

Cyber Fraud as a Relevant Internet of Things Security Threat

Olga R. Afanasyeva¹^a, Valentina I. Shiyan¹^b and Maria V. Goncharova²^c

¹Russian University of Transport, 9 Obraztsova street, Moscow, Russia

²All-union scientific research Institute of the Ministry of Internal Affairs of Russia, 25 Povarskaya Street, Moscow, Russia

Keywords: Cybercrime, Cyber Fraud, Internet of Things, Information and Telecommunication Technologies, Security, Cybercrime Indicators, Counteraction.

Abstract: Based on the official statistical reports of the Ministry of Internal Affairs of the Russian Federation for 2018-2020 and the results of criminological studies on cybercrime, the article describes the relevance of the cyber fraud threat to the security of the Internet of Things. The main indicators characterizing cyber fraud are given - the state, dynamics, structure, amount of damage caused; the number of persons identified for their commission, and the number of victims. The specificity of the method of committing cyber fraud is revealed. The tendencies of cyber fraud, which are the most relevant for the current period, are identified. A conclusion is made about the need to improve the effectiveness of countering cyber fraud by improving the legal mechanisms regulating information legal relations, including international ones, as well as improving the qualifications of the personnel in the field of information security and activating joint comprehensive and coordinated preventive measures of law enforcement agencies.


1 INTRODUCTION


The development of science and technology, the globalization of information processes, the virtualization of life, the continued growth of the number of devices and software systems connected to the Internet, the expansion of the range of their use to permanent and ubiquitous - from individual users to industrial scales; with intersectoral interaction; within the national and interstate framework, - caused the transition from the so-called Internet of People to the Internet of Things. In the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030, approved by the Decree of the President of the Russian Federation dated May 09, 2017, No. 203, the Internet of Things is defined as "the concept of a computer network connecting things (physical objects) equipped with embedded information technologies for interacting with each other or with the external environment without human participation."


The existing extent of the Internet of Things allows us to speak of it as a phenomenon or even an

occurrence, since it is both a concept and a set of interconnected technologies that are widely used in monitoring systems in various fields, robotics, artificial intelligence, machine learning, processing, storage, the transmission of "big data", etc. (Wachter, 2017). And although more than twenty years have passed since its first mention in 1999 by Procter&Gamble employee Kevin Ashton, active development of this technology has occurred in the last few years. It should be pointed out that any social changes (both positive and negative) only contribute to this process. For example, the COVID-19 coronavirus infection pandemic and the imposed restrictions associated with it have significantly increased the segment of Internet users, as well as goods and services provided and used online.

Nowadays, the Internet of Things resulted in structural changes in the economy. It has found application in the areas of industrial production; healthcare (remote monitoring of patients' health and medical equipment); defense (intelligent military equipment, threat identification and prompt response to them); security (smart guard, real-time location determination); telecommunications (cellular

^a <https://orcid.org/0000-0002-4819-8111>

^b <https://orcid.org/0000-0003-1295-4947>

^c <https://orcid.org/0000-0003-3678-2246>

communications, remote control and management of devices, the implementation of high-tech products and services in order to develop a smart city and a smart home (home automation), security solutions, monitoring of transport and environmental conditions, digitalization of manufacturing industries, work of state institutions and organizations); housing and communal services (management of energy resources, elevators, maintenance of buildings); transport complex (geolocation systems, development of communication along the roads, improvement of vehicles by embedding in GSM-modules, smart alarms with remote control units, insurance telematics trackers, video recorders, monitoring of commercial vehicles and fuel consumption, a system for collecting payments from heavy vehicles (Platon project)); trade (on-line retailers are already competing with traditional stores by offering unique and personalized services to customers).

In addition, wearable devices (smartphones, tablets, smartwatches, fitness trackers), which are available to almost every person, are an example of everyday use of the Internet of Things. Their design features, having built-in electronics, software, means, and sensors that provide communication, allow them to exchange information with other devices, including in automatic mode, without human intervention.

Like any progressive technical innovation, the Internet of Things is fraught with serious threats, creates additional risk zones, giving rise to special types of criminal behavior and new forms of crime (cybercrime), making its users more and more vulnerable from external cyber threats (Afanasyeva, 2020; Dechamp, 2005).

