Research on Brute Force and Black Box Attacks on ATMs

Pavel V. Revenkov [1], Alexander A. Berdyugin [1], and Pavel V. Makeev [1]

[1] *Financial University under the Government of the Russian Federation, Scherbakovskaya Street, 38, Moscow, 105187, Russia*

Abstract

As computer technologies are widely used in credit and financial institutions, risk management is an extremely relevant topic in the information technology security in banking structures. This article is focused on the problems of assessing the risks of information security breaches in automated teller machine (ATM). To increase the level of security of banking services for individuals and legal entities in accordance with the recommendations of information security standards by analyzing the risk of information security violations in electronic banking technologies (on the example of the "Brute force" and "Black box" attacks). Empirical methods of scientific knowledge (observation, measurement, experiment), theoretical methods (analysis, synthesis, induction, deduction, abstraction, formalization), graphical interpretation of information, probability theory methods. Standards for effective management of information security management at the enterprise are considered. The advantage of social engineering methods over the "Brute force" method of PIN codes is shown quantitatively. The time characteristics of commission and protective measures against attacks of the "Black box" type are analyzed. A method for improving the effectiveness of the response and protection of ATMs from attacks of the "Black box" type is proposed. The influence of school literature on scientific and technical progress is analyzed. Based on this, recommendations of the authors are given.

Keywords

Standards, PIN code, probability of selection, ATM, dispenser, cybercriminal, duration of a cyberattack

1. Introduction

Over the past decades, the conditions for the operation of commercial banks in all countries of the world have undergone significant changes. The factors of scientific and technological progress have led both to the emergence of new financial instruments and opportunities for banks [1], and to the need to manage completely new types of risks in accordance with new standards [2, 3, 4] that are the topic of discussion in this article.

The ISO/IEC 27000 series of international standards includes information security standards published jointly by the International Standardization Organization (ISO) and the International Electrotechnical Commission (IEC). The set consists of best practices and recommendations in the field of information security for creation, development and maintenance of information security management systems (ISMS). The combined application of these technical documents is depicted on the Figure 1. Each of them aims to investigate specific problems in information security management.

BIT-2021: XI International Scientific and Technical Conference on Secure Information Technologies, April 6-7, 2021, Moscow, Russia
EMAIL: pavel.revenkov@mail.ru (A. 1)
ORCID: 0000-0002-0354-0665 (A.1); 0000-0002-5298-5177 (A. 2)

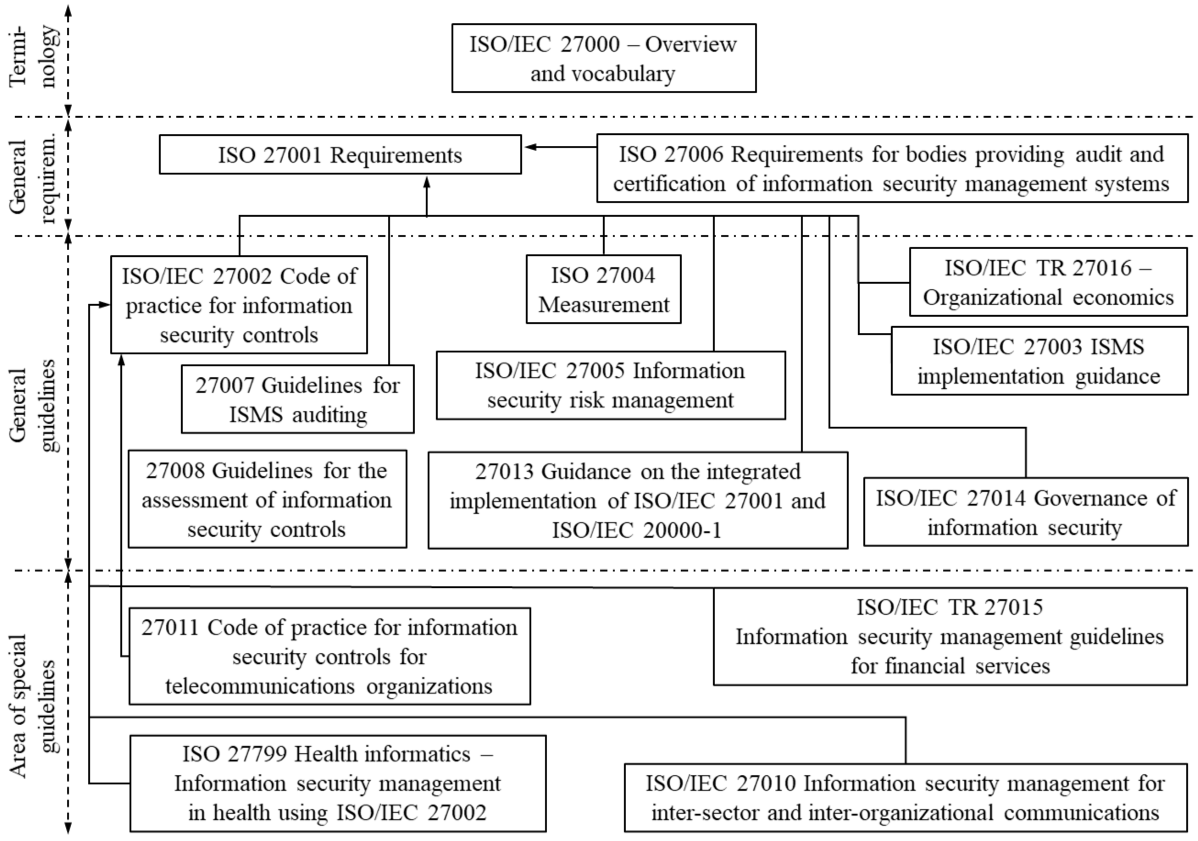
Termi-nology
ISO/IEC 27000 – Overview and vocabulary
General requirem.
ISO 27001 Requirements
ISO 27006 Requirements for bodies providing audit and certification of information security management systems
General guidelines
ISO/IEC 27002 Code of practice for information security controls
ISO 27004 Measurement
ISO/IEC TR 27016 – Organizational economics
ISO/IEC 27003 ISMS implementation guidance
27007 Guidelines for ISMS auditing
ISO/IEC 27005 Information security risk management
27008 Guidelines for the assessment of information security controls
27013 Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
ISO/IEC 27014 Governance of information security
Area of special guidelines
27011 Code of practice for information security controls for telecommunications organizations
ISO/IEC TR 27015 Information security management guidelines for financial services
ISO 27799 Health informatics – Information security management in health using ISO/IEC 27002
ISO/IEC 27010 Information security management for inter-sector and inter-organizational communications

