14. Kasian, V.I. (2008), *Filosofiya : Vidpovidi na pytannya ekzamenatsiinykh biletiv : navch. posib.* [Philosophy : Answers to exam questions : study guide], Znannya, Kyiv, Ukraine.

15. Bezklubyi, I.A., Hrytsenko, I.S., Koziubra, M.I. et al. (2017), *Metodolohiya v pravi : monohrafiya* [Methodology in law : monograph], Hramota, Kyiv, Ukraine.

16. Podolska, Ye.A. (2006), *Filosofiia : pidruchnyk* [Philosophy : textbook], Firma «Inkos», Tsentr navchalnoi literatury, Kyiv, Ukraine.

17. "On Counterintelligence Activities" : Law of Ukraine on 26.12.2002 [as amended on 05.01.2017], *Vidomosti Verkhovnoi Rady Ukrainy*, 2003, no. 12, art. 89.

УДК 343.98.06: 004.056.5: 005.576621.39

ПРО СУЧАСНІ ФОРМИ ТА МЕТОДИ РОБОТИ З ПОШУКОВОЮ ІНФОРМАЦІЄЮ

Узунова О.В., к.ю.н., доцент

Запорізький національний університет, вул. Жуковського, 66, м. Запоріжжя, Україна
chornenkaya@ukr.net

Статтю присвячено комплексному дослідженню форм і методів передачі інформації за допомогою різних видів (у тому числі новітніх) засобів та прийомів зв'язку (Інтернет, комп'ютерні й мобільні мережі, спецзв'язок) задля встановлення особи злочинця. Аналізуються можливості пошуку й збору інформації, її обробки та аналізу, структурування та зберігання. Крім того, звернено увагу на такий наслідок пошуку й збору інформації, як вирішення оптимізаційних завдань і здобуття нової інформації про особу злочинця. Розглядаються нагальні потреби теорії та практики застосування сучасних досягнень техніки й методики.

Ключові слова: боротьба зі злочинами, Інтернет, інформація, інформаційні технології, метод, особа злочинця, пошук, форма.

О СОВРЕМЕННЫХ ФОРМАХ И МЕТОДАХ РАБОТЫ С ПОИСКОВОЙ ИНФОРМАЦИЕЙ

Узунова О.В.

Запорожский национальный университет, ул. Жуковского, 66, г. Запорожье, Украина
chornenkaya@ukr.net

Статья посвящена комплексному исследованию форм и методов передачи информации с помощью различных видов (в том числе новейших) средств и приемов связи (Интернет, компьютерные и мобильные сети, спецсвязь) для установления личности преступника. Анализируются возможности (параметры) поиска и сбора информации, ее обработки и анализа, структурирования и хранения. Кроме того, обращено внимание на такой результат поиска и сбора информации, как решение оптимизационных задач и получение новой информации о личности преступника. Рассматриваются насущные потребности теории и практики применения современных достижений техники и методики.

Ключевые слова: борьба с преступлениями, Интернет, информация, информационные технологии, метод, личность преступника, поиск, форма.

ABOUT MODERN FORMS AND METHODS OF WORK WITH SEARCHING INFORMATION

Uzunova O.V.

Zaporizhzhya National University, str. Zhukovskogo, 66, Zaporizhzhya, Ukraine
chornenkaya@ukr.net

Social and political changes, that take place in life of Ukraine nowadays, are accompanied by crime intensifying, increase of quantitative and quality indexes of criminality. Thus, except the general crime intensifying, the tendency of complication of criminal charts and facilities to avoid responsibility for their feasance that negatively influences on organization of fight against them takes place. Accordingly

counteraction to criminality, next to strengthening of legality, comes forward to one of important tasks that stand before the state and its organs, and efficiency of their work from investigation of crimes in a great deal depends on the level of application of all potential of modern criminalistics recommendations, their timely and able use.

It is marked that new informative technologies have the opportunity to be inculcated wider in practice of law enforcement authorities. Such volume of operational search and prophylactic setting functions in the organs of internal affairs of Ukraine runs, where the enormous arrays of information including secret or intended for the official use are processed.

In the modern terms of scientific and technical progress a tendency to computerization, creation of the ramified handling systems of data appears, that includes both powerful calculable complexes and personal computers. The amount of communication local, branch, national and intergovernmental networks increases every day. Computer technologies are inculcated practically in all spheres of public life, inclusive with law-enforcement activity, medicine, connection, transport, national safety and others.

Total informatization of society, Internet-dependence, became the reason of flowing of vital functions of most individuals simultaneously in the real and virtual spaces with corresponding consequence in both measuring as a result of the use of mobile communication, e-mail, electronic systems of payments, credit, pay and discount cards means. More often chronology of life of modern person is represented in instantaneous and sms-reports, content of e-mail, records in address e-books and calendars, snapshots and video, statuses on pages in social Internet-networks, blogs created by a person, and also in the paths of electronic tracks that is generated by the electronic devices used by a man regardless of his will.

An author marks that methodical recommendations are absent for today from an exposure, fixing, exception of "digital" information and expert methodologies of research of data are worked not enough out on machine transmitters, that is why the use of them in a court remains ineffective.

New informative technologies that inculcated wider in practice of law enforcement authorities is considered in the article. Such the operational search and prophylactic setting functions in the organs of internal affairs of Ukraine, where the enormous arrays of information including secret or intended for the official use are processed. Therefore problem of defence of information, that kept and processed in the computer systems organs of internal affairs from an unauthorized division, its imitation, penetration of computer viruses.

