UDC 343.98
DOI https://doi.org/10.32849/2663-5313/2023.6.16

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). The follow-up stage of investigation of criminal offences related to using internet banking (problematic issues). *Entrepreneurship, Economy and Law, 6*, 88–92, doi https://doi.org/10.32849/2663-5313/2023.6.16

THE FOLLOW-UP STAGE OF INVESTIGATION OF CRIMINAL OFFENCES RELATED TO USING INTERNET BANKING (PROBLEMATIC ISSUES)

Abstract. *Purpose.* The purpose of the article is to study the further stage of investigation of criminal offences related to using Internet banking. ***Results.*** The article focuses on certain aspects of investigation of criminal offences related to using Internet banking. The further stage of investigation of relevant unlawful acts is studied. According to most scientists in criminalistics, the follow-up stage of the investigation begins from the moment of serving a suspicion. We support this position, so accordingly, all investigative (search) actions, covert investigative (search) actions and other procedural actions, as well as search measures during the investigation of criminal offences related to using Internet banking, will be considered in accordance with this division. There are a number of undoubtedly important actions in the category of criminal proceedings under study that need to be implemented promptly and efficiently. These include interrogation of a suspect to establish the mechanism and circumstances of the offence, simultaneous interrogation of previously interrogated persons and a search. We have studied these procedural actions and obtained certain tactical recommendations for their implementation. In particular, the use of the following tactics: generating a suggestion of awareness of the authorised person; fast pace of interrogation; a factor of surprise; creating tension; presentation of material evidence; using video recording. It was also found that in 63 % of cases during simultaneous interrogation between the victim and the suspect, the latter fully or partially testified to the evidence he had previously denied. ***Conclusions.*** The author distinguishes tactical search techniques, such as: removal of the suspect from the place of search; involvement of the suspect in the procedural action; comparison of information from the suspect's answers; use of technical means. Tactical techniques also include the way in which information is exchanged between those conducting the search and the manner in which they behave. Since the person being searched and his/her family members are psychologically unprepared to resist the investigation, it is more difficult for them to hide their anxiety. Frequently, these persons do not have enough time to use certain means of disguise or destroy the search items.

Key words: criminal offences, Internet banking, cybercrime, follow-up stage of investigation, investigative (search) action, tactical technique.

1. Introduction

According to most scientists in criminalistics, the follow-up stage of the investigation begins from the moment of serving a suspicion. We support this position, so accordingly, all investigative (search) actions, covert investigative (search) actions and other procedural actions, as well as search measures during the investigation of criminal offences related to using Internet banking, will be considered in accordance with this division. There are a number of undoubtedly important actions in the category of criminal proceedings under study that need to be implemented promptly and efficiently. These include interrogation of a suspect to establish the mechanism and circumstances of the offence, simultaneous interrogation of previously interrogated persons and a search.

An important contribution to the development of the investigation of criminal offences has been made by scientists such as Yu.P. Alenin, V.P. Bakhin, V.K. Veselskyi, A.F. Volobuiev, A.V. Ishchenko, O.N. Kolesnichenko, V. O. Konovalova, V. S. Kuzmichev, B. Ye. Lukianchykov, Ye. D. Lukianchykov, M. V. Saltevskyi, R. L. Stepaniuk, V. V. Tishchenko, K. O. Chaplynskyi, Yu. M. Chornous, L. D. Udalova, V. Yu. Shepitko, and others. However, our study specifies certain positions of the follow-up stage of investigation in criminal proceedings of this category, with due regard to the current forensic practice and viewpoints of scholars.

