İSTANBUL UNIVERSITY PRESS

Ceza Hukuku ve Kriminoloji Dergisi-
Journal of Penal Law and Criminology
JPLC 2024; 12 (1): 16–24
DOI: 10.26650/JPLC2023-1367714

RESEARCH ARTICLE

Unauthorised Access to Computer Information: The Motives for Committing a Crime

Ilya MOSECHKIN[1]

[1]Associate Professor of Vyatka State University, Department of Criminal Law, Criminal Procedure and National Security, Kirov, Russian Federation

ABSTRACT

The purpose of this study is to identify the main internal motives that led to the commission of illegal access to computer information. The motive in the study is defined as the internal motivation of a person to achieve a specific result, due to needs, and causing the determination to commit a crime. To conduct the study, 300 acts of the courts of the Russian Federation were analysed, they were issued in connexion with committing unauthorised access to computer information. It was revealed that in most of the considered cases, there was no relationship between the criminal and the victim, but 17.6% of the victims were not accidental. The study of judicial acts revealed the most common motives: desire to commit further theft; desire to get payment for the received information; personal discountenance; desire to get secure data; revenge. At the same time, more than 80% of acts of unauthorised access are committed for reasons directly related to money and property. The material being studied made it possible to divide them into two categories: "interested in financial gain" and "non-interested in financial gain". Depending on the category, different preventive measures are proposed.

Keywords: Unauthorised access, motive of financial gain, revenge, multiple victimisation

INTRODUCTION

Every year digitalisation covers more and more spheres of human life. This process will certainly have far-reaching effects on individuals, society and organisations (Trittin-Ulbrich et al., 2021). Most people use the digital space for good, in accordance with the norms of law and morality, but there are also many who use technology for illegal purposes. This study focuses on the latter category of people.

There are several reasons why the digital space attracts criminals. In particular, it allows traditional crimes (such as fraud, extortion or incitement to suicide) to be carried out remotely. anonymity and remoteness lead to a high latency of illegal acts and a sense of impunity for the criminal. Crime detection rates often remain low because of inconsistencies between methods and technologies used by law enforcement and the level of innovative methods used by criminals (Sturc, Gurova and Chernov, 2022). In addition, the Internet makes it possible to commit qualitatively new crimes: unauthorised access to computer information or distribution of malicious software.

The significant prevalence of cybercrime is undeniable. In particular, unauthorised access to a computer in the Netherlands is more common than bicycle theft, once one of the most common traditional crimes (Leukfeldt, Notté and Malsch, 2020). According to a survey conducted in Switzerland, approximately 13% of respondents were victims of unauthorised use of personal data (Milani, Caneppele and Burkhardt, 2022). A huge number of Internet users in China has led to the emergence of several cybersecurity problems. Approximately one-third of all crimes in this country are committed in the digital space. The annual damage exceeds 95 billion yuan (i.e. approximately US$15 billion in 2021), and the number of illegal acts is steadily increasing. For example, in 2016, there were approximately 70,000 ransomware attempts, 197 million intercepted phishing attacks, and 20,000 reports of monetary losses and security vulnerabilities (Jiang, 2021). Surveys show that 12% of mobile phone owners in the US reported that another person illegally accessed the contents of their phone. They perceived this as an invasion of privacy (Marques et al., 2019).

The Russian Federation is no exception. Due to the actions of cybercriminals in 2020, the damage amounted to approximately 70 billion rubles, and in 2021-90 billion rubles (that is, approximately 1.3 billion US dollars in 2021). In the future, experts predict only an increase in the amount of damage (RIA Novosti, 2021). At the same time, according to official statistics, the number

Corresponding Author: Ilya Mosechkin **E-mail:** Weretowelie@gmail.com
Submitted: 28.09.2023 • **Revision Requested:** 29.04.2024 • **Last Revision Received:** 22.06.2024 • **Accepted:** 03.05.2024

of cases of unauthorised access to computer information was 1,761 in 2018, 2,420 in 2019, and 4,105 in 2020. The increase is very significant, even without considering the hidden part of illegal acts. The number of registered cases of using and distributing malicious computer programmes in 2018 was 733, in 2019 it was 455, and in 2020 it was 371 (Gladkikh and Mosechkin, 2021).

The foregoing allows us to say that the problem of cybercrime prevention is common to most countries. However, it is still impossible to discuss a full and comprehensive study of the features of individual crimes. Within the framework of this article, it should be noted that there is a lack of research on motives for unauthorised access to computer information, which has recently undergone significant changes (Li, 2017).