Figure 1. Structure of the ISO/IEC 270xx series of regulations and standards

In addition, the set of standardization documents of the Central Bank of the Russian Federation contains a unified approach to ensuring information security of banking system organizations (ISBS) and recommendations for standardization (RS) with regard to the requirements of Russian legislation. The fundamental standard in the reviewed area is STO BR IsBS-1.0-2014 “Ensuring information security of organizations in the Russian Federation’s banking system. General Provisions", its goals and objectives can be found at [5].

Cyberspace is an important component of modern society. If one country launches a large-scale attack on the power plants or commercial banks of another country, military measures can be taken not only in the virtual, but also in the real world. A cyberattack that disrupts normal functioning, leads to panic, riots or loss of life, can trigger a loud forceful response [6].

2. Attacks on ATMs: “Brute force” and social engineering

According to the data achieved by the FinCERT of the Bank of Russia and the information represented in the reporting form 0403203, the main reason for the execution of cyberattacks in the banking sector is misinformation (97% in 2018, and 92% in 2017). For legal entities, the indicator was 39%[2].

PIN code should contain four characters, each represented with digits from 0 to 9. Omitting the real situation when automated teller machines (ATMs) block or “eat” the card after three incorrect PIN codes, and considering the fact that PIN code brute forcing is technically not harder than social engineering, we will determine the time required for the search.

The number of possible code combinations is $N = 10^4 - 10 = 9990$ (ten digits appearing together in four positions, excluding numbers with four identical digits).

[2] Main Development Trends in Information security in Credit and Finances for the Period 2019–2021. Moscow: Central Bank of the Russian Federation, 2019, 26 p. URL: https://www.cbr.ru/Content/Document/File/83253/onrib_2021.pdf (accessed on 02.04.2020) (in Russian).

1. The probability of correct guess at the first step is $P_1 = 1/N$;

2. The product of the $1/(N-1)$ probability (one step less) and the conditional probability after completing the first step $1-\frac{1}{N}=\frac{N-1}{N}$. The probability of correct guess at the second step is $P_2 = \frac{1}{N-1}\cdot\frac{N-1}{N}=\frac{1}{N}$;

3. The product of the $1/(N-2)$ probability (two steps less), the conditional probability after the second step $1-\frac{1}{N-1}=\frac{N-2}{N-1}$, and the conditional probability after the first step (known) $1-\frac{1}{N}=\frac{N-1}{N}$. The probability of correct guess at the third step is $P_3 = \frac{1}{N-2}\cdot\frac{N-2}{N-1}\cdot\frac{N-1}{N}=\frac{1}{N}$;

4. The product of the $1/(N-3)$ probability (three steps behind), the conditional probability after the third step $1-\frac{1}{N-2}=\frac{N-3}{N-2}$, the conditional probability after the second step (known) $1-\frac{1}{N-1}=\frac{N-2}{N-1}$, and the conditional probability after the first step (known) $1-\frac{1}{N}=\frac{N-1}{N}$.

The probability of finding the correct answer at the fourth step is $P_4 = \frac{1}{N-3}\cdot\frac{N-3}{N-2}\cdot\frac{N-2}{N-1}\cdot\frac{N-1}{N}=\frac{1}{N}$.

