Особое внимание уделяется определению термина «геноцид» в соответствии с национальным и международным законодательством (определение срока рассматривается в Уголовном кодексе Украины и Конвенции о предупреждении преступления геноцида и наказании за него).

Исследуется процедура признания действий как геноцида (Голодомор 1932–1933 гг. в Украине; депортация из Крыма крымских татар в 1944 г.) и освещение таких событий международному сообществу.

Рассматривается процесс расследования геноцида с учетом срока совершения преступления, числа потерпевших лиц и нанесенного ущерба.

Ключевые слова: геноцид, Голодомор, депортация, процесс расследования, доказывания, уголовное производство.

Summary

Mykola Gerasymenko. Features of the investigation of genocide.

The article is devoted to the consideration of such a resonant crime as genocide. The purpose of the article is to form an idea of genocide as a crime, its investigation on the basis of analyzed regulations and investigations of this category of crimes.

Particular attention is paid to the definition of the term “genocide” in accordance with national and international law (the definition of the term is considered in the Criminal Code of Ukraine and the Convention on the Prevention and Punishment of the Crime of Genocide).

The procedure of recognizing acts as genocide (the Holodomor of 1932–1933 in Ukraine; deportation of Crimean Tatars from Crimea in 1944 as genocide of the Crimean Tatar people) and coverage of such events by the international community is studied.

The process of genocide investigation is considered, taking into account the term of the crime, the number of victims and the damage caused.

One of the most resonant crimes provided by the Law of Ukraine on Criminal Liability is genocide. The scale of this illegal act has aroused civil society for a long time, but only now, in the territory of independent Ukraine, it is possible to identify those responsible for the genocide and bring them to justice. It is impossible to ignore the fact that the investigation of genocide and the prosecution of those responsible for its commission is an extremely relevant process that requires special knowledge and skills in conducting an investigation. Officials who gather evidence in criminal proceedings, find persons involved in the crime and carry out other actions aimed at establishing the truth in the case, bear a huge burden of responsibility in the form of evidence.

The investigation process consists of a set of necessary investigative (search) actions and must meet the requirements for their conduct. It is necessary to involve in the investigation trained officers who have knowledge in this area and can clearly formulate a plan of investigative (search) actions, and move in this direction.

Key words: genocide, Holodomor, deportation, investigation process, evidence, criminal proceedings.

DOI: 10.36695/2219-5521.2.2020.78

УДК 343.13

О.В. ДЕГТЯРЬОВА

**Ольга Володимирівна Дегтярьова, аспірантка
Академії праці, соціальних відносин і туризму***

ORCID: 0000-0002-0510-1914

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Постановка проблеми. Впровадження інформаційних технологій в кримінально-процесуальну діяльність стало актуальним питанням, а їх застосування зумовило необхідність торкнутись тематики забезпечення інформаційної безпеки у кримінальних провадженнях. При розслідуванні проваджень особи, які проводять розслідування, користуються базами даних та вносять в ці бази інформацію, яка має бути надійно захищена. Інформація у кримінальних провадженнях потребує особливого захисту, оскільки є об'єктом посягання з боку заінтересованих осіб щодо її розкриття та передачі.

Забезпечення інформаційної безпеки полягає у створенні належних умов для зберігання, обробки та обміну інформацією, яка будь-яким чином належить до розслідування кримінального провадження. Втручання в діяльність органів досудового розслідування через інформаційні системи – це підрив принципу незалежності правоохоронної системи. Важливо не тільки боротись з несанкціонованим втручанням, а й посилити міру відповідальності за вчинення таких дій. Оскільки всі зібрані дані в межах кримінального провадження охороняються законом та є таємницею слідства.

Аналіз останніх досліджень та публікацій. Науковою основою даної статті стали праці таких українських науковців, як П.Д. Біленчук, М.І. Демура, Д.І. Клепка, І.О. Крицька, М.І. Малій, Г.В. Муляр, О.С. Ховпун, а також інших дослідників, які вивчали питання забезпечення інформаційної безпеки у кримінальних провадженнях. При цьому низка проблемних питань потребує розгляду та більш детального вивчення. Проблема забезпечення інформаційної безпеки стає більш актуальною через швидкий розвиток та застосування інформаційних технологій у розслідуванні кримінального провадження.

