UDC 343.98
DOI https://doi.org/10.32849/2663-5313/2023.5.16

Valerii Sysoliatin,
External Postgraduate Student, Scientific Institute of Public Law, 2a, H. Kirpa street, Kyiv, Ukraine, postal code 03055, valerii_sysoliatin@ukr.net
ORCID: *orcid.org/0000-0003-3228-8845*

Sysoliatin, Valerii (2023). Problematic aspects of the initial stage of investigation of criminal offences related to using Internet banking. *Entrepreneurship, Economy and Law, 5*, 108–113, doi https://doi.org/10.32849/2663-5313/2023.5.16

PROBLEMATIC ASPECTS OF THE INITIAL STAGE OF INVESTIGATION OF CRIMINAL OFFENCES RELATED TO USING INTERNET BANKING

Abstract. ***Purpose.*** The purpose of the article is to study the initial stage of investigation of criminal offences related to using Internet banking. ***Results***. The article focuses on certain aspects of the investigation of criminal offences related to using Internet banking. The article examines the initial stage of investigation of a certain category of unlawful acts. It is noted that at the initial stage of investigation there are numerous investigative (search) actions, CISA and other procedural actions, as well as search activities that should be carried out in any case. Of course, they should be correlated with the specific unlawful act committed. In particular, during a murder investigation, this includes examination of the corpse and its expertise to establish the circumstances and mechanism of death; theft – examination of the scene to determine the mechanism of the unlawful act and identify material evidence; fraud – interrogation of the victim to determine the method of its commission, etc. During the investigation of criminal offences related to using Internet banking, there shall be mandatory procedural steps to ensure an adequate evidence base. ***Conclusions.*** It is established that the initial stage accumulates the procedural actions necessary for the maximum collection of evidence at the beginning of criminal proceedings. The article identifies the forensic versions that are put forward at the initial stage of the investigation: a criminal offence related to using Internet banking for obtaining material gain by a "hacker" or an employee of a certain institution with skills in working with computer equipment, or for the purpose of obtaining restricted information by a person who has free access to certain computer equipment. It is established that during the investigation of the category of unlawful acts under study, it is necessary to ensure the maximum preservation of information stored on flash drives, hard drives, cache memory of the relevant device, cloud storage, etc.

Key words: criminal offences, Internet banking, cybercrime, initial stage of investigation, investigative (search) action, version.

1. Introduction

At the initial stage of investigation there are numerous investigative (search) actions, CISA and other procedural actions, as well as search activities that should be carried out in any case. Without doubt, they should be correlated with the specific unlawful act committed. In particular, during a murder investigation, this includes examination of the corpse and its expertise to establish the circumstances and mechanism of death; theft – examination of the scene to determine the mechanism of the unlawful act and identify material evidence; fraud – interrogation of the victim to determine the method of its commission, etc. During the investigation of criminal offences related to using Internet banking, In addition, there are also mandatory procedural steps that shall be taken prior to entering information into the URPI and immediately thereafter to ensure a proper evidence base.

An important contribution to the development of criminal investigation has been made by scholars such as Yu.P. Alenin, V.P. Bakhin, A.V. Ishchenko, B.Ye. Lukianchykov, Ye.D. Lukianchykov, S. Yu. Petriaiev, V.V. Piaskovskyi, M.V. Saltevskyi, R.L. Stepaniuk, V.V. Tishchenko, K.O. Chaplynskyi, Yu.M. Chornous, V.Yu. Shepitko, and others. However, our study specifies certain positions of the initial stage of investigation in criminal proceedings of this category, with regard to the current forensic practice and perspectives of scholars.

The purpose of the article is to study the initial stage of investigation of criminal offences related to using Internet banking.

2. Particularities of the initial stage of investigation of criminal offences

Considering the initial stage of the investigation, we refer to the thesis by S.V. Velikanov, who states that: "The element of "the investiga-

tion stage" as a component of spatial and temporal localisation has the following meanings: "primary", "subsequent", "final"; the element "professional qualities of the person conducting the investigation" – "highly competent", "competent", "insufficiently competent", "incompetent", etc; the element "consequences of the crime" is composite, and depending on the type of crime under investigation, it changes its structure, including various linguistic variables, for example, when investigating lucrative crimes, its part, such as the linguistic variable "damage caused", has the following meanings "significant", "large", "especially large". Therefore, depending on the situation, linguistic variables take on appropriate meanings. The set of such meanings is individual in each case" (Velikanov, 2002). According to O.S. Sainchin, there are initial, subsequent and final stages of investigation. In addition, the author indicates that the initial stage of the investigation begins from the moment when signs of a criminal offence are found. The scholar also notes that this stage lasts until the person suspected of committing the offence is identified and the degree of his/her guilt is determined, and the issue of serving a notice of suspicion is resolved (Sainchyn, 2018). As we can see, different researchers define the names of the "primary-initial" stages in different ways. But the difference in name does not change their content. In our work, we have decided to use the terms "initial" and "following" stages of the investigation.