At any step, the probability of guessing the PIN code is $P_N = \frac{1}{N}$ [7]. The mathematical expectation of the number of steps is the product of the probability and the sum of the first *N* terms of the arithmetic progression

$$M_N = \frac{1}{N}\cdot 1+\frac{1}{N}\cdot 2+...+\frac{1}{N}\cdot N=\frac{1}{N}\cdot(1+2+...+N)=\frac{1}{N}\cdot\frac{(N+1)\cdot N}{2}=\frac{N+1}{2} \qquad (1)$$

Let's assume that each step takes $15\text{ sec}=\frac{15}{60\cdot 60}\text{ hour}=\frac{1}{240}\text{ hour}$. Then, the mathematical expectation of finding the PIN code is $\frac{9991}{2\cdot 240}\approx 21\text{ hour}$.

Successful social engineering techniques are limited to minutes, so they are definitely better to use for criminal purposes [7]. Today for new SIM cards, the contact list is updated only with the operator's reference numbers (Service Dialing Numbers – SDNs). The authors propose to include the numbers of credit institutions and of the Bank of Russia in the SDN. This will allow to:

- attract user attention (once they understand the relevance of credit organization numbers, they will add the necessary ones themselves and delete the ones they don’t need);
- filter incoming phone numbers;
- encourage customers to call back to the bank once they receive a call from “Bank's security service”.

Thus, mutually beneficial cooperation is organized: mobile operators list phones of popular banks in their SIM card SDN, banks advertise these operators on their plastic cards, while customers improve their literacy and security.

3. “Black box” ATM Attacks

Ensuring the security of banking information systems is a complex process performed according to a number of different methodologies and requires compliance with many standards, such as IS DB ISBS, GOST R ISO/IEC 15408 [8] and PCI DSS [9]. But in the case of ATMs, security is often implemented through obscurity (by hiding information about the internal ATM subsystems, interfaces and component interaction protocols). This makes attacks difficult but does not guarantee security.

A significant threat to the banking sector is hardware and software systems designed to steal money from ATMs, that are called Black boxes - equipment with special software that connects to a dispenser (money issuing mechanism) instead of commercial bank's experts' working computers. Further, the ATM gets controlled by cybercriminals, and the data is transferred using contactless technologies (for example, from a smartphone) [10, 11].

Thus, according to the Black box cyberattack statistics for 2012–2018, there is a rapid increase in the number of cases in all sampled countries (Figure 2).

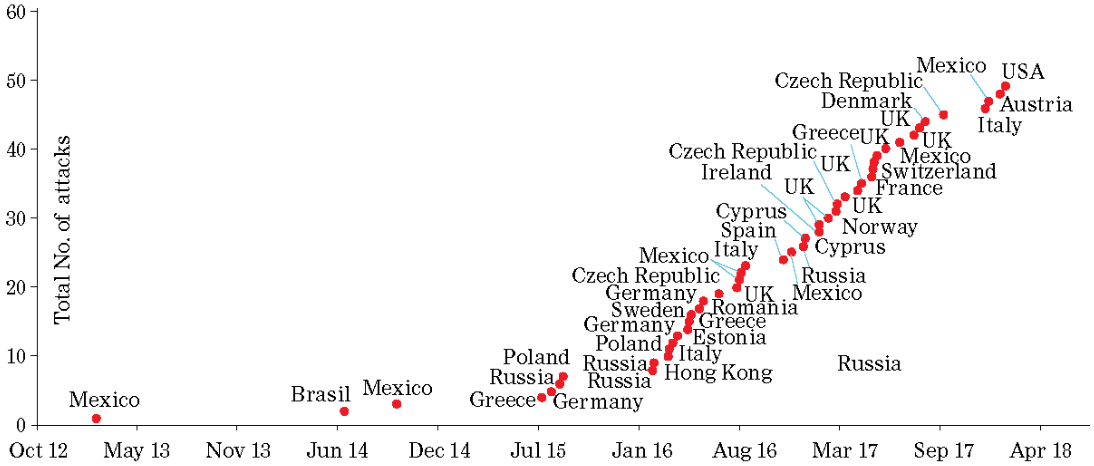

Figure 2. Number of recorded cases of Black box attacks in various countries

The statistics published in the European Payment Terminal Crimes Report (Table 1) [10, 11, 12] indicates an increase in the number of logical attacks on ATMs by 269% compared to 2019. More specifically, all logical cyberattacks registered in 2020 are Black box attacks. According to the report of the 22nd EAST EGAF meeting, Black box attacks rank second in the number of cases, giving way only to skimming. It is also worth mentioning the reports on new methods of conducting this type of cyberattack appearing in 2020 [11–14], which indicates the relevance of the methods of this attack and the interest of cybercriminals in it.