Виклад основного матеріалу. Перехід до інформаційного суспільства характеризується впровадженням інформаційних технологій у важливі частини суспільного життя, в тому числі процес розслідування

© О.В. Дегтярьова, 2020

* *Olha Dehtiarova, Postgraduate student of the Academy of Labor, Social Relations and Tourism*

кримінальних проваджень. У ході розслідування використання інформаційних технологій стало щоденною справою у діяльності слідчого, прокурора, оперативних підрозділів тощо. Службові особи, уповноважені на проведення розслідування, використовують інформаційні бази даних, де не виходячи зі службового кабінету мають змогу отримати потрібну інформацію. Саме таким чином можна внести дані про злочин, особу, яка його вчинила та інші відомості; перевірити повноваження адвоката; отримати відомості про нерухоме майно; провести допит в режимі відеоконференції тощо.

Законом України «Про інформацію» визначено захист інформації як сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї. Закон передбачає, що інформація є відкритою або з обмеженим доступом. Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація¹. Будь-яке втручання, розповсюдження інформації без належного дозволу передбачає притягнення до відповідальності.

Стратегією розвитку системи Міністерства внутрішніх справ України до 2020 р. визначено основні пріоритети своєї діяльності, серед яких: безпечне середовище розвитку вільного суспільства, забезпечення високої ефективності діяльності органів системи МВС, зміцнення суспільної довіри до неї з урахуванням визначальної ролі громадянина у розбудові України як безпечної європейської держави². Фактично пріоритетом діяльності є створення безпечного середовища, у тому числі забезпечення такої безпеки під час проведення розслідувань.

І.Г. Каланча, як теоретик та практичний працівник, у науковій статті «Інформаційна безпека електронного кримінального провадження України» (2018 р.) висловила думку, що «інформаційна безпека електронного кримінального провадження» – це стан захищеності інформаційного середовища електронного кримінального провадження (апаратного і програмного сегментів та суб'єктів кримінального провадження), що забезпечує його функціонування, формування, використання і розвиток для ефективного виконання завдань кримінального провадження. В свою чергу, І.Г. Каланча наголошує, що виникає потреба в комплексному забезпеченні інформаційної безпеки електронного кримінального провадження, що зумовлює актуальність дослідження цього питання³. В практичній діяльності переведення частин кримінального провадження в електронне стало кроком не тільки вдосконалення процесу розслідування, а й обміну інформацією в електронному вигляді. Саме тому збереження електронної інформації кримінального провадження набуло активного дискурсу.

Г.В. Муляр та О.С. Ховпун у своїй статті «Особливості доказування кіберзлочинів» (2019 р.) висловили позицію, що під час розслідування кіберзлочинів актуальним залишається питання проведення всебічного та швидкого досудового розслідування із вказаних кримінальних проваджень, збір та закріплення усіх необхідних доказів, збереження юридичних властивостей доказів та в подальшому встановлення наявності або відсутності вини особи. Значну увагу під час проведення досудового розслідування у кримінальному провадженні приділяють особливості доказування кіберзлочинів, встановлення механізму доказування та визначення джерел доказів⁴. Доцільно вказати, що популяризовано такий вид доказів, як електронні, а саме: їх закріплення та передачу органу досудового розслідування з метою приєднання до матеріалів провадження. Збереження інформації в електронному вигляді значно спростить роботу органу досудового розслідування, але й виникне новий вид несанкціонованого втручання в їх роботу через інформатизовані системи баз даних.

П. Біленчук та М. Малій у своїй роботі «Новітні засоби захисту інформації в процесі електронного кримінального провадження» (2019 р.) розглянули забезпечення захисту у кримінальному провадженні та приділили особливу увагу ідентифікації особистості користувача. Науковці дійшли висновку, що серед чотирьох основних способів ідентифікації особистості користувача в процесі електронного кримінального провадження (за предметом, яким володіє людина; за паролем або особистим ідентифікаційним кодом, який вводиться в електронно-обчислювальну машину з клавіатури; за фізичними характеристиками особистості, притаманними індивідуально лише їй; за електронним цифровим підписом) найбільш перспективними та надійними вважаються останні два способи⁵. Питання ідентифікації особистості користувача нерозривно пов'язано з забезпеченням інформаційної безпеки у кримінальних провадженнях.