In this regard, criminological information on the state and trends of cybercrime is essential for targeted and timely prevention (Smushkin, 2020).

2 STUDY METHODOLOGY

The research is based on the general scientific dialectical method of cognition. Furthermore, a set of research methods that had been multiply proven in criminological science were used, including analysis, synthesis, deduction, induction, systemic structural (when studying the results of criminological research, the cyber fraud rate and methods, identifying their tendencies), statistical (when studying statistical data characterizing the number of registered cyber frauds and the persons who committed them, as well as victims of such crimes), formal-logical (when formulating proposals to improve countering cyber

fraud), differentiation, integration, etc., which allowed the research group to achieve the set objective.

3 STUDY RESULTS

According to the statistics of the Federal State Institution “GIAC of the Ministry of Internal Affairs of Russia”, a significant increase in cybercrimes is recorded annually (Table 1).

Table 1: Dynamics of cybercrimes in the Russian Federation in 2018-2020.

Cybercrimes	2018	2019	2020
Total	174,674	294,409	510,396
Increase/decrease,%	–	68.5	73.4

This situation is typical not only for Russia, but also for foreign countries. Thus, in 2020, 791,790 cybercrime allegations were registered in the United States (+ 69% compared to 2019) (Figure 1).



Figure 1: Trends in the number of reported cybercrime allegations and the amount of damage caused by cybercrimes in the United States in 2016-2020.

The virtual nature, anonymity, and the variety of possible criminal actions are most attractive for the implementation of all kinds of fraudulent schemes that are impossible in the real world (Goncharova, 2017; Shiyan, 2010; Wagen W. van der, 2015). It is about cyber fraud, i.e. the embezzlement or the acquisition of the right to another person's property by deception or abuse of trust, committed with the use or application of information and telecommunication technologies. This is confirmed by the fact that frauds occupy the most significant share in the structure of cybercrimes (total: 237,074; 46.45%) (Figure 2).

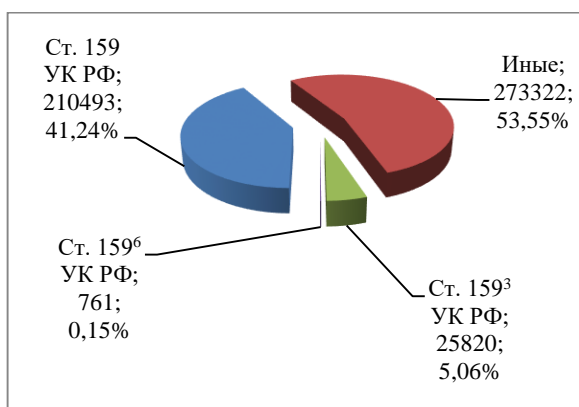


Figure 2: Cybercrime structure in the Russian Federation in 2020.

99.7% of cyber frauds are detected by employees of the internal affairs bodies.

At the end of 2020, there is an increase in indicators characterizing cyber fraud (Table 2).

Table 2: The dynamics of cyber fraud in the Russian Federation in 2018-2020.

Cyber fraud	2018	2019	2020
Art. 159 of the Criminal Code of the Russian Federation	90,664	119,903	210,493
Increase/decrease, %	-	32.2	75.6
Art. 159³ of the Criminal Code of the Russian Federation	4,242	16,119	25,820
Increase/decrease, %	-	280.0	60.2
Art. 159⁶ of the Criminal Code of the Russian Federation	970	687	761
Increase/decrease, %	-	-29.2	10.8

The methods of cyber fraud are the commission of criminal acts using: the Internet (35.60%), mobile communications (28.43%), payment (plastic) cards (12.83%), methods of social engineering (psychological manipulation) (9.04%), social networks (3.80%), electronic payment systems (3.03%), SIP telephony (2.50%), instant messaging (Internet messengers) (2.20 %), computer hardware (1.62%), software (0.77%) and fictitious electronic payments (0.19%).

11,969 people were identified for committing cyber fraud (one third (29.1%) are women), among whom the most criminally active age groups are traditionally: 30-49 years old (33.6%) and 18-24 (11.8%) (Broadhurst, 2014).

223,841 people were recognized as cyber fraud victims, which is more than half (56.0%) of the victims of all cybercrimes. At the same time, in the

structure of cyber fraud victims, the proportion of pensioners and minors is 17.0% and 0.9%, respectively.

