 зеттабайт. (Якщо записати 40 зеттабайт даних на диски Blu-ray, загальна вага дисків (без паперової та пластикової упаковки) буде дорівнювати вазі 424 авіаносців.) Одним з основних чинників цього зростання є збільшення частки автоматично генеруюємих даних: з 11% від загального обсягу у 2005 р. до понад 40% у 2020 р.

З усього океану інформації за оцінками фахівців менш 1% піддається аналізу. Разом з тим, реєстрація та зберігання інформації має сенс (тобто вона корисна) лише в тому випадку, якщо вона затребувана, тобто якимось чином обробляється. А на сьогоднішній день навіть сама елементарна обробка, така як простий перегляд, при величезному обсязі інформації людиною просто фізично неможлива.

Такий стан можна спостерігати і в правоохоронній сфері в Україні. Якщо ще зовсім недавно практичні всі накопичуювані і обробляємі дані зберігалися в файлах системи «Інформаційний портал Національної поліції України» (ІП НПУ) в регламентованій строго структурованій формі, то зараз з інтенсивним впровадженням систем відеофіксації - це потокові відеодані, які в них реєструються і обробляються в реальному режимі часу (on-line). Причому кількість таких даних з введенням систем відеофіксації у всіх регіонах буде постійно зростати, і їх кількість у порівнянні зі строго структурованими даними переважатиме.

У свою чергу, інтеграція процесів зберігання і обробки інформації призводить до неефективності традиційних розподілених систем обробки даних і доцільності створення централізованих систем на основі комбінації технологій хмарних обчислень і клієнт-серверної технології і створення ЦОД (центрів обробки даних) на їх основі. Саме в цьому напрямку заплановано подальший розвиток системи інформаційного забезпечення НПУ (за матеріалами квітневого семінару керівників ДОАЗОР і ДІАП 2018 р. в м.Ужгороді).

Всі ці процеси призводять до явища, яке можна назвати як «криза перевиробництва інформації». Суть його полягає в тому, що люди фізично не в змозі засвоїти всю генеруєму все більш швидкими темпами інформацію або навіть усвідомити всі можливості її використання.

Мало того, що ми не встигаємо прочитати опубліковане, так ці дані швидко втрачають свою актуальність, а на їх місце приходять нові дані.

З цього випливає, що людина повинна отримувати тільки потрібну і корисну «вижимку» з усіх даних, що підлягають аналізу, і в тому обсязі, в якому вона здатний її ефективно сприйняти. А весь препроцесінг (попередня обробка) повинен виконувати інтелектуальний робот-парсер. Причому, в ідеалі не тільки препроцессінг, але і прийняття рішень, оскільки часто час, що відводиться на прийняття рішення, обчислюється частками секунди, а людина просто фізично не в змозі це зробити.

Окремим напрямком, який останнім часом дуже інтенсивно розвивається, можна вважати обробку даних, що циркулюють у відкритих мережах. Це своєрідний океан різнотипних, здебільшого неструктурованих даних. З урахуванням вищесказаного про ефективну ручній обробці цієї категорії даних не може бути й мови. І на даний момент в світі вже розроблено кілька систем, які в автоматичному режимі обробляють такі потоки даних, зокрема продукти фірми Palantir.

Таким чином, розвиток подій в сфері обробки даних в останні роки призводить до неминучого висновку про те, що традиційні засоби обробки інформації двохтисячних років, зокрема інформаційно-пошукові системи, до яких належить пошуковик Google, а також ІП НПУ, представляють засоби минулого технологічного покоління. На передній план виходять інструментальні засоби наступного технологічного покоління - епохи четвертої промислової революції, які в своїй основі мають моделі і методи Data Science (Data Mining, Text Mining, Web Mining, Visual Mining) і

штучного інтелекту на основі квазі-квантових і квантових обчислень і хмарних технологій.

Другий важливий висновок полягає в тому, що і зараз і в подальшому на інформаційному ринку будуть розвиватися все більш вузькі спеціалізації і відповідні потоки даних, і затребувані вузькі фахівці, які вміють ефективно працювати з ними. І це чудово розуміють керівники силових структур в США, Великобританії, Німеччини.

У розвинених країнах останні роки в розвитку і застосуванні сучасних технологічних інструментів обробки даних в правоохоронних структурах зроблений в буквальному сенсі прорив [1, 2]. Основними передумовами для такого прориву стали наступні фактори:

1) централізована (зверху) стимуляція і мотивація цих процесів на рівні керівництва силових структур;

2) активна співпраця силових структур з провідними науковими структурами (провідними університетами, провідними комерційними фірмами - світовими лідерами в передових сучасних галузях, в першу чергу, в IT-сфері та робототехніки) в найбільш перспективних технологічних напрямках;

3) потужне фінансування перспективних проектів.

Список використаних джерел:

1. Овчинский В. С. Криминология цифрового мира : учеб. Москва. Норма. ИНФРА–М, 2018. 352 с.

2. Gartner: Топ-10 стратегических трендов развития технологий в 2019 году. URL: https://ain.ua/2018/10/26/gartner-top-10-trendov-razvitiya-texnologij/.

УДК 681.3.06

ВЛАДИСЛАВ ВЛАДИСЛАВОВИЧ ГУДІЛІН
курсант 2 курсу факультету №4 Харківського національного університету внутрішніх справ
ВОЛОДИМИР МИХАЙЛОВИЧ СТРУКОВ
кандидат технічних наук, доцент, професор кафедри інформаційних технологій та кібербезпеки факультету №4 Харківського національного університету внутрішніх справ

ПРОБЛЕМИ ЗАХИСТУ ЗАШИФРОВАНИХ ДАНИХ В ЕПОХУ КВАНТОВИХ ТЕХНОЛОГІЙ

На сьогоднішній день більша частина інформації, яка передається по відкритих каналах передачі даних, шифрується з впровадженням криптографічних систем з відкритим ключем. Принцип роботи даних систем полягає у використанні двох ключів. Відкритий ключ кореспондента використовується при шифруванні вихідного повідомлення. Він публікується у відкритому доступі. Закритий або секретний ключ вживають при

розшифровці отриманого повідомлення. З кінця 70-х років XX століття найбільш використовуваною системою з відкритим ключем є алгоритм RSA. Стійкість алгоритму RSA ґрунтується на тому, що факторизація великих чисел – дуже складна математична задача, для розв'язання якої до сих пір не існує достатніх обчислювальних потужностей, а також ефективного алгоритмічного рішення. Саме тому криптографічна система з відкритим ключем довгий час вважалася однією з найнадійніших систем шифрування [1].

Однак в 1994 році американський вчений Пітер Шор розробив квантовий алгоритм факторизації (алгоритм Шора). Отриманий квантовий алгоритм, на відміну від класичних алгоритмів, справляється із завданням факторизації за поліноміальний час. Виходячи з цього факту алгоритм Шора може бути використаний для злому RSA. Суть алгоритму полягає в зведенні задачі факторизації до пошуку періоду деякої функції. Якщо відомий її період, то факторизація здійснюється за допомогою алгоритму Евкліда за реальний час на класичному комп'ютері. Таким чином, підхід Шора включає в себе дві частини: класичну і квантову. Квантова частина займається пошуком періоду функції, а класична частина спочатку готує цю функцію, а потім перевіряє період, знайдений квантовою частиною. Якщо період знайдений правильно, то задача буде вирішена. Таким чином, Пітер Шор показав, що досить потужний квантовий комп'ютер може з легкістю зламати алгоритм RSA, і це викликало шок серед спеціалістів з інформаційної безпеки.

Вважалося, що для злому RSA-шифрування, на якому побудовані сьогодні майже всі системи, що передають і зберігають конфіденційну інформацію, необхідний квантовий комп'ютер з мільярдом кубітів. Однак нещодавно дослідження квантових обчислень, проведене Крейгом Гідні з Google і Мартіном Екерой з Королівського інституту в Стокгольмі, відкрило більш ефективний метод злому систем шифрування і на порядок скоротило вимоги до ресурсів. Вони довели, що для злому знадобиться всього 20 млн кубіт і вісім годин роботи. Крім того, вони підрахували, що пристрої з 20 млн кубіт, що неможливі сьогодні, можуть стати реальністю через 25 років [2].

Прогрес в області створення квантового комп'ютера йде швидше ніж передбачалося. Кращого результату у розробці квантового комп'ютера домоглася компанія IBM, яка за допомогою квантового комп'ютера з п'яти кубітів змогла розкласти на множники число 15. Канадська компанія D-Wave випускає квантові комп'ютери з тисячі кубітів, з якими експериментують в Google і NASA. Однак машина D-Wave – не універсальний квантовий комп'ютер, і її перевага в порівнянні з класичними комп'ютерами багатьма оскаржується. Поряд з успіхами компаній IBM і Google, наукові групи з Гарварда та університету Меріленду практично одночасно реалізували дві нові системи для квантових обчислень з 51 і 53 кубітами.

Отже, зі збільшенням загроз шифрування даних за допомогою традиційного алгоритму RSA, слід впроваджувати нові підходи шифрування інформації. Спеціалісти пропонують застосувати квантову та постквантову криптографію. Перший підхід – постквантова криптографія пропонує нові алгоритми шифрування, які базуються на математичних задачах, що

представляють складність для злому як «класичними», так і квантовими комп'ютерами. На цей момент в сфері постквантової криптографії ведуться наукові дослідження з пошуку таких алгоритмів, виконуються перевірки існуючих рішень і пілотні проекти їх реалізації. Однак до сих пір на ринку відсутні єдині визнані стандарти постквантового шифрування, які довели свою ефективність. Можлива ситуація, при якій з розвитком квантових комп'ютерів обраний алгоритм вже не забезпечить необхідний рівень захисту, і його доведеться міняти. Тому важливо вибрати оптимальний алгоритм відразу. Інша особливість постквантової криптографії – це високі вимоги до обчислювальних ресурсів. З одного боку, дані алгоритми можна реалізувати практично в будь-якому програмному коді, з іншого боку – при зростанні обсягів даних, що захищаються, потужності наявного обладнання може виявитися недостатньо.

Другий підхід – квантова криптографія, яка для забезпечення секретності інформації використовує основні закони квантової механіки. У квантовій криптографії можна виділити наступні основні напрямки: технології квантової передачі даних, технології квантового розподілу ключів, квантове шифрування, технології квантової цифрового підпису, технології квантового хешування. Математично було доведено, що квантові канали передачі даних є найбезпечнішими, що дозволяє отримати новий рівень захисту інформації. Носієм інформації, яка зашифрована з використанням законів квантової механіки, в даному випадку буде квантовий об'єкт, наприклад, фотон. Згідно фундаментальним законам квантової фізики вимір квантового об'єкта або будь-який інший вплив на нього призводить до зміни його стану. З цього випливає, що спроба перехопити повідомлення або прослуховування каналу призведе до зміни стану фотона, що відразу ж стане відомо одержувачу. Складність перехоплення та розшифрування інформації полягає у поляризації фотона. Поляризація використовується, як для шифрування так і для дешифрування. Наприклад, фотони, що поляризовані по вертикалі, можуть кодувати одиницю, а по горизонталі – нуль. Виміряти поляризацію можна тільки один раз, після чого стан незворотньо змінюється. Квантові канали передачі даних є основою для реалізації алгоритмів квантового розподілу ключів – головного напрямку розвитку квантової криптографії. Технологія квантового розподілу ключів дозволяє розподіляти ключі між віддаленими користувачами по відкритих каналах зв'язку, ґрунтуючись на законах квантової фізики. Технологія квантового розподілу ключів будується на неможливості копіювання невідомого квантового стану, неможливості прослухати сигнал, неможливості абсолютно надійно розрізнити два різних стани [3].

Квантова криптографія є цілком працюючою технологією. Наприклад, швейцарська приватна компанія ID Quantigue забезпечувала захист даних при пересиланні результатів підрахунку голосів на виборах в Швейцарії за допомогою квантової криптографії. Перешкодою для повсюдного застосування квантової криптографії є обмежена відстань, на яке можна передавати фотони. Проходячи через оптичне волокно, половина фотонів

втрачається кожні 10-15 км, що робить передачу ключа на відстань більше 200-300 км практично неможливою. Але Китай запропонував вирішити цю проблему, запустивши квантовий супутник. Супутник проводить сеанси квантового зв'язку зі станціями, що розташовані на Землі, поки пролітає над ними. Це дозволяє суттєво збільшити відстань при передачі даних у зашифрованому стані між віддаленими точками.

Таким чином, з розвитком квантових технологій всі традиційні асиметричні та симетричні алгоритми шифрування стають все менш надійними. Так, для вирішення цієї масштабної задачі державним та приватним установам слід спрямувати увагу на впровадження постквантової та квантової криптографії.

Список використаних джерел:

1. Simon Singh The Code Book. Doubleday. 1999. 416 c.
2. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits by Craig Gidney and Martin Ekera. URL: https://www.researchgate.net/publication/333338015_How_to_factor_2048_bit_RSA_integers_in_8_hours_using_20_million_noisy_qubits.
3. Willi-Hans Steeb, Yorick Hardy Problems and Solutions in Quantum Computing and Quantum Information (third edition). World Scientific. Singapore. 2011.

УДК 004.056

ОЛЕКСАНДР ОЛЕКСАНДРОВИЧ МОЖАЄВ
доктор технічних наук, професор, професор кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ
ЮРІЙ ПЕТРОВИЧ ГОРЕЛОВ
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ ІМУННИХ АЛГОРИТМІВ У СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

У зв'язку з безпрецедентно швидким розвитком комп'ютерних і телекомунікаційних технологій та переходом до інформаційного суспільства проблема забезпечення кібербезпеки і побудови інформаційно-безпечних розподілених обчислювальних систем стала однією з найбільш актуальних.

Традиційні методи виявлення вторгнень, що застосовуються сьогодні, не здатні забезпечити надійний захист комп'ютерних систем від проникнення комп'ютерних вірусів, несанкціонованого доступу, вторгнень і ін. Методи штучного інтелекту дозволяють створити принципово нові алгоритми виявлення шкідливих програм та значно підвищити рівень захищеності

комп'ютерних систем шляхом реалізації систем виявлення вторгнень (СВВ), які розглядаються як один з базових елементів системи захисту інформаційної системи.

Під СВВ розуміються програмні та програмно-апаратні технічні засоби, що реалізують функції автоматизованого виявлення в інформаційних системах дій, спрямованих на навмисний несанкціонований доступ до інформації, а також спеціальних впливів на інформацію з метою її добування, знищення, перекручення або блокування. Виділяються два типи СВВ: системи виявлення вторгнень рівня мережі (Network Intrusion Detection System, NIDS) і системи виявлення вторгнень рівня вузла (Host-based Intrusion Detection System, HIDS).

Основне завдання СВВ - аналіз зібраних даних з метою виявлення вторгнень. Для її вирішення використовуються одночасно сигнатурні і евристичні методи. Спосіб пізнання сигнатури полягає в описі атаки у вигляді сигнатури і пошуку даної сигнатури в контрольованому просторі (мережевий трафік, журналі реєстрації і т.д.). Як сигнатура атаки може виступати шаблон дій або рядок символів, що характеризують аномальну активність в інформаційній системі. Незважаючи на ефективність сигнатурного методу, існує проблема створення такої сигнатури, яка б описувала всі можливі модифікації атаки. Для вирішення цієї проблеми застосовуються евристичні методи. Дані методи допомагають виявляти відхилення від нормального функціонування автоматизованої системи, використовуючи еталонну модель функціонування. Спочатку визначається типові значення для таких параметрів, як завантаженість ЦПУ, активність роботи диска, частота входу користувачів в систему і інші. Потім при виникненні значних відхилень від цих значень система сигналізує про загрозливу ситуацію.

Перспективними для розробки алгоритмічного забезпечення систем захисту інформації, що мають вищезгадані властивості, є методи, засновані на принципах роботи нейронної мережі, імітаційного моделювання та імунної системи. Використання останнього методу в СВВ є одним з найбільш перспективних, оскільки сам принцип роботи імунної системи і властивості, якими вона характеризується, максимально орієнтовані на вирішення завдання виявлення інцидентів інформаційної безпеки. Штучна імунна система (ШІС) будується, як правило, тільки на двох центральних поняттях: антиген - антитіло. Як антигени виступають системні виклики або мережеві пакети. При первинній зустрічі імунної системи з антигеном він вивчається, і на підставі складеного шаблону виробляються антитіла, яки знищують, блокують або пропускають антиген.

Одним з можливих варіантів створення системи, заснованої на принципах роботи імунної системи людини, є реалізація алгоритму негативного відбору. Для пояснення того, як імунна система "бореться" проти чужорідних антигенів, використовується теорія клональної селекції. Коли антиген проникає в живий організм, він починає розмножуватися і вражати своїми токсинами клітини організму. Ті клітини, які здатні розпізнавати чужорідний антиген, розмножуються способом, пропорційно

ступеня їх розпізнавання: чим краще розпізнавання антигену, тим більша кількість потомства (клонів) буде створене. Протягом процесу репродукції клітини окремі клітини піддаються мутації, яка дозволяє їм мати більш високу відповідність (афінність) до антигену, що розпізнається. Навчання в імунній системі забезпечується збільшенням відносного розміру популяції і афінності тих лімфоцитів, які довели свою цінність при розпізнаванні представленого антигену. Основними імунними механізмами при розробці алгоритму є обробка певної множини антитіл з набору клітин пам'яті, видалення антитіл з низькою афінностю, дозрівання афінності та повторний відбір клонів пропорційно їх афінності до антигенів.

ШІС з клональною селекцією дозволяють виявити навмисні зміни в даних, що контролюються. Таким чином, застосування ШІС як евристичного блоку систем превентивного захисту інформації дозволяє ефективно вирішувати завдання виявлення аномалій в діях користувачів систем та мережевого трафіку.

У доповіді розглядаються деякі особливості реалізації алгоритму клональної селекції з використанням процедури мутації, побудови детекторів та антигенів, а також розрахунку афінності антитіл.

УДК 004.056

СЕРГІЙ ГЕНАДІЙОВИЧ СЕМЕНОВ
доктор технічних наук, професор, професор кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

КАССЕМ ХАЛІФЕ, ИССАМ СААД
PhD, Researcher, Sarepta Technical Institute, Ліван

КОМПЛЕКС МАТЕМАТИЧНИХ МОДЕЛЕЙ ПРОЦЕССУ УПРАВЛІННЯ РОЗРОБКОЮ ПРОГРАММНОГО ЗАБЕЗПЕЧЕННЯ

Проведені дослідження показали, що в даний час існує декілька найбільш популярних методологій розробки ПЗ. Серед них доцільно виділити сімейство «гнучких» методологій Agile (XP, SCRUM) і методології «дбайливого виробництва» (Kanban). У кожної з них є свої особливості, які варто враховувати, вибираючи ту чи іншу методологію для управління проектом.

Крім того, для успішного управління процесом розробки програмного забезпечення буває недостатньо вибрати чи іншу методологію і дотримуватися її протягом усього процесу. У разі досить великого проекту, розробка якого ведеться досить довгий період часу, важливою може виявитися здатність швидко адаптувати використовувану в даний момент методологію відповідно до обставин, що змінюються, тобто по суті синтезувати різні варіанти використання «гнучких» і «дбайливих» методологій в один проект.

Таким чином, в даний час питання, пов'язані з оптимізацією процесу розробки ПЗ, незважаючи на різноманіття «гнучких» методологій управління, залишаються актуальними.

Питання оптимізації нерозривно пов’язані з питаннями моделювання та прогнозування. Стосовно процесу розробки програмного забезпечення одним із шляхів вирішення завдання прогнозування є використання підходу, заснованого на оцінці часових витрат на окремі етапи розробки ПЗ, з урахуванням функцій залежно поточного числа активних дефектів додатка від часу, отриманих експериментальним шляхом, а також за допомогою математичного моделювання. Таке комплексне використання апріорних та апостеріорних даних має дозволити врахувати специфіку сучасних методик розробки ПЗ з можливою динамічною зміною (розширенням) рамок проекту за бажанням замовника або з інших причин.

У доповіді запропоновано комплекс математичних моделей процессу розробки программного забезпечення, що включає моделі ініціалізації та реалізації функціоналу ПО. Математична модель етапу ініціалізації процесу розробки ПО заснована на концептуальних положеннях Agile. Це дозволило виділити ряд найбільш важливих параметрів оцінки часових витрат ініціалізації і визначити їх залежності від якісних характеристик учасників проекту. Математична модель етапу реалізації функціоналу ПЗ відрізняється від відомих урахуванням показників безпечного програмування. Це дозволило підвищити точність результатів моделювання на 3%.