Table 1.
Statistics of cyberattacks on payment terminals and ATMs (European payment terminal crime statistics – summary)

Terminal Related Fraud Attacks	H1 2016	H1 2017	H1 2018	H1 2019	H1 2020	% +/– 19/20
Total reported Incidents	10,820	11,934	6,760	10,723	3,631	–66%
Total reported losses	€174m	€124m	€107m	€124m	€109m	–12%
ATM Related Physical Attacks	H1 2016	H1 2017	H1 2018	H1 2019	H1 2020	% +/– 19/20
Total reported Incidents	1,604	1,696	2,046	2,376	1,829	–23%
Total reported losses	€27m	€12.2m	€15.1m	€11.4m	€12.6m	+11%
ATM Malware & Logical Attacks	H1 2016	H1 2017	H1 2018	H1 2019	H1 2020	% +/– 19/20
Total reported Incidents	28	114	61	35	129	+269%
Total reported losses	€0.41m	€1.51m	€0.25m	€0.00m	€1.00m	N/A

Source: European Association for Secure Transactions (EAST)[3]

According to the Director of Security at BI.ZONE [10], the number of cyberattacks, involving the usage of technical means has increased by 4% of the total number of attacks in 2019. He attributes this to favorable conditions in the form of anti COVID-19 measures: almost all cybercriminals used medical masks as disguises [12].

Considering the above-mentioned facts, it can be affirmed that Black box attacks are a relevant and dangerous attack vector in the current environment, despite the protective measures applied by banks. Let's consider their main characteristics and offer relevant protection methods.

3.1. Main Characteristics of Black Box Attacks

As we know, Black box is a logical type of cyberattacks that allows criminals to steal money from the ATM safe [10, 13, 14]. It is performed by connecting a special device to the dispenser bus in order to send unauthorized commands to withdraw cash. On the Figure 3, the location of this type of attacks in the general classification of banking attacks is indicated, based on the materials of the article [15].

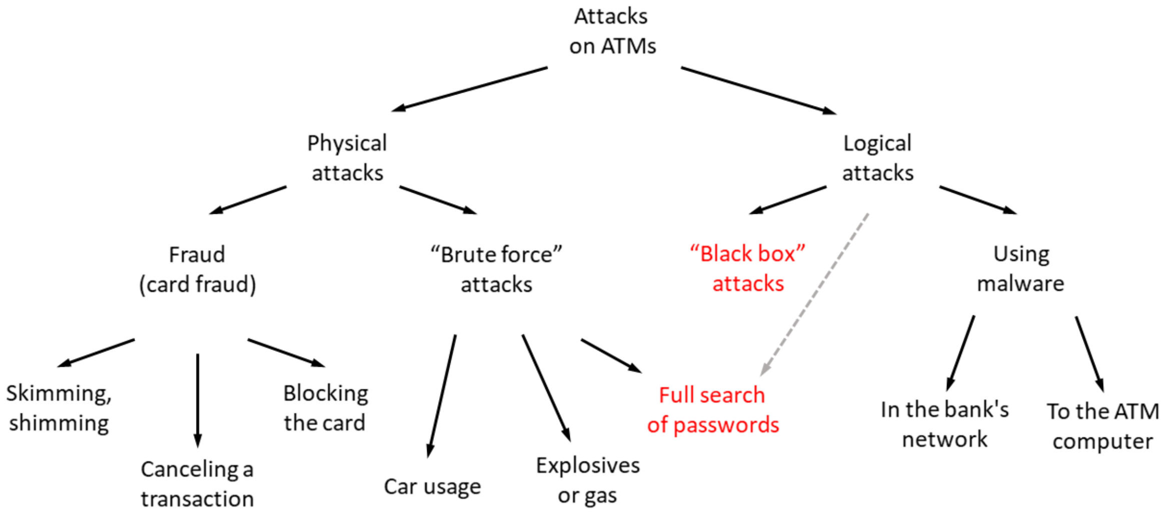

Figure 3. Classification of attacks on ATMs

To perform a Black box attack, criminals need a device with interface controllers to connect to the dispenser port and a software to manage it. Typical interfaces are RS232, RS485 or USB. Single-board computers or laptops are usually used as a control device due to their mobility. To connect the Black box device, it is necessary to disconnect the dispenser from the ATM control unit, but if the RS485 protocol is used, it can be paralleled. There have also been recorded cases of using smartphones, controlled from the outside, as Black box devices [16, 17]. Let us consider the scheme for performing a Black box attack (Figure 4). It indicates the location of the main functional blocks, their interconnection, and the place where cybercriminals infiltrate during the cyberattack.

[3] European Association for Secure Transactions. Black Box attacks increase across Europe. URL: https://www.association-secure-transactions.eu/black-box-attacks-increase-across-europe/ (accessed on 10.03.2021).