It is concluded, that the use of modern information technologies in establishment and equation of personality of criminal will assist more rapid investigation of crimes.

Key words: fight against crimes, information, information technologies, method, personality of criminal, search, form.

Суспільно-політичні зміни, які сьогодні відбуваються в житті України, супроводжуються загостренням криміногенної ситуації, зростанням кількісних і якісних показників злочинності. При цьому, крім загального загострення криміногенної ситуації, має місце тенденція ускладнення злочинних схем та засобів уникнення відповідальності за їх вчинення, що негативно впливає на організацію боротьби з ними. Відповідно, протидія злочинності поряд зі зміцненням законності є одним із важливих завдань, що стоять перед державою та її органами, а ефективність їх роботи з розслідування злочинів багато в чому залежить від рівня застосування всього потенціалу сучасних криміналістичних рекомендацій, своєчасного та вмілого їх використання.

Окремі аспекти цієї проблеми в різні часи досліджували такі вітчизняні та зарубіжні науковці: Т.В. Авер'янова, В.Д. Басай, Р.С. Бєлкін, Т.В. Варфоломєєва, В.В. Голіна, І.М. Даньшин, В.Є. Емінов, В.А. Журавель, А.В. Іщенко, Н.С. Карпов, В.О. Коновалова, В.Г. Лукашевич, Є.Д. Лук'янчиков, В.Т. Нор, В.О. Образцов, І.В. Пиріг, О.Р. Ратінов, О.С. Саінчин, В.Г. Танасевич, В.В. Тіщенко, Є.О. Центров, Ю.В. Чуфаровський, В.Ю. Шепітько, М.Г. Щербаковський, М.П. Яблоков, А.М. Яковлєв та інші. У працях цих дослідників закладено методологічне й методичне підґрунтя для комплексного, системного дослідження теоретичних і прикладних проблем форм та методів роботи з інформацією про особу злочинця (оперативно-розшуковою, криміналістично значущою тощо), застосування сучасних інформаційних технологій у практиці розслідування кримінальних злочинів.

Викладене свідчить про наявність наукової проблеми, яка полягає в недостатній розробленості у вітчизняній юридичній літературі технічного й методичного забезпечення

практики роботи з інформацією. З огляду на показники, представлені в роботі Н.О. Мар'янчук «Інформаційні технології в сучасному державному управлінні» (див. http://www.kds.org.ua/blog/maryanchuk-n-tvorcha-robota-informatsijni-tehnologii-v-suchasnomu-derzhavnomu-upravlinni), а також аналізуючи звіти із численних форумів і конгресів, виставок та ярмарок досягнень науково-технічного світу, доходимо висновку, що злочинний світ має у своєму розпорядженні дуже великий арсенал «озброєння». Сучасний світ практично неможливо уявити без нових інформаційних технологій, в основі яких лежить широке використання комп'ютерної техніки та новітніх засобів комунікацій, їх упровадження в різноманітні галузі людської діяльності. Безліч організацій та установ широко використовують їх у своїй діяльності.

Нові інформаційні технології дедалі ширше мають можливість упроваджуватись у практику правоохоронних органів. Так, в органах внутрішніх справ України функціонує значна кількість автоматизованих систем оперативно-розшукового та профілактичного призначення, де обробляються величезні масиви інформації, у тому числі таємної чи призначеної для службового користування.

Місцями зосередження домінуючих масивів достовірних персональних даних стали інтегровані автоматизовані банки даних та автоматизовані інформаційно-пошукові системи різних державних органів, банки даних кредитних історій, програм лояльності різних суб'єктів господарювання, online-анкети соціальних інтернет-мереж.

Інтегровані банки даних та автоматизовані інформаційно-пошукові системи є найскладнішими утвореннями, різновидом інформаційних систем. Інформаційні системи незалежно від їх підпорядкування й основного призначення є одним із надійних джерел інформації, яка може використовуватись у розслідуванні та набути криміналістичного значення залежно від реальної ситуації. Необхідність використання в розслідуванні злочинів даних інформаційних систем інших відомств зумовлює потребу в їх інтеграції до інтегрованого банку даних на певному рівні.

Таким чином, використання сучасних інформаційних технологій у встановленні й ототожненні особи злочинця буде сприяти більш швидкому розслідуванню злочинів.

У сучасних умовах науково-технічного прогресу чітко вимальовується тенденція до комп'ютеризації, створення розгалужених систем обробки даних, що включають у себе як потужні обчислювальні комплекси, так і персональні комп'ютери. Щодня збільшується кількість комунікаційних локальних, галузевих, загальнодержавних та міждержавних мереж. Комп'ютерні технології впроваджуються практично в усі сфери громадського життя, у тому числі в правоохоронну діяльність, медицину, зв'язок, транспорт, національну безпеку тощо.

Тотальна інформатизація суспільства, інтернет-залежність стали причиною протікання життєдіяльності більшості індивідів одночасно в реальному та віртуальному просторах із відповідним слідоутворенням в обох вимірах унаслідок використання засобів мобільного зв'язку, електронної пошти, електронних систем платежів, кредитних, платіжних і дисконтних карт. Дедалі частіше хронологія життя сучасної людини відображається в миттєвих та sms-повідомленнях, вмісті електронної пошти, записах в електронних адресних книгах і календарях, фотознімках та відеороликах, статусах на сторінках у соціальних інтернет-мережах, блогах, створюваних самою особою, а також у доріжках електронних слідів, що генеруються використовуваними людиною електронними пристроями незалежно від її волі.

