2. Mar'yan M., Seben V., Yurkovych N. *Synergetics of Computer Modeling, Research and Technology Education. Concepts&Methods.* Lambert Academic Publishing, Riga, 2018. P. 120.

3. Mar'yan M. I., Seben V., Yurkovych N. V. Synergetics of thermoinduced instabilities and hypersensitivity of the non-crystalline materials in sybersecutity systems. IV International Scientific and Practical Conference «Actual Issues of Ensuring Cybersecurity and Information Protection». February 21-24, 2018, Kyiv, European University (Ukraine), P. 148-150.

Одержано 23.10.2018

УДК 343.43

Олександр Маркович БАНДУРКА,
доктор юридичних наук, професор,
академік Національної академії правових наук України, заслужений юрист України,
професор кафедри теорії та історії держави і права
факультету № 1 (слідства)
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0002-0240-5517

ПРИВАТНІ ОНЛАЙН-ПРОЕКТИ ЯК СУЧАСНИЙ ІНСТРУМЕНТ ДЛЯ ПРОТИДІЇ ЗЛОЧИННОСТІ

Трансформація суспільних процесів у сучасному світі відбувається надшвидкими темпами. Те, що працювало ще місяць тому, сьогодні може виявитися застарілим і малопридатним для застосування у практичній діяльності.

Все це стосується і правоохоронної сфери. Її реформування відбувається весь час, проте стара ієрархічна структура управління не дозволяє ефективно та своєчасно відповідати на виклики сьогодення. Поряд із необхідністю заохочення ініціативи в частині запровадження інновацій на місцях потрібно також звернути увагу на більш широке делегування частини забезпечувальних функцій діяльності поліції приватному сектору. Особливо це стосується інформаційної сфери. Професійне супроводження окремого інформаційного завдання потребує залучення значних матеріальних та фінансових ресурсів, а також кваліфікованого персоналу. Вказана обставина в сучасних умовах унеможливлює ефективне виконання таких завдань поліцією, а тому було б цілком логічним залучати до їх виконання приватних підрядників.

Окремі приватні компанії та громадські формування продемонстрували достатньо великий потенціал розвитку онлайн-проектів, які можуть бути задіяні у протидії злочинності, та не могли б бути швидко та якісно виконані у забюрократизованих державних органах.

Наведемо декілька таких проектів:

– «Миротворець» (myrotvorets.center) – сайт, який містить інформацію про осіб, у діях яких учасники проекту вбачають ознаки злочинів проти національної безпеки України, життя та здоров'я людини, миру, безпеки людства та міжнародного правопорядку. У рамках проекту «Миротворець» було реалізовано сервіс (identigraf.center), що здійснює розпізнавання облич за фотографіями, порівнюючи їх з мультимедійними даними з бази «Миротворець»;

– YouControl (youcontrol.com.ua), ipLex-Контрагенти (iplex.com.ua) – аналітичні системи для ділової розвідки та перевірки контрагентів України. У них формуються досьє на кожну компанію України на основі відкритих даних, відстежуються зміни в держреєстрах та візуалізуються зв'язки між афілійованими особами;

– Clarity Project (clarity-project.info) – система, подібна до попередніх, що аналізує інформацію про осіб, які беруть участь у публічних закупівлях з використанням ProZorro;

– Wigle (wigle.net) – сервіс, який накопичує консолідовану інформацію про точки доступу до безпровідних мереж та надає можливість побачити місце розташування цих об'єктів на карті;

– Pipl (pipl.com) – система пошуку інформації про осіб за електронною поштою, особистими даними в соціальних мережах, телефонним номером;

– боти Телеграм, які надають консолідовану інформацію з відкритих реєстрів про фізичних та юридичних осіб (@OpenDataUABot, @e007bot, @OpenDeclarationBot);

– системи зберігання та пошуку інформації про ДНК (myheritage.com, gedmatch.com, dna.land, geni.com, ancestry.com, 23andme.com).

Останній вид сервісів уже активно застосовується поліцією США, що дозволило їм вийти на слід кількох злочинців, які вчинили серію особливо тяжких злочинів, а в подальшому затримати їх (див., наприклад, [1; 2]).

Слід зауважити, що наведений перелік проектів відображає лише невеличку частку алгоритмів роботи, які б могли бути успішно засвоєні правоохоронними органами для виконання завдань протидії злочинності. Однак для їх використання, перш за все, необхідно змінити філософію роботи правоохоронців, заохочувати застосування ними новітніх технологій та орієнтувати їх на попередження злочинів. Окремі кроки в цьому напрямі вже робляться, зокрема це стосується запровадження моделі стримування злочинності Intelligence Led Policing в Національній поліції України.

Таким чином, сучасна правоохоронна діяльність потребує сучасних підходів у роботі. Ігнорування цієї простої істини може тільки прискорити відставання вітчизняних правоохоронців від колег із розвинених країн. Зважаючи на це, слід більше сприяти впровадженню інновацій у регіональних підрозділах поліції та більш

широко використовувати в роботі онлайн-проекти, здатні поліпшити систему протидії злочинності.

Список бібліографічних посилань

1. Law enforcement credits genetic genealogy in 1987 cold case arrest // The Monroe monitor & Valley news. May 18, 2018. URL: https://t/co/E1rsWpEANj (дата звернення: 26.10.2018).

2. Romano A. DNA profiles from ancestry websites helped identify the Golden State Killer suspect // VOX. Apr 27, 2018, 5:20pm EDT. URL: https://www.vox.com/2018/4/27/17290288/golden-state-killer-joseph-james-deangelo-dna-profile-match (дата звернення: 26.10.2018).

Одержано 26.10.2018

УДК 004.056.8

Вадим Андрійович БОКОВ,
слухач магістратури факультету № 6
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0002-0512-725X

ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ВІД МЕРЕЖЕВОГО НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Захист інформації в сучасних реаліях перебуває на першому місці, через велику кількість загроз несанкціонованого доступу до неї.

В рамках чинного кримінального законодавства під несанкціонованим доступом необхідно розуміти: проникнення до комп'ютерів, їх систем чи мереж і вчинення дій, які змінюють режим роботи машини, її системи чи комп'ютерної мережі, або ж повністю чи частково припиняють їх роботу, без дозволу (згоди) відповідного власника або уповноважених ним осіб, а також вплив на роботу автоматизованих ЕОМ за допомогою різних технічних пристроїв, здатних зашкодити роботі машини.

Загально прийнятими методами захисту інформації є установка перешкоди, системи управління доступом, та авжеж, маскування інформації. Зупинимося більш детально на визначених методах захисту інформації.

Найбільш розповсюдженим є метод встановлення перешкоди – це метод фізичного перегородження шляху зловмиснику до інформації, що захищається, у тому числі для попередження спроб з використанням технічних засобів знімання інформації і дії на неї.

Управління доступом, як метод захисту інформації передбачає регулювання використовування всіх інформаційних ресурсів, у тому числі автоматизованої інформаційної системи підприємства. Управління доступом включає наступні функції захисту: