УДК 351:355.02](477)

Кравчук Олег Вікторович
доцент кафедри кримінального права та процесу
Хмельницького університету управління та права,
кандидат юридичних наук

ДЕРЖАВНЕ УПРАВЛІННЯ ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВІЗАЦІЇ

Анотація. *У статті розглядаються напрямки державного управління розвитком приватних криміналістичних теорій і вчень в умовах «цифровізації» для забезпечення безпеки держави та суспільства загалом. Подано тенденції розвитку теорії ідентифікації, теорії криміналістичного прогнозування, учення про сліди, криміналістичної тактики й методики розслідування окремих видів злочинів. Криміналістичні знання, «цифровізація», електронний образ, електронний слід – усі ці напрямки розвитку криміналістично-експертної науки мають формувати новий напрямок державного управління державною безпекою та охороною громадського порядку.*

Ключові слова: *державне управління забезпечення державної безпеки, «цифровізація», державне управління розвитком криміналістики.*

Kravchuk O.V. Public administration of national security under conditions of digitization

Annotation. *The directions of public administration of the private forensic theories and trainings development under conditions of digitalization for ensuring security of the state and society as a whole are considered in the article. The tendencies of the identification theory development, the theory of forensic forecasting, the doctrine of traces, forensic tactics and methods of certain types of crimes investigation are also presented. Forensic knowledge, digitalisation, electronic image, electronic trace, all these directions of forensic-expert science development are intended to form a new direction regarding public administration of national security and public order protection.*

Key words: *public administration of national security, digitalization, public administration of forensic development.*

Постановка проблеми в загальному вигляді. Процес відродження України як сильної й незалежної держави, що почався останніми роками, пов’язаний із подоланням чималих труднощів соціально-економічного, державно-правового й іншого характеру. Однією з таких труднощів є злочинність, що багаторазово зросла останніми роками, з чим мусить борися як держава, так і суспільство. Цей напрямок став активно досліджуватися та розвиватися в науці державного управління щодо державної безпеки та охорони громадського порядку.

Аналіз останніх досліджень і публікацій. Проблема державного управління розвитком криміналістичних теорій і методів забезпечення державної безпеки й порядку, процесу розслідування злочинів, особливо в умовах «цифровізації», розглядалася як українськими, так і зарубіжними вченими, серед яких В. Бесчастний, С. Полторак, С. Домбровська, В. Шульгіна, О. Яковлев, H. Kujat [1;7;8; 9].

Виділення не вирішених раніше частин загальної проблеми. Поряд із тим недостатньо дослідженими залишаються особливості державного управління розвитком приватних криміналістичних теорій і вчень в умовах «цифровізації» для забезпечення безпеки держави.

Формулювання цілей статті. Метою статті є аналіз методів державного управління забезпеченням державної безпеки в умовах «цифровізації».

Виклад основного матеріалу. У сучасних умовах забезпечення державної безпеки та державне управління розвитком криміналістики зіштовхнулася з низкою викликів і загроз, таких, як «цифровізація» способів підготовки, здійснення й приховання злочинів, збільшення кількості злочинів, зроблених дистанційним способом, використання криптовалют у кримінальних взаєморозрахунках, зростання транскордонної злочинності й ін. Такі умови надають колосального імпульсу розвитку криміналістики. І цей розвиток, як уявляється, здійснюється у двох напрямках [2].

Перший напрямок – актуалізація наявних і розроблення нових криміналістичних технологій виявлення, розкриття, розслідування й попередження злочинів. Теорія криміналістичної ідентифікації як фундамент усієї науки криміналістики є однією з найбільш розроблених. Ще з 60-х рр. минулого століття аксіомою вважається існування 4-х видів криміналістичної ідентифікації: з матеріально фіксованих ознак; за ознаками загального походження; за описом ознак; за уявним образом. При цьому вирішення таких експертних завдань, як визначення взаємної відповідності інформації,

що втримується на різних електронних носіях, або визначення наявності на електронному носії інформації із заданими характеристиками, не уявляється можливим віднести до жодного з позначених вище видів криміналістичної ідентифікації. У зв'язку з цим є підстави стверджувати про наявність п'ятого виду ідентифікації – ідентифікації за електронним образом об'єкта [1].

Відмінність цього виду від раніше зазначених полягає в особливих фізичних властивостях ідентифікованого (шуканого) й ідентифікувального (що перевіряється) об'єктів, особливому (специфічному) наборі ідентифікувальних ознак, самостійній методичній і інструментальній базі подібних досліджень. Розвиток державного управління теорією криміналістичного прогнозування має випливати в напрямку розвитку можливостей прогнозування реалізації механізму здійснення одиничного, конкретного протиправного діяння. В основі подібного прогнозування мають перебувати насамперед закономірності передкримінальної поведінки суб'єкта злочину як елемента механізму його здійснення. При цьому «цифровізація» поповнює інструментарій криміналістики новими технологіями, що вже довели свою ефективність.

Назвемо окремі з них:

– метод систематизації інформації в мережі Інтернет за допомогою семантичних фільтрів;

– моніторинг відкритих ресурсів мережі Інтернет для виявлення й попередження інформаційних атак спеціалізованими центрами на об'єктах критичної інформаційної інфраструктури в межах державної системи виявлення, попередження й ліквідації наслідків комп'ютерних атак на інформаційні ресурси України.

Зазначені методи здатні надати теорії криміналістичного прогнозування «другого подиху», забезпечуючи цілеспрямовану діяльність органів попереднього розслідування, дізнання та їх посадових осіб із виявлення ознак

підготовлюваних злочинів. До забезпечення державного управління державною безпекою входить також і розвиток криміналістичного вчення про сліди, зумовленого тим, що сліди злочинів, здійснених з використанням інформаційно-комунікаційних технологій, вимагають розроблення принципово інших методів, засобів і технологій їх виявлення, фіксації й вилучення, оскільки вони через свою специфіку мають інформаційний характер, відбиваючи викликану розслідуваною подією зміну інформації, а не її носіїв, тобто матеріальних об'єктів.

Ось лише деякий перелік слідів, що дозволяють установити особу, яка здійснила злочин із використанням інформаційно-комунікаційних технологій: Ір-адреса комп'ютера в мережі, Мас-адреса мережного устаткування, адреса електронної пошти, ідентифікатор соціальної мережі, номер банківської карти, зроблені з нею транзакції, номер телефону, інформація про з'єднання абонента, інформація базових станцій мобільному зв'язку, дані систем геолокації тощо. Очевидно, що ці сліди не розглядаються в межах трасології, оскільки при їх створенні не відбувається контактної взаємодії об'єктів, а самі події відбуваються в результаті тих або інших змін у комп'ютерній інформації шляхом її створення, знищення, модифікації, копіювання, блокування [8] .

Сутність таких слідів полягає в тому, що вони, залишаючись на електронних носіях інформації, відбивають зміни в них інформації порівняно з вихідним станом. Відповідно криміналістичне вчення про сліди одержує свій розвиток, розробляючи технологію роботи з такою категорією криміналістичних об'єктів. Розвиток учення про криміналістичну реєстрацію зумовлене змінами об'єктів обліку, системи реєстрації, способів ведення обліків, упровадженням нових видів автоматизованих інформаційно-пошукових систем, удосконаленням технології одержання інформації (з різних джерел),

необхідної для ухвалення суб'єктами розслідування як процесуальних, так й організаційних рішень.

Як ми вже відзначали, виявлення, фіксація й вилучення електронних слідів злочину вимагає використання особливих криміналістичних технологій, розроблених у державі, удосконалення яких упродовж кількох років є винятково актуальним напрямком державного управління у сфері криміналістики. Сказане підтверджує поява самостійного підрозділу криміналістичної техніки – криміналістичного дослідження електронних носіїв інформації, спрямованого на забезпечення однакового підходу до роботи з такими об'єктами. До останніх слід віднести будь-які обладнання, конструктивно призначені для постійного або тимчасового зберігання інформації у вигляді, придатному для використання в електронних обчислювальних машинах, а також для її передання в інформаційно-телекомунікаційних мережах або оброблення в інформаційних системах.

До об'єктів криміналістичного дослідження електронних носіїв інформації, поза всяким сумнівом, належать і засоби рухливого радіотелефонного (мобільного) зв'язку з доступом до мережі Інтернет (смартфони), й інші інформаційно-комунікаційні обладнання, уключаючи планшетні комп'ютери. У зв'язку з наявністю в абсолютній більшості сучасних смартфонів модуля одержання геопросторової інформації, перспективним напрямком розвитку вищеназваного підрозділу криміналістичної техніки є й дослідження цих засобів навігації.

Крім перерахованих, до об'єктів криміналістичного дослідження електронних носіїв інформації належать: системи оброблення інформації або окремі функціональні обладнання таких систем; системні блоки персональних комп'ютерів, ноутбуків, нетбуків і т. ін.; машинні носії (накопичувачі на твердих і гнучких магнітних дисках, флеш-накопичувачі, карти пам'яті, оптичні диски й т.п.); уже згадані навігатори, трекери; мобільні телефони й сім-карти до

них; радіоелектронні обладнання; платіжні пластикові карти; плати ігрових автоматів; відеореєстратори та інше [7]. При цьому розширення спектра об'єктів криміналістичного дослідження електронних носіїв інформації супроводжується розвитком засобів отримання криміналістично значущої інформації з обладнань мобільного зв'язку, зокрема «Cellebrite UFED», «Мобільний криміналіст», «BelkasoftEvidenceCenterUltimate», «ElcomsoftMobileForensicBundle» й ін.