УДК 343.98

МИХАЙЛО ОЛЕКСАНДРОВИЧ МОЖАЄВ
кандидат технічних наук, завідувач лабораторії КТТДДВЗ Харківського НДІСЕ
ВІКТОРІЯ ЄВГЕНІВНА РОГ
старший викладач кафедри інформаційних технологій та кібербезпеки факультету №4, Харківського національного університету внутрішніх справ
МАКСИМ ВІТАЛІЙОВИЧ УСАТЕНКО
студент 3 курсу факультету – інституту підготовки кадрів для органів юстиції України, Національного юридичного університету імені Ярослава Мудрого

ДОСЛІДЖЕННЯ ФАКТІВ ЗНИЩЕННЯ ЦИФРОВОЇ ІНФОРМАЦІЇ НА МАГНИТНИХ НОСІЯХ

За останні кілька десятиліть комп'ютерні інформаційні технології міцно увійшли в наше життя і стали складовою частиною документообігу. Спочатку відпрацьовані механізми забезпечення інформаційної безпеки не в повній мірі відповідають загрозам, актуальним для нових комп’ютерних систем, тому сьогодні потрібно їх істотна модернізація або навіть повний перегляд.

У більшості обчислювальних систем (ОС) в якості основного енергонезалежної носія інформації використовується накопичувач на

жорсткому магнітному диску (НЖМД). Тому аналіз можливих можливих несанкціонованих вторгнень в пам'ять інформаційної системи є досить актуальної метою У цей доповіді розглядається визначення фактів знищення інформації у цифрових носіях для уніфікації підходів визначення ознак знищення інформації та їх інтерпретації.

Відомо, що у більшості ОС інформація зберігається в ієрархічних базах даних – файлових системах. Будь-яка файлова система має два типи елементів: файли, що містять прикладні дані та елементи-контейнери (каталоги, папки), які можуть містити файли або інші елементи-контейнери. Файли ідентифікуються за допомогою файлових записів, розташованих у каталогах або спеціальних системних таблицях. Місцезнаходження даних файлу (тобто номера секторів НЖМД, в яких вони записані) частково, а іноді і повністю визначається вмістом його файлового запису.

При видаленні файлу стандартними засобами файлової системи, інформацію, яка містилася в файлі, також не буде перезаписано. Драйвер файлової системи просто фіксує, що відповідній файловий запис не використовується і сектора, що містили дані віддаленого файлу, вільні для запису нової інформації.

Очевидно, що до тих пір, поки дані знищених таким чином файлів не будуть перезаписані, їх можна відновити. Якість відновлення залежить від файлової системи. Так, для поширених файлових систем FAT і NTFS [9, 11] можливості по відновленню файлів відрізняються. У файлової системи родини FAT файл буде повністю відновлений тільки в тому випадку, якщо він не був фрагментований, тобто його дані розташовувалися на диску послідовно, в одному ланцюжку секторів. У файлових системах NTFS файл може бути відновлений при будь-якому рівні фрагментації.

Для того, щоб процес перезапису секторів віддалених файлів стався «природним» чином, в ході звичайної роботи файлової системи може знадобитися тривалий час – тижні або навіть місяці, в залежності від режиму експлуатації.

Якщо інформація на жорсткому диску була переписана, то отримати до неї доступ програмним способом неможливо. Однак, як було вказано вище, сліди вихідного запису можуть зберігатися по краях дискових доріжок навіть після кількох перезаписів. Існує цілий ряд методів, що дозволяють проаналізувати розподіл областей намагніченості на поверхні магнітного диска, що дає потенційну можливість отримати доступ до перезаписаної інформації.

Найбільш ефективними є різні методи візуалізації магнітних полів, що дозволяють створювати візуальне уявлення робочих поверхонь носія з дозволом, достатнім для побітового дослідження інформації. У даний час розроблено понад десяти різних методів візуалізації. На відміну від прийнятого в техніці магнітного запису трактування поняття «сигналограма», як тимчасового розподілу амплітуд сигналу запису/зчитування, техніка візуалізації даних на магнітних носіях використовує інший підхід. Під магнітною сигналограмою розуміється просторовий розподіл амплітуд залишкової намагніченості. Магнітна сигналограма дає можливість

«побачити» дані на носії. Найбільш часто для дослідження магнітних полів носіїв використовуються наступні методи:

– метод Біттера;
– магнітооптичні методи;
– магнітна силова мікроскопія.

Для візуалізації магнітних доменів Біттер застосував колоїдну суспензію магнітних частинок, кожна з яких за формою нагадує мікроскопічну голку розмірами всього декілька мікронів. Перебуваючи в підвішеному стані і практично не відчуваючи тертя, такі частинки можуть швидко переорієнтовуватися в залежності від напрямку прикладеного магнітного поля. Якщо нанести на намагнічену поверхню тонкий шар суспензії, вони концентруються уздовж ділянок зразка, де намагніченість змінює свій знак, формуючи так звані картини Біттера, які можна спостерігати за допомогою оптичного мікроскопа. Для досягнення більшого контрасту зразок іноді поміщують у невелике зовнішнє магнітне поле, спрямоване уздовж його поверхні.

Таким чином, використовував запропонований метод візуалізації магнітних доменів можна отримати інформацію про несанкціоноване вторгнення в систему пам'яті інформаційної системи, та визначити факт знищення інформації.

УДК 004.05

ОЛЕКСІЙ ВЯЧЕСЛАВОВИЧ ПЕРЕЦЬ
курсант 2 курсу факультету № 4 Харківського національного університету внутрішніх справ
ОКСАНА ПЕТРІВНА МЕЛАЩЕНКО
Старший викладач кафедри інформаційних технологій та кібербезпеки Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ УСТАНОВЛЕННЯ МІСЦЕЗНАХОДЖЕННЯ РАДІОЕЛЕКТРОННОГО ЗАСОБУ В ДІЯЛЬНОСТІ ПОЛІЦІЇ

Одним з основних засобів отримання доказів у кримінальному процесі на стадії досудового розслідування є негласні слідчі (розшукові) дії, завдяки яким доводиться вина особи у вчиненні злочинів та розслідується левина частина тяжких та особливо тяжких злочинів [1]. Одним із таких засобів доказування - негласною слідчою (розшуковою) дією, є використання в діяльності поліції установлення місцезнаходження радіоелектронного засобу.

Як відомо, у сучасному інформаційному суспільстві мобільний телефон стає продовженням нашої особистості і нашого інтелекту. Не дивно, що аналіз даних із телефону та установлення його місцезнаходження стає все більш важливою навичкою при розкритті злочинів. Установлення місцезнаходження радіоелектронного засобу здійснюється для реалізації окремих завдань кримінального впровадження. Як зазначає О. Комарницька,

дані дії не обмежують конституційні права та свободи людини, оскільки їх об’єктом є технічний засіб, а не фізична особа [2].

Щодо технічної сторони установлення місцезнаходження радіоелектронного засобу, то у відповідності з технічними вимогами, кожен мобільний телефон повинен мати спеціальний засіб ідентифікації. IMEI (англ. International Mobile Equipment Identity – міжнародний ідентифікатор мобільного обладнання) – серійний номер мобільного пристрою (п'ятнадцятизначне число, тобто 14 цифр коду плюс 15-та контрольна цифра), який встановлюється заводом-виробником та є унікальним для кожного мобільного телефону. Цей номер встановлюється заводом-виробником при виготовленні апарату та служить для точної і повної ідентифікації телефону в мережах форматів GSM та UMTS: автоматично передається апаратом у мережу оператора при підключенні [3]. Тому, слідчі або спеціалісти оперативних підрозділів їдуть на місце злочину і проводять радіорозвідку, тобто визначають, які базові станції знаходяться поряд, а отже – могли мати з’єднання із мобільним телефоном зловмисника. За результатами проведення цієї негласної слідчої (розшукової) дії може бути встановлене місцезнаходження кінцевого обладнання рухомого (мобільного) зв'язку, яке використовується особою, підозрюваною або причетною до вчинення злочину, інших радіовипромінювальних пристроїв, активованих у мережах операторів рухомого (мобільного) зв'язку, тощо [4].

Але, незважаючи на ефективність цього негласного розшукового заходу, він має і певні недоліки. Зокрема, як вказує Л. В. Бобрицький, що хоча є чіткий механізм проведення даної процедури, але здійснення такого оперативно-розшукового заходу достатньо складне, відносно довготривале і не забезпечує оперативного вирішення завдань щодо встановлення особи злочинців, або свідків та їх місцезнаходження [5].

Також, як зазначає Луцик В. В. у [6] у правозастосовний практиці виникають ситуації, коли один і той самий номер IMEI належить декільком телефонам. Така ситуація є результатом недобросовісної комерційної діяльності виробників телефонів.

Таким чином, щодо використання установлення місцезнаходження радіоелектронного засобу в діяльності поліції можна вказати, що це дійсно ефективний засіб доведення вини особи у вчиненні злочинів та розслідування тяжких та особливо тяжких злочинів. Однак при його застосуванні слідчим або спеціалістам оперативних підрозділів слід, по-перше, дотримуватися вимог механізму проведення даної процедури, передбаченої КПК України, по-друге, враховувати технічні особливості і специфіку використання радіоелектронного засобу та установлення його місцезнаходження, по-третє, знати «підводні камені», які можуть виникнути під час застосування цієї негласної слідчої (розшукової) дії.

Список використаних джерел:

1. Синявський С. М. Правові аспекти проведення негласної слідчої (розшукової) дії – установлення місцезнаходження радіоелектронного засобу.

Право і суспільство. 2016. № 4. С. 221–224. URL: http://nbuv.gov.ua/UJRN/Pis_2016_4_39.

2. Комарницька О., Прядко В. Установлення місцезнаходження засобу радіоелектронного зв'язку: підготовка та проведення негласної слідчої (розшукової) дії. Вісник Національної академії прокуратури України. 2014. № 2. С. 71–78. URL: http://nbuv.gov.ua/UJRN/Vnapu_2014_2_14

3. Кримінальний процесуальний кодекс України: Науково-практичний коментар. У 2 т. Том 1. О. М. Бандурка, Є. М. Блажівський, Є. П. Бурдоль та ін. ; за заг. ред. В. Я. Тація, В. П. Пшонки, А. В. Портнова. Харків. Право, 2012. 768 с.

4. Бобрицький Л. В. Практичні аспекти застосування кримінального процесуального законодавства України щодо установлення місцезнаходження радіоелектронного засобу. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2013. № 3(спец. вип.). С. 155–160. URL: http://nbuv.gov.ua/UJRN/boz_2013_3(spets.

5. Луцик В. В. Установлення місцезнаходження радіоелектронного засобу. Юридичний науковий електронний журнал. № 4. 2014. С. 199– 202.

УДК 004.05

ВІТАЛІЙ АНАТОЛІЙОВИЧ СВІТЛИЧНИЙ
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та кібербезпеки Харківського національного університету внутрішніх справ

КІБЕРБЕЗПЕКА УКРАЇНИ ТА ОСОБЛИВОСТІ КІБЕРЗЛОЧИНІВ

Відповідно до законодавства України, кібербезпека – це захищеність життєво важливих інтересів людини й громадянина, суспільства та держави у процесі використання кіберпростору, яка забезпечує сталий розвиток інформаційного суспільства і цифрового комунікативного середовища, своєчасне виявлення, запобігання та нейтралізацію реальних і потенційних загроз національній безпеці України у кіберпросторі (ст. п. 5 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України»). У глобальному розумінні, кібербезпекою є реалізація заходів із захисту мереж, програмних продуктів та систем від цифрових атак.

В державі на законодавчому рівні приймаються відповідні закони та нормативні акти, які регулюють відносини в цій сфері. Станом на 2019 р. до правової основи кібербезпеки України входять такі нормативно-правові акти: Конституція України, Кримінальний кодекс України, закони України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки» та інші закони, Доктрина інформаційної безпеки України, Конвенція Ради Європи про кіберзлочинність та інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

Аналіз першопричин кіберзлочинів призводить до цілої низки системних проблем у галузі, ігнорувати які з кожним наступним інцидентом стає дедалі важче. Одна з головних – неефективна нормативна база та система управління.

Так, наприклад закон України "Про захист інформації в інформаційно-телекомунікаційних системах" та серія нормативних документів про технічний захист інформації на теперішній час є безнадійно застарілі. Більше того, вони зобов'язують органи державної влади, об'єкти критичної інфраструктури та приватні компанії, які хочуть надавати послуги державним органам (наприклад, Інтернет-провайдери), впроваджувати Комплексну систему захисту інформації, яка окрім того, що морально застаріла, впродовж багатьох років довела свою неефективність.

Відповідно до Конвенції про кіберзлочинність, яка є частиною українського законодавства з 11.10.2005 р., кіберзлочини умовно поділяються на чотири види.

До першого виду належать правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем. До цього виду кіберзлочинів можна віднести всі злочини, спрямовані проти комп’ютерних систем і даних (наприклад, навмисний доступ до комп'ютерної системи або її частини; навмисне пошкодження, знищення, погіршення, зміна або приховування комп'ютерної інформації; навмисне вчинення, не маючи на це права, виготовлення, продажу, придбання для використання, розповсюдження або надання для використання іншим чином пристроїв, включаючи комп'ютерні програми).

До другого виду кіберзлочинів належать правопорушення, пов'язані з комп'ютерами. Такі злочини характеризуються умисним діянням, що призводить до втрати майна іншої особи шляхом будь-якого введення, зміни, знищення чи приховування комп'ютерних даних або будь-якого втручання у функціонування комп'ютерної системи, з шахрайською або нечесною метою набуття, не маючи на це права, економічних переваг для себе чи іншої особи.

Третій вид кіберзлочинів охоплює правопорушення, пов'язані зі змістом (контентом), що полягає у здійсненні умисних незаконних дій щодо вироблення, пропонування або надання доступу, розповсюдження дитячої порнографії, а також володіння такими файлами у своїй системі.

Четвертим видом є умисні дії, пов'язані з порушенням авторських та суміжних прав, відповідно до вимог Бернської Конвенції про захист літературних і художніх творів, Угоди про торговельні аспекти прав інтелектуальної власності та Угоди ВОІВ про авторське право, а також національного законодавства України.

Існують також інші класифікації кіберзлочинів, проте запропонована конвенцією є найбільш популярною. В Україні політика щодо кібербезпеки покладається на низку державних органів, а саме на Державну службу спеціального зв'язку та захисту інформації України, Національну поліцію України, Службу безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи,

Національний банк України. В кожному із зазначених органів діють відповідні підрозділи. Але при цьому кожна людина що використовує кіберпростір грає певну роль в забезпеченні своєї кібербезпеки кіберпростору, включаючи пристрої та мережі, які вона використовує.

УДК 351.741:343.45:342.721
ПЕТРО СЕРГІЙОВИЧ КЛІМУШИН
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ
ЄЛИЗАВЕТА ГЕОРГІЇВНА БЄЛЯЄВА
курсант 4 курсу факультету № 4 Харківського національного університету внутрішніх справ

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Одним із напрямків розвитку України є підвищення захисту персональних даних та забезпечення прав осіб на недоторканність приватного життя. Захист основоположних прав і свобод людини щодо обробки персональних даних безпосередньо впливає на авторитет держави, зокрема, її здатність реалізовувати ефективну внутрішню і зовнішню політику в галузі прав людини. Як показує практика, процес гармонізації національного законодавства у сфері захисту персональних даних є складним, тому повинен бути безперервним і слідувати постійним змінам, які відбуваються в цій області. В даний час кожен володілець та розпорядник персональних даних визначає власну політику безпеки щодо обробки даних, яка має відповідати вимогам законодавства [2].

У 2015 році був прийнятий Закон України «Про Національну поліцію», який передбачає повноваження поліції в безпрецедентному масштабі формувати і використовувати інформаційні ресурси (бази даних). Сучасні інформаційні технології та законодавство відкривають можливості для правоохоронних органів обробляти величезний обсяг персональних даних. Проте, з огляду на численні переваги цих технологій, слід визнати, що при несанкціонованому їх використанні (без дотримання вимог закону), це може призвести до серйозних наслідків [3].

Серед поширених порушень можна виділити [1]:

– Доступ до персональних даних за відсутності повноважень, законної підстави і обґрунтованої мети такого доступу.

– На практиці поширеними є випадки, коли працівники підрозділів з протидії наркозлочинності масово витребовують з медичних закладів дані щодо осіб, які стоять на обліку як такі для формування баз даних про цих осіб. Суспільство так і не отримало відповідь, яка мета і законна підстава збирати інформацію про здоров‘я людини, яка не вичинила правопорушення.

– Залишається відкритим питання щодо обробки відеозаписів з нагрудних камер поліцейських, а також систем відеоспостереження (збір, доступ, формування баз, порядок та термін зберігання такої інформації). Зокрема, як відеозаписи з камер з‘являються в мережі Інтернет, без дотримання вимог законодавства про захист персональних даних.

– Відсутність належної політики безпеки персональних даних розпорядником таких даних, затвердженої шляхом розробки та прийняття відповідної внутрівідомчої нормативно-правової бази.

– Відсутність прозорого управління у сфері захисту даних. Міжнародними стандартами визначено, що суспільство має право знати, яку інформацію збирають, які умови безпеки, зберігання та знищення персональних даних.

– У більшості випадків інформація, яка збирається і використовується в поліції не архівується в формати, які забезпечують певний рівень безпеки та конфіденційності, а також не ведеться належний її облік.

Однією з причин, яка призводить до порушення вимог законодавства у сфері захисту персональних даних є низки знання співробітників зобов’язань щодо забезпечення конфіденційності і заходів безпеки під час обробки даних.

Особливим випадком до порушення вимог законодавства є обробка «чутливої» категорії персональних даних (про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров’я, статевого життя, біометричних або генетичних даних).

Серед причин порушень безпеки обробки персональних даних можна виділити [1]:

– відсутність розроблених і затверджених положень щодо безпеки персональних даних, які б відповідали потребам даного відомства/структурного підрозділу, а також національним і міжнародним стандартам у сфері захисту персональних даних;

– низький кваліфікаційний рівень співробітників у сфері захисту персональних даних;

– передача персональних даних по незахищених каналах зв’язку;

– відсутність осіб, відповідальних за захист персональних даних;

– не ведеться належний облік зібраної або переглянутої інформації.

Для підвищення рівня захисту персональних даних про особу в базах даних Національної поліції необхідно: визначити порядок (постанова, інструкція, наказ) захисту та збереження інформації, оброблення та накопичення персональних даних про особу в базах персональних даних; визначити вповноважений орган з питань захисту персональних даних і притягнення до відповідальності за незаконну обробку й доступ до них без письмової згоди фізичної чи юридичної особи; розробити кодекс України про захист персональних даних.

Список використаних джерел:

1. Костенко І. В. Проблеми правового захисту персональних даних у діяльності Національної поліції. Юридичний часопис Національної академії внутрішніх справ. 2018. № 1 (15). С. 296–302.
2. Про захист персональних даних. Закон України від 1 черв. 2010 р. № 2297-VI. URL: http://zakon1.rada.gov.ua/laws/show/2297-17.
3. Про Національну поліцію. Закон України від 2 лип. 2015 р. № 580-VIII. URL: http://zakon1.rada.gov.ua/laws/main/580-19.

УДК 004.056

КСЕНІЯ ОЛЕКСАНДРІВНА КРАТАСЮК
курсант 4 курсу факультету №4 Харківського національного університету внутрішніх справ
ВОЛОДИМИР ВОЛОДИМИРОВИЧ ТУЛУПОВ
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ПИТАННЯ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВТОРГНЕНЬ В СУЧАСНИХ СИСТЕМАХ ВІДЕОСПОСТЕРЕЖЕННЯ

На теперішній час в Україні на державному та регіональних рівнях впроваджуються різні програми, проекти та заходи публічної безпеки. Так, у більшості міст в Україні створюються проекти забезпечення публічної безпеки й порядку та протидії злочинності. Наприклад, у місті Києві в рамках проекту Kyiv Smart City «Безпечне місто» у загальноміській системі відеоспостереження працює 5823 камер та створені програмні модулі розпізнавання обличчя і номерів автомобілів. Також відкрито три ситуаційні центри та налагоджена взаємодія з оперативними частинами МВС та СБУ. У майбутньому до системи підключать пожежну, рятувальну, медичну, дорожню й інші комунальні та державні служби [2].