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

2. Stages of investigation of criminal offences related to using Internet banking

According to O. M. Dufeniuk, the follow-up stage of the investigation begins when a set of primary and urgent investigative (search) actions is performed after the information is entered into the URPTI and the pre-trial investigation is commenced. Depending on the results obtained during urgent investigative (search) actions, two lines of investigation can be distinguished. With regard to the first line, when an unlawful act is detected and the offender is identified, the author argues that it covers the adoption of a procedural decision – notification of suspicion in accordance with Article 278 of the CPC, intensification of efforts to secure evidence of the person's guilt; establishment of the circumstances of the criminal offence, in particular those which mitigate or aggravate liability; application of measures to ensure criminal proceedings, in particular, the choice of preventive measures; CISA. Regarding the second line (in cases where the criminal offence is not detected), the researcher notes that it is characterised by intensified efforts to find forensically relevant information about the event and its participants, collecting and examining the evidence already found, verifying the versions put forward, etc. In conclusion, O.M. Dufeniuk emphasises that in this case it is typical to conduct repeated and additional investigative (search) actions, give instructions to operational units, send requests to enterprises, institutions and organisations, conduct CISA (Priakhin, 2016, p. 512).

With regard to the follow-up stage of the investigation, A.F. Volobuiev makes the following statements. In particular, the author argues that this stage begins from the moment a person is notified of suspicion of committing an unlawful act. Moreover, the main tasks of this stage of the investigation are as follows: "...1) formation of a system of evidence to accuse a person of committing a crime (to be reflected in the indictment); 2) identification of all accomplices to the crime and collection of evidence for their prosecution; 3) ensuring compensation for damages, collection of information about the identity of the suspect". In addition, the researcher argues that each individual investigation methodology at this stage considers typical investigative situations and sets of investigative and search actions that correspond to them. According to A.F. Volobuiev, typical investigative situations are determined by the position taken by a person who has been notified of suspicion of committing a criminal offence (Volobuiev, Stepaniuk, Maliarova, 2018).

With regard to the category of criminal proceedings under study, D.V. Pashnev and M.G. Shcherbakovskyi most accurately formulated the necessary procedural steps of the follow-up stage of investigation. The authors make the following list: "...searches for the purpose of seizure of computer equipment used to commit the offence (in case of indirect network access to a computer by the offender), as well as computer data storage devices obtained as a result of the offence: paper printouts, hard drives of system units, CDs, flash memory; appointment of a computer-technical examination after detection of the listed objects and their inspection; an important means of verifying and confirming the testimony of a suspect is to conduct an investigative experiment with his/her participation; the purpose thereof is to confirm that the person has professional skills in working with computer facilities, programming and the skill to make unauthorised access, to check the possibility of making unauthorised access in a certain way or with the help of certain means; investigative experiment at a certain place is conducted to confirm the presence of a person in a certain place related to the preparation and commission of a crime or concealment of its traces; interrogation of witnesses, in particular those indicated by the suspect to verify his testimony" (Volobuiev, Stepaniuk, Maliarova, 2018).

We will consider each of them individually. In particular, during the interrogation of a suspect, according to A. I. Kuntyi, the following circumstances should be established: "... 1) where and who he/she works for; 2) what computer information he/she has access to, what operations with information he/she is entitled to perform; 3) what is his/her level of training as a programmer, experience in creating programs, what programming languages he/she knows; 4) what identification codes and passwords are assigned to him/her; 5) what types of software he/she has access to; 6) what operations he/she performed during the investigated time; 7) from what source or from whom he/she learned about the information stored on the computer; 8) from whom information about computer information security measures was received, what methods were used to overcome them; 9) how the unlawful access was made, what means were used for this purpose; 10) to whom the information was transferred, for what purpose; 11) what was the purpose of the crime, what material benefit was received for it; 12) how traces of unlawful access to the computer were destroyed; 13) how often unlawful access to computer information was committed; 14) who assisted the suspect in committing the crime and how" (Priakhin, 2016).

3. Tactical methods of interrogation of a suspect during the investigation of criminal offences related to using Internet banking

Regarding the tactical techniques of interrogating a suspect, we support the group of scholars who argue that they are chosen depending on the investigative situation: the authorised person may use the presentation of evidence, the announcement of the testimony of other persons, methods of persuasion, and the asking of detailed, reminiscent, controlling questions, etc. In addition, the authors note that in cases where a suspect gives truthful testimony, the investigator's task is to clarify this information, provide maximum detail, etc. If the suspect gives false testimony, the researchers emphasise the need to take measures to expose the lie: "... explain the provisions of the criminal procedure legislation on mitigating circumstances, detail that person's testimony, conduct repeated interrogations on the same circumstances, present written and material evidence: documents drawn up by him/her, expert opinions, acts of documentary audits, testimony of witnesses, other persons, etc." (Yefimov, Pavlova, Chuchko, 2022, p. 148).