З переходом на новітні інформаційні технології знизились рівень і якість криміналістичного, судово-експертного забезпечення багатьох категорій злочинів, пов'язаних із використанням комп'ютерної техніки, особливо у сфері економіки, бізнесу та підприємництва. З огляду на відсутність методичних рекомендацій із виявлення, фіксації, вилучення «цифрової»

інформації та на недостатнє розроблення експертних методик дослідження даних на машинних носіях використання їх у суді залишається малоефективним [1].

Розглядаючи джерела комп'ютерної інформації, А.Г. Волеводз підкреслює, що самі носії інформації не можуть розглядатись як об'єкти криміналістичних досліджень, якщо вони не містять у собі слідів вчиненого злочину [2, с. 159]. У разі присутності таких цифрових слідів існує ще одна проблема – яким чином пред'явити таку інформацію в суді, щоб не виникало сумнівів у її оригінальності та щоб вона не втратила процесуальної сили доказу.

Щодо цього питання існують декілька методик, проте найпоширенішою є методика, запропонована американськими криміналістами, які після вилучення носія інформації, використовуючи спеціальне легітимне програмне забезпечення, знімають точну копію цієї інформації, а оригінальний носій опечатують і більше не використовують. Вивчення потрібної їм інформації вони здійснюють зі знятої копії, а в суд пред'являють роздрукований варіант інформації (на так званому твердому носії). У разі виникнення підозри щодо достовірності пред'явленої в суді інформації суддя може витребувати оригінальний носій цієї інформації для звірки. Однак це тільки одна з можливих проблем із доказами, тому що комп'ютерна інформація може бути зашифрована злочинцем або частково знищена, і подальші дії з її відновлення чи розшифрування правоохоронними органами будуть досить суперечливими з погляду чинного кримінально-процесуального законодавства.

Як справедливо зазначає В.В. Крилов, для «цифрових» слідів характерні специфічні якості, що визначають перспективи їх реєстрації, вилучення та використання як доказів під час розслідування злочину [3, с. 27]. По-перше, комп'ютерна інформація існує на певних носіях, проте не доступна для безпосереднього спостереження. Тобто для її виявлення й дослідження необхідне використання технічних і програмних засобів, що ставить під загрозу її подальше доказове значення, адже вказані засоби повинні бути сертифікованими та використовуватись відповідними спеціалістами. По-друге, комп'ютерна інформація не змінюється з плином часу, а також за багаторазового копіювання. Ця якість машинних даних пояснюється тим, що вони представлені в числовій формі за допомогою знаків «1» і «0», а вся інформація іншого характеру, яка вноситься в комп'ютер (тексти, графіка, відео, аудіо), перетворюється на форму, зрозумілу для ЕОМ, – цифрову. По-третє, така інформація, хоч і є стабільною за змістом, може бути по-різному сприйнята залежно від засобів зчитування, декодування та відображення. Наприклад, використання неправильного засобу декодування тексту особою, яка бажає ознайомитися з електронним документом, призведе до виводу на дисплей або принтер незрозумілого набору символів [4, с. 76]. Джерелами комп'ютерної інформації можуть слугувати фізичні носії комп'ютерної інформації (жорсткі диски, компакт-диски, флеш-карти, накопичувачі на гнучких магнітних дисках), оперативний запам'ятовуючий пристрій комп'ютера, оперативний запам'ятовуючий пристрій периферійних пристроїв, комп'ютерна мережа [4, с. 77].

Основною метою створення й функціонування будь-яких інформаційних систем у тій чи іншій галузі є сприяння вирішенню завдань, для вирішення яких їх було створено. Сприяти розкриттю та розслідуванню злочинів безпосередньо призначені криміналістичні інформаційні системи. Однак у такому складному різновиді людської діяльності, як розслідування злочинів, криміналістичного значення може набути інформація, отримана як із криміналістичних, так і з некриміналістичних інформаційних систем, незалежно від первинної мети їх створення й основного призначення інформації. Залежно від ситуації, що склалася, вона залучається до процесу, актуалізується та посідає своє місце в установленні певних об'єктів чи обставин.

Одним із перших питання використання інформації, отриманої з інформаційних систем, у розслідуванні злочинів, виходячи з конкретних слідчих ситуацій, що склалися, запропонував розглядати російський криміналіст С.А. Ялишев [5, с. 104-108]. Проте аналіз наукових праць, у яких розглядаються питання, пов'язані з розробленням і вдосконаленням криміналістичних

методик розслідування злочинів та проведення криміналістичних експертиз, дає підстави стверджувати, що сьогодні, на жаль, у них питанням використання інформації, що міститься в інформаційних системах, увага майже не приділяється. Як виняток можна назвати лише окремі праці Н.І. Клименко [6, с. 93-103]. Ці питання недостатньо висвітлені також у криміналістичних методиках [7, с. 113].

Розслідування злочинів являє собою процес добування, осмислення та використання інформації, за допомогою якої формується уявлення про пізнаваний об'єкт. Інформація в цьому разі є і об'єктом пошуку, і засобом пізнання. Слідчий, здійснюючи розслідування, отримує її з різних джерел. Істотне значення для встановлення певних об'єктів і фактів має інформація, яка може бути отримана з інформаційних систем, кіберпростору.