Серед завдань таких проектів і програм є: удосконалення науково-методичного, матеріально-технічного та інформаційного забезпечення правоохоронних та інших органів, що беруть участь у забезпеченні публічної безпеки та порядку; безперервний моніторинг криміногенної ситуації в області, в т.ч. за рахунок соціологічних технологій та забезпечення своєчасного реагування на негативні зміни; здійснення посиленого контролю за ситуацією у публічних місцях, передусім при проведення заходів за участю значної кількості громадян; запобігання правопорушенням, що вчиняються з використанням телекомунікаційних мереж та мережі Інтернет.

На теперішній час у системі Міністерства внутрішніх справ впроваджено низку аналітичних систем з можливістю проведення глибокого аналізу великих масивів інформації, включаючи відкриті джерела де на першому рівні є система відеомоніторингу наприклад - єдиний аналітичний

сервісний центр (UASC) поліції, створений за прикладом системи безпеки Абу-Дабі при ГУНП в Донецькій області [1, с. 271].

При створенні технічного завдання для проектування оптимальної системи відеоспостереження слід розглянути типові технології побудови таких систем, їх переваги та недоліки.

Кожна мережева відеокамера, якщо ми використовуємо IP-камери має свою власну IP-адресу, обчислювальні функції та вбудоване ПЗ, що дозволяє їй функціонувати як повноцінний мережевий пристрій.

На відміну від аналогової відеокамери, IP-камера не потребує прямого підключення до комп'ютера або до будь-яких інших апаратних або програмних засобів. Її підключення може здійснюватися як за допомогою дротяного з'єднання (по міді або оптичному волокну), так і безпровідного (Wi-Fi, GPRS/EDGE, 3G, 4G, супутниковому зв'язку та ін.). Таким чином, досягається повна або часткова мобільність користувача, який здатний стежити за видаленими об'єктами практично з будь-якої точки земної кулі.

Тому слід виділити наступні переваги таких систем IP – відеоспостереження, а саме:

1. Оператор системи може здійснювати візуальний контроль як локально, так і віддалено (з ПК, мобільного телефону і так далі), здійснювати функції адміністрування системи відеоспостереження використовуючи переваги веб-технологій.

2. Спрощеність та малі витрати на встановлення й монтаж. Мережеві відеосистеми IP не вимагають прокладення додаткового коаксіального кабелю, як в аналогових системах, а підключаються до існуючої локальної мережі відеоспостереження за об'єктом з допомогою безпровідних технологій.

3. Якість відеозображення. В сучасних IP-системах застосовується формат MPEG-4, який дозволяє ефективніше використовувати ресурси мережі в порівнянні з форматом M-JPEG.

4. Можливість передавати по одній лінії зв’язку не лише відеосигнал, але й звук, а також управляти та адмініструвати IP-камери.

5. Гнучкість й масштабованість систем IP- відеоспостереження полягає в можливості будівництва фізично розподілених мереж відеомоніторингу, контролю і дистанційного керування без прив'язки до відстані.

6. Інтеграція з багатьма існуючими на даний момент системами відеоспостереження.

Критеріями вибору на користь IP – камер при проектуванні таких систем на теперішній час також є [3]:

– наявність каналу зв’язку з високою пропускною спроможністю від 100 Мб/с і вище та вільних портів Ethernet;

– за рахунок вбудованих в камери WEB серверів при рішенні завдань моніторингу контрольованого об'єкту (без використання архівної інформації) з використанням мережі Інтернет;

– завдання вимагають високого розділення, при невисоких вимогах до освітленості, розміру кадру та ін. (З дозволом більш 1 Мп).

Виходячи з проведеного аналізу існуючих на ринку готових систем відеоспостереження, найбільш перспективними технологіями відеоспостереження є IP–відеоспостереження, яке легко розгортається та базується на сучасних комп'ютерних мережах стандарту Ethernet.

Нормальне функціонування комп'ютерних мереж та її складових таких як мережеві екрани, брандмауери, фаєрволи, системи резервного копіювання, антивірусні засоби та інші) неможливо без стандартних засобів захисту, тому існує необхідність використання IDS (СВВ – систем виявлення вторгнень), які є основним засобом боротьби з мережними атаками [4].

Системи виявлення вторгнень починають усе ширше впроваджуватися в практику забезпечення безпеки корпоративних мереж які у свою чергу можуть використовувати системи IP-відеоспостереження.

Список використаних джерел:

1. Тулупов В. В., Колісник Т.П. Особливі питання захисту систем IP-відеоспостереження. Актуальні питання протидії кіберзлочинності та торгівлі людьми: зб. матеріалів Всеукр. наук. – практ. конф. (23 листопада 2018 р., м. Харків) / МВС України , Харків. нац. ун-т внутр. справ; Координатор проектів ОБСЄ в Україні. ХНУВС, 2018. С. 270–274.

2. Kyiv Smart City. URL: https://www.kyivsmartcity.com/projects/safe-city.

3. Системи відеоспостереження (CCTV). URL: https://guard-lviv.com.ua/uk/sistemi-videonablyudeniya/index.html.

4. Intrusion Detection System (IDS). URL: https://ru.wikipedia.org/wiki/IDS.

УДК 343.98

ПЕТРО СЕРГІЙОВИЧ КЛІМУШИН
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій і кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ
АРТУР ГЕННАДІЙОВИЧ ПЛАКСЮК
курсант 3 курсу факультету № 4 Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ БІОМЕТРИЧНИХ ДАНИХУ ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Поява біометричних механізмів ідентифікації включає в себе кілька різних технологій, які з певних вимірюваних характеристик з високою часткою ймовірності ідентифікують конкретну людину. До таких технологій належать фото- та відеосистеми розпізнавання осіб, голосів, відбитків пальців, райдужної оболонки, сітківки ока, ДНК та ін. [1].

Всі вони можуть застосовуватися комплексно або окремо і зараз в основному є додатковим чинником безпеки у діяльності правоохоронних

органів. Світовий досвід показує, що мультибіометрія (розпізнавання особи відразу за кількома індивідуальними характеристиками – за обличчям, голосом або відбитками пальців) можлива при використанні смартфона як терміналу, через який підтверджується транзакція.

Біометрію вигідно використовувати в комбінації з іншими способами ідентифікації особи без обмежень, оскільки плюси є очевидними: авторизація за біометричними характеристиками відбувається швидко, вона зручна і має високий ступінь захисту. Крім того, саме ідентифікацію за обличчям доцільно застосовувати не тільки для підтвердження доступу до персональних баз даних, а й у внутрішній роботі правоохоронного органу, на-приклад при доступі до службових кімнат.

Для широкого втілення біометричних технологій на всіх рівнях у діяльності правоохоронних органів необхідно формування єдиної бази біометричних даних осіб, але сьогодні така база у необхідному обсязі поки що відсутня. Але прогнози говорять, що в перспективі п'яти-восьми років біометрична ідентифікація стане основним способом підтвердження особи у діяльності правоохоронних органів. Поки ж будуть використовуватися в сукупності кілька способів ідентифікації особи одночасно.

В Україні застосовуються такі біометричні дані (параметри) як відцифровані відбитки пальців рук, відцифроване зображення обличчя. При цьому, *біометрична ідентифікація* – здійснення пошуку за принципом “один до багатьох” шляхом розпізнавання і зіставлення одного або двох біометричних даних (параметрів) особи з біометричними даними (параметрами) осіб у відомчих інформаційних системах суб’єктів національної системи; *біометрична верифікація* – здійснення пошуку за принципом “один до одного” між біометричними даними (параметрами), отриманими від особи в даний момент, і біометричними даними (параметрами), наявними у відомчих інформаційних системах суб’єктів національної системи [1].

У контексті протидії злочинності, переваги застосування документів з персональними біометричними даними забезпечують: більш високий ступінь захисту від підробки; можливість автоматичної перевірки приналежності власника документу, що скорочує час на ідентифікацію особистості, збільшує швидкість даної процедури і виключає суб'єктивізм при оцінці її результатів; значний технологічний потенціал даного документа, тобто на чіп, крім ідентифікаційних даних, можуть записуватися різноманітні інші персональні дані; втрачає сенс підробки та незаконного використання електронних документів з біометричними даними; біометричні персональні дані що збираються при оформленні електронних паспортів можуть застосовуватися в діяльності з розслідування правопорушень [2].

Застосування біометричних технологій є надзвичайно важливими у боротьбі з тероризмом. Це стало зрозуміло з поширенням авіатероризму. На питанні застосування біометричних технологій у боротьбі з тероризмом зосереджено основні акценти Резолюції 2396 (2017) Ради безпеки ООН. В

даний час Інтерпол має біометричні дані більш як 41 000 іноземних бойовиків – терористів.

У 2018 р. в Україні створено національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства (далі – національна система). Суб'єктами національної системи є ДМС, Адміністрація Держприкордонслужби, Національна поліція, МВС, МЗС, закордонні дипломатичні установи, Мінінфраструктури, СБУ, Служба зовнішньої розвідки та Міноборони. Розпорядником системи є ДМС.

Останнім часом значного поширення в світі набувають інформаційно-пошукові системи біометричної ідентифікації особистості по зображенню обличчя за оперативними даними від камер, розміщених у громадських місцях. Ураховуючи це, слід дослідити можливості удосконалення систем автоматизованих інформаційних систем та Інтегрованої інформаційно-пошукової системи органів внутрішніх справ України, що стоять на озброєнні правоохоронних органів України.

Найбільш відомі загрози безпеки для біометричної ідентифікації є: крадіжки біометричної інформації з сервісу авторизації; перехоплення біометричної інформації з мережі; читання біометричної інформації з фізично або програмно зламаного пристрою автентифікації; крадіжка біометричної інформації «з людини »або з носія інформації; зчитування біометричної інформації за допомогою методів соціальної інженерії або підроблених пристроїв; отримання біометричної інформації насильно.

В цілому, застосування біометрії не вирішить проблем надійності ідентифікації для систем з великою кількістю користувачів, але може підвищити достовірність ідентифікації при доступі до критично важливих систем як частини системи контролю і управління фізичним доступом або в якості додаткового фактору автентифікації.

Для середніх і великих правоохоронних органів поліції, а також для об'єктів з максимальною вимогою до безпеки рекомендується використовувати райдужну оболонку в якості засобу біометричного доступу. Для об'єктів з кількістю персоналу до декількох сотень чоловік оптимальним буде доступ за відбитками пальців. Для інформаційних систем з великою кількістю користувачів створення систем доступу на основі біометрії не виправдано економічно. Для таких систем можна використовувати біометричні характеристики з національної бази даних (наприклад, паспорта нового типу) як додатковий фактор.

Список використаних джерел:

1. Положення про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства. Затверджено постановою КМУ від 27 грудня 2017 р. № 1073. URL: http://zakon.rada.gov.ua/laws/show/1073-2017-п

2. Філіппов С. О. Біометричні технології: значення для протидії транскордонній злочинності. Вісник Національної академії Державної

прикордонної служби України. Серія : Юридичні науки. 2018. Вип. 2. URL: http://nbuv.gov.ua/UJRN/vnadpcurn_2018_2_6.

УДК 621.34

ОЛЕКСАНДР СЕРГІЙОВИЧ ТКАЧЕНКО
студент 3 курсу факультету №6 Харківського національного університету внутрішніх справ
ВОЛОДИМИР ВОЛОДИМИРОВИЧ ТУЛУПОВ
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій факультету № 4 Харківського національного університету внутрішніх справ

ПИТАННЯ БЕЗПЕКИ ПРИ ВИКОРИСТАННІ СУЧАСНОГО СТАНДАРТУ LTE

У розвинених країнах світу продовжується перехід до інформаційної сервісно-технологічної економіки. На теперішній час в Україні використовується стандарт зв'язку четвертого покоління LTE (Long Term Evolution), який вважається перспективним. За даними компанії HUAWEI, LTE забезпечує швидкість до 326,4 Мбіт/с від базової станції до користувача і до 172,8 Мбіт/с у зворотному напрямку.

Метою створення стандарту LTE є збільшення можливостей високошвидкісних систем мобільного зв'язку, зменшення вартості передачі даних, можливість надання широкого спектру недорогих послуг.

Мобільний зв'язок четвертого покоління передбачає використання цілого спектру технологій, які раніше розвивалися паралельно. Всі вони внесли свій внесок у специфікацію LTE реалізованої в двох основних варіантах технологій: з дуплексним частотним поділом LTE-FDD (Frequency Division Duplex) і часовим поділом LTE-TDD (Time Division Duplex).

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

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

виконання таких важливих операцій, як кодування та розшифрування користувачів даних, а також зберігання ключів.

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

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

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

– користувальницький рівень повинен забезпечувати безпечний доступ до мобільного пристрою; рівень додатків повинен гарантувати безпечний обмін повідомленнями;

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

Є також проблеми і з самим стандартом. По-перше, дуже гостро стоїть завдання взаємодії з не LTE мережами. Якщо трафік між користувальницьким обладнанням і базовою станцією шифрується (це вимога стандарту) і загроза порушення конфіденційності стає неактуальною, то взаємодія базової станції з радіоконтролером мережі 3G по умовчанню ніяк не захищене а, отже, це пролом для можливих атак з боку зловмисників. По-друге, відсутність обов'язкової аутентифікації між ядром мережі і базовою станцією. Цю опцію оператор зв'язку для зниження своїх витрат щодо розгортання мережі LTE може і не задіяти зовсім. Не можна забувати і про обмеження LTE. Наприклад, збільшення швидкості підключення зазвичай обертається зменшенням радіусу дії базової станції, який в середньому для 4G становить близько 5 км і залежить від використовуваного частотного діапазону . Тому базових станцій в мережі стає більше, і вони розташовуються ближче одна до одної.

Ще одна особливість LTE в тому, що ця технологія орієнтована на підключення інтелектуальних пристроїв, з поширенням яких число потенційно небезпечних сервісів буде тільки зростати, що дозволить зловмисникам отримати доступ до конфіденційної інформації провайдера і побудувати нові витончені схеми інформаційних злочинів.

Всі функції захисту в LTE об'єднані стандартом і передбачають захист на декількох рівнях: на рівні доступу до мережі, на рівнях мережевого і користувальницького доменів, на рівні додатків та на рівні відображення і конфігурацій.

Кожен з цих рівнів передбачає аутентифікацію і авторизацію всіх пристроїв, чого немає в Інтернеті. Технологія LTE передбачає використання не тільки IP-адреси, але і системи розповсюдження ключів шифрування для всіх пристроїв, підключених до мережі з можливістю переходу зі 128 до 256-бітові ключі і введення нових алгоритмів, зберігаючи зворотну сумісність. Крім алгоритмів шифрування і забезпечення комплексної безпеки в мережах 4G використовуються додаткові алгоритми, які навіть за умови того, що один з них буде зламаний, решта забезпечать безпеку мережі LTE. Крім того, в

LTE зберігаються і методи аутентифікації користувачів по прив'язці до SIM карти, як в традиційному мобільному зв'язку. Користувач може заблокувати доступ до телефону з PIN-кодом.

Таким чином, виходячи з вище сказаного, головною особливістю з точки зору захисту абонента розглянутого стандарту четвертого покоління рухомого зв'язку LTE, процес обслуговування приховується тимчасовими ідентифікаторами.

УДК 378.091
МАРИНА ОЛЕГІВНА БУЧКО
АНАСТАСІЯ ОЛЕКСІЇВНА ЗАБЛОЦЬКА
здобувачі вищої освіти ІІ курсу факультету економіко-правової безпеки
Дніпропетровський державний університет внутрішніх справ
ОЛЬГА ГЕННАДІЇВНА КОСТЕНКО
старший викладач кафедри українознавства та іноземних мов
Дніпропетровський державний університет внутрішніх справ

ПЕРСПЕКТИВИ ЗАПРОВАДЖЕННЯ МЕДІА В ОСВІТНІЙ ПРОЦЕС

В нашому житті великий вплив на різні сфери життя людини мають інноваційні технології, які зростають з кожним днем. Від людини вимагається не лише знання сучасних технічних пристроїв та уміння з ними працювати, а й певний рівень критичного мислення (здатності інтерпретувати інформацію, яку було отримано із різноманітних засобів масової інформації, розуміння різноманітних медіа текстів тощо), навичок самостійної роботи, пов'язаної з обробкою та пошуком, презентацією інформаційного матеріалу тощо.

Сучасні учні, студенти (курсанти) є активними споживачами інформації різноманітних медіа. Уже в середині ХХ сторіччя у зарубіжних країнах світу в педагогічній науці був сформований спеціальний напрям під назвою – медіа освіта, покликаний допомогти їм, краще адаптуватися в умовах медіа культури. Цілі та задачі медіа освіти зарубіжних вчених трактуються по-різному, але в педагогічному аспекті даний напрям вивчає взаємодію медіа з процесами виховання та навчання. Тому за мету для нашої праці є саме дослідження інтеграції медіа в навчальний процес.

Розвиток засобів масової інформації комунікації і залучення їх до навчально-виховного процесу, значно активізували творчі уроки педагогів у багатьох країнах світу. Існуючий процес комп'ютеризації та інформатизації сучасного суспільства визначив напрями вітчизняних і зарубіжних досліджень, які аналізують різні аспекти проблеми інтеграції сучасних медіа в освітній процес. В. Робак зазначає, що у Німеччині було відкрито багато науководослідних інституту які проводять дослідження цієї галузі. Видатний німецький вчений Б. Щерб став першим професором медіа педагогіки. Він

вважає,що медіа педагогіка, застосовується у позаурочній роботі і саме там має найкращі перспективи.

На його думку, настав час впровадити у навчальних закладах медіа психологічних та медіапедагогічних курсів, поряд із курсами з комп'ютерних технологій [1]. Німецький дослідник та професор С.Ауфенангер зазначає, що медіа педагогіка як наукова галузь зазнала істотних змін, ставши комплексною наукою,шо акумулює відомості з багатьох дисциплін (загальної психології,філософії, освітніх технології, психології розвитку тощо) [2].

У медіа педагогіці німецькі дослідники виділяють такі взаємопов'язані напрями як політично вмотивована та суспільнокритична медійна педагогіка. Перша має за мету боротьбу проти маніпуляцій за допомогою медій. При застосуванні сучасних медіа у навчальному процесі значно змінюється. А друга, в свою чергу ставить за мету зміну суспільства за допомогою таких її засобів як здатність ідеологічної критики, впливу на медіасистему, використання альтернативних медій.

Саме сучасні медіатехнології дозволяють нам індивідуалізувати і активізувати освітній процес у рамках колективного навчання. Сучасний учень, студент (курсант) може на свій розсуд ілюструвати текст, що вивчається, зробивши більш зрозумілішим для себе. Самостійно для себе він може перетворювати інформацію, яка отримується з мережі, підбирати певні аргументи, будуючи їх за логікою, яка буде відображати його власні уявлення, напрямки та думки. У результаті цього студенти (курсанти) більш суттєво проникають в сутність самого питання,після цього у них з'являється інтерес більш активно працювати з навчальною літературою. Використання медіа спрямоване на індивідуалізацію навчання у межах навчально-виховного процесу.

При цьому кожен студент (курсант) опановує активну, зорієнтовану конкретно на нього діяльність. При цьому збільшується мисленнєвий процес, більше реалізуються пізнавальні потреби, стимулюється творча активність, після цього студенти (курсанти) отримують можливість обирати оптимальний темп навчання саме для себе, коригувати та контролювати вивчення матеріалу, прицьому результати роботи будуть безпосередньо видні на самому занятті. Отже, сучасні медіа – це комплексний засіб опанування для людини навчального процесу, оточуючого світу в його соціальних, психологічних, художніх, інтелектуальних аспектах, що викликає необхідність вивчення і врахування дидактичного потенціалу нових медіа.

Список використаних джерел:

1. Робак В. До питання про розвиток медіа педагогіки у Німеччині Другий український педагогічний конгрес: Зб. Матеріалів конгресу. Львів. 2006. 601 с.

2. Шариков А. В. Медиаобразование: мировой и отечественный опыт. Москва. Изд- во Академи педагогических наук. 1990 год.

