UDC 34.096

"IDENTITY THEFT" IN THE STRUCTURE of CYBERCRIME

YANA KURTO
ALIAKSEI RADZIUK
Polotsk State University, Polotsk, Belarus

The implementation of multiple technologies has changed the perception of delinquency. Individuals are under the risk of previously unknown crimes. The article proposes conceptions, means and motives of such crime as «identity theft». We conclude that the increased probability of this cybercrime should be taken into account by scientific society.

The transition to the information society has led to a profound realignment of various spheres of public life. Mass computerization, introduction and development of the latest information technologies have transformed the fields of education, scientific research and social life. However, this process has led to the occurrence of new crimes related to the virtual space, the so-called cybercrimes. In order to make the Internet usage easier and convenient, individuals began providing various cybersystems with their data, which, by accumulating information, pose a threat of data leakage and violation of the right to privacy, honour and dignity. The spread of the Internet has contributed to the appearance of new opportunities and an enabling environment where perpetrators can use personal information of others to commit previously unrecorded crimes.

"Identity theft" is a relatively new name for an old-age phenomenon – impersonation [1, p. 5]. The impostor, both in the classic definition and in the projection to the core of "identity theft", is a person who took somebody else's name or a rank disguised as another person claiming to be someone else [2]. The term "identity theft" was introduced in 1964 and is translated to Russian as "theft of the personality" verbatim. This translation is not accurate, since it is impossible to steal a person's personality. The deviation from the original meaning could appear due to the implied intent of the crime - the usage of identifying information, which is usually understood as a part of the personality.

Identity theft should be meant by the crime of using someone's personal information in order to pretend to be them and to get money or goods in their name. [3]. The notion of "identity theft" is not sustainable. The meaning of the term depends on the context. This needs to be considered when qualifying a cybercrime. For instance, in §943.201 for of Wisconsin Statute, "identity theft" is defined as «unauthorized use of an individual's personal identifying information or documents». Nevertheless, in State v. Baron case Wisconsin State suggested another alternative meaning of the phenomenon — using someone's personal identifying information to harm that person's reputation. [4].

Furthermore, the emergence of previously unknown techniques of committing cybercrime has created dispute over the distinction of key terms that describe identity-related offences. Nowadays, there is no unified view on the difference of concepts of "identity theft" and "identity fraud". The exception of the first definition is the obligatory usage of someone's identifying information in varied ways and amounts. Identity fraud refers to the gaining of money, goods, services or other benefits through the use of a false identity [5]. Terms should not be mistaken with the akin identity-related crimes. For example, the creation of a false identity involving data that does not exist in reality differs with means of committing "identity theft".

In most cases "identity theft" is committed with the use of personal identification numbers (Social Security Number (SSN), passport number, driving license number or credit card number), personal address, personal telephone numbers, personal characteristics (handwriting), biometric data (fingerprints, voice). The main feature of "business identity theft" as a form of "identity theft" is the accomplishment of goal through the use of the name of the business, its address, telephone number, e-mail address, logo, trademark, Web site, corporate credit card number, checking account number, and tax identification numbers [1, p. 3].

"Identity theft" is highly dependent on the leakage of information from large organizations and, particularly, from social networks. Facebook, the largest social network in the world has been the target of major attacks several times in recent years. They have led to data leaks. In April 2021, the dataset was posted on the hacker forum for free, making it available to anyone with basic data skills. This data set included their phone numbers, Facebook IDs, full names, locations, birthdates, bios, and, in some cases, email addresses [6].

It's worth mentioning, that "identity theft" does not occur at the time the offender receives the identifying information, but in subsequent crimes involving the use of stolen information.

Those who gain access to information illegally will not always commit following criminal acts only by themselves. They can sell the material to people with the proper skills, who, in their turn, will commit the crime. On top of that, "identity theft" is a crime that enables offenders to commit other socially dangerous acts more effectively. Fraudsters use stolen bank card numbers to purchase names, addresses, Social Security Numbers through intermediaries and then use illegally obtained data to commit the crime.

The development of the newest means of communication and the global flow of information on the Internet have also led to the emergence of various motives and purposes of committing crimes. The following motives of "identity theft" can include:

1. Infliction of harm for profit or with revenge purposes
2. Social motive. It encompasses the criminal's desire to express his superiority over others.
3. Political motive. This motive includes achieving access to identification information of public organizations or political parties. The possession of such information makes it possible to make statements on behalf of an institution or to manipulate state powers for fraudulent purposes.

In 2002, when cybercrime was not a common crime, The Federal Trade Comission (FTC, the USA) estimated that 10 million people were victims in 2002 [7]. The Commission's report as of February 2021 revealed frightening statistics on the increase of "identity theft" cases from 444,344 (2018), 650,523 (2019) to 1,387,615 (2020) in the United States [8]. In 2020, the number of cybercrimes had doubled in comparison with 2019. Due to the reliance of society on the Network due to the COVID-19 pandemic, it is now easier for fraudsters to implement their illegal intentions, as the protection options have become more fragile. Additionally, there is a tendency of the increase of electronic payments. Undoubtedly, we can observe a corresponding increase in the level of "identity theft" along with other cybercrimes.

The computerization and the development of new technologies have led to the rise of various cybercrimes, particularly "identity theft". The foregoing demonstrates that "identity theft" is one of the most urgent and rapidly growing forms of cybercrime. "Identity theft" is a serious challenge to the established system of personal security in view of the complexity of the crime, as well as the painful consequences for the victim. The survey on the phenomenon of "identity theft" should be continued with the purpose of preventing this criminal act.

REFERENCES

1. Hoffman, Sandra K. Identity theft : a reference handbook / S.Hoffman – Praeger, 2010. – 262 p.
2. Толковый словарь живого великорусского языка [Электронный ресурс] – Mode of access : https://dal.slovaronline.com/. – Date of access : 15.04.2021.
3. Cambridge Dictionary [Electronic resource] – Mode of access : https://dictionary.cambridge.org/ru/. – Date of access : 11.04.2021.
4. Brenner, Susan W. Cybercrime : criminal threats from cyberspace / S. Brenner – Praeger, 2010. – P. 98.
5. Wayback Machine: Internet Archive : website. – Standardisation of Definitions of Identity Crime Terms – Mode of access : https://web.archive.org/web/20090630021710/http://www.acpr.gov.au/pdf/Standdefinit.pdf. – Date of access : 15.04.2021.
6. Holmes, A. 533 million Facebook users' phone numbers and personal data have been leaked online [Electronic resource] / A. Holmes // Insider. – April, 3 2021. – Mode of access : https://www.insider.com/ . – Date of access : 14.04.2021.
7. Loberg, Kristin Identity theft : how to protect your name, your credit and your vital information — and what to do when someone hijacks any of these. – Los Angeles, Calif.: Silver Lake Pub., 2004. – P.6.
8. Consumer Sentimel Network [Electronic resource] // Federal Trade Commission. – February 2021. – Mode of access : https://www.ftc.gov . – Date of access : 05.04.2021.