Не викликає сумніву, що наявність знань про сучасний стан обліків як криміналістичного, так і некриміналістичного призначення, принципові основи їх побудови й функціонування, уміння правильно орієнтуватись у величезних потоках облікової інформації, визначати місця її концентрації та носії тієї, що необхідна, уміння її кваліфікованого вилучення й використання для встановлення окремих обставин у процесі розслідування є необхідною умовою професійної діяльності сучасного правоохоронця. О.О. Денисова справедливо зазначає: «Очевидно, що правознавець повинен знати, як можна застосовувати інформаційні технології у своїй роботі та які правові інформаційні системи вже створено й упроваджено. Проте незалежно від майбутнього місця роботи йому необхідні знання про комп'ютерні технології загалом, про тенденції комп'ютеризації та інформатизації, про інформаційні системи підприємницьких фірм, банків, органів державної влади тощо. Без цього юрист не може ефективно виконувати свої функціональні завдання» [8, с. 24].

Характерна криміналістична особливість кіберпростору полягає в тому, що об'єкти (файли даних і програм), які взаємодіють у ньому та беруть участь у процесі створення слідів, що виникають при цьому, не мають зовнішньої будови. Відповідно, весь арсенал засобів і методів роботи з матеріальними слідами, накопичений трасологією, у цьому разі виявляється практично непридатним, що зумовлює актуальність криміналістичного дослідження електронних носіїв інформації.

Місцями зосередження домінуючих масивів достовірних персональних даних стали інтегровані автоматизовані банки даних та автоматизовані інформаційно-пошукові системи різних державних органів, банки даних кредитних історій, програм лояльності різних суб'єктів господарювання, online-анкети соціальних інтернет-мереж, у яких загалом у світі вже зареєстровано понад 5,7 млрд профілів [9].

Інтегровані банки даних являють собою складні інформаційні системі, основу яких становлять окремі інформаційні системи, призначені для вирішення певних завдань, що стоять перед певним підрозділом, службою, управлінням. Кожна з таких систем обробляє частку інформації про об'єкт, який взято на облік в інших системах за іншими параметрами.

Сьогодні інтегровані банки даних Міністерства внутрішніх справ (далі – МВС) України становлять сукупність окремих автоматизованих інформаційних систем, зведених у єдину розподілену систему, яка має високоорганізовану систему забезпечення з організацією доступу через одну адресу – ядро інтегрованого банку даних. Зв'язок між складниками цієї системи здійснюється з використанням сучасних телекомунікаційних технологій. Усі складники інтегрованих банків даних використовують типове програмне забезпечення та операційні системи. Ідея створення інтегрованого банку даних ґрунтується на цільовому призначенні інформаційних систем і зручності отримання різноманітної інформації про один об'єкт з однієї адреси. Наведемо визначення цього поняття: інтегрований банк даних – це сукупність окремих інформаційних систем (обліків), що мають спільне застосування, високоорганізовану систему забезпечення з організацією доступу до інформації будь-якої його складової частини через одну адресу – ядро інтегрованого банку даних.

Надійність роботи інтегрованого банку даних безпосередньо залежить від надійності мережевих технологій зв'язку. Доступ до інформації інтегрованого банку даних може здійснюватися з віддалених місць доступу. Наприклад, до інформації інтегрованих банків даних Управління інформаційних технологій Управління МВС України в Луганській області такий доступ можна здійснити із чергової частини будь-якого районного відділу Управління МВС України. Водночас інтегрований банк даних Управління інформаційних технологій Управління МВС України в Луганській області має вихід до інтегрованого банку даних Департаменту інформаційних технологій при МВС України. Інтеграція інформаційних систем має тенденцію до централізації.

Особливе значення для встановлення окремих факторів може мати використання сучасних можливостей інтегрованого банку даних і системи «АРМОР», які, аналізуючи введену на запит інформацію про певний об'єкт обліку, дають можливість установити його взаємозв'язки з іншими, а також отримати найрізноманітнішу інформацію про нього. З огляду на завдання статті спробуємо визначитися з типовими ситуаціями та алгоритмами дій, спрямованими на встановлення особи злочинця з використанням можливостей, які сьогодні надають нам інформаційні системи [10, с. 243].

У ситуації, коли особа злочинця невідома, проте є матеріально фіксовані сліди, які вона могла залишити, особливе значення мають криміналістичні обліки, які здійснюють підрозділи експертної служби МВС України. Варто зазначити, що вид обліку, яким можна скористатись із цією метою, прямо залежить від того, які сліди наявні. Для пошуку можуть бути використані насамперед обліки оперативно-розшукового призначення, причому саме ті, які створюють умови для ідентифікації об'єктів за певними слідами, що є в розпорядженні органів слідства. Поряд із дактилоскопічними й балістичними (залежно від наявних слідів) можуть використовуватись обліки слідів взуття, слідів транспортних засобів, зразків почерку тощо.

У ситуації, коли особа злочинця відома, проте вона не затримана та відомостей про її місцезнаходження немає, за допомогою інформаційних систем можна встановити місце її проживання, роботи, імовірні місця перебування тощо. Для цього можна скористатись як криміналістичними обліками, так і інформаційними системами іншого призначення, які ведуть структурні підрозділи МВС України, а також підрозділи й установи інших відомств, у тому числі інших правоохоронних органів. Також може виникнути ситуація, коли необхідно буде звернутись до міжнародних інформаційних систем Інтерполу, Європолу, а також Міжнародної інформаційної бази країн Співдружності Незалежних Держав.