УДК 004.89
АРТЕМ ОЛЕКСІЙОВИЧ ЛАНОВИЙ
аспірант ІІ-го року навчання кафедри системотехніки Харківського національного університету радіоелектроніки
ОЛЕКСІЙ ФЕЛІКСОВИЧ ЛАНОВИЙ
кандидат технічних наук, доцент, доцент кафедри програмної інженерії Харківського національного університету радіоелектроніки

СУЧАСНИЙ РІВЕНЬ РЕАЛІЗАЦІЇ DAAS В ХМАРІ

На теперішній час одним з ключових напрямків розвитку інформаційних технологій є використання інформації в якості сервісу за допомогою хмарних технологій на основі принципів Data as a Service (DaaS) та Big Data as a Service (BDaaS). Суть хмарних технологій полягає в перенесенні обробки даних з персональних комп'ютерів і робочих станцій на сервери всесвітньої мережі. В області комп'ютерного моделювання це означає розгортання програмних комплексів на ресурсах Інтернет. Користувач стає не покупцем обчислювальних програм і комплексів, а їх орендарем, якому надаються різноманітні послуги. Форма купівлі–продажу товару з відчуженням прав власності від продавця до покупця змінюється на форму оренди, в даному випадку – продажу не продукту, а послуг з його використання клієнтом без зміни власника продукту. При цьому забезпечена повна відповідність виробничих потужностей інфраструктури фактичним потребам користувача. Хоча термін "хмарні технології" є сталим, в українській мові він має інше значення, ніж оригінал. "Cloud" окрім хмари має й інше значення – розсіяний; власне значення "розсіяний" і мається на увазі в англомовній термінології.

Розглянемо основні відмінності хмар від традиційних хостинг-рішень:

– на відміну від dedicated-серверів, установка і налаштування яких займає багато часу, хмарні сервіси повинні бути доступні для використання відразу після покупки, те ж саме стосується більшості класичних послуг дата-центрів;

– на відміну від shared-хостингу, в хмарах є можливість нарощувати обсяг закуплених потужностей миттєво, без звернення до служби технічної підтримки оператора;

– на відміну від того, що було на ринку хостингу до хмар, хмарні продукти надають схему оплати за фактом, тобто оплату тільки тієї потужності, яку користувач дійсно використовує з досить коротким проміжком тарифікації.

На ринку представлено кілька типів хмарних сервісів зберігання, призначених для користувача даних:

1. Сервіси, в яких користувачеві надається екземпляр СУБД на віртуальній машині.

2. Сервіси, в яких користувачеві надається СУБД без прив'язки до віртуальних машин і управління віртуальними машинами, масштабованість і відмовостійкість зберігання даних забезпечується постачальником сервісу.

3. Сервіси, в яких користувачеві надається можливість зберігання даних у вигляді таблиць, написання простих додатків для обробки цих даних деякою спеціалізованою мовою.

4. Сервіси зберігання файлів.

В контексті створення хмарного сервісу зберігання даних користувачів за допомогою DaaS-приладів інтерес викликає друга група, як найбільш повно реалізує переваги від застосування хмарних технологій і максимально зручна для користувача, що пов'язано з розробкою спеціального ПЗ для збірки різнорідних джерел даних за запитом клієнтів. Це дозволяє усуспільнити довільні дані за рахунок програмної інтеграції і запобігти невиправдану надмірність даних в мережі на основі сервіс-орієнтованої архітектури та відповідних протоколів.

Загальновизнаним стандартом представлення даних на транспортному рівні є XML. Якщо на транспортному рівні використовувати XML-подання, то опис структури збережених даних стає синонімом файлу визначення синтаксису XML-файла DTD. XML-схеми витіснили DTD в силу їх великих можливостей і універсальності. В цьому випадку схеми подання інформації в XML файлі стає деяким аналогом таблиці в реляційної СУБД або класу об'єктів в об'єктно орієнтованих базах даних.

Проблема адміністрування сховищ передбачає дослідження стандартних завдань розгортання, міграції, розмежування повноважень, резервного копіювання та відновлення, балансування завантаження, підтримання живучості на достатньому для клієнтів рівні готовності системи за рахунок реплікації копій даних, добре відомих в хмарних технологіях. Їх опрацювання істотно залежить від орендованої інфраструктури хмари і функціональних можливостей наданих провайдерами віртуальних машин і їх програмного забезпечення в рамках DaaS чи BDaaS.

Масштабованість, відмовостійкість і безпека – автоматичне виділення і звільнення необхідних ресурсів залежно від потреб додатку. Технічне обслуговування, оновлення ПЗ здійснює провайдер послуг.

Розглядаючи переваги “хмарних” обчислень, варто сказати і про недоліки, з якими зв’язаний перехід на “хмари”. Найбільш суттєвий з них – загроза інформаційної безпеки. Для захисту можна використовувати шифрування даних або їх знеособлення. При цьому шифрувати треба не лише ті дані, що зберігаються в провайдера, а й канал зв’язку з ним.

Ще одним недоліком можна назвати прив’язку “хмарної” технології до конкретного постачальника послуг, збоїв на стороні провайдера, вихід з ладу інтерфейсу адміністрування, банкрутство і поглинання оператора.

До інших ризиків можна віднести втрату зв’язку з мережею провайдера, DDoS-атаки і втрату відповідності вимогам регулювальників. Ці ризики можна понизити за допомогою правильного складання угоди про рівень обслуговування (Service Level Agreement, SLA), яке дозволить компенсувати частину збитків. Нормативні вимоги можуть змінюватися з часом, а закон “Про персональні дані” і зовсім робить “хмарні” обчислення непридатними на практиці. Проте, в деяких випадках хмарну систему можна

зробити навіть більш захищеною, ніж традиційну архітектуру, за рахунок розподілу обов'язків і правильно складених домовленостей.

УДК 343.1:351.746
ВІКТОРІЯ ВОЛОДИМИРІВНА ВІНЦУК
кандидат юридичних наук, доцент кафедри кримінального процесу, криміналістики та експертології факультету № 6 ХНУВС

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ПРАВООХОРОННИХ ОРГАНАХ: ПРОБЛЕМИ ВИКОРИСТАННЯ

Розвиток нашої держави у напрямку євроінтеграції передбачає не тільки вирішення соціальних питань суспільства, а й підвищення ефективності діяльності правоохоронних органів яка направлена на протидію злочинності і цього можливо досягнути шляхом використання сучасних інформаційних технологій. У сьогоднішніх реаліях неможливо собі уявити ефективну роботу правоохоронних органів без використання сучасних інформаційних технологій.

Величезна кількість статистичної, аналітичної та довідкової інформації використовується в діяльності судових органів, прокуратури, нотаріальних та адвокатських контор, юридичних офісів, і, звичайно ж, в оперативно-розшуковій, слідчій та експертній роботі органів внутрішніх справ. Для цього застосовують не лише універсальне, але й спеціальне програмне забезпечення. Ті темпи, з якими нові інформаційні технології зараз створюються та впроваджуються в практичну діяльність правоохоронних органів, настільки високі, що іноді навіть фахівці у галузі ІКТ, а тим більше, інші категорії користувачів не встигають оцінити масштаби й глибину всього, що відбувається [1].

Багатьма науковцями досліджувались теоретичні і прикладні аспекти використання сучасних інформаційних технологій у правоохоронній діяльності щодо протидії окремим видам злочинів; проблемні питання підготовки фахівців у галузі інформаційних технологій для органів Національної поліції України; актуальні питання підвищення якості інформаційно-аналітичної підготовки фахівців для підрозділів кримінальної поліції та інше, але, мабуть, з деяких причин не усе набуло практичного застосування. Проблемам використання інформаційних технологій в роботі правоохоронних органів й суміжним питанням у кримінальному процесі та ОРД присвячені роботи зарубіжних й вітчизняних науковців: М. І. Ануфрієва, І.В. Арістової, О. М. Бандурки, В.П. Бахіна, А.Й. Берлача, Р.С. Бєлкіна, В.В. Бірюкова, Ф. П. Васильєва, М.С. Вертузаєва, І.О. Воронова, В.І. Галагана, В.Г. Гончаренка, І. В. Горошка, Е.О. Дідоренка, І.Б. Денисової, О.М. Джужи, М. П. Дубініна, В. Р. Женіла, В.Ю. Журавльова, В.А. Журавля, В.П. Захарова, А.В. Іщенка, С. Я. Казанцева, Р.А. Калюжного, Д.Й. Никифорчука, Н.С. Карпова, Ю.Ю. Орлова, Н.І. Клименка,

В.П. Кувалдіна, В.С. Кузьмічова, О.І. Козаченка, В.О. Коновалової, В.С. Овчинського, С.С. Овчинського, І.М. Паршина, Н. С. Павлюченка, М.А. Погорецького, А. Л. Полєжаєва, О. М. Різника, О.В. Рибальського, Б.Г. Розовського, Е.В. Рижкова, М.В. Салтевського, В.Г. Самойлова, В.П. Столбового, О.Г. Фролової, І.Ф. Хараберюша, О.М. Чистолінова, В.Ю. Шепітька, Г. В. Єпура, Г.О. Юхновець та ін. Але на практиці стикаються з інформаційною некомпетентністю та низьким рівнем володіння інформаційними технологіями працівниками правоохоронних органів. Приймаю думку, що на практиці застосування науково-технічного потенціалу перебуває на вкрай низькому рівні, а постійні кадрові реформи не дозволяють щодо цього сформувати стратегічну лінію[2].

О.В. Бочковий наголошує, що сучасні ґаджети дозволяють повністю перенести кабінетну роботу в будь-яке зручне місце та без проблем передавати інформацію у різних формах: від звичайних текстових повідомлень, документів до складних розрахунків, зображень і відеофайлів. Невже незрозуміло, які перспективи новація створює в разі застосування її в правоохоронній діяльності? [2, с. 225]. Зрозуміло, але є але, і полягає воно в дотриманні конфіденційності та таємності зберігання інформації отриманої негласним шляхом під час використання цих гаджетів. А по яких каналах її передавати? І треба пам’ятати, що система способів захисту інформаційного простору включає в себе правові прийоми, які полягають у створенні адміністративно-правових і кримінально-правових норм, що встановлюють відповідальність за несанкціоноване використання даних [3, с. 104-105]. Тобто, перш за все необхідно правове закріплення цього процесу, а також розробка алгоритму дій оперативних працівників щодо збору, накопичення, обробки, узагальнення та збереження отриманої інформації. Як не крути, а комп’ютерну техніку ніхто не відміняв… Застосування засобів комп’ютерної техніки навіть у найбільш складних формах, заснованих на використанні методів «штучного інтелекту», аж ніяк не означає, що слідчий або оперуповноважений стають бездумними виконавцями рішень, що приймаються комп’ютером. По-перше, комп’ютерний «інтелект» є в цьому разі узагальненим передовим досвідом слідчої (експертної) діяльності, а по-друге, мова йде виключно про рекомендації, які не мають обов’язкового характеру [4, с. 356].

Імовірно ця ситуація виправиться після закінчення навчання курсантами ВНЗ системи МВС в яких існують спеціальні факультети з поглибленим вивченням інформаційних технологій. А доки, необхідно звернути увагу по-перше, на отримання курсантами знань інформаційних ресурсів й навичок роботи з новою технікою, новими підсистемами та автоматизованими банками даних правоохоронних органів; по-друге, працівникам НП України, а особливо оперативним співробітникам проводити підвищення кваліфікації не банально на рівні теорії, а з отриманням навичок застосування інформаційних технологій та роботи з новими підсистемами, які впроваджуються та використовуються в практичній діяльності правоохоронних органів; по-третє, вдосконалити правове регулювання сфери інформаційного забезпечення правоохоронних органів.

Список використаних джерел:

1. Снегірьова Т. Л. Інформаційні технології в діяльності правоохоронних органів та необхідність їх вивчення курсантами вищих навчальних закладів системи МВС. URL: http://bo0k.net/index.php?p=achapter&bid.

2. Бочковий О.В. Ігнорування інформаційно-технічного прогресу органами досудового розслідування в Україні: хронічна риса чи тимчасове явище? Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка. 2016. Вип. 3. С. 223–231.

3. Хорт І.В. Особливості інформаційного забезпечення органів внутрішніх справ у сфері охоронної діяльності / І. В. Хорт // Наукові праці МАУП, 2015. Вип. 44(1). С. 100–107.

4. Криміналістика: підручник / [В.Ю. Шепітько, В.О. Коновалова, В.А. Журавель та ін.] ; за ред. В.Ю. Шепітька. – 5-те вид. переробл. та доповн. Київ : Ін-Юре, 2016. 640с.

УДК: 351.74:004.9

ДІАНА АРТУРІВНА ТУПОТІНА
курсант 2 курсу факультету підготовки фахівців досудового розслідування Дніпропетровського державного університету внутрішніх справ
НАТАЛІЯ СЕРГІЇВНА РЕЗЦОВА
викладач кафедри кримінального процесу Дніпропетровського державного університету внутрішніх справ, майор поліції

ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

У міру розвитку і ускладнення комп'ютерних систем і програмного забезпечення зростає обсяг і підвищується вразливість даних, які зберігаються в них. Тому все більшої уваги набувають проблеми захисту інформації. Важлива роль захисту інформації випливає з розуміння того, що захист інформації є не тільки однією з головних складових національної безпеки держави, а й невід'ємним компонентом всіх її складових; інформаційні стратегії в сучасних умовах набувають важливого значення під час реалізації різних моделей співробітництва, захисту населення та дотримання законності або відіграють роль своєрідної "інформаційної зброї"; руйнування та дезорганізація інформаційної інфраструктури держави прирівнюються за наслідками до застосування зброї масового знищення; витік інформації в процесі діяльності органів внутрішніх справ призводить до зростання злочинності, її безкарності та зневіри населення тощо. Інформація повинна бути захищеною як правовими актами, так і технічними засобами. [1]

Захист інформації особливо важлива проблема в умовах інформаційного суспільства. Проблемою технічних засобів захисту інформації у свій час

займались такі українські вчені: Ю. Добути, О. Рибальський, І. Горбенко, В. Захаров, Г. Гулак, В. Хорошко, Ю. Орлов, О. Потій, Ю. Горбунко та інші.

Ідею захисту інформації в контексті економічної безпеки регіону за допомогою тільки технічних засобів в умовах інформаційного суспільства не можна вважати достатньо ефективною. Цей напрямок можна посилити математичними і методами, істотно при використанні криптографічних алгоритмів. Запропоновано електронно-криптографічний систему і алгоритми виконання, використовують елементи штучного інтелекту для захисту інформації. Таким чином, авторами запропоновано проект малогабаритного шифрувального пристрою, який може бути застосований у практичній діяльності оперативних підрозділів, особливо в тих випадках, коли є підозра, що в процесі проведення оперативно-розшукових заходів або операцій можуть прослуховуватись розмови оперативних працівників.

На даний час, за оцінкою Міжнародного союзу електрозв'язку, Республіка Білорусь за підсумковим індексом розвитку інформаційно-комунікаційних технологій (ІКТ) піднялася з 52-го місця в 2011 року на 31-е в 2016 р серед 175 країн. За даний період в Білорусі створено базовий комплекс електронного уряду, в який входять такі компоненти, як загальнодержавна автоматизована інформаційна система, система міжвідомчого електронного документообігу, державна система управління відкритими ключами перевірки електронного цифрового підпису, єдиний розрахунковий інформаційний простір. [2] Відповідно до Концепції національної безпеки Республіки Білорусь, одним з основних національних інтересів в інформаційній сфері є забезпечення надійності та стійкості функціонування критично важливих об'єктів інформатизації.

Виходячи з викладеного, представляється необхідним стратегічне управління інформаційною безпекою в правоохоронній сфері розглядати в якості унікальної системи, яка повинна своєчасно розпізнавати проблеми, висувати науково-обгрунтовані стратегічні цілі, шляхи та способи їх досягнення; формувати уявлення про стан системи в майбутньому зі збереженням традиційних і придбанням (створенням) нових здібностей і можливостей управління, своєчасно вловлювати і розпізнавати можливості і загрози, що виходять із зовнішнього середовища; виробляти способи зміни зовнішнього оточення, реформування правоохоронної сфери, системи оперативного управління в міру збільшення власного потенціалу, виконання стратегічних завдань.

Список використанної літератури:

1. Варенко В.М. Інформаційно-аналітична діяльність. Навч. посіб. Київ: Університет «Україна», 2014. 417 с.

2. Інформаційні технології в правоохоронній діяльності. Посібник / В.А Кудінов., В.М.Смаглюк, Ю.І. Ігнатушко, В.А. Іщенко: НАВСУ, 2013. 82с.

3. Проект закон України «Про технічний та криптографічний захист інформації»URL:http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article%3Bjsessionid=2D026D15A28D130D7C40D9F2186DF6AE?art_id=73862&cat_id=38837

УДК 343.9[343.346.8:004](477)
ВОЛОДИМИР АНАТОЛІЙОВИЧ ЄВТУШОК
старший викладач кафедри тактичної та спеціальної фізичної підготовки Харківського національного університету внутрішніх справ, підполковник поліції

ЗАСТОСУВАННЯ СУЧАСНИХ ТЕХНОЛОГІЙ ДЛЯ БОРОТЬБИ ЗІ ЗЛОЧИННІСТЮ

Метою роботи є дослідження питання впровадження сучасних інформаційних технологій для підвищення ефективності боротьби зі злочинами, вчиненими з використанням комп'ютерних та мережевих можливостей.

З урахуванням збільшення чисельності користувачів, мережа Інтернет закономірно породжує залежність людей від інформаційного співтовариства і вразливості від різного роду кіберзлочинів. Сучасні інформаційні технології займають в економіці країни особливе місце, а їх ефективне функціонування є одним з найважливіших факторів, які сприяють вирішенню ключових завдань політики. Необхідно звернути увагу на виявлення, розкриття і розслідування злочинів, скоєних в кіберпросторі. Поширення комп'ютерних вірусів, шахрайства з платіжними картами, розкрадання грошових коштів з банківських рахунків, комп'ютерної інформації, порушення правил експлуатації автоматизованих електронних систем, різного роду протиправні дії з використанням криптовалют - далеко не повний перелік злочинів, скоєних за їх допомогою. Великою проблемою є те, що інформація індивідуальна, ірраціональна та анонімна, а кожна людина в сучасному світі, від звичайного робітника до великої компанії, банку і держави, ризикує в будь-який момент стати жертвою зловмисників в кіберпросторі. Отже постійно винаходять нові, складні та різноманітні схеми шахрайських операцій.

З настанням нового століття рішенням таких злочинів стало приділятись багато уваги як на національних рівнях, так і в рамках реалізації програм міжнародного співробітництва державних правоохоронних органів. Головна криміналістична особливість кіберзлочинів полягає в тому, що їх запобігання, виявлення, розкриття і розслідування неможливо без використання сучасних інформаційних технологій. На жаль теперішня система протидії злочинним посяганням, вчиненим з використанням сучасних інформаційних технологій, поки помітно відстає у своєму розвитку.

Відповідно до цього виникла необхідність у підготовки фахівців для боротьби з такими злочинами за допомогою виявлення, вилучення і використання різного роду електронних доказів. Також вивчення різних форм існування цифрової інформації дозволить правоохоронним органам адаптуватися до нових умов життя в епоху значних технологічних змін. Інтернет і система електронних платежів досить складна, вона потребує детального і тривалого документування, фактів злочинної діяльності, значної кількості залучених сил і оперативно-технічних засобів

Можна сказати, що для забезпечення безпеки громадян, враховуючи складність і специфічність інформаційного впливу, життєво необхідний спеціальний провідний орган з контролю за створенням, зберіганням і застосуванням «інформаційної зброї». Знизити подібну активність шляхом грамотної організації розкриття і розслідування подібного роду діянь неможливо без відповідного методичного забезпечення організаційно-тактичного характеру, а також ефективної взаємодії з іншими спец. службами.

УДК 351.74
ЄВГЕНІЯ ІГОРІВНА МАТВІЄНКО
здобувач вищої освіти факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ
ДМИТРО ОЛЕКСІЙОВИЧ АНІСІМОВ
викладач кафедри спеціальної фізичної підготовки Дніпропетровського державного університету внутрішніх справ

АКТУАЛЬНІ ПИТАННЯ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ПРАВООХОРОННИХ ОРГАНАХ

На сьогоднішній день використання інформаційних технологій в діяльності правоохоронних органів займає провідну роль. Зокрема, як відомо в Україні існує з 5 жовтня 2015 року Кіберполіція, як структурний підрозділ Національної поліції. Даний підрозділ відповідно до функцій використовує у своїй діяльності новітні інформаційні технології з метою попередження, виявлення, припинення та розкриття кримінальних правопорушень, механізмів підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних та комп'ютерних інтернет-мереж і систем. Наразі, наша країна знаходиться на етапі масштабного використання мережі інтернет, перехід до електронних інформаційних систем сприяв розвитку країни, але існує багато негативних явищ таких як кіберзлочини, наприклад (викрадення готівки з банкомату шляхом встановлення на шатер банкомату спеціальної утримуючої накладки, несанкціоноване списання коштів з банківських рахунків за допомогою систем дистанційного банківського обслуговування, заволодіння коштами громадян через інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку, протиправний контент, який пропагує екстремізм, тероризм, наркоманію, культ жорстокості і насильства) та інші[1].