With regard to the specifics of work in banking institutions, we support V.V. Kornienko and V.I. Strelianyi's perspective that an authorised person should consider the specifics of voluntary participation of bank employees in committing economic crimes related to banking operations. The authors emphasise that in this case it is inappropriate to involve persons suspected of involvement in a criminal offence in investigative (search) actions until all the necessary evidence of his or her guilt is collected and analysed. According to scholars, interrogation of a person as a suspect plays the most important role at this stage. Moreover, it is necessary to ensure comprehensive and thorough preparation for the interrogation, during which to collect complete information about the bank employee's involvement in the commission of a criminal offence (Korniienko, Strelianyi, 2015, p. 67).

The analysis of the respondents' survey reveals that during the investigation of criminal offences related to using Internet banking, they see the need and possibility of using the following tactics: generating a suggestion of the authorised person's awareness – 89%; fast pace of interrogation – 56%; a factor of surprise – 57%; creating tension – 69%; presentation of material evidence – 33%; use of video recording – 45%.

The study of criminal proceedings reveals that in order to eliminate discrepancies in the testimony of victims, witnesses and suspects in the studied category of criminal proceedings, in 23% of cases, two or more persons were interrogated simultaneously.

With regard to this procedural action, we support the position of the group of researchers who argue that it is advisable to conduct it in the following cases: "... 1) if a person who gives truthful testimony has influence on another and is able to facilitate a change in his/her position during the simultaneous interrogation; 2) between persons, one of whom gives truthful testimony and the other is honestly mistaken about it due to certain circumstances; 3) between a suspect who provides truthful testimony and a witness who, in the opinion of the authorised person, provides deliberately false testimony" (Yefimov, Pavlova, Chuchko, 2022, p. 151).

The analysis of forensic practice materials suggests that simultaneous interrogation of previously interrogated persons has been conducted: between the suspect and the victim – in 91% of cases; between the suspect and witnesses – in 2%; between suspects – in 7%.

A review of criminal proceedings reveals that in 63% of cases, during the procedural action between the victim and the suspect, the latter fully or partially testified to evidence that he had previously denied.

With regard to the search in the studied category of criminal proceedings, we support the perspective of I.O. Kovalenko, who highlights a number of specificities during the search. The author argues that, first of all, attention should be paid to the computer equipment located in the premises, as well as to the state of the Internet network, and that portable USB flash drives, including those that are disguised, should be searched for when inspecting the premises. The researcher emphasises that it is of great importance to find a mobile phone or tablet at the place of search, as they can usually contain very important information that will serve to quickly investigate an unlawful act. In addition, the scientist emphasises that the equipment must be properly packed and sealed before seizure, and it is also important to disconnect it from the power supply before entering the premises, which will make it impossible to quickly destroy the information stored on electronic media. As an example, I. O. Kovalenko observes that attackers can destroy any electronic medium in a matter of seconds using a microwave oven. The author concludes that the type of unlawful act under study differs significantly from others in that its main feature is the use of the World Wide Web with the involvement of electronic means (Kovalenko, 2019, p. 117).