With regard to the initial stage of criminal proceedings, we consider it appropriate to cite the perspective of V.V. Tishchenko that the following tasks are implemented during it, namely: "1. Identify and record evidentiary information regarding the crime being investigated in hot pursuit. 2. Take measures to prevent the loss of evidential information contained in traces, documents, other objects, its timely detection and recording. 3. Clarify and assess the investigative situation after the initiation of a criminal case. 4. Identify sources of information about the crime under investigation. 5. Determine the direction of the investigation and development of an investigation plan. 6. Choose the form and methods of interaction with the bodies and services that carry out operative-search work. 7. Search and obtain information about the mechanism and environment of the crime. 8. Collect and study information about the victim's identity. 9. Search for, obtain and analyse information about the perpetrators of the offence, their search and detention" (Tishchenko, 2007, p. 137).

According to O.M. Dufeniuk, the initial stage of the investigation involves "...collecting and evaluating primary information, establishing the presence or absence of signs of a criminal offence in the act of a person (persons) or in an event (fact) that occurred; making a decision to enter information into the URPI and initiate a pre-trial investigation; conducting urgent investigative (search) actions; taking measures to solve a criminal offence in "hot pursuit"; determining the directions of investigation; formulating initial versions. At the initial stage, we can state the existence of an investigative situation, which will determine the sequence of certain procedural actions, procedural decisions, and other measures. The forensic situation that exists before the start of criminal proceedings usually has a small amount of evidential information. Therefore, the main task of the initial stage of the pre-trial investigation is an intensive process of collecting (identifying, recording, seizing, storing) evidence" (Priakhin, 2016).

Another group of scholars (O.V. Uzunova, K.V. Kaliuha), based on their own research, concludes that "...the initial stage of the investigation is characterised by uncertainty due to lack of information and its incompleteness, so the dominant activity of the investigator at this stage is identification of the necessary evidentiary and tactical information and its carriers (sources). This task is solved with due regard to the current investigative situation by conducting a set of investigative, other procedural and organisational actions. Frequently, the ground for conducting investigative actions is a forensic version. The main task of the initial stage is usually to identify the person involved in the commission of the crime. Therefore, the collection of information about the person begins with a retrospective study of the traces left at the crime scene, in the memory of eyewitnesses, etc. The information obtained is used to put forward versions of the perpetrator of the crime, to determine the direction of the search" (Uzunova, Kaliuha, 2018). Relying on the above statements, we can conclude that the initial stage accumulates the procedural actions necessary to maximise the collection of evidence at the beginning of criminal proceedings.

With regard to the initial stage of investigation of criminal offences related to using Internet banking, for example, a separate group of scholars (B.Ye. Lukianchykov, S.Yu. Petriaiev) states that reports of unauthorised intrusion into a computer system or computer network are more often received from users who have discovered such a fact. The authors emphasise that this happens when a computer starts reporting false data, there are frequent crashes, some or all useful information is destroyed, and customers of the computer network complain. In addition, scientists emphasise that these may be signs of illegal actions: unauthorised entry

or use of malware or violation of operating rules. Moreover, forensic scientists suggest the following possibilities for putting forward and processing the following typical versions of the initial stage of the investigation: "...1) a computer crime is committed for the purpose of obtaining material benefit: a) by an employee of the institution with skills in working with computer equipment; b) by a group of persons by prior conspiracy or an organised group with the participation of an employee of the institution; c) by a group of persons without the participation of employees of the institution, one of the perpetrators has skills in working with computer equipment; 2) the crime is committed for the purpose of obtaining restricted information: a) by a person (persons) who has free access to computer equipment; b) by a person (persons) who does not have free access to computer equipment; 3) the crime is committed with the purpose of preparing for the theft of material assets: a) by a person (persons) who has free access to computer equipment; b) by a person (persons) who does not have free access to computer equipment; 4) the crime is committed with the purpose of copyright infringement: a) by a person(s) having free access to computer equipment; b) by a person(s) not having free access to computer equipment; 5) the crime is committed with the purpose of violating the algorithm of information processing, destruction or damage of computer programmes and databases, as well as their carriers: a) by a person who has access to computer equipment; b) by a person who does not have access to computer equipment; c) destruction or violation of the algorithm of information processing occurred as a result of a failure or malfunction in an automated system and is not a computer crime" (Lukianchykov, Lukianchykov, Petriaiev, 2017, p. 473). In support of this position, relying on the analysed criminal proceedings, we will try to determine the forensic versions that are put forward at the initial stage of the investigation:

– a criminal offence related to using Internet banking for obtaining material gain by a "hacker";

– a criminal offence related to using Internet banking committed for obtaining material gain by an employee of a certain institution with skills in working with computer equipment;

– a criminal offence related to using Internet banking for obtaining restricted information by a person (persons) who has free access to certain computer equipment;

– a criminal offence related to using Internet banking for obtaining restricted information by a person who does not have free access to certain computer equipment;

– a criminal offence related to using Internet banking for violating the data processing algorithm, destroying or damaging computer programmes and databases, as well as their carriers.

3. Investigation of criminal offences related to using Internet banking

D.V. Pashniev and M. H. Shcherbakovskyi describe the following tactical tasks. For example, the researchers emphasised the need to establish the following facts: the place of unlawful penetration into a computer network (from within the organisation or from outside); the method of unlawful access (copying, modification, destruction of information, introduction of malware) and its results; means used to commit the crime (hardware, software, data storage media); ways to overcome security (selection of keys and passwords, password theft, disabling security means, etc.); detection of traces of an unlawful act. In addition, the authors argue that the following priority investigative (search) actions should be taken to implement the above tasks: "...inspection of the scene (if it was not carried out before the criminal proceedings were commenced), interrogation of witnesses (staff of the organisation where the offence was detected) and the victim, appointment of a computer-technical examination. Then, procedural decisions are made on temporary access to documents and measures to identify and search for the perpetrator, search for his workplace from where the computer (computer system) was intruded. Forensic records are checked to obtain data that enables conclusions to be drawn about the involvement of a particular person in a crime, the commission of several crimes in one way, etc. On this ground, CISA may be conducted (audio and video control of a person – Article 260 of the CPC, arrest, inspection and seizure of correspondence – Articles 261–262 of the CPC, removal of information from transport telecommunication networks and electronic information systems – Articles 263–264 of the CPC, surveillance of a person, thing or place – Article 269 of the CPC, audio and video control of a place – Article 270 of the CPC, etc." (Volobuiev, Stepaniuk, Maliarova, 2018).

For their part, V.V. Kornienko and V.I. Strelianyi argue that the head of the investigative team shall prepare in advance for the conduct of investigative (search) actions. According to scholars, it is worthwhile to carefully examine, for example, the bank's geographical location, determine whether the bank is located in a built-in, attached, or detached building, examine entrances and exits (main and backup), and the number of locations of currency exchange offices. In addition, the authors state

that it is necessary to clearly identify "...the location of the bank's internal premises: vault; special cash desk; recounting cash desk; night cash desk; operating room; automated information processing centre (computer server centre, archiving, Bank-Client modem); premises where individual safes for storing valuables are located; offices of the bank's management, chief accountant (to know which offices have computers that are connected to the network); utility rooms, especially rooms in front of vaults (they should be inspected thoroughly); warehouses" (Korniienko, Strelianyi, 2015).

According to O.V. Kurman, unlawful interference with the operation of electronic computers and computer networks is possible under the following conditions: "...1) the owner of the information should determine the conditions and rules for obtaining and processing information; 2) the owner of computers, automated systems, computer networks or telecommunication network operator should develop measures to protect information in the system; 3) the owner of computers, systems and network operators should develop rules for the system; 4) the owner (operator, provider) of the system and the owner of the information should conclude an agreement on the protection of information in the system; 5) the offender has performed at least one of the following operations, in particular: collection, input, recording, reading, storage, destruction, registration, acceptance, receipt, transmission of information" (Kurman, 2017, p. 247).