Беззаперечно, що використання інформаційних технологій може стати чи не головним чинником зміцнення законності, забезпечення обороноздатності країни, соціально-політичної стабільності та розвитку демократичних засад в управлінні державою.

На думку О.Г. Фролової значна, а в багатьох випадках пріоритетна роль інформаційного забезпечення у процесі здійснення ефективного

управління в Органах національної поліції та функціонування усієї правоохоронної системи підтверджується на практиці боротьби зі злочинністю. Важлива роль системи інформаційного забезпечення управління в правоохоронних органах підтверджується на нормативному рівні, зокрема наказами та розпорядженнями МВС України[2, с. 55].

На нашу думку, ми вважаємо доцільним для нашої країни застосовувати якісний та ефективний досвід розвинутих зарубіжних країн. Значної уваги заслуговує досвід Сполученого Королівства Великої Британії та Північної Ірландії в реалізації та втіленні корпоративної об'єднаної інформаційної моделі даних для потреб поліції. Як зауважив А. Москвичов, даний проект розміщує декілька основних елементів. Відповідно основною корпоративної інформаційної моделі стає каталог інформаційних об'єктів [3, с. 30]. Особливої уваги вартий той факт, що як звичайний словник він визначає кожен елемент інформації, використовуваний різними поліцейськими підрозділами, – від ордерів на арешт до листків тимчасової непрацездатності. Але на відміну від звичайного словника він створений таким чином, що встановлює і наочно показує ієрархічні взаємовідносини між інформаційними об'єктами.

Як вказував В. Заросило, реалізація цих відносин під час попередження правопорушень та їх швидкого розкриття у Великій Британії забезпечується введенням новітніх комп'ютерних відеоспостережень, створених завдяки фінансуванню міських адміністрацій та приватних підприємств [4, с. 85]. Ми вважаємо, що таким чином забезпечується значне скорочення кількісного складу поліцейських, які задіяні для спеціальної поліцейської діяльності.

Таким чином, як ми можемо бачити використання інформаційних технологій в правоохоронних органах є складовою їх діяльності, що забезпечує по перше, це – викриття, припинення, та боротьбу зі злочинністю за допомогою отриманої інформації, а також за допомогою міжнародного досвіду розвинутих країн здобуття доцільних та ефективних технологій у вдосконаленні цілої системи інформаційних технологій.

Список використаних джерел:

1. Що таке кіберполіція? Трибуна. 2019. URL: https://tribuna.pl.ua/news/shho-take-kiberpolitsiya/.

2. Фролова О.Г. Проблеми правового регулювання інформаційнометодичного управління в органах внутрішніх справ. Проблеми правознавства та правоохоронної діяльності. 2002. № 1. С. 53–62.

3. О разработке корпаративной информационной системы в английской полиции / пер. Москвичева А. И. Борьба с преступностью за рубежом // Ежемесячный информационній бюлетень. Москва: ВИНИТИ. 2004. № 10. С. 42.

4. Заросило В. О. Порівняльний аналіз адміністративної діяльності міліції України та поліції зарубіжних країн (Великобританії, США, Канади та Франції) : дис. ... канд. юрид. наук : 12.00.07. Київ, 2002. 250 с.

УДК 351.746.2:004
ВАЛЕРІЯ ВОЛОДИМИРІВНА ЛАКТІОНОВА
курсант 2 курсу факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ
НАТАЛІЯ СЕРГІЇВНА РЕЗЦОВА
викладач кафедри кримінального процесу Дніпропетровського державного університету внутрішніх справ, майор поліції

РОЛЬ І ЗНАЧЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОПЕРАТИВНО-РОЗШУКОВІЙ ДІЯЛЬНОСТІ

На сьогоднішній день задля ефективної протидії злочинності необхідно широко використовувати сучасні досягнення у сфері технічного прогресу, які зробили великий прорив у сфері інформаційних технологій.

Україна – 66-та держава за рівнем розвитку інформаційних технологій. У попередньому рейтингу Україна займала 71 місце. Єдиною конкурентною перевагою, яку має наша країна у цьому аспекті - це професійні кадри, адже у нашій державі дуже високий рівень підготовки майбутніх програмістів.

Використання інформаційних технологій переважно зростає у зв'язку з інтенсивним застосуванням у діяльні правоохоронних органів засобів комп'ютерної техніки. Для здійснення розшукових заходів ми маємо великий досвід щодо застосування новітніх технологій під час попередження, виявлення та розслідування злочинів, розшуку підозрюваних, здійснення судових експертиз [1].

Однак, цим методам в оперативно-розшуковій діяльності приділяється мало уваги, хоча їхнє значення все більше зростає, особливо під час встановлення місця знаходження особи. Під час аналітично-інформаційної роботи працівник вирішує основні тактичні завдання, що постають у ході розслідування злочинів. Взагалі, виявити місцеперебування підозрюваного та обвинуваченого, а також виявити їхні злочинні зв'язки не можливо вирішити без добре налагодженої інформаційно-аналітичної роботи. Отже, очевидним є те, що однією з найважливіших умов підвищення рівня протидії злочинності є широке використання досягнень технічного прогресу. Основним завданням функціонування системи інформаційного забезпечення діяльності правоохоронних органів є інформатизація підрозділів, які здійснюють оперативно-розшукову діяльність.

Наказом Національної Поліції України № 228 від 30 грудня 2015 р. було створено Департамент інформаційної підтримки та координації поліції «102», який здійснює інформаційно-пошукове забезпечення правоохоронної діяльності, а також захист персональних даних під час їх обробки у структурних підрозділах Національної поліції України. Цей Наказ регулює інформаційно-пошукову та інформаційно-аналітичну діяльність, а також обробку персональних даних в органах і підрозділах Національної поліції [2].

Головним завданням використання інформаційно-комунікаційних технологій у підрозділах Національної Поліції України є: отримання інформації у зручному для користування вигляді співробітниками та

підрозділами Національної Поліції для розслідування кримінальних правопорушень, а також розшуку злочинців, збирання та оброблення аналітичної, статистичної та контрольної інформації для оцінки ситуації та прийняття відповідних рішень на всіх рівнях підрозділів Національної поліції, а також для забезпечення захисту інформації.

Отже, можна зробити висновок, що використання інформаційно-комунікаційних технологій є однією з головних умов покращення роботи щодо встановлення особи підозрюваного, а також його розшуку та функціонування правоохоронної системи загалом. Але, нажаль, повною мірою це застосувати неможливо через проблеми фінансового забезпечення та недостатній рівень володіння співробітниками відповідними навичками поводження з новою технікою та новими системами. У нашому сучасному світі абсолютно кожен працівник правоохоронних органів повинен бути прогресивним користувачем інформаційно-комунікаційних технологій. Також працівникам варто проходити курси підвищення кваліфікації задля отримання нових навичок, знать та умінь та підвищення своєї професійної майстерності.

Список використаної літератури:

1. Рогатюк І.В. Використання інформаційних технологій у досудовому розслідуванні: сучасний стан і перспективи розвитку/ І.В. Рогатюк // Науковий вісник Національної академії внутрішніх справ. – 2013.

2. Департамент інформаційної підтримки та координації поліції «102» Національної поліції України. URL: https://declarations.com.ua/office/

УДК 340.134

ЕДУАРД ОЛЕКСАНДРОВИЧ МУЗИЧУК
студент факультету № 6 Харківського національного університету внутрішніх справ

ВИДИ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ В УКРАЇН ТА ЇХ ІНФОРМАЦІЙНО-СОЦІАЛЬНЕ ПРИЗНАЧЕННЯ

Беручи до уваги загальносвітовий історичний досвід будування громадянських суспільств та державних утворень, який досліджували різноманітні вчені, більшість представників демократично-розвиненого, правового людства дійшли до логічного висновку про те, що одним з ключових фундаментальних засад стабільності та благополуччя в суспільстві, окремій державі й у світі в цілому є юридична відповідальність суб'єктів суспільних правовідносин.

Ця правова дійсність стосується однаково як відносин у сфері публічного, так і відносин у сфері приватного права. Адже у першому випадку мова йде про невідворотність покарання для особи, яка наносить, або вже принесла шкоду певним законним інтересам держави, суспільства чи окремій людині. Тобто діяння правопорушника зачіпляють сфери суспільного життя,

які охороняються законом і саме тому визначаються як суспільно-небезпечні, винні діяння. Як правило, в більшості випадків протиправні діяння більшості суб'єктів суспільних правовідносин охоплюються, вивчаються та систематизуються галузями права. До сфери публічного права, окрім кримінального, входять ще такі галузі права як конституційне, адміністративне, фінансове та інші. Більш того, суб'єктами правовідносин, які нестимуть юридичну відповідальність у разі скоєння ними певного злочину чи правопорушення можуть бути не тільки фізичні, але й юридичні особи. За для яскравого та зрозумілого навіть звичайному громадянину, не наділеному глибокими юридичними знаннями прикладу, можна взяти випадок забруднення навколишнього середовища певним промисловим заводом чи фабрикою, які входять до складу якогось підприємства. У такому випадку, увесь встановлений, юридично доведений у судовому порядку обсяг шкоди, завданої природному середовищу, а також життю і здоров'ю окремих фізичних осіб зокрема, буде відшкодовуватися з активів юридичної особи (в даному випадку підприємства-власника заводу), а вже потім шляхом регресної вимоги з боку цього підприємства деякий обсяг майнових витрат буде стягнений з конкретних осіб-винуватців цієї трагедії.

Наведена ситуація є прикладом застосування одразу декількох правових сфер, адже наслідки такої шкідливої діяльності підприємства будуть розглядатися не тільки з точки зору публічно-правових галузей, які тут вочевидь присутні. Окрім кримінального та екологічного права, в цій справі наявним є порушення норм приватного права. Бо, окрім високої вірогідності спричинення шкоди життю та здоров'ю фізичних осіб, які охороняються кримінальним правом, існує також загроза заподіяння майнової шкоди фізичним та юридичним особам, на кшталт штучно заподіяного неврожаю на ділянках, які постраждали від шкідливих промислових викидів, або спричинення умов, за яких суб'єкти правовідносин будуть вимушені не з'являтись на своїх ділянках та користуватися ними деякий час, через високий рівень забрудненості. Усі ці питання у подальшому неодмінно будуть розглядатися як приватноправові спори. Сторонами таких спорів відповідно стануть підприємство, як юридична особа, діяльність якої спричинила шкоду і збитки, а з іншого боку будуть фізичні та юридичні особи, яким ці лиха були завдані, і які, згідно з чинним законодавством будуть вимагати відшкодування, або компенсації ним усіх нанесених перешкод. Отже з цього походить що усі ці приватноправові процесуальні спори у даному випадку неминуче будуть охоплюватись галуззю цивільного права.

Такий приклад був наведений для того, щоб якомога краще проілюструвати вплив юридичної відповідальності на будь-які суспільні правовідносини, до якої б галузі права вони не відносились. Саме такі риси юридичної відповідальності як неодмінна невідворотність суспільно-правових наслідків за кожне вчинене діяння, а також забезпечене державним примусом заохочення осіб-учасників суспільних правовідносин за дотримання встановлених у державі правових норм, які натомість знайшли своє юридично-оформлене відображення у різноманітних законах, та підзаконних нормативно-

правових актах (укази, рішення, ухвали, розпорядження) є головними для визначення сутності та соціального призначення юридичної відповідальності. Поруч із цим, необхідно зазначити що фактор юридичної відповідальності має величезне значення для майбутнього створення в країні надійного державно-правового механізму, який би ефективно охороняв та забезпечував свободи, права та законні інтереси усіх, без винятку суб'єктів правовідносин.

В наші часи, коли політичним керівництвом держави відкрито проголошується намір підтримувати безперервний рух країни на шляху до євроінтеграції, поряд з необхідними для цього економічними реформами має бути проведена ретельна і зважена перевірка чинного законодавства щодо його відповідності заявленим про-європейським критеріям і принципам, а також сучасного стану вітчизняної правової системи загалом. Багатьма фахівцями зазначається що до питань, які потребують більш прискіпливішого вирішення, окрім судової та правоохоронної сфери, відноситься також і питання сучасного місця юридичної відповідальності у вітчизняній правовій системі. Більш того, абсолютно доведеним є те, що юридична відповідальність за своєю природою тісно взаємодіє та співіснує з багатьма іншими галузями і сферами публічних й приватних суспільно-правових відносин. Адже вона є однією з невід'ємних рис функціонування вітчизняного судоустрою, який здійснює правосуддя на території держави, а також відіграє важливу роль у повсякденній діяльності правоохоронних органів України. Отже у підсумку слід зазначити, що юридична відповідальність є однією з невід'ємних складових функціонування державно-правового механізму сучасної держави.

УДК 378.14

АЛІНА ГРИГОРІВНА ГАРКУША
старший викладач кафедри кримінального процесу, к.ю.н., доцент Дніпропетровський державний університет внутрішніх справ
ЄВГЕНІЯ МИКОЛАЇВНА ЧУГАЙ
курсант факультету підготовки фахівців для органів досудового розслідування Дніпропетровський державний університет внутрішніх справ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У ПІДГОТОВЦІ КАДРІВ ДЛЯ ОРГАНІВ ДОСУДОВОГО РОЗСЛІДУВАННЯ

Трансформаційні зміни у системі Національної поліції України (далі НП України) задали новий напрямок реформування правоохоронного органу, а саме діяльність у відповідності із загальноприйнятими міжнародними стандартами, впровадження інноваційних технологій підготовки поліцейських тощо. Одним із основних напрямків процесу стабілізації діяльності органів НП України, зокрема органів досудового розслідування, є розробка єдиного діючого механізму підготовки професійних кадрів для правоохоронних органів. Одним із найбільш важливих аспектів підготовки майбутніх слідчих, на наше стійке переконання, є впровадження активного вивчення інформаційного простору.

Теоретична підготовка, яку здійснюють заклади, що займаються підготовкою кадрів для органів досудового розслідування НП України, хоча і є фундаментальною, однак без проведення практичних занять не дає особливо вагомого результату для подальшої діяльності. Серед ефективних способів та методів, якими охоплюється практична підготовка майбутніх правоохоронців, особливо важливою є використання здобутків інформаційних технологій, адже значний обсяг процесуальних дій виконується шляхом роботи з різними державними реєстрами, пошуковими системами, базами даних і звичайними текстовими редакторами.

На даному етапі розвитку технологічних систем неможливо помислити діяльність слідчого без використання інформаційних технологій, адже саме за допомогою них акумулюється уся інформація, об'єднується, оброблюється та систематизується для подальшого її використання. Так, наприклад, уся робота слідчого у рамках кримінального провадження здійснюється із використанням інформаційних технологій (внесення відомостей до ЄРДР, робота з текстовими редакторами, використання інтернет-ресурсів тощо). Ми впевнені, що успішність такої діяльності прямо залежить від сформованих у навчальному закладі навичок використання інформаційного простору.

Впровадження активної підготовки курсантів шляхом використання інформаційних технологій є такі особливості: 1) інтерактивність (у тому числі забезпечення тренінгового характеру навчально-пізнавальних завдань); 2) забезпечення зворотного зв'язку, у тому числі здійснення автоматизованого контролю, моніторингу, діагностування, 3) підвищення інтелектуальності освітнього процесу шляхом: позбавлення суб'єктів викладання від репродуктивних дій та операцій; впровадження в навчальний процес складних навчально-пізнавальних завдань; використання глобальних інформаційних ресурсів; підвищення інформаційної компетентності користувачів інформаційними технологіями; забезпечення актуальності навчального контенту. Іншою особливістю використання інформаційних технологій в підготовці курсантів є оптимізація зворотного зв'язку суб'єктів навчання та суб'єктів викладання їх засобами [1, с.48]. Зокрема, використання інформаційних технологій дозволяє розробити різні інтерактивні навчальні заняття, що відображують реальне використання окремих здобутків інформаційного простору у роботі працівника поліції, викликаючи більший інтерес до навчального процесу.

Прикладом поглибленої практичної підготовки майбутніх працівників органів поліції шляхом впровадження інноваційних методів інформаційних технологій є використання під час навчальних занять імітованих інформаційних систем, робота курсантів в емульгаторах ЄРДР, ЦУНАМІ та інших штучно створених імітованих навчальних системах. У процесі таких навчань курсанти засвоюють комплекс практичних заходів працівників поліції, набувають та вдосконалюють навички, зокрема складання реєстраційних та процесуальних документів, користування технічними засобами фіксації інформації, кваліфікації правопорушень, процесуального порядку проведення слідчих (розшукових) дій, тактичних прийомів дій

працівників поліції, аналізу отриманої інформації тощо [2, с. 156]. Проблемою залишається лише те, що такі практичні заняття не є достатньо поширеними, а якщо вони і проводяться, то не охоплюють багато навчального часу і дають можливість лише поверхневого ознайомлення, а не поглибленого вивчення для подальшого користування.

Відтак, запровадження активного використання інформаційних технологій у навчальному процесі курсантів закладів системи МВС дозволить покращити не лише теоретичний рівень оволодіння отриманої інформації, а й забезпечить підготовку якісних кадрів для подальшої роботи у практичних органах. На разі у закладах МВС курсантами 4 курсів вивчається теоретична дисципліна «Досудове розслідування», тому ми вважаємо, що для досягнення поставленої мети необхідним є впровадження у навчальний процес майбутніх працівників органів досудового розслідування вивчення також додаткової дисципліни стосовно вивчення інформаційних систем, які використовує слідчий у своїй діяльності, у більшій мірі поглиблене вивчення Єдиного реєстру досудових розслідувань.

Список використаних джерел:

1. Федоренко О. Сучасні тенденції удосконалення професійної підготовки майбутніх офіцерів поліції. *Новий колегіум.* 2016. Вип. № 4. С. 46-52.

2. Краснобрижий І.В., Прокопов С.О., Рижков Е.В. Інформаційне забезпечення професійної діяльності : навч. посіб. Дніпро : ДДУВС, 2018. 218 с.

АЛЬВІНА МИХАЙЛІВНА СТАРУСЬОВА
курсант 4 курсу факультету підготовки фахівців для підрозділів кримінальної поліції Дніпропетровського державного університету внутрішніх справ
ЄВГЕНІЯ ВОЛОДИМИРІВНА СТРЮК
старший викладач кафедри українознавства та іноземних
Дніпропетровського державного університету внутрішніх справ

РОЗВІДКА З ВІДКРИТИХ ДЖЕРЕЛ – ВИЯВЛЕННЯ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

На даний час люди є неабиякими свідками глобального переходу та стрімких світових змін від індустріального суспільства до інформаційного. Тому це прямо впливає на оновлення способів та умов праці у всіх видах діяльності людини. Змінюється абсолютно все починаючи від аграрної промисловості та закінчуючи космічним дослідженням всесвіту. Виникають найрізноманітніші способи застосування збройних сил, також створюються нові фактори збройної боротьби. Щоб виявити та запобігти злочини ,які стосуються інформаційної безпеки перш за все потрібно розробити певні методи,які будуть тим чи іншим способом запобігати здійсненню впливу на криміногенні об’єкти.

Динамічний інформаційний розвиток сучасного суспільства створив об’єктивні чинники для виникнення умов, коли все більше інформації, яка

необхідна для прийняття рішення, можливо знайти у відкритих джерелах кіберпростору [1]. Неодмінною складовою збору інформації різних форм власності в умовах воєнної обстановки, а також швидкого збільшення інформаційного потоку стає робота з відкритими джерелами інформації, вона проводиться розвідувальними службами.