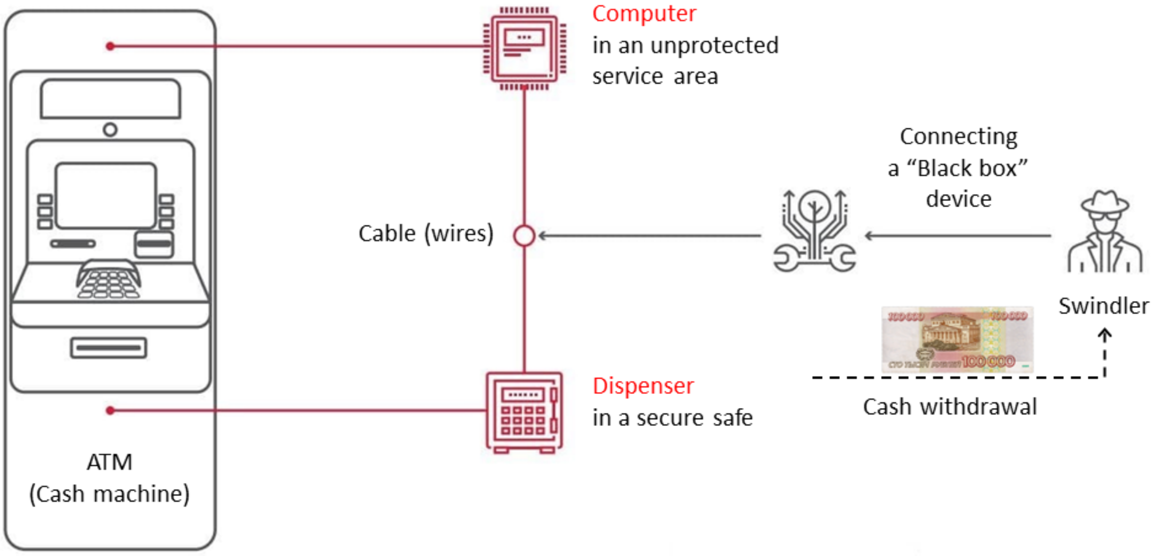

Figure 4. Diagram of a Black box ATM cyberattack

Let's list the key features of Black box attacks:

1. The attacker needs to gain access to the dispenser interface or the central bus of ATM devices.

2. Interaction with the ATM dispenser occurs from a separate device, so the attack does not leave traces of the operations performed in security logs.

3. To create a Black box device, cybercriminals require knowledge of the ATM's internal mechanisms and its software.

4. The success of the attack does not depend on the operating system (OS), processing center and ATM management software.

5. Official utilities issued by banking software developers are used to interact with the dispenser. Usually, utilities have protection against malicious use, yet cybercriminals bypass it by changing the program code.

3.2. Duration of a Black box attack

Having received an idea of the attack method and the resources required for it, we will analyze the temporal characteristics of its execution.

According to the analytical article [15], the average duration of this type of attack is 10 minutes. To obtain more accurate data, it is necessary to consider each of the attack stages:

1) opening the ATM service area - T_v. Depending on the method, it takes from 3 seconds to 2 minutes;

a. using a physical key (genuine or a copy) to open the service zone cabinet (T_{v1}) – few seconds;

b. opening the lock of the service zone cabinet (T_{v2}) – from 30 to 60 seconds;

c. cutting a hole in the ATM front panel (T_{v3}) - from 60 to 150 seconds.

2) connecting the Black box device to the interface or data bus (T_p). Depending on the cybercriminal's skills, the process takes 20 to 60 seconds.

3) withdrawal of funds through the dispenser (T_i). Depending on the model, the ATM safe can hold up to 8000 banknotes of different denominations, which are in four special cassettes. The ATM contains from 3 to 14 million rubles. This variation is caused by a number of factors, such as the ATM type, its location, banknote discharge rate, and the amount insured.

The ATM type determines the set of functions: cash deposit or cash withdrawal. ATMs for withdrawal initially have more money cassettes, and ATMs for depositing – more empty cassettes.

There are also ATMs that work for both withdrawing and depositing cash. They use both full and empty cassettes.

Cassettes can be filled with a different number of bills and bills of various denominations. It depends on the place of installation and the banknote discharge rate. The ATM insurance amount also affects, banks cannot store more funds in an ATM than provisioned in the insurance contract.

The average amount of funds usually found in a fully loaded universal ATM is about 7-8 million rubles. At a time, the dispenser retrieves a maximum of 40 banknotes from the safe, and the delay between operations is 20 seconds. Thus, the complete removal of banknotes from the safe will take 4000 seconds (1 hour 7 minutes), which means from 4000 rubles to 200,000 rubles in 20 seconds. According to the information about the performed attacks, each cash withdrawal procedure took from 1 to 3 hours [10, 11].

Information about the time frame of the operations was obtained by analyzing publicly available video materials [19] and information from experts in the field of ATM attacks[4].

The decisive factor limiting the duration of a cyberattack (T_a) is the actions of certain defense systems, including the alarms being triggered and the arrival of the police. The rules for the arrival of law enforcement agencies are not regulated by law, but usually the minimum time for the arrival of a police squad or employees of a private security company (T_n) is 4-7 minutes.

$$T_a < T_n \tag{2}$$

The execution a cyberattack consists of three stages, and its duration can be represented as:

$$T_a = T_v + T_p + T_i \tag{3}$$

The first two stages are preparatory stages and the last stage is fundraising.

$$T_a = T_{prep} + T_{extr} \tag{4}$$

Let’s consider the minimum and maximum possible duration of the preparatory stage of a cyberattack:

$$T_{prep.\ \min} = T_{v1\ \min} + T_{p\ \min} = 3\text{ sec} + 20\text{ sec} = 23\text{ sec} \tag{5}$$

$$T_{prep\ \max} = T_{v3\ \max} + T_{p\ \max} = 150\text{ sec}+ 60\text{ sec} = 210\text{ sec} \tag{6}$$