In the context of our study, we consider the position of D.V. Pashnev and M.G. Shcherbakovsky to be relevant, as they state that "upon arrival at the scene, the investigator shall take such preventive measures that ensure the integrity and immutability of information on computer carriers: – protect and secure the premises where the computer equipment is located; – keep people away from the equipment and power sources; – identify the state of the computer equipment (switched off or on); – make sure that under no circumstances will the switched-off computer be switched on. During the inspection (search), the specialist directly assists the investigator: – in identifying computer equipment, its individual components, documentation and other objects that may contain traces of illegal actions; – in disconnecting computer equipment from the power supply correctly (from the point of view of preserving traces of the crime); – in describing the computer equipment, its individual components and documentation to be seized, in the protocol and annexes thereto; – in deciding on the composition of the computer equipment or its individual components to be seized or isolated from free access; – in preparing the computer equipment for transportation (packing, sealing)" (Volobuiev, Stepaniuk, Maliarova, 2018). Indeed, during the investigation of the category of unlawful acts under study, it is necessary to ensure the maximum preservation of information stored on flash drives, hard drives, cache memory of the relevant device, cloud storage, etc.

Therefore, we support the opinion of V.V. Korniienko and V.I. Strelianyi, who determined the following procedure for the work of the investigative team: "1) thoroughly study the plan of the bank's premises with the location of all internal offices; 2) if necessary, ensure the protection of main and emergency entrances and exits; 3) review the documents defining the bank's organisational structure, regulations on management (departments), an order on the distribution of duties between the management, and a licence to conduct operations issued by the NBU; 4) ensure the presence of bank officials and, in some cases, representatives of the NBU. During investigative actions, it is necessary to: 1) ensure the presence of employees at their workplaces (no employee should be allowed to leave the workplace); 2) closely monitor cashiers (the location of their personal belongings); 3) control the actions of employees of the automated information processing centre, preventing them from conducting transactions at the time of the investigation, as well as of all employees working on computers connected to the network; 4) inspect the bank's premises to identify computer equipment that may be "illegally" operating on behalf of a fictitious company; 5) monitor telephone communications, as a bank employee can give an order to debit funds from any account of a banking institution or enterprise; 6) ensure external surveillance of the bank and internal security of the main and backup entrance and exit, ensuring that only those who wish to enter the bank can do so; 7) during the inspection of the operating room, quickly identify fictitious firms using a printout based on the following signs: firms with high turnover that have started operating recently (from 1–3 days to 2–3 months). After identifying the director and chief accountant of these firms, determine whether the data held by the bank matches the address bureau (whether the documents presented when opening the account were previously lost or stolen). Check whether the company is located at the legal address according to the bank documents. 8) in case of suspicion, it is necessary to immediately stop the movement of non-cash funds in terms of conducting expenditure transactions on bank accounts (current, settlement, deposit) simultaneously for all departments" (Korniienko, Strelianyi, 2015, p. 49).

4. Conclusions

To sum up, the initial stage accumulates the procedural actions necessary for the maximum collection of evidence at the beginning of criminal proceedings. The article identifies the forensic versions that are put forward at the initial stage of the investigation: a criminal offence related to using Internet banking for obtaining material gain by a "hacker or an employee of a certain institution with skills in working with computer equipment, or for the purpose of obtaining restricted information by a person who has free access to certain computer equipment or does not have such access; a criminal offence committed for the purpose of violating the data processing algorithm, destroying or damaging computer programmes and databases, as well as their carriers. It is established that during the investigation of the category of unlawful acts under study, it is necessary to ensure the maximum preservation of information stored on flash drives, hard drives, cache memory of the relevant device, cloud storage, etc.

References:

Korniienko, V.V., Strelianyi, V.I. (2015). Orhanizatsiia rozsliduvannia faktiv nesanktsionovanoho perekazu koshtiv z rakhunkiv kliientiv banku, yaki obsluhovuiutsia za dopomohoiu system dystantsiinoho obsluhovuvannia [Organization of the investigation of the facts of unauthorized transfer of funds from the accounts of bank clients, which are serviced using remote service systems]. Kharkiv: Kharkivskyi natsionalnyi universytet vnutrishnikh sprav [in Ukrainian].

Kurman, O.V. (2017). Sposoby nesanktsionovanoho vtruchannia v robotu informatsiinykh (avtomatyzovanykh), elektronnykh komunikatsiinykh, informatsiino-komunikatsiinykh system, elektronnykh komunikatsiinykh merezh [Ways of unauthorized interference in the work of information (automated), electronic communication, information and communication systems, electronic communication networks]. *Pravo i suspilstvo*. no. 4. pp. 245–249 [in Ukrainian].

Lukianchykov, B.Ie., Lukianchykov, Ye.D., Petriaiev, S.Iu. (2017). Kryminalistyka [Forensics]. Kyiv : Natsionalnyi tekhnichnyi universytet Ukrainy "Kyivskyi politekhnichnyi instytut im. Ihoria Sikorskoho" [in Ukrainian].