М.І. Демура, Д.І. Клепка, І.О. Крицька в науковій статті «Забезпечення прав та законних інтересів особи в умовах «діджиталізації» кримінального провадження» (2020 р.) висловили думку, що впровадження інформаційних технологій зумовлює так само виникнення нових перепон і під час здійснення досудового розслідування, оскільки суттєво ускладнюються процедура та можливості встановлення й доказування ознак таких кримінальних правопорушень (можливість видалення повідомлень у Telegram, Viber). У зв'язку з цим доводиться констатувати, що норми чинного кримінального процесуального законодавства відрізняються певною архаїчністю щодо новітніх проявів протиправних дій у мережі, оскільки містять загальні правила захисту прав та законних інтересів особи від загроз у реальній дійсності, при цьому не враховуючи можливість вчинення кримінальних правопорушень в Інтернет-просторі. А тому традиційні методи запобігання та боротьби з кримінальними правопорушеннями не завжди є дієвими; до того ж труднощі можуть виникати і на етапі встановлення факту вчинення правопорушення⁶. Ми погоджуємось з думкою науковців про необхідність врахування того факту, що злочинці з кожним днем стають більш вигадливими у вчиненні злочинів, а тому необхідно застосовувати не тільки новітні методи розслідування, а й забезпечувати такий інформації належний захист.

Розслідування кримінального провадження розпочинається з внесення відомостей до Єдиного реєстру досудових розслідувань. Вхід до системи здійснюється за допомогою електронного ключа та введення паролю з метою доступу до бази даних. У разі отримання такого ключа та паролю доступу може відбутись несанкціонований доступ (проникнення) до системи, відповідно дані можуть бути видалені, спотворені, втрачені або розголошені. Згідно зі ст. 214 Кримінально-процесуального кодексу України (далі – КПК) після подання

заяви про злочин слідчий/прокурор зобов'язані зареєструвати таку заяву, при цьому всі можливі відомості, які містить заява, внести до Реєстру. До Реєстру вносять: дату заяви, коротку фабулу злочину, правову кваліфікацію та інші відомості, які передбачені КПК⁷.

Після початку розслідування до Реєстру можуть вноситись відомості про особу, яка вчинила злочин (повідомлення про підозру, зміну підозри, нову підозру); відомості про затримання особи; дані щодо розшуку; інформацію про об'єднання, виділення матеріалів; завдані збитки; запобіжний захід; інші відомості. Реєстр містить величезну кількість персональних даних громадян, які не можуть бути оприлюднені, передані, спотворені або виключені з бази даних. Інформація, яка вноситься уповноваженою службовою особою до Реєстру, має статус слідчої таємниці, оскільки стосується проведеного розслідування.

У Положенні про порядок ведення Єдиного реєстру досудових розслідувань міститься розділ про захист відомостей, внесених до Реєстру, який необхідно розширити, а захисту інформаційної безпеки приділити особливу увагу.

Положенням передбачено, що адміністратор здійснює комплекс програмних, технологічних та організаційних заходів щодо захисту відомостей, які містяться у Реєстрі, від несанкціонованого доступу; адміністратор за кожним фактом втрати або пошкодження Реєстратором електронного ключа доступу невідкладно вживає заходів до його блокування та повідомляє про це Держателя Реєстру; адміністратор негайно інформує відповідного керівника прокуратури та органу досудового розслідування про намагання Реєстратора отримати інформацію за межами наданого йому доступу (Розділ IV)⁸. Необхідно посилити заходи щодо збереження відомостей, які вносяться до Реєстру. Особа, яка підтримує належний рівень інформаційної безпеки, має володіти знаннями у галузі інформаційних технологій та постійно підвищувати свій професійний рівень.

Висновки. Важливо зазначити, що впровадження інформаційних технологій зумовило виникнення електронного кримінального провадження. У свою чергу, розслідування такого кримінального провадження передбачає застосування заходів щодо збереження інформації. Інформаційна безпека у кримінальному провадженні – це захищеність інформаційного середовища електронного кримінального провадження за допомогою засобів та методів збереження інформації, що забезпечує належне функціонування кримінального провадження та сприяє виконанню його завдань.

