Artificial intelligence as an instrument against social engineering

V V Britvina\textsuperscript{1}, D A Musatova\textsuperscript{2}, A V Altoukhov\textsuperscript{2}, A S Zueva\textsuperscript{3} and A Y Sorokin\textsuperscript{4}

\textsuperscript{1}Moscow Polytechnic University, 38, st. Bolshaya Semyonovskaya, Moscow, 107023, Russia
\textsuperscript{2}Lomonosov Moscow State University, 1, Leninskie Gory, Moscow, 119991, Russia
\textsuperscript{3}Financial University under the Government of the Russian Federation, 49, Leningradsky avenue, Moscow, 125993, Russian Federation
\textsuperscript{4}Academy of Civil Protection of the Ministry of Emergency Situations of Russia, 1, Sokolovskaya, Khimki, 141435, Russia

E-mail: itlaw@audit.msu.ru

Annotation. This article discusses the use of artificial intelligence technologies in the fight against social engineering. The purpose of this study is to analyze the technologies of artificial intelligence, its main features and the possibilities of its application. The article also examines the issue of improving the legislation of the Russian Federation, taking into account the use of artificial intelligence technologies. This problem is extremely relevant today due to the growth of crimes involving social engineering methods.

1. Introduction.
Nowadays the technological progress has reached its peak amplitude, covering more institutions and social sectors as ever before. Creation of robotics, fast mobile networks, biotechnology, a development of cybersecurity systems are all due to AI application. In recent past, technologies that are able to create unique outputs by applying logical analysis, not encoded features that a developer allowed it to perform, seemed to be unachievable and mostly fictional. However, today’s artificial intelligence is able to perform specific tasks, interact with the outside world, adapt to its changes, self-study and improve based on the analysis of the actions that have already been performed.

2. Materials and methods
In the process of writing this article, the following methods were used: methods of analyzing the literature, analyzing regulatory documents, comparing the experience of different states in the observable area, specific legal and comparative legal methods.

3. Results
For this article, let us start with giving a definition to AI. Artificial Intelligence can be seen as a specific system that collects observable information and data, creates its own logic, and makes its independent decisions in a manner of a human being. AI consists of three main components: a database, a solver (a system that sorts data and finds a solution) and an interface, that allows a user to communicate with the system.
A program has to include these features in order to be treated as AI:

- Partial or complete autonomy, i.e. the ability to perform assigned tasks without human intervention, depending on the current state of the surrounding world and its perception by the system (cognitive and adaptive autonomy; spatial-kinetic autonomy);
- Self-regulation;
- Adaptation to changing environmental conditions;
- Ability to find independent solution of the assigned tasks and goals;
- Testing and self-testing of virtual and physical realities.

Technologies that implement artificial intelligence are able to instantly make the necessary optimal decisions in real time based on the analysis of a huge amount of data, ensuring the effectiveness of its work in almost all areas of application. In particular, artificial intelligence technologies can be used to combat fraud and social engineering.

**Types of social engineering**

Social engineering can be understood as a complex combination of various psychological techniques for obtaining confidential information on behalf of further fraud. Over the past two years, with the help of social engineering, about 2 billion dollars have been stolen from Russians from their bank deposits. Criminals use these methods as the human factor is a weaker and more vulnerable link in the information security system than the computer. As for the most popular types of social engineering, it is needed to denote the following fraud strategies:

1. **Pretexting** is a set of worked out actions according to a specific, pre-compiled scenario, as a result of which the victim can give out any information or perform a certain action. To use this technique, the attacker must initially have some data about the victim (name; date of birth; place of residence or registration; place of work, etc.);

2. **Phishing** is a type of Internet fraud, the purpose of which is to gain access to confidential user data - logins and passwords. This is achieved by sending bulk emails. The letter often contains a direct link to the site, indistinguishable from the real one, or to a site with a redirect. After the user lands on a fake page, the scammers, by using various psychological methods, try to induce the user to enter their username and password on a fake page, which an individual uses to access a certain site, which later allows fraudsters to gain access to Internet accounts and bank accounts;

3. **Trojan** is a type of Internet fraud, the purpose of which is to "fish out" confidential data from the victim - logins, passwords, bank details. Scammers create fake sites, after which the scammers send emails to users on behalf of popular brands or from government agencies, banks, lawyers with scary messages (fines, outstanding debt, account blocking), with a direct link to the fake site (or to a site with re-direct). The user is informed that he must enter his credentials in order to solve certain problems. As a result, fraudsters gain access to accounts (e-mails, social networks) and bank accounts;