The Internet Crime Complaint Center research on cybercrime victims indicates that the countries other than the United States with the highest numbers of victims of cyber attacks are the United Kingdom, Canada, India, Greece, Australia, South Africa, France, Germany, Mexico, and Belgium.

The amount of material damage from cyber fraud only in the Russian Federation amounted to 27,784,093 thousand rubles.

The analysis of statistical information on cyber fraud and the results of criminological studies allow us to highlight the following most relevant trends inherent in the development of the investigated type of crime.

In the banking sector, this is social engineering, defined by Yu.V. Truntsevsky as a fraudulent attack committed by deceiving or abusing the trust of a bank client in order to obtain confidential information from him (Truntsevsky, 2020).

Phishing is one of the most common types of fraudulent attacks. Phishing is a universal threat that works across all platforms. Technically, phishing is constantly evolving. Currently, it is carried out via SMS (smishing) or voicemail (vishing). For example, in SMS phishing, a text message may contain a malicious link that will download malware or spyware to your device.

Fake sites have a design similar to the original, have quite convincing URLs, in some cases, they use a secure connection (HTTPS), even with genuine certificates. Due to the technical features of mobile phones and tablets, it is often more difficult to recognize a fake site than on a computer or laptop.

Pharming and vishing are types of phishing. Farming provides to get confidential data not through a letter and following a link, but directly on the official website. Farmers change the digital address of the official website on the DNS server to the address of the spoofed site, and as a result, the unsuspecting user is redirected to the fake site.

Vishing is to obtain information through the use of telephone communications. The notification letter indicates the phone number to call back in order to eliminate the "problem that has arisen". Then, during the conversation, the operator or answering machine asks the user to provide identification data to solve the problem.

The extended targeting attack of increased complexity - Metel (a banking Trojan known as Corkow) is particularly alarming. It was detected in 2011. At that time, on-line banking systems were the

place of its distribution. Since 2015, fraudsters have begun to subject banks themselves (especially ATMs) and financial institutions to cyberattacks. As a result of these actions, bank cards were turned into unlimited credit cards, since after withdrawing money from the attacked bank card at ATMs of other banks, the system automatically cancels the withdrawal of funds and maintains the same balance.

By the end of 2020, Kaspersky Lab mobile products and technologies alone detected 156,710 new mobile banking Trojans.

It should be noted that the provisions of the Federal Law dated June 27, 2018, No. 167-FZ "On Amendments to Certain Legislative Acts of the Russian Federation Regarding Countering the Theft of Funds" empowered financial institutions to timely block illegal transactions. This is facilitated by the launch of the FinCERT and Feed-Antifraud automated systems.

Cyber fraud with personal data and digital accounts is also widespread, which often leads to enormous damage (Muzhchinina, Erakhmilevich, 2019). In 2020, the average "cost" of a single data breach all over the world was nearly 4 million US dollars. The most expensive of these occur in the health sector (7.13 million US dollars), as well as the energy and financial segments (6 million US dollars). At the same time, any companies, including large ones, are susceptible to data leaks (Figure 3).

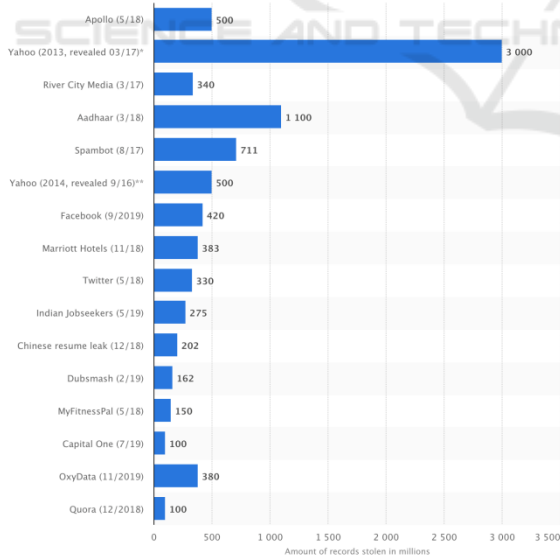


Figure 3: Number of compromised data records in cases of data breaches (as of January 2021, in millions).