The motive largely explains why a particular illegal act was committed. This is also typical for unauthorised access to computer information. At the same time, in the legislation of a number of countries, motive is a secondary element of the crime, which often does not affect the amount of punishment or whether a person is found guilty or not guilty (Leka, 2019). However, in the Russian Federation and some countries with similar systems of law (CIS countries and some countries of the legal family of civil law), the situation is different. At the level of law, motives are divided into legally significant for the qualification of a crime and other motives that acquire legal meaning in further implementation of the criminal law (when imposing punishment, exempting from criminal liability and punishment, etc.). In addition, Article 73 of the Rules of Criminal Procedure of the Russian Federation directly prescribes the obligation to prove the guilt of a person in committing a crime, the form of his/her guilt, and motives. Otherwise, the decision taken by the court may be annulled. Thus, in Russian legislation and the legislation of a number of countries, the motive plays an important role in qualifying a crime, imposing punishment, and proving guilt; therefore, its correct identification and understanding is necessary.

It seems that the study of motives for unauthorised access to computer information in the Russian Federation can be useful for the whole world because this country is multinational (over 160 nationalities), multi-confessional (over 70 confessions), and multicultural. These factors greatly contribute to an objective and representative sample.

1. Literature Review

It is traditionally believed in Russian criminology that a motive is an internal motivation of a person to achieve a specific result, due to certain needs, and causing a determination to commit a crime (Oganesyan, 2012). At the same time, such an impulse is formed under the influence of both internal (dispositional) and external (situational) conditions. Neufeld notes the presence of internal and external motivation, including in relation to cybercrime (2023).

Grabosky (2001) believes that computer crime does not significantly differ from traditional crime. This is especially noticeable when studying motives. Among them, the most obvious are: greed, lust, power, revenge, adventure, and the desire to taste forbidden fruit. Neufeld made a great contribution to the study of the motives of cybercrime (2010). According to his research, the most common is the interest motive or the motive for obtaining financial profit (68.1%). Motives of revenge, entrepreneurial gain, thirst for thrills, curiosity, and others are much less common (Neufeld, 2010). However, Neufeld studied the insides of various cybercrimes, which can be quite different from one another. In another scientific work on cybercrime, a rather ambiguous statement is noted: the motive for cybercrime is the desire to cause psychological and physical harm to the victim using modern telecommunications networks (Azad, Mazid and Sharmin, 2017).

Many scientists have made the subject of their research the features of motives of exclusively unauthorised access to computer information. In the work devoted to the ratio of hacking to white-collar crime, it is substantiated that this crime is characterised by economic motives. At the same time, unauthorised access may be due to intellectual challenge, revenge, or even boredom (Duff and Gardiner, 1996). Jordan and Taylor (1998) list the motives common among hackers as addiction, curiosity, information seeking, peer recognition, and security vulnerability detection. Kremen (1998) identifies many types of hackers, depending on their motivation. The following types are among them: curious; thrill seekers; vandals; spies; terrorists and others.

Maiwald (2003) identified three dominant motives: skill testing, greed, and vandalism. Liu and Cheng (2009) take a different position. According to their research, cyberattacks are mostly driven by hatred, the desire to commit theft, terrorist beliefs, or the desire to play a hoax on another person. Based on a review of law enforcement activities and previous research, Li (2017) identified 29 motives for illegal activity in the digital space. Among them, the following should be mentioned: self-expression; curiosity; testing; hatred; financial benefit; academic progress; harassment; desire to destroy evidence, etc.

Marthala stated that theft is the most common motive for hackers (2018). Another study examining the behaviour of hackers emphasises that the motives of criminals are heterogeneous. Their range includes the following: desire to break into secure computer networks without permission; propaganda of terrorism; credit card theft; identity theft; theft of intellectual property; and software corruption. Such hackers are called "black hats". "White hat" hackers have noble motives—helping the state, exposing criminals, and others (Lazarov and Petrova, 2022). Polyakov and Shiryaev (2018) note that a separate group of victims should be distinguished in which victim personality traits predominate. Unlike accidental victims, such victims can actively provoke the

commission of a computer crime against themselves (for example, publicly speak negatively about “hackers”). That is, the motive will be closely related to provocation. One of the newest classifications identifies five key motives: proof of skill, skill training, money, ideology, and curiosity (Ismail and Aamar, 2019).

Thus, the features of the motives for unauthorised access to computer information (hacking) have not gone unnoticed in science. However, the studies were conducted selectively and in individual countries. New empirical evidence may help deepen existing knowledge or highlight weaknesses in previous findings.