Основною базою даних, що може зазнати посягання в процесі розслідування, є Єдиний реєстр досудових розслідувань, який містить інформацію про повідомлення особі про підозру, зміну підозри, нову підозру; затримання особи; дані щодо розшуку; інформацію про об'єднання, виділення матеріалів; завдані збитки; запобіжний захід; інші значимі дані, які можуть стати відомі органу досудового розслідування. Інформація такого характеру має бути надійно захищена від впливу інших осіб та маніпулювання даними, тому слід забезпечити інформаційну безпеку. Існує ймовірність, що дані можуть бути видалені, спотворені або знищені, що надасть змогу особам, які вчинили злочин, уникнути відповідальності.

¹ Про інформацію: Закон України. *Відомості Верховної Ради України (ВВР)*. 1992. № 48. Ст. 650. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>

² Стратегія розвитку системи Міністерства внутрішніх справ України до 2020 р. URL: <https://cyberpolice.gov.ua/strategy-2020>

³ Каланча І.Г. Інформаційна безпека електронного кримінального провадження України. *Науковий часопис Національної академії прокуратури України*. 2018. № 3. С. 11–22.

⁴ Муляр Г.В., Ховпун О.С. Особливості доказування кіберзлочинів. *Право. Людина. Довкілля: наук.-практ. журнал* 2019. Т. 10. № 3. С. 132–138. URL: <http://journals.nubip.edu.ua/index.php/Pravo/article/view/law2019.03.017/11129>

⁵ Біленчук П., Малій М. Новітні засоби захисту інформації в процесі електронного кримінального провадження: матеріали круглого столу (25 липня 2019 р.). Київ: Національна академія прокуратури України, 2019. 56 с.

⁶ Демура М.І., Клепка Д.І., Крицька І.О. Забезпечення прав та законних інтересів особи в умовах «діджиталізації» кримінального провадження. *Часопис Київського університету права*. 2020. № 1. С. 295–301. URL: http://kul.kiev.ua/images/A/Chasopis/CHAS20_1.pdf

⁷ Кримінальний процесуальний кодекс України. *Відомості Верховної Ради (ВВР)*. 2013. № 9–10, № 11–12, № 13. Ст. 88. URL: <https://zakon.rada.gov.ua/laws/show/4651-17#n5941>

⁸ Положення про порядок ведення Єдиного реєстру досудових розслідувань: наказ Генеральної прокуратури України від 06.04.2016 р. № 139. URL: <https://zakon.rada.gov.ua/laws/show/z0680-16#Text>

Резюме

Дегтярьова О.В. Забезпечення інформаційної безпеки у кримінальному провадженні.

У науковій статті розглядається питання захисту інформації під час розслідування кримінальних проваджень, забезпечення інформаційної безпеки. Досліджується позиція наукових та практичних працівників щодо забезпечення інформаційної безпеки на стадії досудового розслідування кримінальних проваджень.

Аналізуються положення Закону України «Про інформацію», Стратегії розвитку системи Міністерства внутрішніх справ України до 2020 р., Положення про порядок ведення Єдиного реєстру досудових розслідувань щодо забезпечення інформаційної безпеки у провадженнях.

Ключові слова: інформація, інформаційні технології, кримінальне провадження, забезпечення безпеки, інформаційна безпека.

Резюме

Дегтярева О.В. Обеспечение информационной безопасности в уголовном производстве.

В научной статье рассматривается вопрос защиты информации при расследовании уголовных производств, обеспечение информационной безопасности. Исследуется позиция научных и практических работников по обеспечению информационной безопасности на стадии досудебного расследования уголовных производств.

Анализируются положения Закона Украины «Об информации» Стратегии развития системы Министерства внутренних дел Украины до 2020 г., Положение о порядке ведения Единого реестра досудебных расследований по обеспечению информационной безопасности в производствах.

Ключевые слова: информация, информационные технологии, уголовное производство, обеспечение безопасности, информационная безопасность.

Summary

Olha Dehtiarova. Ensuring information security in criminal proceedings.

The scientific article considers the issue of information protection during the investigation of criminal proceedings, information security. The position of researchers and practitioners on information security at the stage of pre-trial investigation of criminal proceedings is studied.