Аби отримати необхідну інформацію, яка потрібна для вирішення певного питання, для цього потрібно здійснити пошук по даним питанням, відокремити питання за їх певними ознаками, зробити аналіз інформації на її достовірність, новизну, об'єктивність, після чого відібрати найкращі джерела та зробити певну систему, в результаті чого ми отримаємо повний результат проблеми, яку ми відібрали для дослідження. Завдяки цьому підходу дослідження можна отримати більш точну інформацію по певній проблемі, яка досліджується. Різні пошукові системи використовуються у сьогоденні сучасним суспільством в мережі Інтернет. Це такі універсальні пошукові системи як, Yandex, Yahoo, Ask, загалом їх використовують для пошуку фотографій, ілюстрацій, мультимедійного контенту, відео та аудіо файлів, а також спеціалізовані пошукові системи TinEye та Bing. Кожна пошукова система має свої пріоритети, свій власний механізм, який допомагає користувачеві обрати саме ту, яка йому більш комфортна та яка робить пошук більш спрощеним. Країни Європи вже доволі давно проводять курси,семінари та конференції , де надають знання, щодо роботи з відкритими джерелами, їх можуть відвідати усі бажаючі за відповідну плату. Прикладом являється Швейцарія,яка проводить курси для бізнес-персоналу, та коштують вони 640 швейцарських франків та тривають усього два дні [2].

Інформація, яка добувається з відкритих джерел, а саме: телебачення,газети, журнали, аналізується розвідувальними структурами за для того аби доповнювати розвідувальну інформацію, яка вже була добута з інших каналів. Не дивлячись на це експерти зазначають,що можна отримати значну кількість інформації не застосовуючи агентуру. Як зазначав Н.Ротшильд "Хто володіє інформацією – той володіє світом", став рушійною силою в наш час в пошуку необхідної інформації.

За для того, аби все ж таки розібратися у значенні терміну «розвідка з відкритих джерел» потрібно проаналізувати думки вітчизняних та іноземних науковців. Основоположником терміну "розвідка з відкритих джерел" (Open Source INTelligence – OSINT) є розвідувальне співтовариство США, яке почало його активно використовувати з моменту створення Інформаційної служби закордонного віщання (Foreign Broadcast Information Service – FBIS, лютий 1941 року). Відповідно до Інструкції з організації роботи з відкритими джерелами інформації в розвідувальних цілях FMI 2-22.9 "Open Source Intelligence" [3] OSINT є одним з видів воєнної розвідки, вона призначена для пошуку, збору та аналізу інформації з загальнодоступних джерел. Не дивлячись на це необхідно не плутати «розвідку з відкритих джерел» та «конкурентна розвідка» (competitive intelligence) та схожим йому терміном «бізнес-розвідка» (business intelligence)– це система заходів щодо постійного пошуку, виявлення, збору з різних джерел (відкритих, корпоративних або з

обмеженим доступом), накопичення інформації стосовно змін умов комерційної діяльності, її аналізу з метою своєчасної підготовки звітів про її реальний стан справ та визначення тенденцій розвитку ситуації [4]. Вивчаючи праці вітчизняних науковців термін «розвідка з відкритих джерел» ніде не застосовується. Проте в законі України «Про Інформацію» є визначення терміну «інформація», а також зазначається класифікація доступу до інформації. Так, «інформація» – це будь які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом, причому, будь-яка інформація вважається відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

Інформація являється найважливішим видом забезпечення законодавчої діяльності, вона має свою самостійну цінність,вона має вплив на державну політику, визначає вибір варіанта політичного розвитку, поведінки різноманітних соціальних груп та окремих громадян. Складова єдиної системи розвідувальної діяльності, правильне використання розвідки на основі аналізу відкритих джерел інформації, може забезпечити споживачів достатньо повною розвідувальною інформацією, необхідною для прийняття ними обґрунтованих рішень.

Список використаних джерел:

1. Тоффлер Э. Война и антивойна. Москва: АСТ Транзиткнига, 2005. с 240.

2. За матеріалами сайту компанії “I-intelligence”. URL: http://www.i-intelligence.eu

3. Open Source Intelligence. FMI 2-22.9. December 2006. Federation of American Scientists. URL: http://www.fas.org/irp/doddir/army/fmi2-22-9.pdf.

4. Доронин А. И. Бизнес-разведка. Москва: “Ось-89”, 2003. 384 с.

УДК 681.3

ТЕТЯНА ПЕТРІВНА КОЛІСНИК
кандидат педагогічних наук, доцент, доцент кафедри інформаційних технологій та кібербезпеки факультету №4 Харківського національного університету внутрішніх справ
ДІАНА ОЛЕКСІЇВНА БЛЄДНА
курсант 2 курсу факультету №4 Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ БОРОТЬБИ ЗІ ЗЛОЧИННІСТЮ В УМОВАХ СЬОГОДЕННЯ

Одним з важливих підходів для реалізації цілей «Стратегії розвитку органів системи Міністерства внутрішніх справ України на період до 2020 року», затвердженої розпорядженням Кабінету Міністрів України від 15 листопада 2017 року № 1023-р, є інформатизація діяльності, а саме,

підвищення ефективності роботи і взаємодії через максимальне використання інформаційно-комунікаційних технологій у реалізації завдань органами системи МВС [1].

У науково-технічній літературі інформаційна технологія - цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розподіл даних, доступ до джерел інформації незалежно від місця їх розташування. Упорядкована послідовність взаємозв'язаних дій, що виконуються з моменту виникнення інформації до одержання результату, називається технологічним процесом. Інформаційна технологія, таким чином, невід'ємна від того специфічного середовища, в якому вона реалізується, тобто від технічного і програмного середовища.

Інформаційно-комунікаційні технології (ІКТ, від англ. Information and communications technology, ICT) - це сукупність методів, засобів та прийомів пошуку, зберігання, опрацювання, подання та передавання графічних, текстових, цифрових, аудіо та відеоданих на базі персональних комп`ютерів, комп`ютерних мереж та засобів зв`язку. Термін ІКТ в сучасному освітленні також використовується для позначення об'єднання (конвергенції) аудіовізуальних та телефонних мереж з комп'ютерними мережами. Іншими словами, ІКТ складається з ІТ, а також телекомунікацій, медіа-трансляцій, усіх видів аудіо і відео обробки, передачі, мережевих функцій управління та моніторингу. Ефективне управління інформаційними ресурсами, їх надійний захист від кібератак, уміння використовувати аналітичні інструменти це основа для підтримки управлінських рішень керівництва Міністерства внутрішніх справ.

Загальною ознакою злочинів у сфері ІТ є їх підвищена суспільна небезпека, а також інноваційність, обумовлена невідомими раніше схемами скоєння злочинів, новизною самих технологій. Сучасність яскраво демонструє стрімкий розвиток високих технологій. Цей період ознаменував собою стрімкий розвиток кібернетичних технологій, різке збільшення обсягів впливу глобальної мережі інтернет, всеосяжність інформаційних потоків і глобалізацію інформаційних процесів. Це, у свою чергу, прямо сприяє на розвиток злочинності в даній сфері. Отже, одночасно з прогресом, спостерігається і зростання злочинності у сфері інформаційної безпеки.

Проблема забезпечення інформаційної безпеки України знайшла відображення в законах «Про основи національної безпеки України», «Про концепцію національної програми інформатизації», «Про національну програму інформатизації», а також у Концепції національної безпеки України. Утворений кібернетичний простір являє собою не просто сукупність окремих технічних об'єктів, здатних сприймати сліди активності людини, та утворює щільно пов'язане середовище, в якому криміналістичні зображення можуть перетворюватися, копіюватися і передаватися від одного пристрою до іншого. В результаті ці сліди шляхом великої кількості локальних взаємодій починають передаватися на великі відстані та зберігатися в

цифровому вигляді в необмеженій кількості місць і практично необмежений час. Такі особливості привели до того, що криміналістика була змушена дослідити особливості цих об'єктів, вивчати специфіку механізмів кіберпростору.

На законодавчому рівні визначено, що кіберзагроза – наявність та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів [2].

Серед найбільш розповсюджених кіберзлочинів слід відзначити наступні:

– наявність пристрою, зараженого вірусом чи іншою загрозою безпеці (53%);

– проблеми з дебетовими або кредитними картками (38%);

– усунення пароля облікового запису (34%);

– несанкціонований доступ або хакерство електронної пошти чи облікового запису соціальних медіа (34%);

– придбання онлайн, яке виявилося шахрайським (33%);

– натискання на шахрайську електронну пошту або надання конфіденційної інформації у відповідь на шахрайство з електронною поштою (32%).

Зазначимо, що сьогодні експерти звертають увагу на нові кіберзагрози, які пов'язані з масовим розвитком технологій І 4.0, концепція яких передбачає швидкий розвиток та нарощування сегменту технологій четвертої хвилі в економічній і позаекономічній сферах. Причому станом на 2018-2019 р. р. цей процес лише розпочався. І на поточному етапі розвитку І 4.0 точкою входу для найбільшої кількості кібератак є персональні, підключені до Мережі портативні пристрої (смартфони, планшети тощо), парк яких набув тотального охоплення і продовжує швидко зростати, збільшуючи можливості кібератаки для зловмисників [3].

У 2018 році увагу працівників кіберполіції було зосереджено на розслідуванні злочинів, вчинених у сфері високих інформаційних технологій. Так протягом року працівники Департаменту кіберполіції були залучені до розслідування більше 11 тисяч кримінальних проваджень.

Зокрема, протягом року найбільша кількість злочинів була зосереджена у місті Києві, а також на території Одеської, Миколаївської та Львівської областей. Упродовж року поліцейські виявили 6 тисяч злочинів, вчинених у сфері використання високих інформаційних технологій.

У 2018 році працівники поліції викрили більше 800 осіб, які були причетні до вчинення злочинів у сфері високих інформаційних технологій. Водночас, у сфері кібербезпеки найбільше виявлено користувачів шкідливого програмного забезпечення, які вчиняли злочини, використовуючи придбані віруси у DarkNet.

Сьогодні українська кіберполіція розробляє і успішно впроваджує у практичну діяльність поліції сучасні методики виявлення, фіксації і дослідження цифрових доказів. Зокрема, упродовж 2018 року спеціалістами з кіберполіції оглянуто та проаналізовано 5,5 петабайтів інформації, яка у подальшому була визначена як цифрові докази.

За результатами міжнародної співпраці у 2018 році було викрито 8 транснаціональних хакерських угруповань та взято участь у понад 30 міжнародних операціях.

Крім того, у 2018 році було підписано договори про взаємодію у сфері боротьби з кіберзлочинністю з організаціями як державного, так і приватного секторів. Серед них – представники міжнародних кампаній у сфері інформаційної безпеки та ІТ-компанії, а також поліцією Австралії, Сінгапуру, Катару та ще ряду країн. Крім того, налагоджено ефективну взаємодію з найвідомішими світовими соціальними мережами [4]. Зростання інформатизації країни та зростання тиску кібервпливів актуалізує роль держави та відповідного державного регулювання у забезпеченні кібернетичної безпеки. Це обумовлено тим, що саме держава визначає політику національної безпеки, сталого розвитку, цифровізації економіки і т. ін.

Список використаних джерел:

1. Розпорядження КМУ від 15 листопада 2017 р. № 1023-р «Про схвалення Стратегії розвитку органів системи Міністерства внутрішніх справ на період до 2020 року». URL: https://zakon.rada.gov.ua/laws/show/1023-2017-%D1%80

2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-YIII. Відомості Верховної Ради (ВВР). 2017. № 45. ст.403.

3. Гнатюк С.Л. Кібербезпека в умовах розгортання четвертої промислової революції (industry 4.0): виклики та можливості для України. Аналітичні матеріали. URL: https://www.niss.gov.ua/doslidzhennya/analitichni-materiali/informaciyni-strategii/kiberbezpeka-v-umovakh-rozgortannya

4. Підсумки 2018 року в цифрах. Кіберполіція України: офіц. сайт. URL: https://cyberpolice.gov.ua/results/2018/

5. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 за № 2594-IV. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80/conv

УДК 681.3.06
ОЛЕНА ГЕОРГІЇВНА СОКОЛОВСЬКА
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та кібербезпеки факультету №4 Харківського національного університету внутрішніх справ
АМІНА ІГОРІВНА ГОЛОВНЯ
курсант 1 курсу факультету №4 Харківського національного університету внутрішніх справ

ЗАСТОСУВАННЯ НАГРУДНИХ КАМЕР ПРАЦІВНИКАМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Нагрудний відеореєстратор – це спеціальний пристрій, що використовується для запису, обробки та збереження інформації у форматі відео.

Body-камери, які повинні носити патрульні мають декілька недоліків. По перше, вони знімають не постійно. По друге, дуже легко виявити ведеться зйомка чи ні. По третє, записану картинку поліцейський самостійно видалити не може.

Українські правоохоронці тільки нещодавно спростували слухи, що з'явилися з початком запуску патрульної поліції про те, що body-камери працюють безперервно, в реальності все зовсім інакше. Так, патрульний в будь-який момент може увімкнути чи вимкнути нагрудну відеокамеру, що пов'язано з об'єктивними причинами. Зокрема, з зарядом батареї – не дивлячись на досить містку ємкість акумулятора, він не взмозі працювати безперервно від 10 до 14 годин робочої зміни. Тому існує наказ керівництва вмикати body-камеру при будь-якому контакті з громадянами. Але на практиці, як правило, поліцейські її активують при конфліктних ситуаціях - при неадекватній, агресивній і некоректній поведінці громадянина.

Нагрудні відеореєстратори мають деякі переваги і володіють широким спектром технічних характеристик, які визначають їхнє цільове призначення. Розглянемо їх.

3G-4G онлайн трансляція – функція, що дозволяє вести трансляцію в режимі реального часу при підключенні до 3G-4G зв'язку. Наявна у моделі Tecsar B27-4G-M-GPS-MOB.

Вбудований мікрофон дозволяє запис звуку при відеозйомці. Знятий матеріал може бути доказом у суді при відкритті провадження. Функція представлена у багатьох моделях, зокрема Patrul X-05, Patrul X-01, Protect R-01S 32gb, Tecsar B42-BAT-MOB та інших.

Функція, що дозволяє ведення трансляції з місця подій в режимі реального часу при умові підключення пристрою до Wi-Fi. Модель Patrul-DX-Wifi-02 оснащена даною функцією

Змінна батарея дозволяє довготривалий безперервний режим зйомки. В комплекті Protect R-02A – 32 gb представлено дві батареї, які за необхідністю можна змінювати та продовжувати зйомку.

GPS логгер клас радіоприймачів, що може працювати в режимі звичайного GPS-приймача, або в режимі логера для запису інформації в свою вбудовану

пам’ять. Вбудований GPS логер представлений у Patrul X-05, Protect R-08+GPS, Tecsar B26-GPS-MOB та інших.

Циклічний запис забезпечує запис відео фрагментами по декілька хвилин кожен. Завдяки даній функції можна вести безперервний запис, незважаючи на його тривалість, а також полегшує пошук потрібного фрагменту за потреби. Циклічний запис характерний для всіх нагрудних відеореєстраторів. Циклічний запис, функція, що дозволяє робити безперервний запис. У випадку заповнення пам'яті, відеореєстратор видаляє найстаріший запис та звільняє місце для нового, тим самим виключаючи потребу підключення до ПК та «ручного» видалення записів.

Інфрачервона підсвітка забезпечує режим нічної зйомки. Камери, обладнані ІЧ підсвіткою, місять спеціальні світодіоди, які передають випромінювання, майже невидиме для людського ока. В складі нагрудних відеорестраторів необхідні для зйомки в темну пору доби, що важливо для працівників патрульної поліції, охоронців та інших представників силових структур.

Максимальна тривалість зйомки відео залежить від потужності батареї, що встановлена в пристрої. Боді-камери для поліцейських виготовляють з можливістю безперервної зйомки від 7-ми годин до 15-ти годин. Зважаючи на можливість зміни батареї, сумарна кількість годин зйомки без підзарядки може перевищувати добу. Така моливість присутня у моделі Protect R02A, в якої є можливість заміни батареї

Кут огляду це кут, який осягає камера в зафіксованому положенні. Для нагрудних відеореєстраторів сягає до 170°.

Роздільна здатність фотозйомки – це величина, що характеризує кількість точок на одиницю площі та визначає якість та чіткість отриманого знімку.

Таким чином, вбудована пам'ять це постійне місце збереження файлів. Об'єм внутрішньої пам'яті повинен відповідати кількості годин безперервної зйомки для того, щоби вся інформація могла бути збережена та при потребі використана.

ДМИТРО СЕРГІЙОВИЧ НИКИТЕНКО
здобувач вищої освіти ІІ курсу Факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ
НАТАЛІЯ СЕРГІЇВНА РЕЗЦОВА
викладач кафедри кримінального процесса Дніпропетровського державного університету внутрішніх справ

НЕОБХІДНІСТЬ ВПРОВАДЖЕННЯ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ В УКРАЇНІ

Актуальність теми дослідження щодо необхідності впровадження інтелектуальної системи відеоспостереження в Україні обумовлена зростаючою у сьогоденні поширеністю інформаційних технологій не тільки серед працівників правоохоронних органів, а й серед громадян в цілому. Зі стрімким

розвитком технологій у світі з’являється багато покращених пристроїв які поліпшують життя людям, але є й такі прилади, якими повинні забезпечити себе поліцейські. Актуальним впровадженням новітніх інформаційних технологій для працівників Національної поліції буде встановлення інтелектуальної системи відеоспостереження, що позитивно вплине на ефективність, швидкість, професіональність та оперативність роботи поліцейських.

Інтелектуальна система відеоспостереження дозволяє вести контроль за транспортним потоком та правопорушеннями на дорозі, вона сканує номерні знаки транспортного засобу, а також колір та марку автомобіля. Штучний інтелект спроможний навіть виявити злочинця, який знаходиться у розшуку та перебуває у машині. Якщо раніше за камерами слідкували спеціально відділи, то зараз є можливість скоротити кількість працівників цього відділу до одного або двох поліцейських, тому-що система сама спостерігає через камери, які розташовані у місті, за ситуацією навкруги та у разі виявлення будь-чого негайно фіксує все та зберігає інформацію, а також виводить кадри з місця події прямо на головний монітор відеоспостереження в установі Національної поліції.

Основним завданням інтелектуальної відеокамери є намагання у повній мірі змоделювати можливості зору людини і навіть відтворити певні можливості її мозку, шляхом прийняття, логічної обробки та відтворення інформації у переробленому вигляді.

Щодо аналізу інтелектуальних систем відеоспостереження працівниками правоохоронних органів у світовому досвіді слід зазначити, що система має велику кількість переваг, зокрема:

– Кращий у порівнянні з іншими системами відеоспостереження збір інформації та її обробку (ідентифікація об’єктів);

– Отримання на логічна обробка інформації шляхом її поєднання з інформацією у відкритих інтернет джерелах, базах даних та інших інформаційних ресурсах;

– Автоматизована робота системи;

– Оперативність розшукових дій поліцейськими шляхом швидкого пошуку конкретної інформації у всіх можливих інтернет джерелах та базах даних;

– Наявність функції ефективного аналітичного аналізування інформації та сповіщення нею оператора системи.

Інтелектуальна система відеоспостереження може реалізувати себе у можливості працівників Національної поліції вирішувати наступні завдання:

– Виявлення та розпізнавання обличчя, а також звернення до розшукових баз даних та інших ресурсів. У тому числі це дасть змогу автоматизувати систему пропускного режиму способом розпізнавання обличчя особи;

– Розпізнавання номерних знаків на транспортних засобах, їх кольору, типу та моделі, а також інформації про її власника та виробника. Прогнозування можливих загроз на стратегічно важливих об’єктах;

– Автоматизоване встановлення відповідностей між існуючими реєєстраційними номерами, марками та кольором автомобіля та їх офіційним затвердженням у базі даних, виявлення можливих невідповідностей;

– Фіксація та аналізування траєкторії руху як будь-яких осіб так і транспортних засобів, контроль швидкості руху автомобілів, спостереження та аналіз ситуації на дорозі та усіх її елементах для забезпечення безпеки дорожнього руху, дотримання ПДД та регулювання завантаженості магістралей;

– Контроль за транспортним потоком у великих містах;

– Забезпечення та гарантія безпеки у місцях значного скупчення людей, наприклад: вокзали, аеропорти, торгівельні, розважальні та спортивні комплекси, а також інших місця де перебуває велика кількість людей, особлива увага приділяється місцям у яких наявне велике скупчення дітей;

– Виявлення певних подій, яку відбулися у різних місцях у різний проміжок часу але є пов’язані між собою спільним павутинням злочинної діяльності, для подальшого спостереження та аналізу таких подій.