The fundraising process will continue until the arrival of the law enforcement forces:

$$T_{extr} = T_n - T_p \tag{7}$$

Then, the maximum and the minimum duration of fundraising equals to:

$$T_{extr\ \min} = T_{n\ \max} + T_{prep\ \min} = 420\text{ sec} - 23\text{ sec} = 217\text{ sec} \tag{8}$$

$$T_{extr\ \max} = T_{n\ \min} + T_{prep\ \max} = 240\text{ sec} - 210\text{ sec} = 30\text{ sec} \tag{9}$$

Every 20 seconds ATM dispenses 40 bills, therefore, with bills of the maximum denomination (5,000 rubles), criminals can withdraw 200,000 rubles every 20 seconds.

Thus, the maximum and minimum amount of money that cybercriminals manage to withdraw before the arrival of law enforcement agencies is equal to:

$$S_{\max} = \frac{T_{extr\ \min}}{20\text{ sec}} \cdot 5000\text{ rub} = \frac{217\text{ sec}}{20\text{ sec}} \cdot 5000\text{ rub} = 2\,000\,000\text{ rub} \tag{10}$$

$$S_{\min} = \frac{T_{extr\ \max}}{20\text{ sec}} \cdot 5000\text{ rub} = \frac{30\text{ sec}}{20\text{ sec}} \cdot 5000\text{ rub} = 200\,000\text{ rub} \tag{11}$$

According to the calculations, cybercriminals can withdraw from 200,000 to 2,000,000 rubles. The Figure 5 shows the dependence of the amount of theft on the arrival time of the police, red lines indicate the interval of the maximum and the minimum amounts if the arrival of the police is in the interval from 4 to 7 minutes. If the opening of the service area was not noticed, then the amount of losses will be even greater, up to the complete withdrawal of the funds available in the safe.

[4] A. Osipov and O. Kochetova, Hack Your ATM with Friend's Raspberry.Py, Video, 15:57, 2015. URL: https://www.youtube.com/watch?v=q5tQWe6YsLM (accessed on 15.01.2021).

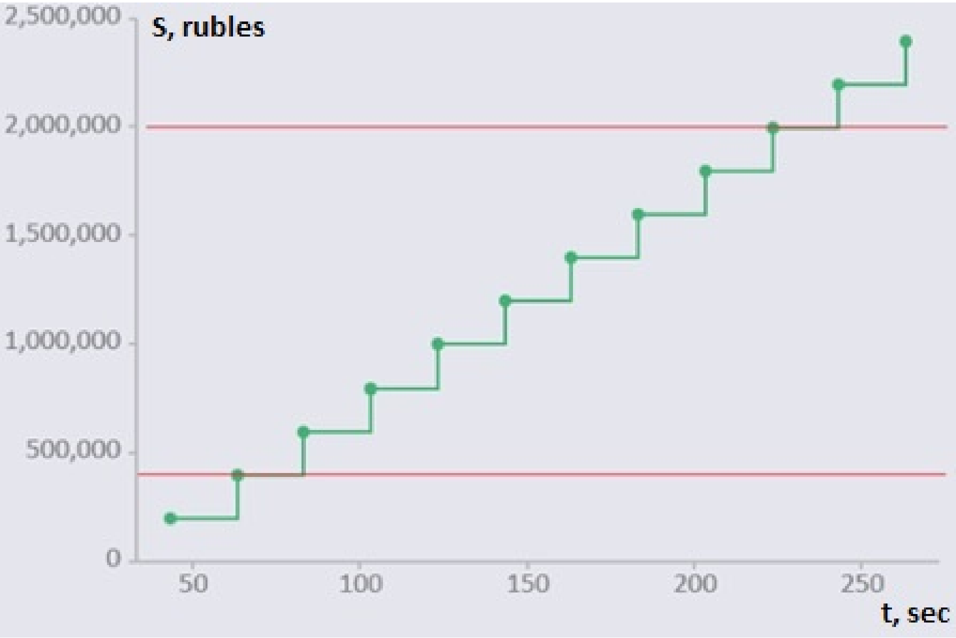

Figure 5. The correlation of the damage and the arrival time of law enforcement agencies

Thus, when a Black box attack is performed, damage is possible even with an immediate response to the fact of its occurrence. This requires monitoring systems and transaction indicators that can signal an attack, but to completely prevent damage, it is necessary to prevent the opportunity for the attacker to start using the ATM receiver in such a short time. Next, we will consider the available protective measures against this type of attacks and propose additional protection methods [11, 16-19].

3.3. Improving the response and protection of ATMs against Black box attacks

According to ATM vendors' recommendations, it is recommended to use current versions of XFS platforms that provide strong encryption and support physical authentication between the OS and the dispenser. With physical authentication, encryption keys are transmitted only if the legality of access to the safe is confirmed. These measures do not guarantee security, for example, there is a case when cybercriminals managed to bypass physical authentication [20-23].