2. Aim and Methodology

The empirical base of the study consists of 300 acts of courts (guilty and acquittal verdicts, decisions) that were issued in connexion with the commission of unauthorised access to computer information. The studied number of judicial acts is representative, since during the period under review there were only 414 convictions (according to the statistical information of the Supreme Court of the Russian Federation). This crime is provided for in Art. 272 of the Criminal Code of the Russian Federation, which includes the following wording: "Unauthorised access to computer information protected by law, if this act entailed the destruction, blocking, modification, or copying of computer information." This article qualifies all cases of hacking computers or other technical devices, accounts, e-mail, or Internet systems. If the hacking resulted in the theft of property or certain information, the deed is additionally qualified under a different article. The acts of the courts were issued from 2017 to 2021. Acquittals were not excluded from the analysis; citizens were found not guilty only because their actions did not entail the harmful consequences specified in the law. However, the courts have reliably established the facts of the commission of dangerous acts on the basis of specific motives. The source of data is legal reference systems (the state automated system “Pravosudie”) and the official websites of the Russian courts, where the issued acts are presented for review. To obtain judicial acts, search terms were used: “illegal access”, “motive”, “purpose”, “inducement”, “article 272”. The sample of judicial acts made it possible to cover 74 constituent entities of the Russian Federation out of 85, which allows us to speak about a sufficient degree of representativeness. Note that the use of judicial acts as research data is not free from limitations. A significant amount of information about the accused and the victim is removed from the published verdicts, which makes analysis difficult. In addition, cases of incomplete clarification by the courts of the circumstances of the case and bias towards the offender should not be excluded.

The selection of cases for the study was made without taking into account the individual characteristics of criminals and was carried out in a continuous manner, i.e., the cases presented in the reference system in a row were analysed (if they matched the parameters of the study). This made it possible to maintain the objectivity of the study. First, the motives, areas of activity in which the illegal act occurred, and the relationship between the victim and the criminal were analysed and systematised. The motive in this study is understood as the internal motivation of a person to achieve a specific result, due to certain needs and causing the determination to commit a crime.

The purpose of this study is to identify the main internal motives that, along with other factors, led to the commission of illegal access to computer information. To achieve this purpose, the following tasks were set and solved: to analyse the judicial acts issued in connexion with the commission of a crime provided by Art. 272 of the Criminal Code of the Russian Federation; to determine the relationship between the criminal and the area of activity in which the crime was committed; to determine the motives for unauthorised access; and to explain the predominance of some motives over others.

In particular, this paper attempts to answer the following research questions:

1. What reasons do Russian offenders have while committing unauthorised (illegal) access?
2. What impact does the relationship between a victim and an offender have on motivation and victimisation in computer crime?
3. What influence does the sphere of crime activity have on the formation of the motive for unauthorised (illegal) access?
4. Is it necessary to develop measures to counter unauthorised (illegal) access, considering the differing motives for the crime?

3. Findings

Three hundred judicial acts were analysed. One and the same crime sometimes caused harm to several people at once, so the number of victims studied was 421. The illegal act in relation to each victim was considered a separate case. The percentage by the type of activity in which crimes were committed is as follows. Most often unauthorised access to computer information occurs in banking (50.1%), social networks (24.7%), and mobile communications (18%). Much less often, crimes are committed in connexion with participation in online games (3.8%), internet shopping (1.9%), and other areas, the share of which does not exceed 1.5%. The indicators are more fully shown in table 1.

Table 1. Spheres of activity in which the crime occurred

Sphere of activity	Prevalence
Banking	Two hundred and eleven of 421 (50.1%)
Social networks	One hundred and four cases out of 421 (24.7%)
Mobile communication	Seventy six cases out of 421 (18%)
Online-games	Sixteen cases out of 421 (3.8%)
Internet shopping	8 cases out of 421 (1.9%)
Transport	2 cases out of 421 (0.5%)
Advertising	2 cases out of 421 (0.5%)
Judicial	2 cases out of 421 (0.5%)

In most cases, there was no relationship between the criminal and the victim; in 82.4% of cases, the choice of the victim was random. Clarification of the nature of the relationship between the offender and the victim is traditionally carried out in Russian criminal proceedings. However, in rare cases, the nature of the relationship was not mentioned in judicial acts. For the study, we decided to categorise such cases as "absence of relationships". However, the analysis of judicial acts showed that in certain cases (7.1%) the criminal and the victims knew each other or were even on friendly terms. In addition, 4.8% of victims were intimate partners of the criminal (cohabitation or marriage).

In particular, according to the verdict of the garrison military court in case No. 1-63/2021, it was established that the accused A. Yu. O. was dissatisfied with the victim's refusal to cohabitate and maintain relations with him, as well as her appeal to the court demanding the recovery of alimony. A. Yu. O. used the algorithm and form of restoring access to the victim's page on the social network, which allowed him to access it. He changed the login and password and then copied the correspondence and images of the victim. Subsequently, A. Yu. O. posted personal photographs of the victim and her minor children on the social network, as well as other personal information about her family life (*Case 1-63/2021 2021*).

There were quite rare episodes when the criminal and victim had business relationships (4.2%). Usually, unauthorised access in such cases acts as an act of revenge for a bad attitude or lack of due payment for services. Even more rarely, the criminal and victim were relatives of each other (1.5%). The indicators are more fully shown in table 2.