В Україні є досвід запровадження такої системи, а саме у місті Маріуполі, вона вже показала себе з найкращого боку та залишила за собою статус кращої системи відеоспостереження в очах українців та й усього світу. Запроваджена система у Маріуполі дає змогу стверджувати, що відбулося зниження рівня злочинності, підвищення виявлення та документування кількості правопорушників, здійснення розшуку викрадених транспортних засобів та багато інших позитивних моментів. Нажаль, запровадження інтелектуальної системи відеоспостереження на території України є досить проблематичним питанням, пов’язаним першим чином з нехваткою коштів у Міністерства внутрішніх справ для закупівлі належного обладнання та облаштування ним країни. Тож потрібно зробити висновки, що цілком виправданим та, можливо, навіть необхідним є будь-який вид фінансової підтримки з боку місцевих державних адміністрацій, спонсорів та навіть приватного сектору.

УДК 004.9 +343.1

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

ДЕЯКІ АСПЕКТИ АВТОМАТИЗАЦІЇ РОЗГОРТАННЯ І УПРАВЛІННЯ ТЕСТОВОГО СЕРЕДОВИЩА НАВЧАННЯ КІБЕРБЕЗПЕКИ

Навчання спеціалістів для підрозділів Департаменту кіберполіції Національної поліції України потребує створення, оновлення і підтримки в актуальному стані тестового середовища навчання кібербезпеки і цифрових криміналістичних досліджень.

Суттєва специфіка навчання за цим напрямом полягає у постійній необхідності швидкої зміни налаштувань і оновленні тестового середовища навчання разом із швидким розвитком та виявленням нових вразливостей

інформаційних технологій, що у свою чергу потребує великих витрат часу і зусиль при завжди обмежених ресурсах.

Автоматизувати розгортання і управління тестовим середовищем можна шляхом застосування технологій:

– ізольованих віртуальних контейнерів Docker - для розгортання вразливих застосувань;

– приватної обчислювальної хмари (Private Cloud Computing) - для створення хмарного сховища тестового середовища.

Технологія Docker дозволяє швидко розгорнути у вигляді контейнерів вразливі застосування у тестовому середовищі із значно меншим навантаженням на хостову операційну систему ніж віртуальні машини. Деякі, вже налаштовані, контейнери можна знайти на hub.docker.com. Наприклад, у профілі "vulnerables" (hub.docker.com/u/vulnerables) доступно 18 контейнерів вразливих застосувань. В [1] наведений приклад встановлення і налаштування:

– Damn Vulnerable Web Application (DVWA);
– OWASP Mutillidae;
– OWASP WebGoat;
– bWAPP;
– OWASP Juice Shop;
– WPScan Vulnerable WordPress;
– OpenDNS Security Ninjas;
– Altoro Mutual.

Технологія Private Cloud Computing дозволяє створити хмарне сховище для користувачів тестового середовища. В [2] зазначені три способи розгортання Private Cloud Computing на базі рішення ownCloud (owncloud.com):

– у хостовій ОС Ubuntu 18.04 LTS;
– в Docker контейнері;
– в віртуальній машині Bitnami Owncloud Stack Virtual Machines.

З огляду на зручність і швидкість доцільно використовувати розгортання ownCloud в Docker контейнері.

Окрім ownCloud існують альтернативні рішення Private Cloud Computing з відкритим кодом (Open Source) [3]:

– Nextcloud (github.com/nextcloud);
– Syncthing (github.com/syncthing/syncthing);
– Seafile (github.com/haiwen/seafile);
– IPFS (ipfs.io);
– Cozy (github.com/cozy/cozy-stack);
– та інші.

Розгортання Docker контейнерів вразливих застосувань і приватного хмарного сховища в тестовому середовищі дозволить суттєво підвищити ефективність навчання спеціалістів для підрозділів Департаменту кіберполіції Національної поліції України.

Список використаних джерел:

1. Raj Chandel. Web Application Pentest Lab setup Using Docker. URL: https://www.hackingarticles.in/web-application-pentest-lab-setup-using-docker/.

2. Raj Chandel. Multiple Ways to Setup Cloud Pentest Lab using OwnCloud. URL: https://www.hackingarticles.in/multi-ways-to-setup-cloud-pentest-lab-using-owncloud/.

3. Alternatives to ownCloud for all platforms with Open Source License. URL: https://alternativeto.net/software/owncloud/?license=opensource).

УДК 004.056

ОЛЕКСАНДР ЮРІЙОВИЧ ГОРЕЛОВ
студент магістратури Харківський національний університет радіоелектроніки

ПРОБЛЕМА АДАПТАЦІЇ В СИСТЕМАХ ДИСТАЦІЙНОГО НАВЧАННЯ

В даний час значно зріс інтерес до використання дистанційних комп'ютерних навчальних курсів для підготовки і підвищення кваліфікації співробітників в самих різних організаціях. Одним із шляхів підвищення ефективності навчання при використанні комп'ютерних дистанційних технологій полягає в розробці освітніх Веб-додатків, що мають широки можливості в області адаптації.

Реалізація можливості адаптації дозволяє враховувати індивідуальні особливості користувача (рівень знань, цілі, потреби, когнітивні особливості і т.п.), плануючи процес навчання і пропонуючи йому найбільш підходящий навчальний матеріал в найбільш придатній для нього формі.Під адаптивним навчальним Веб-курсом будемо розуміти гіпермедійних систему, яка має здатність до адаптації різних аспектів своєї роботи до особливостей учня на основі його моделі.

Розробка адаптивного навчального Веб-додатки є складною проблемою, яка передбачає вирішення низки завдань, пов'язаних з певною організацією навчального матеріалу, допускає варіативність його представлення, розробкою методів його модифікації, методів подання моделі учня, реалізацією збору інформації про користувача, розробкою і реалізацією технології адаптації та ін.

Основними питаннями, на які необхідно відповісти в процесі проектування і розробки адаптивного навчального Веб-курсу, є наступні:

– яка мета реалізації адаптаційних технологій в конкретному навчальному курсі (навіщо потрібна адаптація в конкретній системі),

– які фактори будуть враховуватися в якості вхідної інформації при виробленні адаптаційних рішень (до чого буде адаптуватися система),

– які аспекти функціонування системи будуть змінюватися в процесі адаптації (що буде адаптовано),

– які механізми адаптації будуть використовуватися і як вони будуть реалізовані (як буде здійснюватися адаптація).

Більшість адаптивних навчальних систем в якості вхідної інформації для прийняття адаптаційних рішень використовують різні характеристики користувача, серед яких найчастіше використовуються рівень знань користувача, мета користувача, рівень підготовки користувача і досвід роботи з гіпермедіа.

На основі аналізу зазначених параметрів моделі користувача адаптивний навчальний курс повинен дозволяти змінювати зміст досліджуваного матеріалу, його форму подання, послідовність проходження по курсу і можливості навігації на сторінках курсу. З урахуванням того, що основними формами подання навчального матеріалу є текст і мультимедіа, можна розділити проблему адаптації форми на адаптацію тексту і адаптацію мультимедіа.

Адаптація змісту може реалізовуватися шляхом подання навчального матеріалу з різним ступенем деталізації, з урахуванням рівня знань по суміжних темах і поняттях. Більш радикальним методом є використання різних варіантів представлення матеріалу, які вибираються для презентації на основі моделі користувача. Реалізація адаптивної підтримки навігації передбачає наявність певних засобів аналізу моделі користувача і особливостей процесу взаємодії користувача з матеріалом курсу. Ці засоби повинні оптимізувати можливі шляхи проходження матеріалу курсу, адаптуючи систему навігації на навчальних сторінках до розглянутих вище факторам.

Переваги адаптивних навчальних курсів включають в себе, зокрема, наступне:

– автоматизовані процеси оцінки успішності студентів і прогностичного аналізу призводять до значної економії часу викладацького складу;

– адаптивні системи здатні вирішити основну проблему освітнього процесу – тяжку вимогу від вчителів та викладачів бути відповідним за оволодіння практичними навичками безлічі учнів, що відносяться до різних демографічних груп;

– адаптивні системи враховують принципово різні рівні попередніх знань, а також прогрес у ході курсу, заснований на вимірюванні навичок і результатів навчання студентів, зниженні навантаження викладачів на викладання, виправлення ситуації з викладанням та сприянням студентам;

– якщо система створена ефективно, знижається вартість автоматизованого зворотного зв'язку і передачі без втручання офіційного інструктора демонструють значні поліпшення в навчанні студентів;

– регулювання вмісту курсу за ступенем складності призводить до кращого залучення в процес навчання і просуненні по ньому;

– адаптивні системи заохочують зацікавленість учнів у процесі навчання за допомогою автоматизованих циклів зворотного зв'язку;

– адаптивні системи відповідають різним стилям життя окремих учнів на відміну від необхідності студентам відповідати системі;

– викладачі отримують дані, що містять індивідуальні потреби студентів, адже адаптивні системи можуть забезпечити такий рівень

автоматизації, що дозволяє викладачам краще розподіляти час між студентами, яким необхідна допомога, та тими, кому вона не потрібна;

– традиційні методи оцінки інформують викладачів і студентів про їх успішність занадто пізно в ході навчального циклу, але адаптивні системи можуть отримувати інформацію в режимі реального часу.

УДК 372.862

ВОЛОДИМИР ВОЛОДИМИРОВИЧ ТУЛУПОВ
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ
ВАЛЕРІЙ МИКОЛАЙОВИЧ ПЕРЕСІЧАНСЬКИЙ
старший викладач кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ВПРОВАДЖЕННЯ КОМПОНЕНТІВ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОСВІТНЬОМУ ПРОЦЕСІ

Постановка проблеми. Розробка та впровадження компонентів інформаційних технологій для підготовки фахівців технічної ланки а саме фахівців з організації захисту інформації має суттєву прикладну компоненту наближення до проблематики діяльності підрозділів технічного захисту інформації у правоохоронних структурах. Найбільш у цьому сенсі має ефективна комплексна комп'ютеризація та тренажерізація професійної підготовки таких фахівців, яка забезпечують усі стадії життєвого циклу виробу: проектування, розробку, випробування, виробництво, експлуатацію, технічне обслуговування, ремонт та успішного виконання учбового завдання [1, с. 237].

Слід виділити те що розробка однієї години високоефективної навчальної комп'ютерної програми, як показує вже наявний досвід, вимагає витрат багатьох людино-годин праці кваліфікованих програмістів і методистів. При цьому контроль якості навчаючих програм та ефективності тренажерної підготовки є справою складною, що потребує спеціальних знань, тестів, участі експертів тощо. Без такого контролю та сертифікації можливі негативні результати навчання, виникнення помилкових навичок, втрати природного інтелекту у особи, що навчається та ін. [1, с. 237]. Також до цього варто додати констатацію неухильного зросту вартості апаратних і програмних засобів як існуючих тренажерів так і інших навчаючих інтерактивних систем.

На теперішні час високий темп розвитку інформаційних технологій навчання у світі зумовлює: оновлення засобів матеріально-технічного забезпечення навчального процесу новими зразками техніки та інформаційними технологіями; оновлення кадрового потенціалу кафедр зі специфічними умовами навчання та взаємопроникнення інформаційних

технологій та спеціальних знань в суміжні дисципліни, що викладаються; впровадження нових методик й прийомів навчання; комп'ютеризація та інформатизація навчального процесу; тісний зв'язок з передовими науково-технічними розробками в сфері інформаційних технологій та спеціальної техніки.

Метою даної доповіді є виділення кола існуючих проблем щодо програмно-технічного забезпечення нормативних дисциплін кафедр зі специфічними умовами навчання та шляхи їх подальшої реалізації на прикладі створення комп'ютерних навчаючих систем (комп'ютерних тренажерів) та впровадження їх у навчальний процес.

На теперішній час на ринку професійного навчання пропонуються різні тренажерні комплекси (комп'ютерні тренажери) та навчаючи системи для підготовки фахівців, професійна діяльність яких пов'язана не тільки з організації захисту інформації, а із використанням інформаційних технологій в освітньому процесі.

Можливі підходи до розв'язання проблем. Розв'язання деяких вищезазначених проблем знайшли своє відображення у розробках кафедри «Інформаційних технологій та кібербезпеки» Харківського національного університету внутрішніх справ, де здійснюється підготовка фахівців за спеціальністю 125 – «Кібербезпека» наприклад: комп'ютерний тренажер «Селективний мікровольтметр та вимірювач напруги завад SMV- 8.5, SMV- 11» призначений для отримання курсантами та студентами первинних практичних навичок роботи з селективним мікровольтметром та вимірювачем напруги завад SMV 8.5 та SMV- 11.

Тренажери являють собою спрощений інтерактивний аналог (симулятор) пристроїв SMV 8.5, SMV- 11 та мають наступні можливості: ознайомлення користувачів з призначенням пристрою; ознайомлення з технічними характеристиками й можливостями використання; ознайомлення з комплектацією пристрою; ознайомлення з органами управління пристроєм; демонстрація використання пристрою при виконанні учбово-тренувальних задач; безпосереднє виконання учбово-тренувальних задач для оволодіння навичками роботи з пристроєм та тестування користувачів.

Також для забезпечення проведення практичних занять та лабораторних робіт з дисциплін: «Метрологія та вимірювання», «Електроніка та схемотехніка», «Методи та засоби захисту інформації» кафедрою також було розроблено комп'ютерні тренажери а саме: «Виміри за допомогою селективного нановольтметру Unipan-233» та «Вимірювач шуму та вібрацій ВШВ-003-М2» з використанням мультимедійної платформи Adobe Flash та інших технологій. У рамках дипломного проектування розробляються комп'ютерні тренажери для інших пристроїв з подальшим впровадженням їх у навчальний процес.

Висновки. Впровадження таких розробок у навчальний процес дозволить у деякій мірі замінити традиційний науковий інструментарій засобами сучасних інформаційних технологій, шляхом виконання учбово-тренувальних задач на тренажері, у зв'язку з обмеженістю таких приладів як

на кафедрах зі специфічними умовами навчання, так і в практичних правоохоронних підрозділах.

Список використаних джерел:

1. Тулупов, В. В. Пересічанський В. М. Проблеми застосування інформаційних технологій правоохоронними структурами України та вищими навчальними закладами зі специфічними умовами навчання. Зб. наук. статей за матеріалами доповідей Міжнародної науково-практичної конференції 22 грудня 2017 року. Львів: ЛьвДУВС, 2018. С. 234–237.

УДК 378.091:81

МИКИТА РОСТИСЛАВОВИЧ БЕКЕРОВ
здобувач вищої освіти ІІ курсу факультету економіко-правової безпеки
Дніпропетровський державний університет внутрішніх справ
ОЛЬГА ГЕННАДІЇВНА КОСТЕНКО
старший викладач кафедри українознавства та іноземних мов
Дніпропетровський державний університет внутрішніх справ

МЕДІАОСВІТНІ ТЕХНОЛОГІЇ ЯК ЗАСІБ МОТИВАЦІЇ ВИВЧЕННЯ ІНОЗЕМНОЇ МОВИ СТУДЕНТАМИ НЕМОВНИХ СПЕЦІАЛЬНОСТЕЙ

Статус іноземної мови у суспільстві значно змінився. Стрімке входження України у світове співтовариство забезпечило величезний попит на знання іноземних мов. Загальноєвропейські рекомендації з мовної освіти відзначають, що пріоритетною освітньою метою є підготовка школярів до життя у сучасному суспільстві шляхом запровадження методів викладання іноземних мов, які стимулюють незалежність думки, судження, спонукають до відповідальної компетентної діяльності. У такому зв’язку нам видається цілком успішним і актуальним широке запровадження у вивченні іноземної мови новітніх підходів до навчання [4].

Вивчення іноземної мови – крок надто важливий, тобто потребує значних зусиль. Для досягнення високого рівня іноземної мови вчителю важливо знати новітні методи викладання, спеціальні навчальні техніки та прийоми, щоб оптимально підібрати той чи інший метод відповідно до рівня знань, потреб, інтересів учнів. Раціональне та вмотивоване використання методів навчання на уроках іноземної мови вимагає креативного підходу з боку вчителя, адже «педагогіка є наукою і мистецтвом одночасно, тому і підхід до вибору методів навчання має ґрунтуватися на творчості педагога» [3, с. 159-160]. Реалізація методу навчання здійснюється через використання ряду прийомів навчання різноманітних підходів та робочих технік. «Прийоми навчання – сукупність конкретних навчальних ситуацій, що сприяє досягненню проміжної мети, конкретного методу» [1, с. 320].

Сучасні технології в освіті – це професійно орієнтоване навчання іноземної мови, проектна робота в навчанні, застосування інформаційних та телекомунікаційних технологій, робота з навчальними посібниками, програмами з іноземної мови (система мультимедіа) дистанційну технологію в навчанні іноземної мови, використання інтернет ресурсів, навчання іноземної мови в комп'ютерному середовищі (форуми, блоги, електронна пошта). Ефективність застосування новітніх методів залежить від того, чи підібрані вони відповідно до тих завдань, які можуть успішно розв'язуватися з їх допомогою. Також потрібно цілеспрямовувати діяльність учнів та підвищувати інтерес до занять значною мірою, поглибити мовленнєву практику кожного учня на уроці. Застосування новітніх технологій – досить ефективний та доцільний засіб у навчанні учнів іноземної мови, спрямований на розвиток різних здібностей учнів. Методи навчання іноземних мов, які ґрунтуються на гуманістичному підході, допомагають розкрити творчий потенціал учнів і сприяють розвитку та самовдосконаленню навчально-комунікативного процесу, формуванню майбутніх свідомих патріотів своєї країни, толерантних громадян світу.

Список використаних джерел:

1. Волкова Н. П. Педагогіка: навч.посіб. Київ: Академвидав.2007. 616с.

2. Дичківська І. М. Інноваційні педагогічні технології. Київ: Академвидав, 2004. 352 с.

3. Кузьмінський А.І., Омеляненко В.Л. Педагогіка: Підручник. Київ: Знання Прес, 2008. 447 с.

4. Ніколаєва С.Ю. Загальноєвропейські рекомендації з мовної освіти:вивчення, викладання, оцінювання. Київ: Ленвіт, 2003. 273с.

УДК 378:004

РОМАН РУСЛАНОВИЧ ОРЛОВ
курсант 2 курсу факультету № 4 Харківського національного університету внутрішніх справ
ЮРІЙ МИКОЛАЙОВИЧ ОНИЩЕНКО
кандидат наук з державного управління, доцент, доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ОСОБЛИВОСТІ ПІДГОТОВКИ КАДРІВ ДЛЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ ПІДРОЗДІЛІВ НП УКРАЇНИ

Зміни, що відбуваються в даний момент в країні та безпосередньо діяльності органів внутрішніх справ обумовлюють необхідність реформування даної структури та підвищення вимог до професійних і особистісних якостей співробітників, їхньої спеціальної та психологічної підготовленості до служби, пов'язаної з ризиком, високими фізичними та

психічними перевантаженнями, можливим виникненням ситуацій екстремальності і напруженості, що негативно впливають на поведінкові реакції працівників та їх емоційний стан.

Разом з тим діяльність поліцейських нерідко викликає серйозні претензії з боку суспільства, у зв'язку з чим співробітникам необхідно не тільки підвищувати свій професійний рівень, а й формувати морально-психологічну стійкість, психологічну готовність та правову культуру. В сучасних умовах ефективна діяльність працівників органів внутрішніх справ значною мірою залежить не тільки від укомплектованості правоохоронних органів фахівцями, а й від того, наскільки співробітникам, особливо молодим, вдається адаптуватися до нових соціальних і професійних умов роботи. Тому ефективність діяльності правоохоронних органів визначається, в першу чергу, станом потенціалу.

Підготовка кадрів для інформаційно-аналітичних підрозділів Національної поліції України має базуватися на таких принципах:

– інноваційність, що полягає в розробці і впровадженні прогресивних наукових технологій на етапі підготовки та практичної діяльності;

– практична спрямованість, що означає підпорядкованість кадрової політики цілям, завданням та інтересам інформаційно-аналітичної діяльності поліції;

– гуманізм, що базується на поєднанні методів соціальної та професійної мобілізації співробітників з їх громадськими, культурними потребами та інтересами, оновленні та гармонізації методів морального і матеріального стимулювання діяльності.

Пріоритетними завданнями в області роботи з кадрами є:

– забезпечення якості кадрового складу за рахунок комплектування МВС висококваліфікованими фахівцями, які відповідають державним вимогам і громадським очікуванням;

– оновлення кадрового складу і забезпечення передачі досвіду службової діяльності за допомогою якісного відбору громадян на службу в поліцію, оптимальної розстановки особового складу на посадах з урахуванням професійної кваліфікації, особистісних якостей і здібностей.