The progressive movement of cryptocurrency, a digital means of payment, which has a unique transaction code that prevents copying and ensures

the owner's absolute anonymity, has led to the emergence of new fraudulent schemes on cryptocurrency exchanges. In particular, fraudsters find their victims through the Discord cryptocurrency servers and send them to fake crypto exchanges, as well as a network of fake news sites designed to convince investors (cryptocurrency owners) of the legitimacy of fake sites.

Electronic digital signature fraud is quite common. Note that the relationship in the use of electronic signatures in the performance of civil transactions, the provision of state and municipal services, the performance of state and municipal functions, in the performance of other legally significant actions are regulated by the Federal Law dated April 06, 2011, No. 63-FZ (as amended on February 24, 2021) "On electronic signature". At the same time, according to the fair comment of M.M. Darkina, the legislation on electronic signature is insufficiently systematized, the issues of liability for fraud associated with electronic digital signature remain completely unresolved, as well as the risks of abuse and the human factor when using an electronic signature remain (Darkina, 2020). As a result, this type of criminal act is especially popular in the area of real estate, lending, state registration of legal entities, banking, and public procurement. The above circumstances indicate the need to modernize measures to counter this type of fraud.

Another negative trend is that cyber fraudsters have the ability to avoid identification by using software technologies VPN, Tor, Proxy, which allow them to maintain anonymity, bypass blocking, change the IP address of the Internet user, create dynamic or unrecognizable IP addresses, as well as to apply technologies of spoofing subscriber numbers through SIP telephony.

4 DISCUSSION OF RESULTS

The data we have provided on cyber frauds only give a general idea of them as a threat to the Internet of Things, since there are no reliable statistics that reflect the real picture in this area. The reason lies not only in the high level of latency of the crimes under consideration and the often transboundary nature of criminal activity, but also in the absence of reliable methods of collecting information, a uniform practice of generating criminal statistics and the application of relevant legislation in various constituent entities of the Russian Federation.

5 CONCLUSIONS

The results of this study allow us to state the following.

Improving the effectiveness of countering cyber fraud is due to the need to improve the legal mechanisms that regulate:

- information legal relations arising from the search, receipt, consumption of various categories of information, information resources, information products, information services;
- processes of production, transmission and distribution of information, information resources, information products, information services;
- information legal relations arising from the creation and use of information systems, their networks, means of support, telecommunication infrastructure.

Taking into account the transnational nature of cyber fraud, there is still a need for qualified staffing in the information security, increasing the effectiveness of the appropriate rapid response, activating joint comprehensive and coordinated preventive measures and special operations of law enforcement agencies in Russia and foreign countries. The development of the international legal framework for cooperation between states, the improvement and harmonization of national legislation should be carried out taking into account the sign of consistency inherent in law, taking into account the specifics of the criminal situation, political, economic, social and cultural development of each country.

REFERENCES

- Afanasyeva, O.R. (2020). Modern problems of combating crime in Russia. *Investigation of crimes: problems and solutions*, 2 (28), 29-31.
- Goncharova, M.V. (2017). *Factors that determine cybercrime. Problems of crime determination and prevention*. Ed. Professor A.I. Debt. All-Russian public organization "Russian Criminological Association". Moscow, pages 84-88.
- Darkina, M.M. (2020). The practice of using electronic digital signatures in business. *Law and the Digital Economy*, 3: 28-35.
- Muzhchinina, A.S. and Erakhmievich, V.V. (2019). "Internet money" and "Internet property" as the subject of theft. *Problems of legal and technical protection of information*, 7: 90-98.
- Smushkin, A.B. (2020). Selected aspects of using the concept of the Internet of Things to combat crime. *All-Russian Criminological Journal*, 14 (3): 453 - 460.
- Truntsevsky, Yu.V. (2020). Modern banking fraud challenges to e-commerce financial support. *Banking Law*, 6: 28 - 36.
- Shiyan, V.I. (2010). The state and dynamics of frauds committed by women. *Society and Law*, 5 (32): 167-171.
- Broadhurst, R. (2014). Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime. *International Journal of Cyber Criminology*, 8(1).
- Dechamp, C. (2005). *Cybercriminalité. Défense nationale. Paris*, 99-120.
- Wachter, S. (2017). Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR. *Computer Law & Security Review*, 34(3): 436-449.
- Wagen, W. van der (2015). From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks. *The British Journal of Criminology*, 55(3): 578-595.