A. I. Kuntii distinguishes the following characteristics of a search related to computer equipment: "...1) the use of the principle of suddenness when arriving and entering the premises where the search will be conducted or where the computer equipment to be searched is located; 2) the object of the search is not only a technical device or material medium of computer information, which may be a computer hard drive, floppy disk, optical disc, flash card, etc., but also the information stored on them, which is, in fact, the main object of search and seizure in order to establish the circumstances of the computer crime; 3) the place of the investigative action in this case will be not just the premises where the carrier of computer information is located, but the premises, technical means and information array of a particular computer object; 4) seizure of computer objects containing information data may be carried out in different ways. Data storage media or even the entire computer system or its individual parts may be seized if the data cannot be accessed for copying or studying on other equipment. Recovery of such data requires special software, sometimes additional equipment, and the recovery process can take a long time. In these cases, it is not advisable to actually examine the software product during the search or seizure. Under certain circumstances, it may be acceptable to seize data by copying it to separate storage media. In such cases, special measures should be taken to ensure the integrity and safety of the seized data, and the media used for copying should not contain any information. It is not advisable to copy the seized information onto media containing information relevant to the case, even if this information is identical or contains fragments of the information to be seized. Conditions and guarantees must be created to ensure that the copy is identical to the original at the time of the search or seizure and that it is securely stored throughout the investigation; 5) impossibility of using metal detectors or X-ray machines in the process of searching for caches with magnetic media, as their use may lead to the destruction of information on these media; 6) the need to promptly analyse a large amount of information found during the search in order to establish its value for the pre-trial investigation; 7) conducting a search only on one or more computers that are part of a local computer network" (Priakhin, 2016).

According to some scholars, after arriving at the place of search, the authorised person shall offer the person to hand over the items provided for by the investigating judge's decision, as well as other items that have been withdrawn from civilian circulation or illegally obtained. At the initial stage of the search, it is important to establish psychological contact, which is achieved through mutual perception of the parties and the exchange of both verbal and non-verbal information. Such contact can be initiated, for example, when the investigator offers to hand over the searched objects before the search, arguing that it is undesirable for children to see the search scene when they return from school. Even if the answer is negative, this step can be the basis for further contact. If the person being searched is stiff, arrogant or aggressive, you can try to ease their anxiety by talking about family relationships, health (Kazmirenko, 2007, p. 148).

In O. Musiienko's opinion, the effectiveness of a search increases in cases where the fact of criminal proceedings is unknown to the offenders. In this case, the conduct of searches is sudden for them. One of the tasks of a search is to find and seize stolen property: goods obtained in shops and commercial enterprises by criminal means under a sale and purchase agreement; agricultural products, cash, etc. A review of investigative practice reveals that timely searches to identify seized property enabled not only compensation for material damage but also new evidence. In addition to these objects, documents and items used to prepare and commit the crime are also subject to search. Such objects may include: documents that were used to commit fraudulent actions to obtain funds, items that were used to forge documents, forged or stolen seals and stamps; all other items and documents that can serve as means to establish the truth in the case (letters, photographs, private records, receipts) (Musiienko, 2009, p. 129).

With regard to tactical search techniques, we support the opinion of a group of authors who have identified the most effective ones, such as: removal of the suspect from the place of search; involvement of the suspect in the procedural action; comparison of information from the suspect's answers; use of technical means. Tactical techniques also include the way in which information is exchanged between those conducting the search and the manner in which they behave. Since the person being searched and his/her family members are psychologically unprepared to resist the investigation, it is more difficult for them to hide their anxiety. Frequently, these persons do not have enough time to use certain means of disguise or destroy the search items (Yefimov, Pavlova, Chuchko, 2022).

4. Conclusions

To sum up, the follow-up stage of the investigation begins from the moment of serving a suspicion. It is established that during the investigation of criminal offences related to using Internet banking, there are a number of undoubtedly important actions in the category of criminal proceedings under study that need to be implemented promptly and efficiently. These include interrogation of a suspect to establish the mechanism and circumstances of the offence, simultaneous interrogation of previously interrogated persons and a search. We have studied these procedural actions and obtained certain tactical recommendations for their implementation. In particular, the use of the following tactics: generating a suggestion of awareness of the authorised person; fast pace of interrogation; a factor of surprise; creating tension; presentation of material evidence; using video recording. It was also found that in 63 % of cases during simultaneous interrogation between the victim and the suspect, the latter fully or partially testified to the evidence he had previously denied.