Особливе місце в цій діяльності посідають інформаційні системи з автоматичною реєстрацією, які реєструють факти звернення до системи (наприклад, з метою отримання певної послуги, проникнення на певні об'єкті, виходу в ефір). За ними можна встановити останнє місце перебування (точніше, здійснення певної операції) особи, яка зникла безвісти, а також тієї, яка переховується від суду чи правоохоронних органів. Для встановлення ймовірного місця перебування особи, що переховується від суду та правоохоронних органів, доцільно скористатись обліками паспортної служби. Одним із заходів під час оголошення особи в розшук є інформування підрозділів паспортної служби. Сприяти розшуку осіб, місцезнаходження яких невідоме, призначені обліки безвісти зниклих, хворих, що не можуть повідомити свої настановні дані, і невпізнаних трупів, які ведуть відповідні підрозділи МВС України. Зрозуміло, що така особа може бути і невпізнаним трупом, і хворим, який не може пригадати чи надати свої настановні дані (наприклад, хворі або постраждалі в дорожньо-транспортній пригоді). Особливе значення для встановлення ймовірного місця перебування певної особи має застосування потенціалу інформаційно-аналітичних систем «АРМОР», «СОВА», «АРГуС», що ґрунтуються на інтегрованих банках даних. Аналізуючи зв'язки особи, можна також установити її можливе місцезнаходження. Поряд з указаною категорією обліків важливу роль відіграють обліки медичних установ (лікарень, травмпунктів), до яких особа могла звертатися за медичною допомогою (наприклад, у разі поранення чи хвороби).

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

Глобальне поширення й легкодоступність цифрових засобів фотофіксації, аудіо-, відеозапису, а також інтернет-ресурсів, що надають необмеженому колу осіб можливість безкоштовного розміщення різних матеріалів у вільному доступі, зумовили так званий інформаційний ексгібіціонізм, коли найменший рух «звивини мозку» або афективний імпульс виставляються на загальний огляд [11, с. 233]. При цьому лавиноподібний розвиток інтернет-спільнот, основним контентом яких слугує візуальний матеріал (наприклад, Instagram, Pinterest або Pinme, орієнтовані на зберігання, демонстрацію та обмін фото- та/або відеозображеннями), призвів до домінування в змісті комунікації візуального складника та переходу від логосфери до іконосфери, зростання популярності такого жанру фотозйомки, як selfie. Використання тандему фото-/відеокамери та соціальної мережі дає змогу інтернет-користувачам мислити й спілкуватись образами, скорочуючи час для комунікації, а органам досудового розслідування за наявності правових підстав і з дотриманням визначеної законом процедури – установлювати місця їх перебування завдяки автоматичній фіксації у файлі фотозображення даних про географічне місце та час здійснення зйомки.

Відсутність інформаційної культури та нехтування елементарними заходами інформаційної безпеки іноді призводять до курйозів, коли керований марнославством підозрюваний у вчиненні тяжкого злочину здійснює самовикриття, розміщуючи на своїй персональній сторінці в соціальній мережі власне фото (mugshot), запозичене із сайту поліцейського департаменту під грифом «Wanted» («Розшукується»).

Часто в мережу «викладаються» матеріали фото-, відеофіксації злочинної діяльності, здійснюваної їх автором одноособово або в співучасті [12].

Загрозливою є тенденція демонстративного поширення ісламськими бойовиками через всесвітню мережу відеозаписів страти американських журналістів Дж. Фоулі та С. Сотлоффа, шотландського волонтера Д. Хейнса та британського таксиста А. Хеннінга з публічними погрозами на адресу країн Заходу від імені так званої Ісламської держави Іраку й Леванту [13]. А необхідність у збиранні інформації про приховану причетність до тероризму в нашій країні Російської Федерації [14], унаслідок якого станом на 30 вересня 2014 р. загинули 3 627 людей, 8 447 отримали поранення, 379 тис. були вимушені переїхати зі Сходу України в інші регіони, а більше 426 тис. – у сусідні держави, зумовила створення вітчизняними громадськими активістами спеціального інтернет-сайту www.dokaz.org.ua, на якому щоденно акумулюються фото та відео, 90% яких координатори сайту отримують із відкритих джерел – сторінок у соціальних мережах росіян, на яких ті зізнаються у своїй причетності до заворушень на Донбасі, зокрема, розміщують власні світлини зі зброєю, військовою технікою, полоненими й загиблими українськими військовими тощо [15].

Криміналістично значущим можна визнати той факт, що традиційне коло ознак, які сприяють ототожненню живої людини, нині розширилося за рахунок ідентифікаційних ознак використовуваних нею транспортних комунікаційних мереж і кінцевого обладнання. До них варто віднести такі: абонентський номер (сукупність цифрових знаків для позначення (ідентифікації) кінцевого обладнання абонента в телекомунікаційній телефонній мережі загального користування у форматі «код країни – код зони або оператора – абонентський номер у мережі»); ідентифікатор користувача (User Identifier, USER ID); міжнародний

ідентифікаційний номер мобільного терміналу (міжнародний ідентифікатор обладнання мобільної станції – International Mobile Equipment Identity, IMEI); міжнародний ідентифікаційний номер мобільного абонента (міжнародний ідентифікатор мобільного абонента – International Mobile Subscriber Identity, IMSI); ідентифікаційну телекомунікаційну картку (засіб, що використовується для ідентифікації кінцевого обладнання абонента в телекомунікаційній мережі: SIM-карта, USIM-карта, R-UIM-карта); серійний номер обладнання мобільної станції (Electronic Serial Number, ESN); міжнародний ISDN номер мобільної станції (Mobile Subscriber ISDN Number, MSISDN), мережеву адресу в Інтернеті (IP-address). Дослідження віртуальних слідів взаємодії цих пристроїв може сприяти встановленню широкого кола обставин розслідуваної події.