The provisions of the Law of Ukraine «On Information», the Strategy for the Development of the System of the Ministry of Internal Affairs of Ukraine until 2020, the Regulations on the Procedure for Maintaining the Unified Register of Pre-trial Investigations to Ensure Information Security in Proceedings are analyzed.

The introduction of information technology in criminal procedure has become an urgent issue, and their application has necessitated the need to address the issue of information security in criminal proceedings. When investigating proceedings, the investigators use databases and enter into these databases information that must be securely protected. Information in criminal proceedings needs special protection, as it is subject to encroachment by interested parties on its disclosure and transmission.

Ensuring information security is to create appropriate conditions for the storage, processing and exchange of information that in any way relates to the investigation of criminal proceedings. Interference in the activities of pre-trial investigation bodies through information systems is an undermining of the principle of independence of the law enforcement system. It is important not only to combat unauthorized interference, but also to increase the degree of responsibility for such actions. Because all data collected in criminal proceedings are protected by law and are a secret of the investigation.

Information security in criminal proceedings is the protection of the information environment of electronic criminal proceedings with the help of means and methods of information storage, which ensures the proper functioning of criminal proceedings and facilitates the implementation of its tasks.

Key words: information, information technologies, criminal proceedings, security, information security.

DOI: 10.36695/2219-5521.2.2020.79

УДК 343.97, 343.35

В.М. КАБАЄВ

Віталій Миколайович Кабаєв, аспірант Київського університету права НАН України*

ORCID: 0000-0002-6966-8354

ОСОБЛИВОСТІ ОБ'ЄКТИВНИХ ОЗНАК ЗЛОЧИНІВ, ВЧИНЕНИХ СЛУЖБОВИМИ ОСОБАМИ, ЯКІ ЗАЙМАЮТЬ ОСОБЛИВО ВІДПОВІДАЛЬНЕ СТАНОВИЩЕ

Постановка проблеми. Правильна кваліфікація кримінальних правопорушень, що вчиняють службові особи, які займають особливо відповідальне становище, є однією із важливих та, на жаль, невирішених проблем становлення України як демократичної та правової держави. Це насамперед пов'язано з тим, що часто вчинення цих злочинів залишається безкарним у зв'язку із так званим політичним імунітетом осіб, які їх вчиняють, або внаслідок неможливості проведення повного та неупередженого розслідування правоохоронними органами. Однак шкода, що заподіюється такими злочинами, полягає не тільки і не стільки у матеріальних втратах, а й у порушенні законних прав та інтересів людей, виникненні недовіри до державних органів, зокрема, правоохоронних та судових. Питання про кваліфікацію злочинів полягає насамперед у встановленні усіх елементів складу злочину, серед яких об'єктивні ознаки є обов'язковим та важливим аспектом.

Об'єктивні ознаки будь-якого злочину – це передусім об'єкт та об'єктивна сторона злочину. Саме ці елементи складу кримінальних правопорушень, що вчиняють службові особи, які займають особливо відповідальне становище, будуть розглянуті нижче. Вчення про об'єкт злочину – це наріжний камінь вітчизняної кримінально-правової науки, проте, як не парадоксально, саме з приводу цього питання найменшу єдність поглядів виявляють його дослідники. Безумовно, всі згодні, що об'єкт злочину – це те, на що посягає злочинне діяння, чому воно заподіює або може заподіяти шкоду. Але на цьому всяка єдність і закінчується. Питання ж про те, чому саме злочинне діяння заподіює або може заподіяти шкоду, є одним із найбільш спірних у науці.

Аналіз останніх досліджень та публікацій. Питання кримінальної відповідальності службових осіб, поняття службової особи неодноразово висвітлювалися в літературі. Значний внесок у вивчення окреслених проблем зробили П.П. Андрушко, О.Ф. Бантишев, Л.П. Брич, В.Д. Вознюк, Н.О. Гуторова, О.О. Дудоров, М.І. Хавронюк, М.Й. Коржанський, О.М. Костенко, Д.І. Крупко, В.С. Лукомський, В.О. Навроцький та інші

© В.М. Кабаєв, 2020

* Vitalii Kabaiev, Postgraduate student of Kyiv University of Law of the NAS of Ukraine