Table 2. Relationship between the criminal and victim

The type of relationship	Prevalence
No relationship (accidental victim)	Three hundred and forty seven persons out of 421 (82.4%)
Friends/acquaintances	Thirty persons out of 421 (7.1%)
Intimate partners (cohabitants/marriage)	Twenty persons out of 421 (4.8%)
Business	Eighteen persons out of 421 (4.2%)
Relatives	6 persons out of 421 (1.5%)

The study of the motives reflected in the acts of the courts made it possible to establish some features and patterns. In most cases, internal motives were associated with obtaining monetary or other property benefits. Some criminals made money by selling personal data, whereas others used it to commit new crimes.

Thus, a significant number of acts of unauthorised access to computer information were carried out to further embezzle money (theft or fraud). In Russian criminal law, this motive is referred to as "interested in financial gain ". When studying the acts of the courts, it was met 305 times out of 421 and amounted to 72.5%, respectively.

Thus, according to the verdict of the district court in case No. 1-268/2017, at the beginning of January 2015, Ch. O. A. acquired access logins and their corresponding passwords on the Internet from an unidentified person, which allowed access to the pages of users of the social network. Subsequently, Ch. O. A. accessed the information posted on the victim's electronic page and changed the identification data, blocking access to the legitimate user's page. On behalf of the victim, Ch. O. A. sent messages with a request to borrow money, indicating the number of his bank cards. Having received this message, one of the acquaintances of the victim, who was under the influence of deceit, transferred funds in the total amount of 5,000 rubles (*Case 1-268/2017* 2017)

The interested in financial gain motive was also manifested in the fact that the offender transferred or planned to transfer personal data to third parties for a fee. It is advisable to place these internal motives in a separate category because they are not associated

with theft and have a lesser degree of public danger. Most often, the essence of the crime is expressed in the fact that the offender works for a mobile operator company and, taking advantage of the position, sells information about connexions, about subscribers, etc. Such internal motivation accounts for 10.8%.

For example, from the verdict of the district court in case No. 1-77/2020, B. R. K. was employed as a specialist in the MegaFon sales office and was engaged in customer service using a billing application. An unknown person in the messenger offered B. R. K. to provide information about the subscriber for a monetary reward, and he agreed. B. R. K. accessed databases on the office computer, viewed and photographed personal information, and transferred it to an unknown person. For this, B. R. K. received money in the amount of 200 rubles (*Case 1-77/2020* 2020)

The third most frequent motive is discountenance (5.7%). The judiciary uses this definition of internal motives in cases where the victim and the criminal are in conflict, quarrel or fight. At the same time, the criminal's misconduct is not always a response to any actions. In contrast, the criminal can be the instigator of a quarrel.

In particular, according to the verdict of the district court in case No. 1-191/18, it was established that R. E. N., having free access to the victim's cell phone, accessed her personal page on the social network without permission. Subsequently, on the basis of personal hostile relations, R. E. N. repeatedly corresponded on behalf of the victim to her acquaintances. In addition, he posted on the electronic page information about the intimate life of the victim, indicating that she had venereal disease (*Case 1-191/18* 2018)

Only in 5.3% of cases unauthorised access to computer information was carried out in order to obtain protected information (about personal life, commercial secrets, etc.) for private use. That is, there was no intention to use this information for the commission of crimes, business activities, or other purposes in the future.

Thus, case No. 1-44/2018 in the district court found that Ts. G. A. was employed in the sales office of a company providing mobile communications. Wanting to have information about the private life of the victim, she created a request (application) in the information system for receiving details of telephone connexions of the subscriber number. Ts. G. A. attached a false power of attorney to the application, according to which the victim entrusted her with obtaining the details of telephone connexions. As a result of these actions, the system generated in the form of a file information about the telephone connexions made by the victim and granted access to the Ts. G. A. to familiarise with the specified information from the local personal computer (*Case 1-44/2018 2018*)

Revenge served as an internal motive for the commission of a crime in 4.7% of the studied cases. As a rule, the victim allowed immoral or illegal behaviour in relation to the offender, who used unauthorised access in order to perform an act of retribution.

Thus, the district court in case 1-212/18 found that the accused M. provided services to the victim in the field of IT technologies, for which he received payment. At the end of the year, M. performed another service, but did not receive a reward, in connexion with which he repeatedly demanded payment of the amount of money due to him. Having received a refusal to pay, M. accessed information and deleted the information created by the victim from the computer in order to perform activities related to transport services (*Case 1-212/18* 2018)

Other motives were found in less than 1% of the cases examined. In two cases, the motive was careerism—a rather specific internal motivation, meaning a desire to advance in position. In two more cases, the criminals committed crimes for no obvious reason. In Russian criminal law, this is called a hooligan motive. In other words, the offenders acted "just like that", wanting to go beyond the boundaries of what is permitted and show that they are above society. Thus, as a result of studying the judicial acts issued in connexion with commission of unauthorised access, it was possible to establish the most characteristic motives for the crime. All known motives are shown in table 3.