There are special devices that provide protection against unauthorized connection to the dispenser. For example, ZUB-R, Cerber Lock and ATM Keeper. They allow to perform only operations authenticated by the banking software and expand the monitoring of ATM security events. The main problem with this method of countering cyberattacks is the small percentage of ATMs that use these devices. According to the data provided by ANSER PRO LLC and Artifakts LLC, these devices are used in 15,000 ATMs, which is 7% of the total number of ATMs [24-27].

Thus, the above methods do not provide reliable protection against Black box attacks. We need to develop a reliable way to increase the time it takes for a cybercriminal to access the dispenser. A possible way would be to set a time delay for starting the dispenser after it is turned on. The minimum duration of such a delay is 217 seconds. Using reliable signaling means, this will reduce the number of cases of successful Black box ATM operations.

4. A few words about the scientific and technological progress of Russia

Currently, the most powerful computing systems belong to Japan, the USA and China. The Japanese supercomputer Fugaku has a peak performance of 537 petaflops; Russian "Christofari" (owned by Sberbank) - 8 petaflops of capacity[5].

At the beginning of the XXI century, Chinese researchers were concerned about the lack of inventors in China. Therefore, they sent a delegation to well-known American companies (Apple, Microsoft, Google) and asked people who are “inventing the future” about their lifestyle. Identifying common behavioral patterns has shown that one of their favorite genres of literature is science fiction. Corresponding books were introduced into the literature course outline in China schools, and today such manufacturers as Xiaomi, Tencent, and Huawei, are among the world leaders.

It may be explained with a combination of the inherent traditional formation and the functioning of mirror neurons. Mirror neurons are glial cells of the brain that are being activated not only while performing a certain action, but also while a person observes this action performed by others [24]. Scientific and technological progress is discussed in so-called “hard” science fiction (HSF). The authors propose to increase the amount of HSF offered for study in literature classes and included in the “100 books for schoolchildren” list.

5. Conclusion

The Office of the Prosecutor General of Russia called cybercrimes a threat to the country's national security, especially given their low detection rate, recorded at a level of no more than 25%[6]. Banking practice shows the need to improve risk management and information security systems in electronic banking. The implementation of electronic banking systems allows credit institutions to significantly reduce operating expenses, but at the same time, electronic banking is associated with additional sources of traditional banking risks. The advantage of social engineering over technical hacking methods is shown mathematically. Thus, new cybersecurity challenges require the continuous improvement of solutions and the significant revision of risk management procedures applied by banks and their customers while using electronic banking systems (and, in particular, ATMs) [26].

The measures considered in this article are aimed at improving the efficiency of responding to information security incidents and, in particular, at developing a system for protecting customers from social engineering methods and ATMs, from Black box attacks. The article analyzes Brute Force and Black box types of cyberattacks on ATMs. The scientific novelty of the work consists in the solution proposed by the authors on weakening the social engineering techniques as a result of comparing their effectiveness with the effectiveness of the Brute force method. The practical significance of the work lies in determining the temporal features of the Black box attack and developing additional ATM protection measures.

Efficient development of electronic banking requires both traditional measures to improve financial and computer literacy, and the local adaptation of foreign experience to unlock the scientific and technical potential.

6. Acknowledgements

Translation of this article into English was organized with the support of Anna B. Bakh and the Center for translation and internal review of the Financial University under the Government of the Russian Federation. URL: http://www.fa.ru/org/science/cpvr/Pages/Home.aspx.

[5] D. Pisarenko “Russia in a calculation race. Why does our supercomputer power give way even to Saudi Arabia?”. Weekly Newspaper “Arguments & Facts”. 2021. № 8. C. 15.
URL: https://aif.ru/society/science/gonka_vychisleniy_pochemu_nashi_superkompyutery_otstayut_ot_zarubezhnyh (accessed on 04.03.2021).

[6] General Procurator’s Office say that cybercrime constitutes a danger to Homeland Security”. URL: https://tass.ru/obschestvo/11451173 (reference date 24.05.2021).

7. References

[1] Skinner C, Digital Human: The Fourth Revolution of Humanity Includes Everyone, Marshall Cavendish International (Asia) Pte Ltd, 400 p, 2018.

[2] King B, Bank 4.0: Banking Everywhere, Never at a Bank, Singapore: John Wiley & Sons Ltd, 352 p, 2018.

[3] Petrenko S.A., Makoveichuk K.A., Chetyrbok P.V., Petrenko A.S. About readiness for digital economy / 2017 Proceedings of 2017 IEEE 2nd International Conference on Control in Technical Systems, CTS 2017, c. 96-99 doi: 10.1109/CTSYS.2017.8109498.

[4] Probabilistic Modeling in System Engineering / By ed. A. Kostogryzov – London: IntechOpen, 2018. 278 p. DOI: 10.5772/intechopen.71396.

[5] Kozminykh S.I. Development of a Methodology and Mathematical Model for Quality Assurance of an Integrated Security System for a Credit and Financial Facility. Voprosy kiberbezopasnosti [Cybersecurity Issues], 2021, No. 3 (43), pp. 31–42. DOI: 10.21681/2311-3456-2021-3-31-42. (In Russ.)

