


DOI 10.36074/grail-of-science.24.09.2021.07

DRIVERS OF CYBERCRIME IN THE FINANCIAL SPHERE

Bozhenko Victoria Volodymyrivna 

PhD, Associate Professor of the Economic Cybernetics Department
Sumy State University, Ukraine

Yarovenko Hanna Mykolaivna 

PhD, Associate Professor of the Economic Cybernetics Department
Sumy State University, Ukraine

The COVID pandemic provoked an increase in Internet payments, an growth of electronic financial services, and an increase in the use of cryptocurrencies and altcoins as a means of payment and investment tool. These trends indicate the acceleration of the pace of digitalization of the economy and the transformation of approaches to the organization of business processes. Under these conditions, the digital transformation of financial relations opens up new opportunities to increase the efficiency of financial institutions and reduce their costs by optimizing transactions, and threats to their stable operation - the spread of cyberattacks and increase the frequency of their implementation. Thus, the dynamic digitalization of the economy makes financial institutions more vulnerable to cybercrime.

In the event of a financial data breach, confidential data may be used for illegal activities or sold on dark websites, which may lead to the loss of business reputation of both financial institutions and their customers.

In 2020, the damage from cybercrime to the world economy is estimated at 5.5 trillion euros, which is twice as much as in 2015 [1]. At the same time, in recent years, financial services have been and remain the main target for cybercriminals.

Combating cybercrime is a global problem, the consequences of these illegal acts are felt by all countries of the world, regardless of their level of development. In particular, in 2019, 39% of EU citizens who used the Internet faced information security problems [2]. This figure varies widely in different EU Member States: more than 50% in the UK and less than 10% in Lithuania.

Cybercrime has reached unprecedented proportions due to factors:

- powerful development of electronic computers, mobile devices allowed to increase the speed of data processing and gain constant access to financial services. Thus, in 2019 there were about 5.2 billion mobile users in the world, covering 67% of the world's population, while in 2015 - 4.66 billion, in 2010 - 3.219 billion people [3].

- increase the number of devices connected to the Internet;

- increasing the number of users of social networks, which accumulate a significant amount of personal information, which is then used to assess consumer

preferences, as well as serve as an effective channel for promoting innovative financial products. According to Emerketer, the penetration rate of social networks in the world in 2020 was 41.9% of the total population or 3.23 billion users. For comparison: in 2017 - 2.3 billion users or 31.2%, in 2013 - 1.6 billion users or 22.8% [4].

- the possibility of anonymous illegal activities;
- low level of digital culture. In 2019, only 58% of the population in EU countries have at least basic digital skills (compared to 55% in 2015) [2];
- increase the use of the Internet to pay for goods / services, carry out financial transactions, receive administrative services, etc. In 2019, 66% of the EU population will use online banking services, 67% - e-government services and 71% - online shopping [2].

In addition to the above factors of the rapid spread of cyber threats in the world, it is worth highlighting the specific drivers that are inherent in the financial sector, namely: increasing the share of banking processes that are transferred to third parties, including abroad; use of cloud technologies for data transmission; expanded use of robotics or algorithms for automated trading and application development; increasing the use of virtual and digital currencies.

Thus, the growing intensity of cybercrime, the improvement of information technology, creating new opportunities for these crimes, the need for other approaches to combating crimes committed in cyberspace, pose a threat to global information networks and society as a whole.

The paper was executed in the framework of state budget scientific research works: "Data-Mining for Countering Cyber Fraud and Money Laundering in the Context of Digitalization of the Financial Sector of the Ukrainian Economy" (Registration No. 0121U100467), and "National Security Through the Convergence of Financial Monitoring Systems and Cybersecurity: Intelligent Modeling of Financial Market Regulation Mechanisms" (Registration No. 0121U109559).

References:

- [1] Aldasoro I., Frost I., Gambacorta L. & Whyte D. (2021). Covid-19 and cyber risk in the financial sector. *BIS Bulletin* #37. URL: <https://www.bis.org/publ/bisbull37.htm>.
- [2] Digital Economy and Society Index (2020). European Commission. URL: <https://digital-strategy.ec.europa.eu/en/policies/desi>
- [3] The Mobile Economy (2020). GSM Association URL: https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_Global.pdf
- [4] Jayasree V. & Siva Balan R.V. (2016). Anti money laundering in financial institutions using affiliation mapping calculation and sequential mining. *Journal of Engineering and Applied Sciences*. 11(1), 51-56. URL: <http://docsdrive.com/pdfs/medwelljournals/jeasci/2016/51%2D56.pdf>