Table 3. Motives for unauthorised access to computer information

Motive	**Prevalence**
Interested in financial gain motive (desire to commit theft in the future)	72.5%
Interested in financial gain motive desire to receive payment for the received information)	10.8%
Personal discountenance	5.7%
Desire to obtain secure data	5.3%
Revenge	4.7%
Careerism	0.5%
Hooligan motive	0.5%

Discussion

The examination of judicial decisions indicates that the association between the perpetrator and the victim can influence the likelihood of victimization, albeit not consistently. In science, this issue has been studied rather fragmentarily: Ho and Luong argue that previous research has mainly focussed on the relationship between parents and minors (Ho and Luong, 2022). Other types of relationships (relative to the crime in question) are practically not studied. However, the analysis of judicial acts shows that 17.6% of the victims were not accidental. In contrast, they were in a relationship with the criminal (business, family, etc.). This could not but play a role in committing the act.

In traditional crime, relationships can have an extremely strong impact on victimisation (Chiesa et al., 2018). This is less common in cybercrime, but the likelihood of a relative, partner, or business partner committing a crime must be considered. The presence of technical knowledge or a profession related to computer technology is not an indicator. One study correctly notes that most cyberattacks carried out by intimate partners were technically simple. The most common use was password guessing or account password possession (Freed et al., 2018). We agree with the opinion of Polyakov and Shiryaev (2018) that a separate group of victims should be singled out, in which victim personality traits predominate. Unlike accidental victims, such victims can actively provoke the commission of a computer crime against themselves. As an example, they may include people who speak negatively about "hackers" in public. That is, they themselves consciously or unconsciously form the motive for the crime.

The predominance of banking is not surprising because most cybercriminals are focussed on generating financial gain (Miró-Llinares, Drew and Townsley, 2020). Social networks also help them with this. Our results are in good agreement with previous studies that found social media to be fertile ground for cybercriminals because most Internet users spend their time on social media and post personal (and sensitive) information (Milani, Caneppele and Burkhardt, 2022; Smith and Stamatakis, 2021). Thus, companies providing services in these areas and users should pay special attention to security because of the high risk of crime.

The areas of online shopping and gaming, to our surprise, did not show high risks of victimisation. The observed phenomenon can be attributed to the fact that other methods are more frequently used to commit crimes in these areas. For example, fraud is common when a useless cargo is sent instead of goods. That is, for illegal profit making, it is not required to hack accounts. There is another explanation: it can be assumed that organisations in these areas are aware of the possible risks and are making every possible effort to ensure the safety of users.

The results of this study show that the motives for unauthorised access committed by Russian offenders have much in common with the motives for unauthorised access committed by offenders in other countries. Many scholars note that such a crime is mainly carried out because of financial or other property gain (Marthala, 2018; Maiwald, 2003). The predominance of the interest motive, in our opinion, is indeed irrefutable. In essence, both the desire to commit theft in the future and the desire to transfer the information received to third parties for a fee can be attributed to interested motives (despite the fact that they have slight differences). This allows us to say that more than 80% of acts of unauthorised access are committed for reasons directly related to money and property.

Scholars have suggested that there is some evidence for multiple victimisation in cybercrime (Junger et al., 2017). This is primarily related to the fact that cybercrime is a link in the chain: phishing or hacking leads to the theft of personal data, which leads to the withdrawal of money from the bank account of the same victim. The analysis of judicial acts convincingly shows that multiple victimisation in cybercrime not only exists but is also very common. Most criminals made unauthorised access solely to later commit theft. That is, unauthorised access was the first link in the chain. At the same time, subsequent crimes can be very diverse: theft, fraud, dissemination of information about private life, slander, and attacks on commercial, tax, or banking secrets. This pattern should certainly be considered when developing preventive measures and improving the norms of criminal law. In Russian criminal law, for example, there is an aggravating feature "with the aim of concealing another crime or facilitating its commission", but unauthorised access does not have it, which is a serious omission (Gladkikh and Mosechkin, 2021).

Neudeld (2018) found that revenge is the motive for unauthorised access in more than 15% of cases. Other authors have also reported the prevalence of this internal drive too (Liu and Cheng, 2009). Although our study did not reveal high rates of revenge motive (4.7%), it should still be recognised that crimes committed for such reasons are not isolated. Revenge is a well-known and fairly predictable motive that also indicates the existence of any relationship between the victim and the offender. Therefore, a potential victim can take self-defence measures to prevent a crime. At the same time, in several episodes, we found that the offender resorted to unauthorised access in cases where he/she was denied payments. This fact is rather alarming because it may indicate the lack of sufficient legal protection of labour or entrepreneurial activity. If a person chooses an illegal variant of retribution, the legal one seems ineffective. It appears that legislative bodies should reevaluate their stance on ensuring protection of labor and entrepreneurial activities and amend relevant regulatory legislation accordingly.