[6] Clearfield C., Tilcsik A, Meltdown: Why Our Systems Fail and What We Can Do About It, Penguin Press, 304 p, 2018.

[7] Berdyugin A.A., Revenkov P.V. Approaches to Measuring the Risk of Cyberattacks in Remote Banking Services of Russia, CEUR Workshop Proceedings. 2019, V. 2603. pp. 6–11.

[8] Barabanov A., Markov A. Modern Trends in the Regulatory Framework of the Information Security Compliance Assessment in Russia Based on Common Criteria. In Proceedings of the 8th International Conference on Security of Information and Networks (Sochi, Russian Federation, September 08-10, 2015). SIN '15. ACM New York, NY, USA, 2015, pp. 30-33. DOI: 10.1145/2799979.2799980.

[9] Hatfield J.M. Virtuous Human Hacking: The Ethics of Social Engineering in Penetration-Testing. Computers & Security, vol. 83, 2019, pp. 354–366. DOI: 10.1016/j.cose.2019.02.012.

[10] Revenkov P.V., Berdyugin A.A., Makeev P.V., Assessment of the Risk of a Cybersecurity Breach in a Commercial Bank (by the example of an attacks “brute force” and “black box” on ATMs). Voprosy kiberbezopasnosti [Cybersecurity Issues], No. 3 (43), 2021, pp. 20–30. DOI: 10.21681/2311-3456-2021-3-20-30. (In Russ.)

[11] Berdyugin A.A. Risk Management of Information Security Violation in Conditions of Electronic Banking Voprosy kiberbezopasnosti [Cybersecurity Issues], No. 1 (25), 2018, pp. 28-38. DOI: 10.21681/2311-3456-2018-1-28-38. (In Russ.)

[12] Gorach N.N., Filatova I.V. Challenges and Threats to Information Security by Crimes Committed in the Context of the COVID-19 Pandemic. Vestnik of Moscow University of the Ministry of Internal Affairs of Russia, no. 8, 2020, pp. 102–105. DOI: 10.24411/2073-0454-2020-10462. (In Russ.)

[13] Dvoryankin S.V., Antipenko A.O. Applying the Phase Characteristics of Voice Vocalisms in Solving the Problem of Protection of Speech Information. IT Security (Russia), vol. 28, no. 2, 2021, pp. 21–33. DOI: 10.26583/bit.2021.2.02. (In Russ.)

[14] Gavdan G.P., Ivanenko V.G., Salkutsan A.A. Security of Significant Objects of Critical Information Infrastructure. IT Security (Russia), vol. 26, no. 4, 2019, pp. 69–82. DOI: 10.26583/bit.2019.4.05. (In Russ.)

[15] Buldas A., Gadyatskaya O., Lenin A., Mauw S., Trujillo-Rasua R. Attribute Evaluation on Attack Trees with Incomplete Information: A Preprint. Computers & Security, vol. 88, 2020. 21 p. URL: https://arxiv.org/abs/1812.10754 (accessed on 28.02.2021).

[16] Bradbury D. A Hole in the Security Wall: ATM Hacking. Network Security, vol. 2010, iss. 6, 2010, pp. 12–15. DOI:10.1016/S1353-4858(10)70082-9.

[17] Berdyugin A.A. Reengineering of Business Processes of a Commercial Bank in the Information Space. Bezopasnost' Informatsionnykh Tekhnologiy [IT Security], vol. 28, no. 1, 2021, pp. 62–73. DOI: 10.26583/bit.2021.1.05. (In Russ.)

[18] Slavin B. Digital Technologies of Intellectual Collective Activity, in: System Analysis in Economics – 2018. Proceedings of the V International research and practice conference-biennale, 2018, pp. 316–318. DOI: 10.33278/SAE-2018.eng.316-318.

[19] A. Osipov and O. Kochetova, Hack Your ATM with Friend's Raspberry.Py, Video, 15:57, 2015. URL: https://www.youtube.com/watch?v=q5tQWe6YsLM (accessed on 15.01.2021).

[20] Slipenchuk P., Epishkina A. Practical User and Entity Behavior Analytics Methods for Fraud Detection Systems in Online Banking: A Survey. Advances in Intelligent Systems and Computing (see in the books), vol. 948, 2020, pp. 83–93. DOI: 10.1007/978-3-030-25719-4_11.

[21] Barabanov A.V., Markov A.S., Tsirlov V.L. Information Security Controls Against Cross-Site Request Forgery Attacks on Software Application of Automated Systems. Journal of Physics: Conference Series. 2018. V. 1015. P. 042034. DOI :10.1088/1742-6596/1015/4/042034

[22] Wang V., Nnaji H., Jung J. Internet Banking in Nigeria: Cyber Security Breaches, Practices and Capability. International Journal of Law, Crime and Justice, vol. 62, 2020, 100415. DOI: 10.1016/j.ijlcj.2020.100415.