Активно розбудовуються технології штучного інтелекту, аналіз більших обсягів даних здатен бути відбитий у розвитку вчення про планування розслідування злочинів. У літературі висвітлено використання методів штучного інтелекту при вивченні особи серійних убивць. При цьому було створено самонавчальну нейронну мережу, що використовує певні характеристики відомих серійних убивць, уключаючи їх біологічні, соціальні й психологічні параметри. Розробляються й упроваджуються в практичну діяльність експертні правові системи підтримки ухвалення рішень. Такі системи вже практично застосовуються при розслідуванні розкрадань у будівництві, розслідуванні злочинів у сфері безпеки руху й експлуатації транспорту та ін.

Розбудовуються системи комп'ютерного моделювання при плануванні розслідування злочинів, а також програмні засоби управління проектами. Цей напрямок є особливо актуальним, оскільки дозволяє з використанням діаграм Ганта візуалізувати структуру переліку слідчих дій, інших процесуальних і непроцесуальних заходів, а також контролювати своєчасність завершення запланованих заходів на певний момент часу. Це дозволяє використовувати програми управління проектами не тільки для планування розслідування злочинів, але й для здійснення процесуального контролю над дотриманням строків розслідування, обрання запобіжний заходу в досудовому судочинстві.

Не викликає сумнівів обґрунтованість формування такого підрозділу криміналістичної тактики, як одержання інформації для доказування на електронних носіях. Цей підрозділ, як уявляється, зможе включати наукові положення й засновані на них рекомендації з проведення окремих слідчих й інших процесуальних дій, спрямованих на формування доказів на електронних носіях та їх використання в процесі доведення по кримінальній справі.

При цьому слід виокремити два напрямки розвитку криміналістичних знань.

Перший – створення правових підстав виникнення інформації як доказу. У цей час правові підстави виникнення інформації з кримінальних справ про злочини, зроблені з використанням інформаційних і комунікаційних технологій, утримуються в досить широкому масиві нормативно-правових актів різного рівня. Так, одержання інформації про рух грошових коштів на рахунках конкретних осіб ми одержуємо на підставі Закону України «Про банки й банківську діяльність». Обов'язок операторів зв'язку зберігати весь переданий абонентами контент (СМС, ММС, голосові повідомлення та ін.) регламентується Законом України «Про зв'язок». Обов'язок провайдерів ідентифікувати користувачів при наданні доступу в мережу Інтернет установлена Законом України «Про інформацію, інформаційні технології й захист інформації». Контроль за онлайн-платежами передбачено Законом України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму» [3-6]. Це лише кілька прикладів, що показують, як державне законодавство надає суб'єктам розслідування додатковий правовий інструментарій збирання інформації для доказу. Слід відзначити, що така ситуація наявна в будь-якій сфері державного управління, яка регульована нормами й правилами (транспорт, зв'язок, будівництво, енергетика і т. ін.).

Другий напрямок – удосконалення процесуальних засобів одержання інформації для доказування. Удосконалення технологічної основи вчення про фіксацію інформації здійснюється за рахунок таких нових технологій, як перетворення мовної інформації на письмову; прив'язка місцезнаходження об'єкта до геопросторових координат; визначення відстані між об'єктами з використанням лазерних далекомірів; технологія дублювання вмісту електронних носіїв у процесі копіювання й ін. Водночас досить широку дискусію в державно-управлінській науці викликає питання щодо можливості й порядку використання технології блокчейн для цілей фіксації інформації для доказу. Не намагаючись оцінювати переваги й недоліки подібної технології щодо зберігання великого обсягу матеріалів кримінальних справ, слід зазначити безсумнівну цінність процесуальної письмової форми як фундаментальної гарантії дотримання прав усіх учасників судочинства [9].

Висновки з даного дослідження. У зв'язку з цим є передчасним здійснення відмови від письмової форми карного судочинства на досудових стадіях, заклики до якого виникають у літературі. Доти, поки рівень проникнення цифрових технологій не дозволить повністю замінити власноручний підпис документів кожним учасником карного процесу, повний перехід з письмової форми на цифрову не є можливим, що не виключає при цьому «цифровізацію» окремих процесуальних дій: направлення й одержання запитів, доручень, довідок і т. ін.