The motive of personal discountenance has a significant similarity to revenge. It is almost as common but more typical for crimes committed by intimate partners (former or present). There are quite widely known cases when a former intimate partner

resort to violence to offend or establish his/her illegal control over a person. Obviously, unauthorised access can play the same role.

In the studied array, we failed to find some motives mentioned in previous works by scientists. In particular, there has never been an instance of unauthorised access done to change academic performance or to prepare for murder (Li, 2017). There were also no terrorist motives (Lazarov and Petrova, 2022), espionage motives (Kremen, 1998), or a desire to prank another person (Liu and Cheng, 2009). The aforementioned internal motives may strongly influence offenders to engage in unauthorized access, yet it is our observation that they are not prevalent or entirely absent in contemporary criminal offenses.

The diversity of the found motives makes it possible to classify them according to the principle of dichotomy, i.e., division into two parts. Since most internal motives are somehow related to the extraction of financial benefits, one of the categories should take this into account. The second category (less common) is intended to cover all other motives. Thus, depending on the offender's attitude to property gain, motives can be divided into "interested in financial gain " and "non-interested in financial gain ".

This division has not only theoretical but also important practical significance. Interested acts of unauthorised access are more often committed in relation to previously unfamiliar victims. In addition, such violations prevail in areas with large financial flows: banking, mobile communications, and social networks. However, most cybercrimes occur because of ignoring the risks associated with online interaction (Odunze, 2018). In other words, both technical measures and measures to inform potential victims can be effective in preventing this category of crimes. Scholars have repeatedly noted that experienced users are better able to avoid risky behaviours such as opening random links and downloading media from unsafe sources, etc. (Reyns et al., 2019; Ali-Ali, & Al-Nemrat, 2017). The authors suggested the need to improve the security of online banking, including the development of more sophisticated and reliable systems for monitoring the activities of computer fraudsters and hackers, using strong passwords and different combinations of usernames for different sites (Ali et al., 2017). It is also right to say that cooperation between government agencies and Internet companies should be developed and the latest software should be introduced to protect against viruses, malware, and other online threats (Odunze, 2018).

However, all these measures may be ineffective in relation to non-interested in financial gain unauthorised access to computer information. The use of strong passwords and different combinations of usernames will be useless if the victim discloses them to his/her intimate or business partner. Cooperation between government agencies and Internet companies will also have little impact if a potential victim leaves the device in the field of view of friends, relatives, or cohabitants. This problem has been relevant since the beginning of global digitalisation, despite the widespread use of computer technology. On the other hand, the measures proposed by scientists to prevent family and white-collar crime can have a significant effect. The use of protection orders and the application of more stringent enforcement measures (Backes, Fedina and Holmes, 2020), the introduction of prevention mechanisms based on the analysis of crime scenarios (Rorie, 2019), and the testing of integrity and loyalty in the recruitment and selection of potential employees (Pusch and Holtfreter, 2021) are worth mentioning. There are several such measures, and it is inappropriate to consider them all in the framework of this study. At the same time, we express confidence in their effectiveness in relation to non-interested in financial gain unauthorised access to computer information.

CONCLUSION

The study made it possible to develop several important conclusions. In most of the examined cases, there was no relationship between the criminal and victim. However, 17.6% of the victims were not accidental. They were in an intimate, friendly, business, or family relationship with the offender. Accordingly, due diligence on the part of such victims may help to predict or prevent unauthorised access to computer information.

The most risky areas are banking, social networks, and mobile communications. Each of them is associated with working with the personal data of users and generating large amounts of income, which attracts offenders. Apparently, this trend will continue in the near future; therefore, additional efforts should be focussed on crime prevention in these areas. On the contrary, the areas of online shopping and gaming have not shown high risks of victimisation, so their experience in countering acts of unauthorised access can be studied and borrowed by organisations and government agencies.

The analysis of judicial acts issued in connexion with the commission of acts of unauthorised access made it possible to identify the features of the motives. In most cases, there were interest in financial gain motives, that is, the crime was committed with the purpose of obtaining property gain. Less common, but not isolated, motives are connected with discountenance, revenge, and the desire to obtain secure data. The material being studied made it possible to divide them into two categories: "interested in financial gain " and "non-interested in financial gain".

Interested acts of unauthorised access are more often committed in relation to previously unfamiliar victims and prevail in areas with large financial flows. Therefore, to prevent this category of crimes, both technical measures and measures to inform potential victims can be effective. Non-interested in financial gain acts of unauthorised access are more often committed by offenders who

are in some way related to the victim. This significantly reduces the role of technical preventive measures. However, it is our belief that the measures outlined by researchers for addressing domestic and white-collar offenses may yield a positive preventative impact.