Priakhin, Ye.V. (red.). (2016). Kryminalistyka [Forensics]. Lviv : LvDUVS [in Ukrainian].

Sainchyn, O.S. (2018). Slidchi sytuatsii ta alhorytmy dii v metodytsi rozsliduvannia seriinykh vbyvstv [Investigative situations and action algorithms in the methodology of investigating serial murders]. *pravoznavec.com.ua*. Retrieved from http://www.pravoznavec.com.ua/period/article/22719/%CE [in Ukrainian].

Tishchenko V.V. (2007). Teoretychni i praktychni osnovy metodyky rozsliduvannia zlochyniv [Theoretical and practical foundations of crime investigation methodology]. Odesa : Feniks [in Ukrainian].

Uzunova, O.V., Kaliuha, K.V. (2018). Problemy pryiomiv analizu otrymanoi z mistsia podii informatsii ta obgruntuvannia prypushchen stosovno osoby zlochyntsia [Problems of methods of analysis of information obtained from the scene of the incident and substantiation of assumptions regarding the identity of the criminal]. *pravoznavec.com.ua*. Retrieved from http://bo0k.net/index.php?bid=18860&chapter=1&p=achapter [in Ukrainian].

Velikanov, S.V. (2002). Klasyfikatsiia slidchykh sytuatsii v kryminalistychnii metodytsi [Classification of investigative situations in forensic methodology]. *Extended abstract of candidate's thesis*. Kharkiv: Natsionalna yurydychna akademiia Ukrainy imeni Yaroslava Mudroho [in Ukrainian].

Volobuiev, A.F., Stepaniuk, R.L., Maliarova, V.O. (red.). (2018). Kryminalistyka [Forensics]. Kharkiv: Kharkiv. nats. un-t vnutr. sprav. [in Ukrainian].

Валерій Сисолятін,
здобувач, Науково-дослідний інститут публічного права, вул. Г. Кірпи, 2а, Київ, Україна, індекс 03035, valerii_sysoliatin@ukr.net
ORCID: *orcid.org/0000-0003-3228-8845*

ПРОБЛЕМНІ АСПЕКТИ ПОЧАТКОВОГО ЕТАПУ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ ІЗ ВИКОРИСТАННЯМ ІНТЕРНЕТ-БАНКІНГУ

Анотація. ***Мета.*** Метою статті є дослідження початкового етапу та окремих аспектів розслідування кримінальних правопорушень, пов'язаних з використанням інтернет-банкінгу. ***Результати.*** Зазначено, що на початковому етапі розслідування є досить багато слідчих (розшукових) дій, НСРД та інших процесуальних дій, а також розшукових заходів, які варто провести в будь-якому випадку, корелюючи їх у відповідності до конкретного протиправного діяння, яке було вчинено. Зокрема, під час розслідування вбивства – це огляд трупа та його експертиза для встановлення обставин та механізму смерті особи; крадіжки – огляд місця події для з'ясування механізму вчинення протиправного діяння та виявлення матеріальної доказової інформації; шахрайства – допит потерпілого для визна-

чення способу його вчинення тощо. У розслідуванні кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, наявні обов'язкові процесуальні дії для забезпечення належної доказової бази. ***Висновки.*** Встановлено, що початковий етап акумулює процесуальні дії, необхідні для максимального збору доказової інформації на початку кримінального провадження. Визначено криміналістичні версії, які висуваються на початковому етапі розслідування кримінальних правопорушень з використанням інтернет-банкінгу: кримінальне правопорушення, пов'язане з використанням інтернет-банкінгу, вчинене з метою отримання матеріальної вигоди «хакером» або співробітником певної установи, яка володіє навичками роботи з комп'ютерною технікою, чи з метою заволодіння інформацією з обмеженим доступом особою, що має вільний доступ до визначеної комп'ютерної техніки. З'ясовано, що під час розслідування досліджуваної категорії протиправних діянь потрібно максимально забезпечити збереження інформації, яка перебуває на флеш-накопичувачах, жорстких дисках, кеш-пам'яті відповідного пристрою, в хмарних сховищах тощо.

Ключові слова: кримінальні правопорушення, інтернет-банкінг, кіберзлочинність, початковий етап розслідування, слідча (розшукова) дія, версія.

The article was submitted 16.10.2023
The article was revised 07.01.2023
The article was accepted 27.11.2023