З метою забезпечення органів кримінальної юстиції інноваційним «продуктом», призначеним для своєчасного встановлення місцезнаходження та ототожнення розшукуваних осіб (у тому числі дистанційно), на думку В.Ю. Шепітька та В.В. Білоус [16, с. 8-10], перспективними напрямами розвитку криміналістики варто визнати такі:

1) створення та пристосовування до виконання криміналістичних завдань широкого спектра інформаційних технологій (наприклад, технологій аналізування метаданих абонентів стільникового зв'язку й мережевого аналізу; автоматичного пошуку, розпізнавання та ідентифікації осіб за цифровими фото-, відеозображеннями, розміщеними в мережі Інтернет; безконтактного автоматизованого розпізнавання емоцій за фотоеталонами (патернами) їх мімічних виразів; побудови картографічних геоінформаційних схем переміщення абонентів тощо), а також розроблення криміналістичних рекомендацій комплексного використання цих інформаційних технологій з урахуванням здобутого позитивного досвіду впровадження наукових розробок [17] і використання відкритих online-джерел суб'єктами, які володіють ресурсами для першочергового впровадження подібних інновацій (власниками найбільших соціальних інтернет-мереж, провідними рекрутинговими агенціями, колекторськими компаніями, операторами ринку таргетованої реклами тощо). Використання потенціалу соціальних інтернет-мереж уже сприяло розшуку органами МВС України 15% зниклих безвісти дітей [18], а мобільного зв'язку – пошуку жертв техногенних катастроф [19];

2) організацію навчання та доведення до автоматизму навичок виявлення, попереднього дослідження, фіксації й вилучення слідчими не тільки традиційних матеріальних чи інтелектуальних, а й віртуальних слідів; самостійної роботи з електронними носіями інформації та електронними засобами фіксації, копіювання, зв'язку, контролю й забезпечення захисту осіб, радіоелектронними засобами, транспортними телекомунікаційними мережами та електронними інформаційними системами; проведення слідчих і спеціальних слідчих дій, зумовлених упровадженням у практику інформаційних та телекомунікаційних технологій, здійснення окремих процесуальних дій у дистанційних режимах відео- та телефонних конференцій. Наприкінці 1980-х – на початку 1990-х рр. у кримінально-процесуальному законодавстві деяких європейських країн виник інститут так званих спеціальних слідчих дій, який відносно недавно був упроваджений і в процесуальне законодавство деяких країн пострадянського простору у вигляді «таємних», «негласних слідчих (розшукових)», «оперативних» та інших дій і заходів. Так, у ст. ст. 260, 263, 264, 267-270 Кримінального процесуального кодексу України законодавчу регламентацію отримала низка негласних слідчих (розшукових) дій, заснованих на використанні інформаційних і телекомунікаційних технологій (аудіо-, відеоконтроль особи; зняття інформації з транспортних телекомунікаційних мереж; обстеження публічно недоступних місць, житла чи іншого володіння особи; установлення місцезнаходження радіоелектронного засобу; спостереження за особою, річчю або місцем; аудіо-, відеоконтроль місця). У ст. ст. 115-118 Кримінального процесуального кодексу Естонії передбачено такі дії, як приховане спостереження, прихований огляд і заміна об'єкта; прихований огляд поштово-телеграфних відправлень; збирання відомостей про повідомлення, що передаються через канали зв'язку загального користування; негласне прослуховування та негласне візуальне спостереження

повідомлень та іншої інформації, переданої через телекомунікаційні мережі загального користування. У ст. ст. 134.2-134.3 Кримінального процесуального кодексу Молдови регламентовано негласний процесуальний моніторинг або контроль фінансових угод і доступ до фінансової інформації; документування за допомогою технічних засобів і методів, а також локалізацію й відстеження об'єктів через глобальну систему позиціонування (GPS) або за допомогою інших технічних засобів; збирання інформації від постачальників послуг електронних комунікацій тощо;

3) модернізацію таких тактичних операцій, як «Викриття злочинця», «Пошук і встановлення осіб, які переховуються від слідства», «Встановлення співучасників злочину» тощо, за рахунок включення в їх структуру ситуаційно зумовлених систем названих спеціальних слідчих дій, у тому числі таких, що сприяють вирішенню тактичного завдання стосовно перевірення «цифрового алібі». Під час планування їх проведення необхідно враховувати тенденції, згідно з якими зі зростанням кількості електронних пристроїв, що використовуються однією особою, а також застосуванням особистих смартфонів і планшетів у корпоративних цілях набувають популярності хмарні сховища інформації, що дають змогу завантажувати особисті дані в Інтернет для віддаленого зберігання файлів із правом доступу до них за допомогою необмеженої кількості засобів комунікації. За деякими оцінками, до 2019 р. аудиторія веб-служб, призначених для віддаленого зберігання файлів, досягне 3,6 млрд користувачів, а сумарний обсяг завантажуваних на ці сховища даних складе 3 520 петабайт проти 685 петабайт у 2013 р. [20]. Більшість потужних дата-центрів (центрів оброблення даних) розташовані за межами країн, резидентами яких є інтернет-користувачі [21]. Унаслідок цього боротьба зі злочинністю як з екстериторіальним суспільно небезпечним явищем вимагає вироблення навичок високого рівня взаємодії в межах надання міжнародної правової допомоги [16, с. 6].

На основі вищевикладеного можна зробити певні висновки.

Так, сучасний світ практично неможливо уявити без нових інформаційних технологій, в основі яких лежить широке використання комп'ютерної техніки та новітніх засобів комунікацій, їх упровадження в різноманітні галузі людської діяльності. Безліч організацій та установ широко використовують їх у своїй діяльності.