Although only Russian judicial practise was studied in this study, the results are also valuable for other countries, since the formation of motives has many common features among people of different cultures. There is certainly a need for more cross-national comparative research on the motives for unauthorised access to computer information and other cybercrimes. It would be useful to assess the correlation between the results of this study and those of studies in other countries. This will allow a better understanding of differences in motives and motivation, and the development of the most effective measures to prevent cybercrime.

Ethics Committee Approval: Ethics committee approval is not required for the study.
Peer Review: Externally peer-reviewed.
Conflict of Interest: The author have no conflict of interest to declare.
Grant Support: The author declared that this study has received no financial support.

REFERENCES

Al-Ali, A. A. H., & Al-Nemrat, A. (2017). Cyber victimization: UAE as a case study. *2017 Cybersecurity and Cyberforensics Conference (CCC)*: 19-24. London, United Kingdom. https://doi.org/10.1109/CCC.2017.14.

Ali, L., Ali, F., Surendran, P., & Thomas, B. (2017). The effects of cyber threats on customer's behaviour in e-Banking services. *International Journal of e-Education, e-Business, e-Management and e-Learning 7*(1): 70-78. https://doi.org/10.17706/ijeeee.2017.7.1.70-78

Azad, M. M., Mazid, K. N., & Sharmin, S. S. (2017). Cyber crime problem areas, legal areas and the cyber crime law. *International Journal of New Technology and Research 3*(5): 1-6.

Backes, B. L., Fedina, L., & Holmes, J. L. (2020). The criminal justice system response to intimate partner stalking: A systematic review of quantitative and qualitative research. *Journal of Family Violence 35*(7): 665-678. https://doi.org/10.1007/s10896-020-00139-3

Chiesa, A. E., Kallechey, L., Harlaar, N., Ford, C. R., Garrido, E. F., Betts, W. R. et al. (2018). Intimate partner violence victimization and parenting: A systematic review. *Child abuse & neglect 80*: 285-300. https://doi.org/10.1016/j.chiabu.2018.03.028

Duff, L., & Gardiner, S. (1996). Computer crime in the global village: strategies for control and regulation — in defence of the hacker. *International Journal of the Sociology of Law 24*(2): 211-228.

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2018). A Stalker's Paradise" How Intimate Partner Abusers Exploit Technology. *Proceedings of the 2018 CHI conference on human factors in computing systems*: 1-13. Montreal, Canada. https://doi.org/10.1145/3173574.3174241

Gladkikh, V. I., & Mosechkin, I. N. (2021). Problems of improving criminal law measures of counteracting crimes in the sphere of computer information. *Russian Journal of Criminology 15*(2): 229-237. https://doi.org/10.17150/2500-4255.2021.15(2).229-237

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies 10*(2): 243-249. https://doi.org/10.1177/a017405

Ho, H. T. N. & Luong, H. T. (2022). Research trends in cybercrime victimization during 2010–2020: a bibliometric analysis. *SN Social Sciences 2*(1): 1-32. https://doi.org/10.1007/s43545-021-00305-4

Ismail, M., & Aamar, O. (2019). Unauthorized access crime in Jordanian law (comparative study). *Digital Investigation 28*: 104-111. https://doi.org/10.1016/j.diin.2019.01.006

Jiang, M. (2021). Cybersecurity policies in China. In *CyberBRICS*, edited by L. Belli, 183-226. Cham: Springer. https://doi.org/10.1007/978-3-030-56405-6

Jordan, T., & Taylor, P. A. (1998). Sociology of Hackers. *Sociological Review 46 (4)*: 757-781.

Junger, M., Montoya, L., Hartel, P., & Heydari, M. (2017). Towards the normalization of cybercrime victimization: A routine activities analysis of cybercrime in Europe. *2017 international conference on cyber situational awareness, data analytics and assessment (Cyber SA)*: 1-8. London, United Kingdom. https://doi.org/10.1109/CyberSA.2017.8073391

Kremen, H. (1998). *Apprehending the computer hacker: The collection and use of evidence*. http://www.shk-dplc.com/cfo/articles/hack.htm

Lazarov, A. D., & Petrova, P. (2022). Modelling Activity of a Malicious User in Computer Networks. *Cybernetics and Information Technologies 22*(2), 86-95. https://doi.org/10.2478/cait-2022-0018

Leka, Y. V. (2019). The Motive of Crime in Foreign Law: A Comparative Legal Analysis. *Actual problems of improving of current legislation of Ukraine* 51: 145-154.