У підготовці співробітників інформаційно-аналітичних підрозділів залишаються системні проблеми:

– відсутність цілісної інформаційної інфраструктури;

– недостатній розвиток інформаційного забезпечення, що полягає в нестачі технічних засобів і програмного забезпечення;

– підготовка переважно спрямована на інформаційну роботу (полягає тільки в зборі інформації, а процес аналізу майже відсутній);

– ігнорується необхідність набуття фахівцями навичок прогнозно-діагностичного, аналітичного та комунікаційного характеру;

– потребує вдосконалення система підвищення кваліфікації.

Нажаль, можна констатувати, що жоден український заклад вищої освіти зі спеціалізованими умовами навчання не здійснює підготовку фахівців-

аналітиків безпосередньо для інформаційно-аналітичних підрозділів Національної поліції України. Отже, пріоритетним завданням реформування системи вищої освіти є збільшення її мобільності та гнучкості, що проявлятиметься у здатності оперативно реагувати на потреби практичних підрозділів Національної поліції у кадрах, підготовлених за певними спеціальностями.

Під час формування кваліфікаційних вимог до підготовки працівників інформаційно-аналітичних підрозділів слід передбачити необхідність наявності в них не тільки навичок роботи з комп'ютерною технікою та спеціалізованим програмним забезпеченням, а й ґрунтовних знань з оперативно-розшукової діяльності. Зважаючи на транснаціональний характер аналітичної роботи, специфіку інформаційного середовища мережі Інтернет та, як правило, англомовний інтерфейс спеціалізованого програмного забезпечення, фахівці-аналітики повинні володіти іноземними мовами, передусім англійською.

УДК 351.746.1:62137

АННА СЕРГІЇВНА БУРЯК
курсант 2 курсу факультету підготовки фахівців досудового розслідування
Дніпропетровського державного університету внутрішніх справ
ЄВГЕНІЯ ВОЛОДИМИРІВНА СТРЮК
старший викладач кафедри українознавства та іноземних
Дніпропетровського державного університету внутрішніх справ

METHODS OF APPLICATION NO-PILOT AVIATION COMPLEXES

Military conflicts of the late XX - beginning of XXI centuries characterized by the use of a large number of new weapons, which allowed the warring parties to distance themselves as much as possible from the posse-day collision with each other. One of the newest examples of weapons on the battlefield was the non-pilot aviation complexes, which during military conflicts proved their ability to perform much more effectively than manned aircraft, conduct aerial reconnaissance and perform other combat support tasks, as well as to strike the enemy.

Now, there is a large body of literature on how to use no-pilot aviation in armed conflicts of the last ten years. In the first stage, the main tasks that were solved with their help were the identification of goals, the evaluation of the results of air strikes; joint operations with manned aircraft and ground units.

Also, noteworthy is that these aircraft are also used to provide information support for hostilities, which has become a crucial solution in providing troop deployment information services using broadband wireless access called High Altitude Platform Station (HAPS).

Consider the main types. The simplest solution is to use airships of different technical designs. At present, the use of modern technologies has allowed raising to a new level the creation and operation of balloons as vehicles. After that, it

significantly influenced the use of balloons as air platforms for communication purposes. The balloon is a payload carrier. The cable holds the balloon during lifting, descending and parking at working height, providing power to the onboard systems and payload. The attached balloons are equipped with modern radio-locating equipment and allow to control the territory with a diameter of up to 200 km. Most often, balloons are used to:

- combating smuggling;
- detection of rockets at low altitude;
- border protection, anti-piracy;
- long-range radar intelligence;
- relaying of different types of communication.

An important milestone in the creation of aero platforms was the use of low-cost unmanned aerial vehicles. Yes, General Atomic offers the Predator RQ-1 as a mid-level platform. It has television and infra-red cameras, radar, communications and control equipment. The control of the Predator RQ-1 is from the Earth by an operator using a special station with a 6.25-meter antenna in the Ku-band.

Within the project ERAST (Environmental Research Aircraft and Sensor Technology), held under the auspices of NASA, a company AeroVironment Inc. develops unmanned airplanes, the source of electricity for which is placed on the upper surface of the wings solar batteries company SunPower Corp. with a total power of 35 kW and a coefficient of 18.4% co-action (the size of one cell of the battery is 32x70 mm).

The first generation was Pathfinder, the use of modern technology has enabled to raise to a new level the creation and operation of aircraft, both heavier and lighter than air, and on their basis to begin the deployment of aerial platforms for the implementation of a new type of telecommunications. The variety of aircraft that can carry telecommunication equipment allows the creation of radio systems of various purposes, which have different requirements for cargo flexibility, altitude hang and power consumption of the air platform. The advantages of aircraft as carriers of telecommunication equipment are that they do not depend as balloons on air flows, may be in planning mode for some time, have developed technologies of their construction and flight support.

The disadvantages of conventional aircraft with fuel engines can be attributed to the constant need for fuel, which significantly limits their stay in the air. Moreover, as the flight height increases, the need for fuel increases.

This disadvantage is not the standalone airplanes on solar panels. They still have one drawback – a small load capacity. Gradually, other tasks specific to previously no-pilot aviation began to be transferred to unmanned aerial vehicles. Among them are the tasks of combat support: detection and disorientation of enemy anti-aircraft missile systems; radio-electronic counteraction; radio interception; mine detection and detection; relay signals.

In the course of the work, the ways of applying the no-pilot aviation in the course of the local conflicts of the last decades were analyzed, as well as the tendencies of their application and development, namely: increasing the volume of

tasks assigned to them; multipurpose use of them; comprehensive application together with other forces and means of various types of military intelligence; 24-hour aerial reconnaissance through no-pilot aviation in all weather conditions; integration with the means of destruction; their use as carriers of lesions; inclusion in a single air traffic management system; use for the benefit of all management units.

УДК 351.74:070.46

АЛІНА АНАТОЛІЇВНА МАРОЧКО
курсант 2 курсу факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ
ЄВГЕНІЯ ВОЛОДИМИРІВНА СТРЮК
старший викладач кафедри українознавства та іноземних Дніпропетровського державного університету внутрішніх справ

FUNDAMENTALS FOR BUILDING AN EFFECTIVE CCTV SYSTEM (STAGES AND SUBJECTS OF IMPLEMENTATION)

The topicality of the chosen topic forms two components, which are the mirror of the present, on the one hand – the globalization of society, which began with the change of world order (development of service component in the activity of the population), the construction of metropolitan areas and, accordingly, the increase of the population that migrates from small towns to large cities. bridge. On the other hand, Moore's Law, which described the trends in technology, and today we have the ability to operate on huge data sets, processing them millions of times faster than ten years ago, the cost of such calculations has in turn decreased thousands of times.

Most developed countries have understood the situation of society and therefore have focused on the use of the latest technologies in management and law enforcement. Adaptation of the already existing experience of the developers of intelligent systems, including video surveillance, will help the city services and law enforcement agencies to organize their activities more rationally, directing human resources to process a smaller amount of data received from the streets. And the whole array of information, according to the identified 13 scenarios will be processed by the intelligent system, in case of violation of the algorithms will be alerted to the relevant services.

Today, the development of smart video analytics is based on two major technologies – tracking and identification. On the basis of the rules laid down in the algorithm of video analysis, all the functionality of the system is built, which is essential for the construction of modern CCTV systems. Within the framework of building Smart City systems, each of the directions, trekking, is urgent to solve the question:

– illegal crossing of a straight line object in a given direction;

- suspicious traffic in a designated area;
- exit of the object from the defined area;
- stop the object in the area;
- subject left in the area.

In turn, identification, that is, image recognition by video, grouping by classes or specific patterns and comparison with a pre-prepared base of reference images is most commonly used for face recognition, car license plate recognition, as well as vehicle identification (type, make, model) .

This functionality is the basis for building an effective video surveillance system, because its presence will satisfy the needs of law enforcement agencies, public utilities and road services. Understanding the tasks entrusted to the various public authorities will allow them to concentrate their efforts on achieving a common goal – to build an effective video surveillance system.

Effective implementation of the CCTV system depends on the head of the regional state administration, the mayor, the head of the police and the active participation of other representatives of the authorities and the public.

Only with fruitful cooperation between these entities can it be possible to build a platform for comprehensive solution of security issues, fight against crime, ensure response to natural and man-made disasters, coordination of forces and means of all services, optimization of processes in the city, creation of comfortable living conditions and community work.

By the example of building an intelligent video surveillance system in Donetsk region, we can distinguish the following subjects of its implementation:

According to Article 13 of the Law of Ukraine "On Local State Administrations, within the limits and forms defined by the Constitution and laws of Ukraine, local state administrations shall have to deal with issues related to ensuring the legality, protection of rights, freedoms and legitimate interests of citizens in the region, socio-economic development of the respective territories, implementation of state regulatory policy, defense work and mobilization training.

Local self-government bodies may be another subject, given the provisions of the Law of Ukraine "On Local Self-Government", their competence also includes powers in the fields of defense, public services, security and financial authority.

The main entity that should initiate projects in its own area is the General Directorate of Police in the area, city administration or central police authorities, they can include the following elements:

1. Overall coordination of the project at all stages of its implementation.
2. Preparation of the terms of reference and legal support for the construction of the system.
3. Search for a room that will be suitable for the location of the hardware of the complex according to the technical requirements.
4. Finding and designating a contractor to meet the minimum requirements.
5. Coordinate the efforts of all actors involved in the implementation.
6. Allocation of persons for training and further support of system activities (both hardware and software).

7. Carry out testing of the system and prepare proposals for its improvement (if necessary).

8. Commissioning of the system (jointly with the contractor), development of principles of information exchange between different bodies (interested in using the system) and in the middle of the police.

As a result of a clear understanding by each subject of the feasibility of building an intelligent video surveillance, the first results can be achieved within one year from the start of the project implementation of the intelligent video surveillance system. In turn, the positive experience of areas where similar projects have been implemented should build confidence in reducing crime, developing traffic management systems, etc.

УДК 343.36:343.57+343.365:343.123.12

ОЛЕКСІЙ МИХАЙЛОВИЧ РВАЧОВ

старший викладач кафедри інформаційних технологій та кібербезпеки факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ

СУЧАСНІ МЕТОДИ ПРИХОВУВАННЯ ФАКТІВ ПРИЧЕТНОСТІ ДО НЕЗАКОННОГО ЗБУТУ НАРКОТИЧНИХ ЗАСОБІВ, ПСИХОТРОПНИХ РЕЧОВИН АБО ЇХ АНАЛОГІВ ЧЕРЕЗ МЕРЕЖУ ІНТЕРНЕТ

На сьогоднішній день, нажаль, в Україні є можливість без особливих зусиль незаконно придбати в безконтактний спосіб наркотики «не встаючи з дивану». При цьому клієнт та продавець не знають один одного та не зустрічаються щоб передати товар та отримати за нього гроші. Продавець може знаходитися в одній країні чи регіоні, а збут відбуватися в іншому [1].

Реклама інтернет-адрес «наркокрамниць» розміщена на об’єктах інфраструктури населених пунктів (стінах будівель, парканах, підземних переходах, зупинках громадського транспорту, асфальті тощо) – зловмисники малюють написи («графіті») та наклеюють «наліпки» з адресами «наркокрамниць», що приймають замовлення щодо незаконного продажу наркотиків через:

1) спеціально створені вебсайти;

2) месенджери (Telegram, Skype тощо).

В месенджері Telegram наркозловмисники можуть створювати (реєструвати) окремі адреси для:

1) розміщення інформації про:

– види наркотиків, їх ціни (прайси), населені пункти та райони де здійснюється збут;

– відгуки покупців;

2) безпосереднього продажу наркотиків:

– в автоматичному режимі – за допомогою чат-ботів;

– в ручному режимі – через операторів;

3) спілкування (чати та канали):

– покупців;

– працівників «наркокрамниці».

Для пошуку потенційних покупців та збуту наркотиків через «наркокрамниці» зловмисники об'єднуються у організовані злочинні групи (далі – ОЗГ) з чітко вираженою ієрархією та розподіленими ролями:

– організатори ОЗГ – власники накрокрамниць;

– виробники («хіміки» та «гровери») – виробляють синтетичні наркотики та вирощую нарковмісні рослини;

– експедитори («перевізники») – перевозять великі партії наркотиків між населеними пунктами;

– працівники складів («кладівники») – розфасовують великі партії на менші;

– оптові кур'єри («мінери», «кладмени») – розміщують партії наркотиків («майстер клади», «мастер-квести», «міни») для роздрібних кур'єрів;

– роздрібні кур'єри («закладчики», «кури») – розфасовують наркотики на невеликі дози для вживання та розміщують, так звані, «клади», «закладки» чи «стафф»;

– диспетчери, менеджери з продажу («оператори») – приймають замовлення та вирішують конфлікті ситуації, що виникають під час продажу наркотиків;

– касири («фінансисти») – отримують гроші за наркотики та «відмивають» їх;

– рекламщики («графітчики») – розміщують в населених пунктах графіті та наліпки з інтернет-адресами «наркокрамниць»;

– ІТ-фахівці – розробляють та займаються подальшою підтримкою вебсайтів та чат-ботів;

– працівники по роботі з персоналом («кадровики») – підшукують на роботу кур'єрів та рекламщиків, проводять з ними первинний інструктаж із заходів безпеки;

– працівники «служби безпеки» («охорона») – слідкують за дотриманням усіма членами ОЗГ правил конспірації, здійснюють охорону нарколабораторій та теплиць з плантаціями нарковмісних рослин [2, С. 211; 3, С. 456– 457; 4].

До безпосередніх обов'язків кур'єрів входить: отримання партії наркотиків; фасування наркотиків; розміщення (приховування) наркотиків на певній території; фіксування на фото місця розміщення «кладу»; пересилання оператору координат, фотографії та опису місця де розміщено «товар».

Реальне існування і функціонування ОЗГ в певній мірі залежить від застосування ними дієвих і ефективних форм та способів протидії судовим, правоохоронним органам, а також від цілеспрямованої можливості здійснювати ними безпосередній вплив як на доказову інформацію, а також на учасників кримінального судочинства. Слідча і судова практика свідчить, що за останні роки правоохоронні органи дедалі частіше зустрічаються з

вмотивованою, цілеспрямованою і спланованою протидією ОЗГ під час розслідування злочинів [5].

Р. С. Бєлкін виділяє наступні форми приховування злочинів:

1) утаювання інформації, як в активній (приховування предмета посягання, речових доказів, грошей та цінностей, ухилення від явки в органи розслідування), так і в пасивній формі (умовчання, недонесення, відмова від дачі показань, тощо);

2) знищення інформації а також слідів злочину, як частково, так і у цілому;

3) маскування інформації;

4) фальсифікація інформації та її носіїв у формі свідомо неправдивих показань і заяв, повна або часткова підробка документації;

5) інсценування злочинів [6, С. 366].

Окрім того, що в сучасних умовах збут наркотиків відбувається без фізичного контакту між продавцем та покупцем, наркозловмисники та їх «клієнти» теж використовують різні сучасні методи приховування їх причетності до незаконного збуту наркотичних засобів, психотропних речовин або їх аналогів через мережу Інтернет.

«Працівники служб безпеки» «наркокрамниць» можуть вдаватися до силових методів покарань членів ОЗГ, які недотримуються заходів конспірації чи привласнили собі наркотики. Наприклад, прибити цвяхами руки, відрізати чи відрубати пальці, побити [7].

На сьогоднішній день в месенджері Telegram функціонують канали, в яких їх анонімні учасники:

1) повідомляють адресами в населених пунктах, де вони нещодавно побачили працівників правоохоронних органів, які можуть виявити та затримати осіб, які мають при собі наркотики;

2) розміщують інформацію про типові прийоми роботи правоохоронних органів;

3) діляться досвідом щодо:

– роботи у якості власників, виробників, «операторів», кур’єрів та покупців наркокрамниць;

– способів камуфлювання наркотиків;

– правил безпечного використання терміналів мобільного зв’язку.

Проведений аналіз таких інформаційних джерел дозволив сформувати перелік рекомендацій, що надають члени незаконного наркобізнесу іншим учасникам наркозбуту (власникам, операторам, кур’єрам та покупцям), у тому числі під час користування сучасними інформаційними технологіями, наприклад, мобільними телефонами:

1) мати два мобільні телефони (один для «роботи», а інший для приватного життя), які ніколи не повинні працювати одночасно;

2) періодично змінювати мобільні телефони та SIM-картки;

3) ніколи не включати мобільний телефон у місцях зберігання та фасування наркотиків;

4) використовувати функцію шифрування вмісту пам’яті телефону;

5) телефон повинен автоматично блокуватися через певний час не користування ним;

6) заборонити у месенджері Telegram зберігання фотографій на телефоні та одразу пересилати їх на інший акаунт;

7) використовувати телефон із двома активними робочими середовищами (робочими столами) (така можливість є, наприклад, в ОС Android, починаючи з версії 7.X.X);

8) встановити пароль на запуск визначених застосунків;

9) можна використовувати виключений екран мобільного телефону та «селфі» камеру для того щоб непомітно подивитися, що робиться позаду;

10) необхідно регулярно очищати історію пошуку певних адрес де розміщуються наркотики, а після цього здійснити пошук нейтральної адреси, наприклад, супермаркету чи закладу харчування;

11) не зберігати фотографію місця розміщення наркотиків на телефоні, а завантажувати їх на файлообмінники доступ до яких здійснюється через TOR-браузер;

12) гіперпосилання на фотографію або його другу частину без назви домену можна зберігати в певному контакті в телефонні книзі телефону;

13) GPS-координати місця знаходження «закладки» можна зберігати в текстовому документі на телефоні.

Для ефективної протидії, виявлення фактів причетності осіб до незаконного збуту наркотичних засобів, психотропних речовин або їх аналогів правоохоронці повинні бути поінформовані про вищезазначені методи приховування причетності осіб до такої незаконної діяльності.

Список використаних джерел:

1. Інтернет надає злочинцям багато можливостей за максимальної конспірації, – Кіхтенко // ЦЕНЗОР.НЕТ : сайт. 22.03.2019. URL: https://censor.net.ua/ua/news/3118184/internet_nadaye_zlochyntsyam_bagato_mojlyvosteyi_za_maksymalnoyi_konspiratsiyi_kihtenko (дата звернення: 30.11.2019).

2. Рвачов О.М., Лактіонов В.В., Дацюк Д.О. Сучасні методи активного залучення населення до протидії збуту наркотичних засобів, психотропних речовин або їх аналогів через мережу Інтернет // Протидія кіберзагрозам та торгівлі людьми (26 листоп. 2019 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2019. С. 210-217.

3. Криминалистика 2-е изд : учебник для вузов / Под науч. ред. Карагодина В. Н., Смахтина Е. В. М. : Издательство Юрайт, 2019. 487 с.

4. Зотова Н. Клад и его мастер: почему россияне уходят в наркокурьеры / Русская служба Би-би-си : офіційний сайт. 10.07.2019. URL: https://www.bbc.com/russian/features-48928092 (дата звернення: 30.11.2019).

5. Біленчук П. Д., Курко М. Н., Остролуцький О. А. Засоби, методи, технології подолання протидії розслідуванню злочинів, що здійснюються організованими злочинними групами. *Криміналістика і судова експертиза*. 2015. Вып. 60. С. 172-183.

6. Белкин Р. С. Курс криминалистики : в 3 т. М. : Юристъ, 1997. Т. 3. 408 с.

7. Как работают закладчики наркотиков. И почему их ненавидят и полицейские, и преступники // Телеканал «Санкт-Петербург» : офіц.сайт. 25 березня 2019 р. URL: https://topspb.tv/news/2019/03/25/kak-rabotayut-zakladchiki-narkotikov-i-pochemu-ih-nenavidyat-i-policejskie-i-prestupniki/ (дата звернення: 30.11.2019).

НАУКОВЕ ВИДАННЯ

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ДІЯЛЬНОСТІ НПУ

Матеріали
науково-практичного семінару

м. Харків, 18 грудня 2019 року

ВИДАНО В АВТОСЬКІЙ РЕДАКЦІЇ

Відп. за випуск В. М. Струков

Формат 60х84/16. Папір офсетний. Гарнітура Times ET.
Ум. друк. арк. 5,12. Наклад 100 пр. Зам. № 1210/2-19.

Надруковано з готового оригінал-макету у друкарні ФОП В. В. Петров
Єдиний державний реєстр юридичних осіб та фізичних осіб-підприємців.
Запис № 24800000000106167 від 08.01.2009 р.
61144, м. Харків, вул. Гв. Широнінців, 79в, к. 137, тел. (057) 78-17-137.
e-mail:bookfabrik@mail.ua