References:

Kazmirenko, L.I. (2007). Yurydychna psykholohiia [Legal psychology]. Kyiv : KNT (in Ukrainian).

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).

Kovalenko, I.O. (2019). Orhanizatsiino-praktychne zabezpechennia provedennia obshuku pry rozsliduvanni shakhraistva u sferi vykorystannia bankivskykh elektronnykh platezhiv [Organizational and practical support for conducting a search during the investigation of fraud in the field of using bank electronic payments]. Visegrad Journal on Human Rights. № 6. pp. 117–122 (in Ukrainian).

Musiienko, O.L. (2009). Teoretychni zasady rozsliduvannia shakhraistva v suchasnykh umovakh [Theoretical foundations of fraud investigation in modern conditions]. Kharkiv : Pravo

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

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

Yefimov, M.M., Pavlova, N.V., Chuchko, S.V. (2022). Metodyka rozsliduvannia shakhraistv, poviazanykh iz kupivleiu-prodazhem tovariv cherez merezhu Internet : teoretychni ta prakseolohichni zasady [The method of investigating fraud related to the purchase and sale of goods via the Internet: theoretical and praxeological foundations]. Odesa : Vydavnychyi dim «Helvetyka» (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*

ПОДАЛЬШИЙ ЕТАП РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ ІЗ ВИКОРИСТАННЯМ ІНТЕРНЕТ-БАНКІНГУ (ПРОБЛЕМНІ ПИТАННЯ)

Анотація. ***Метою*** статті є дослідження подальшого етапу розслідування кримінальних правопорушень, пов'язаних з використанням інтернет-банкінгу. ***Результати.*** Наукова стаття присвячена висвітленню окремих аспектів розслідування кримінальних правопорушень, пов'язаних з використанням Інтернет-банкінгу. Досліджується подальший етап розслідування визначеної категорії протиправних діянь. Зазначено, що подальший етап розслідування починається, як вважає більшість вчених-криміналістів, з моменту пред'явлення підозри. Ми підтримуємо цю позицію, тому відповідно всі слідчі (розшукові) дії, негласні слідчі (розшукові) дії та інші процесуальні дії, а також розшукові заходи при розслідуванні кримінальних правопорушень, пов'язаних з використанням інтернет-банкінгу, будемо розглядати відповідно до вказаного поділу. По досліджуваній категорії кримінальних проваджень є ряд беззаперечно важливих дій, які необхідно швидко та ефективно реалізовувати. Серед них необхідно виокремити допит підозрюваного для з'ясування механізму та обставин вчинення протиправного діяння, одночасний допит раніше допитаних осіб та обшук. Визначені процесуальні дії нами були опрацьовані та отримали певні тактичні рекомендації стосовно їх проведення. Зокрема, застосовуванні таких тактичних прийомів: створення уявлення про інформованість уповноваженої особи; швидкий темп допиту; використання фактора раптовості; створення напруги; пред'явлення речових доказів; застосування відеозапису. Також встановлено, що у 63 % випадках під час проведення одночасного допиту між потерпілим та підозрюваним останній повністю або частково засвідчив свідчення, які раніше заперечував. ***Висновки.*** Виокремлено тактичні прийоми обшуку, а саме: видалення підозрюваного з місця проведення обшуку; залучення підозрюваного до участі в процесуальній дії; зіставлення інформації, яка міститься у відповідях обшукуваного; застосування технічних засобів. До тактичних прийомів відноситься і спосіб обміну інформацією між тими, хто проводить обшук, і манера їхнього поводження. Оскільки обшукуваний, члени його сім'ї виявляються психологічно неготовими до протидії розслідуванню, їм важче приховати хвилювання. Часто в цих осіб немає достатньо часу для вжиття тих чи інших засобів маскування чи знищення предметів пошуку.

Ключові слова: кримінальні правопорушення, інтернет-банкінг, кіберзлочинність, подальший етап розслідування, слідча (розшукова) дія, тактичний прийом.

The article was submitted 17.10.2023
The article was revised 08.11.2023
The article was accepted 28.11.2023