Leukfeldt, E. R., Notté, R. J., & Malsch, M. (2020). Exploring the needs of victims of cyber-dependent and cyber-enabled crimes. *Victims & Offenders 15*(1): 60-77. https://doi.org/10.1080/15564886.2019.1672229

Li, X. (2017). A Review of Motivations of Illegal Cyber Activities. *Kriminologija & socijalna integracija 25* (1): 110-126. https://doi.org/10.31299/ksi.25.1.4

Liu, S., & Cheng, B. (2009). Cyberattacks: Why, what, who and how. *IT professional 11* (3): 14-21. https://doi.org/10.1109/MITP.2009.46

Maiwald, E. (2003). *Network Security: A Beginner's Guide, second edition, California*. USA: McGrawHill Osborne Media.

Marques, D., Guerreiro, T., Carriço, L., Beschastnikh, I., & Beznosov, K. (2019). Vulnerability & blame: Making sense of unauthorized access to smartphones. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*: 1-13. Glasgow, Scotland.

Marthala, H. (2018). Machine Learning in Hacking Attempts. *International Engineering Journal for Research & Development 3* (1): 1-7.

Milani, R., Caneppele, S., & Burkhardt, C. (2022). Exposure to cyber victimization: Results from a Swiss survey. *Deviant Behavior 43*(2): 228-240. https://doi.org/10.1080/01639625.2020.1806453

Miró-Llinares, F., Drew, J., & Townsley, M. (2020). Understanding target suitability in cyberspace: An international comparison of cyber victimization processes. *International Journal of Cyber Criminology 14*(1): 139-155. https://doi.org/10.5281/ZENODO.3744874

Neufeld, D. (2023). Computer crime motives: Do we have it right? Sociology Compass: 1-42. https://doi.org/10.1111/soc4.13077

Neufeld, D. J. (2010). Understanding cybercrime. *43rd Hawaii International Conference on System Sciences*: 1-10. Koloa, Kauai, Hawaii.

Odunze, D. (2018). Cyber victimization by hackers: A criminological analysis. *Public Policy and Administration 8*(1): 8-15.

Oganesyan, B. (2012). The Concept of Motive of a Crime in the Theory of Criminal Law. *Bulletin of the Saratov State Law Academy 89*(6): 153-158.

Polyakov, V. V., & Shiryaev, A. V. (2018). Forensic aspects of the identity of victims of cybercrime. *Criminal procedure and forensic readings in Altai*: 165-172. Barnaul, Altai State University Publishing House.

Pusch, N., & Holtfreter, K. (2021). Individual and organizational predictors of white-collar crime: A meta-analysis. *Journal of White Collar and Corporate Crime 2*(1): 5-23. https://doi.org/10.1177/2631309X19901317

Reyns, B. W., Fisher, B. S., Bossler, A. M., & Holt, T. J. (2019). Opportunity and self-control: Do they predict multiple forms of online victimization? *American Journal of Criminal Justice 44*(1): 63-82. https://doi.org/10.1007/s12103-018-9447-5

RIA Novosti (2021, December 22) The expert assessed the damage from cybercrime in Russia in 2021. https://ria.ru/20211222/kiberprestupleniya-1764832102.html

Rorie, M. L. (2019). *The handbook of white-collar crime*. United Kingdom: John Wiley & Sons. https://doi.org/10.1002/9781118775004.ch16

Smith, T., & Stamatakis, N. (2021). Cyber-victimization trends in Trinidad & Tobago: the results of an empirical research. *International Journal of Cybersecurity Intelligence & Cybercrime 4*(1): 46-63. https://doi.org/10.52306/04010421JINE3509

Sturc, B., Gurova, T., & Chernov, S. (2022). The Specifics and Patterns of Cybercrime in the Field of Payment Processing. *International Journal of Criminology and Sociology 9*: 2021–2030. https://doi.org/10.6000/1929-4409.2020.09.237

Trittin-Ulbrich, H., Scherer, A. G., Munro, I., & Whelan, G. (2021). Exploring the dark and unexpected sides of digitalization: Toward a critical agenda. *Organization 28*(1): 8-25. https://doi.org/10.1177/1350508420968184

Cases Cited

Case 1-63/2021 [2021] Crimean Garrison Military Court (Russian Federation)

Case 1-268/2017 [2017] Leninsky District Court of Cheboksary (Russian Federation)

Case 1-77/2020 [2020] Frunzensky District Court of Vladimir (Russian Federation)

Case 1-191/18 [2018] Novokuznetsk District Court (Russian Federation)

Case 1-44/2018 [2018] Leninsky District Court of Vladikavkaz (Russian Federation)

Case 1-212/18 [2018] Soviet District Court of Kazan

HOW CITE THIS ARTICLE

Mosechkin I, "Unauthorised Access to Computer Information: The Motives for Committing a Crime" (2024) 12 (1) Ceza Hukuku ve Kriminoloji Dergisi-Journal of Penal Law and Criminology, 16.