На сьогодні відсутні методичні рекомендації з виявлення, фіксації, вилучення «цифрової» інформації та недостатньо розроблені експертні методики дослідження даних на машинних носіях, тому використання їх у суді залишається малоефективним.

Нові інформаційні технології дедалі ширше впроваджуються в практику правоохоронних органів. Так, в органах внутрішніх справ України функціонує значна кількість автоматизованих систем оперативно-розшукового та профілактичного призначення, де обробляються величезні масиви інформації, у тому числі таємної чи призначеної для службового користування. Тому постає проблема захисту інформації, яка зберігається та обробляється в комп'ютерних системах органів внутрішніх справ, від несанкціонованого доступу, її підробки, проникнення комп'ютерних вірусів тощо.

Місцями зосередження домінуючих масивів достовірних персональних даних стали інтегровані автоматизовані банки даних та автоматизовані інформаційно-пошукові системи різних державних органів, банки даних кредитних історій, програм лояльності різних суб'єктів господарювання, online-анкети соціальних інтернет-мереж.

Інтегровані банки даних та автоматизовані інформаційно-пошукові системи є найскладнішими утвореннями, різновидом інформаційних систем. Інформаційні системи незалежно від їх підпорядкування та основного призначення є одним із надійних джерел інформації, яка може використовуватись у розслідуванні та набути криміналістичного значення залежно від реальної ситуації. Необхідність використання в розслідуванні злочинів

даних інформаційних систем інших відомств зумовлює потребу в їх інтеграції до інтегрованого банку даних на певному рівні.

Таким чином, використання сучасних інформаційних технологій у встановленні й ототожненні особи злочинця буде сприяти більш швидкому розслідуванню злочинів.

ЛІТЕРАТУРА

1. Яковлев А.Н. Теоретические и методические основы экспертного исследования документов на машинных магнитных носителях информации : автореф. дис. … канд. юрид. наук : спец. 12.00.09 «Уголовный процесс, криминалистика; оперативно-розыскная деятельность» / А.Н. Яковлев. – Саратов, 2000. – 24 с.
2. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волеводз. – М. : ООО Издательство «Юрлитинформ», 2002. – 154 с.
3. Крылов В.В. Информационные компьютерные преступления : [учеб. и практ. пособие] / В.В. Крылов. – М. : Норма – Инфра-М, 1997. – 285 с.
4. Ращенко Є.В. Комп'ютерні дані як носій криміналістичної інформації про злочини у сфері комп'ютерних технологій / Є.В. Ращенко // Правова інформатика. – 2007. – № 1(13). – С. 74-78.
5. Ялышев С.А. Криминалистическая регистрация: проблемы, тенденции, перспективы : [монография] / С.А. Ялышев. – М. : Академия управления МВД России, 1998. – 140 с.
6. Клименко Н.І. Судова експертологія. Курс лекцій : [навч. посібник] / Н.І. Клименко. – К. : Ін Юре, 2007. – 528 с.
7. Бирюков В.В. Современные проблемы использования учетно-регистрационных данных в расследовании / В.В. Бирюков // Проблемы криминалистической науки, следственной и экспертной практики. – 2007. – Вып. 7. – С. 111-116.
8. Гвоздева В.А. Основы построения автоматизированных информационных систем : [учебник] / В.А. Гвоздева, И.Ю. Лаврентьева. – М. : Инфра-М, 2007. – 320 с.
9. Названы самые популярные социальные сети в мире // Фокус. – 2014. – 6 січня. – [Електронний ресурс]. – Режим доступу : http://focus.ua/tech/294534/.
10. Бірюков В.В. Встановлення особи злочинця за допомогою даних інформаційних систем з огляду на складену ситуацію / В.В. Бірюков // Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. – 2012. – № 3. – С. 241-248.
11. Голова А.Г. Трансформации в социальных медиа в сети Интернет: социокультурный анализ / А.Г. Голова // Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». – 2013. – № 1. – С. 233-245.
12. Резонансное преступление в России: групповое изнасилование несовершеннолетней школьницы выложили в интернет // Цензор. Нет. – 2014. – 28 вересня. – [Електронний ресурс]. – Режим доступу : http://censor.net.ua/news/304618.
13. Исламские террористы обезглавили очередного заложника // Дзеркало тижня. – 2014. – 4 жовтня. – [Електронний ресурс]. – Режим доступу : http://zn.ua/WORLD/.
14. Как российские войска из террористов на Донбассе превращаются в «миротворцев» // Цензор. Нет. – 2014. – 3 жовтня. – [Електронний ресурс]. – Режим доступу : http://censor.net.ua/photo_news/305413/.
15. Для збору інформації про причетність РФ до тероризму в Україні створено сайт // 5 канал. – 2014. – 8 липня. – [Електронний ресурс]. – Режим доступу : http://www.5.ua/ukrajina/suspilstvo/item/388427/.

16. Шепітько В.Ю. Роль сучасних інформаційних технологій у встановленні особи злочинця / В.Ю. Шепітько, В.В. Білоус // Теорія та практика судової експертизи і криміналістики. – 2014. – Вип. 14. – С. 5-11.

17. Захарченко О.В. Діяльність слідчого з розшуку та встановлення місцезнаходження обвинуваченого : автореф. дис. … канд. юрид. наук : спец. 12.00.09 «Кримінальний процес і криміналістика; судова експертиза; оперативно-розшукова діяльність» / О.В. Захарченко. – Х., 2012. – 20 с.