4. **Quid pro quo** - this technique involves the attacker to contact the user by e-mail or corporate phone. An attacker can introduce himself, for example, as a technical support employee and inform about technical problems at the workplace. Then he informs about the need to eliminate them. In the process of “solving" such a problem, the attacker pushes the victim to take actions that allow the attacker to execute certain commands or install the necessary software on the victim's computer;

5. **Baiting** - this method is an adaptation of a Trojan and implies the usage of physical data storages (CD, flash drives). An attacker usually drops such item in public places on the territory of a company (parking lots, canteens, employee workplaces, toilets);

6. **Inverse social engineering** - a type of attack that aims to create such circumstances under which the victim will be forced to ask the attacker for "help". For example, an attacker can send an email with phone numbers and contacts of the "support service" and after a while create technical problems in the victim's computer. In this case, the user will call or e-mail the attacker himself, and in the process of "fixing" the problem, the attacker will be able to obtain the data he needs.
4. Discussion

One of possible solutions to prevent social engineering is to try to exclude a person as the target of an attack, by replacing him with an automatic system, or at least installing him as an intermediary between the attacker and the user of the system.

Let us analyze the methods of dealing with malware, phishing websites and viruses. A correctly working code with an implementation of statistical analysis will allow an artificial intelligence to make the most correct decisions in terms of probabilities [10]. In order to prevent social engineering in a corporate sector, AI system can be set up in a way that it can analyze the content of emails in a company's e-mail before being read by an employee, as well as control incoming calls. After analyzing a large number of letters, this system will be able to develop certain templates that can determine who is sending the letter: a business partner or a fraudster. In addition, such system will be able to analyze the links attached to the letter. Here we exclude the human factor, since the employee can, without hesitation, click on it, and the system will perform checking and block the link. More to say, the artificial intelligence system should contain database of phone numbers and e-mails of partner companies and check them less thoroughly, which will undoubtedly speed up its checking process.

Among the most promising solutions, it is worth noting the technologies for protecting against deep-fake threats (a method for synthesizing a human image based on artificial intelligence).

Artificial intelligence systems are particularly effective in preventing credit card fraud, which has grown exponentially in recent years due to the rapid development of e-commerce and online transactions. The system analyzes customer behavior, locations and shopping habits and triggers a safety mechanism when something seems dangerous to the AI system and contradicts the established behavioral pattern.

The most common form of social engineering is telephone fraud. Consider possible ways to combat this type of social engineering using artificial intelligence systems together with the legal regulation of these methods:

1. One of the fairly common methods of telephone fraud is its commission from prisons. According to the order of the Ministry of Justice of the Russian Federation of December 16, 2016 No. 295 "On Approval of the Internal Regulations of Correctional Institutions", the list of things and items that convicts are prohibited from making, having with them, receiving in parcels, parcels, parcels or purchasing includes mobile communications and communications or components for them, ensuring their work [7]. Article 116 of the CEC of the Russian Federation states that suspects, accused and convicted persons cannot be clients of operators, since they are allowed to call relatives only using payphones installed in the institution - it is strictly forbidden to have mobile phones with them. Nevertheless, including due to the corruption of the FSIN employees, telephone fraud committed from prison zones is very common. According to Alexei Istomin, a lawyer and Moscow Digital School expert, the introduction of artificial intelligence systems will drastically reduce the level of corruption in prisons, as well as paralyze the illegal activities of prisoners[11]. Control over prisoners by means of artificial intelligence systems can not only be carried out using security cameras (which is still available today), but also be expressed in identifying the frequency of contacts and external connections among prisoners and colony employees, and it will also be possible, based on the rules of behavioral analytics, to identify signs of potential negative behavior, including situations where prisoners are using mobile phones (for example, the system can detect this by scanning radio waves or through the system's listening devices). With the introduction of artificial intelligence systems, control over the activities of both the prisoners themselves and the employees of the Federal Penitentiary Service will be more transparent, which significantly reduces the risk of corruption. Also, with the interaction of operator companies and companies developing artificial intelligence systems, a situation is possible when the system will be able to track the geolocation of an incoming call and block calls coming from the territory of places of detention.

For the legislative consolidation of the introduction of artificial intelligence systems in places of deprivation of liberty, amendments should be made to the Criminal Executive Code of the Russian
Federation (in particular, section 4). It is also possible to issue a Federal Law regulating this method [1].