Перспективи подальших розвідок. Вектором розвитку методики розслідування окремих видів злочинів є перероблення й доповнення приватних криміналістичних методик, побудованих без обліку електронних слідів злочинів. В основі такого перероблення мають бути універсальні алгоритми вирішення таких типових тактичних завдань для забезпечення державної безпеки, як установлення події злочину в цифровому середовищі; установлення особи, що скоїла злочин, за залишеними нею електронними слідами: Ір-адресі, Мас-адресі, адресі електронної пошти, ідентифікатори соціальної мережі, номера банківської карти, номера телефону, інформації про з'єднання абонента, зроблених транзакціях і т. ін.; установлення збитку й забезпечення його відшкодування; установлення обставин здійснення злочину; доведення винності особи в здійсненні злочину; установлення причин і умов здійснення злочину та ін. Таким чином, відповіддю державного управління розвитком науки криміналістики на загрози сучасності є інтеграція до чинних криміналістичних учень і теорій сучасних інформаційних технологій, а також структурних перетворень, розглянутих нами вище.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Бесчастний, В. М. Шляхи підвищення якості вищої освіти через впровадження інформаційно-комунікаційних технологій та формування інформаційної культури / В. М. Бесчастний // Розвиток продуктивних сил України: від В. І. Вернадського до

сьогодення : міжнар. наук. конф., 20 берез. 2009 р. : тези допов. : 3 ч. – К. : РВПС України НАН України, 2009. – Ч. 2. – С. 44–45.
2. Бесчастний, В. М. Підготовка керівників органів внутрішніх справ : інноваційний підхід / В. М. Бесчастний // Віче : Громадсько-політичний журнал. – 2007. – № 17. – С. 42–43.
3. Закон України «Про банки й банківську діяльність» [Електонний ресурс]. - Режим доступу : https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
4. Закон України «Про зв'язок» [Електонний ресурс]. - Режим доступу : https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
5. Закон України «Про інформацію, інформаційні технології й захист інформації» [Електонний ресурс]. - Режим доступу : https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
6. Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму»[Електронний ресурс]// Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
7. Полторак С. Т. Механізми формування безпеки держави [Електронний ресурс] / С. Т. Полторак, С. М. Домбровська // Теорія та практика державного управління і місцевого самоврядування : електронне наукове фахове видання ХНТУ. – 2015. – №1. – Режим доступу до журн. : http://el-zbirn-du.at.ua/2015_1/21.pdf
8. Шульгіна, В. Д. Розвиток національної освіти в Україні в умовах відкритого інформаційного простору / В. Д. Шульгіна, О. В. Яковлев // Професіоналізм педагога: матеріали Всеукр. наук.-практ. конф., присвяч. 60-річчю Крим. держ. гуманіт. ун-ту. – Ялта, 2004. − Ч. 1. – С. 78–82.
9. Kujat H. The Transformation of NATO's Military Forces And Its Links With US Transformation. Washington: SACLANT Seminar Paper, 2003 P. 1-2.

Statement of the problem. The process of revival of Ukraine as a strong and independent state is connected with overcoming the difficulties of socio-economic, state-legal nature. The criminality has greatly increased in recent years, with both the state and society being fought. This trend has been actively explored and developed in the science of public administration regarding state security and public order protection.

Urgency. The problem of state management of the development of forensic theories and methods of ensuring state security and order, the process of investigation of crimes, especially in the digitalisation, was considered by both Ukrainian and foreign scientists, but the peculiarities of state management of the development of private forensic theories are insufficiently investigated.

The purpose of the article is to analyze the methods of public administration of state security.

Our task was to study the directions of public administration of the private forensic theories and trainings development under conditions of digitalization for ensuring security of the state and society as a whole

Summary. The directions of public administration of the private forensic theories and trainings development under conditions of digitalization for ensuring security of the state and society as a whole are considered in the article. The tendencies of the identification theory development, the theory of forensic forecasting, the doctrine of traces, forensic tactics and methods of certain types of crimes investigation are also presented. Forensic knowledge, digitalisation, electronic image, electronic trace, all these directions of forensic-expert science development are intended to form a new direction regarding public administration of national security and public order protection.

It was determined that the vector of the methodology development of certain types of crimes investigation is the processing and supplementation of the private forensic methods, created without taking into account the electronic traces of crimes. This processing should be based on universal algorithms of solving such typical tactical tasks for ensuring national security as crime detection in the digital environment; identification of the person who committed the crime by the electronic traces left by this person: Ip-addresses, Mac-addresses, e-mail addresses, social networks identification, bank card number, telephone number, subscriber information, transactions made, etc.; ascertaining damage and ensuring compensation; defining the circumstances of a crime; proving a person is guilty in committing a crime; establishing the causes and conditions of the crime commitment, etc.

Conclusions and outcomes. Thus, the response of public administration of the forensic science development to the challenges and threats of the present is

integration into existing forensic teachings and theories of modern information technologies, as well as the structural transformations discussed above.