18. Соцсети помогают украинской милиции искать пропавших детей // Blog Imena.UA. – [Електронний ресурс]. – Режим доступу : http://www.imena.ua/blog/network-helps.

19. Под завалами ТЦ в Риге ищут людей по звонкам на мобильные // Известия в Украине (политические известия). – 2013. – 23 ноября. – [Електронний ресурс]. – Режим доступу : http://izvestia.kiev.ua/ru/news/37197.

20. К концу 2013 года количество аккаунтов в облачных хранилищах достигнет 1 млрд // Internet.ua. – 2013. – 17 грудня. – [Електронний ресурс]. – Режим доступу : http://internetua.com/.

21. Цукрова Т.С. Где хранятся личные данные украинских пользователей / Т.С. Цукрова // Лига.Бизнес. – 2014. – 7 августа. – [Електронний ресурс]. – Режим доступу : http://biz.liga.net/all/it/stati/.

REFERENCES

1. Yakovlev, A.N. (2000), “Theoretical and methodical bases of expert research of documents on the machine magnetic data storage devices”, Thesis abstract for Cand. Sc. (Jurisprudence), 12.00.09, Saratov, Russia.

2. Volevodz, A.H. (2002), *Protivodeystvie kompyuternym prestupleniyam : pravovye osnovy mezhdunarodnoho sotrudnichestva* [Counteraction to the cyber crimes : legal frameworks of international cooperation], OOO Izdatelstvo «Yurlitinform», Moscow, Russia.

3. Krylov, V.V. (1997), *Informatsionnye kompyuternye prestupleniya : uchebnoe i prakticheskoe posobie* [Informative cyber crimes : educational and practical manual], Infra-M-Norma, Moscow, Russia.

4. Rashchenko, Ye. (2007), “Computer data as storage of criminalistics information about crimes in the field of computer technologies”, *Pravova informatyka*, no. 1(13), pp. 74-78.

5. Yalyshev, S.A. (1998), *Kriminalisticheskaya rehistratsiya : problemy, tendentsiyi, perspektivy : monohrafiya* [Criminalistics registration : problems, tendency, prospects : monograph], Akademiya upravleniya MVD Rossiyi, Moscow, Russia.

6. Klymenko, N.I. (2007), *Sudova ekspertolohiya. Kurs lektsiy : navchalnyi posibnyk* [Judicial expertology. The course of lectures : textbook], In Yure, Kyiv, Ukraine.

7. Biryukov, V.V. (2007), “Modern problems of use of registration data in investigation”, *Problemy kriminalisticheskoy nauki, sledstvennoy i ekspertnoy praktiki*, Iss. 7, pp. 111-116.

8. Hvozdeva, V.A. and Lavrenteva, I.Yu. (2007), *Osnovy postroeniya avtomatizirovannykh informatsionnykh sistem : uchebnik* [Bases of construction of informative systems : textbook], Infra-M, Moscow, Russia.

9. (2014), “The most popular social networks in the world are determinated”, *«Fokus»*, January 6, available at : http://focus.ua/tech/294534/.

10. Biriukov, V.V. (2012), “Identification of personality of criminal by means of informative systems, taking into account the made situation”, *Visnyk Luhanskoho derzhavnoho universytetu vnutrishnikh sprav imeni E.O. Didorenka*, no. 3, pp. 241-248.

11. Holova, A.H. (2013), "Transformations in social medias in the Internet : sociocultural analysis", *Visnyk Natsionalnoho universytetu «Yurydychna akademiia Ukrainy imeni Yaroslava Mudroho»*, no. 1, pp. 233-245.

12. (2014), "Resonant crime in Russia : the gang rape of young schoolgirl was laid out in the internet", *«Tsenzor. Net»*, September 28, available at : http://censor.net.ua/news/304618.

13. (2014), "Islamic terrorists beheaded yet another hostage", *Zerkalo Nedeli*, October 4, available at : http://zn.ua/WORLD/.

14. (2014), "As the Russian troops from terrorists on Donbas grow into "peacemakers"", *«Tsenzor. Net»*, October 3, available at : http://censor.net.ua/photo_news/305413/.

15. (2014), "For collection of information about involvement of Russian Federation to terrorism a web-site is created in Ukraine", *5 kanal*, July 8, available at : http://www.5.ua/ukrajina/suspilstvo/item/388427/.

16. Shepitko, V.Yu. and Bilous, V.V. (2014), "A role of modern information technologies in identification of personality of criminal", *Teoriya ta praktyka sudovoyi ekspertyzy i kryminalistyky*, Iss. 14, pp. 5-11.

17. Zakharchenko, O.V. (2012), "Activity of investigator in searching and establishment of location of defendant", Thesis abstract for Cand. Sc. (Jurisprudence), 12.00.09, Kharkiv, Ukraine.

18. "Social networks help the Ukrainian police to search disappearing children", *«Blog Imena.UA.»*, available at : http://www.imena.ua/blog/network-helps.

19. (2013), "Search people by rings on mobile under the obstructions of shopping center in Riga", *Izvestiya v Ukraine (Politicheskie Izvestiya)*, November 23, available at : http://izvestia.kiev.ua/ru/news/37197.

20. (2013), "By the end of 2013 the amount of accounts in cloud depositories will attain 1 milliard", *«Internet.ua»*, December 17, available at : http://internetua.com/.

21. Tsukrova, T. (2014), "Where the personal data of the Ukrainian users are kept", *Lyha.Byznes*, August 7, available at : http://biz.liga.net/all/it/stati/.