2. In the UK, the CEO of an energy company transferred money to cybercriminals after a telephone conversation with a robot. The CEO spoke on the phone with his boss, the head of the head office in Germany. He asked him to urgently transfer almost $ 250 thousand to the Hungarian supplier. The money went to the account of a Hungarian bank, and the British top manager did not even suspect that he had been talking to the robot all this time. Artificial intelligence imitated not only the manner of communication, but also a slight German accent, that is, the system initially considered all the properties of the voice. Accordingly, we can talk about the opposite effect. Artificial intelligence can work through an already existing call base and identify patterns in the manner of communication, as well as determine the same voice in cases when fraudsters call from different numbers. Thus, when processing a voice in an incoming call and identifying similar characteristics with the voices already existing in the database, the system can either send a notification to the victim or block the call. In this case, we are talking about both the voice itself and the manner of conversation (when a fraudster asks certain questions of a certain nature, clarifies details regarding financial details, and more) [12].

In this case, from the point of view of legislation, it is worth talking about the necessary amendments to the Federal Law of July 26, 2006, No. 149-FZ "On Information, Information Technologies and on the Protection of Information" and the Federal Law of July 7, 2003, No. 126-Federal Law "On Communication". It is also worth considering the publication of special orders of Roskomnadzor and the Ministry of Telecom and Mass Communications [2].

3. Due to the fact that fraudsters often change numbers and it is quite difficult to identify them, a situation is possible when the artificial intelligence system will generate incoming complaints about fraud indicating the number of the incoming call, and automatically block this number, even if a small number of complaints are received. to a specific number.

Within the framework of this paragraph, we are also talking about changes in the Federal Law of 07.07.2003 No. 126-FZ "On Communications" [3].

4. Artificial intelligence systems can be used in the case of transferring funds through a mobile bank. The system can process the user's behavior, study his contacts and conduct an in-depth analysis of the history of financial transactions, so that if a transfer is made to a fraudster (provided that this transfer is made for the first time) of funds, this operation is presumed as suspicious and blocked. In order to unlock, the user will need to contact the support service, where the artificial intelligence system, through a conversation with such a user, will determine whether it is possible to approve this operation [8-9].

In this case we are talking about a certain kind of wiretapping, it is worth mentioning the need to make changes for the safety of citizens in the Federal Law "On Personal Data" of July 27, 2006 N 152-FZ and the Federal Law of July 26, 2006 No. 149-FZ "On Information, Information Technologies and Information Protection". Also, it is appropriate to note the possibility of amending the introduction and active functioning of artificial intelligence systems in banks in the Federal Law "On Banks and Banking Activities" dated 02.12.1990 N 395-1[4-6].

5. Conclusion
Based on the analyzed literature and given assumptions, it is appropriate to say that AI has enough evidence to be used against social engineering and cyber frauds. In order for it to perform well, AI has to be regulated by the authorities in order to provide a legal approach and certain rules on how AI should be used, where it can be implemented and against what type of fraud.

AI is an efficient tool against social engineering as it has no human factor and it is able to predict a fraud phone call or e-mail with a database of such events and cases.

References
[1] CEC of the Russian Federation, article 116 Place of origin: Russian Federation
[2] Federal Law of July 26, 2006, No. 149-FZ "On Information, Information Technologies and on the Protection of Information" Place of origin: Russian Federation

[3] Federal Law of July 7, 2003, No. 126- Federal Law "On Communication Place of origin: Russian Federation

[4] Federal Law "On Personal Data" of July 27, 2006 N 152-FZ Place of origin: Russian Federation

[5] Federal Law of July 26, 2006 No. 149-FZ "On Information, Information Technologies and Information Protection" Place of origin: Russian Federation

[6] Federal Law on 02.12.1990 N 395-1 "On Banks and Banking Activities" Place of origin: Russian Federation

[7] Order of the Ministry of Justice of the Russian Federation of December 16, 2016 No. 295 "On Approval of the Internal Regulations of Correctional Institutions" Place of origin: Russian Federation

[8] Omran Salem, Alamgir Hossain and Mumtaz Kamala 2010 Awareness program and AI based tool to reduce risk of phishing attack. 10th IEEE International Conference on Computer and Information Technology 1418

[9] Vahid Behzadan, Arslan Munir and Roman V Yampolskiy 2018 A psychopathological approach to safety engineering in AI and AGI. International Conference on Computer Safety, Reliability, and Security 513-520

[10] Elena A Ostanina 2021 Counteraction to methods of social engineering as one of the areas of information protection of organizations with varying degrees of state participation. Amazonia Investiga 10(38) 123-129

[11] Salgado-Criado J, Fernandez-Aller C 2021 A Wide Human-Rights Approach to Artificial Regulation in Europe. IEEE Technology and Society Magazine 40(2) 55-65

[12] Ryan M and Stahl B C 2021 Artificial intelligence ethics guidelines for developers and users: clarifying their content and normative implications. Journal of Information, Communication and Ethics in Society 19(1) 61-86