ORIGINAL PAPER

CC BY 4.0

DOI: 10.26794/2587-5671-2020-24-6-51-60
UDC 004.056:336(045)
JEL G21, G32, L86

Cyberattack Risk Assessment in Electronic Banking Technologies (the Case of Software Implementation)

A.A. Berdyugin[a], **P.V. Revenkov**[b]
Financial University, Moscow, Russia
[a] https://orcid.org/0000-0003-2301-1776; [b] https://orcid.org/0000-0002-0354-0665

ABSTRACT

The authors investigate the risks of computer attacks on automated banking systems. **The relevance** of the study is due to the need to revise the approaches to risk assessment based on the technical components of banking business processes and the consequences of cyber-attacks aimed at banking automated systems in credit institutions. **The aim** of the study is to describe the developed methods for assessing cyber risks in a commercial bank and provide an option for assessing the risks of information security violations in electronic banking technologies. **The methodology** of the article includes the analysis of domestic and foreign literature on the research topic, the theoretical and probabilistic method of calculation, computer programming and graphic interpretation of information. The authors analysed the operational risk of a commercial bank to develop components of the operational risk management system in the context of developing electronic banking technologies. They designed a computer program to quantify risk probabilities of cyberattacks on electronic banking technologies (by means of Borland Delphi). The work presents a formalised probabilistic model for determining the most vulnerable segment of risk management techniques used by information security structures. **The conclusion** is that it is possible to develop a software package based on a mathematical model that reduces the number of checks of risk factors by several times. **The research results** may be of further use for the development of risk divisions in credit institutions using electronic banking technologies.

Keywords: the risk of cyberattacks; electronic banking technologies; information security; risk assessment; probabilistic model; computer program; typical banking risks

For citation: **Berdyugin A.A., Revenkov P.V. Cyberattack risk assessment in electronic banking technologies (the case of software implementation).** ***Finance: Theory and Practice.*** **2020;24(6):51-60. (In Russ.). DOI: 10.26794/2587-5671-2020-24-6-51-60**

© Berdyugin A.A., Revenkov P.V., 2020

INTRODUCTION

Scientific and technological progress contributes to the transition of traditional banking services to remote ones and the expansion of risk profiles. According to a number of experts (B. King [1] and C. Skinner [2]), in the 2020s some countries will completely give up cash (Sweden, China, Canada).

The monotown Neryungri (Yakutia) became the first case of smart card technology in Russia, which demonstrated the potential of cashless payments of the future. The restructuring of the USSR caused cash problems. The city-forming enterprise JSC Yakutugol (today a subsidiary of PJSC Mechel) used high-quality equipment from Japan as salaries to workers (barter). In 1995, by means of the city's main bank "Neryungribank" (now "Coalmetbank"), it put the salaries of all employees to plastic cards "Zolotaya korona" [3].

The Centre of Financial Technologies in Novosibirsk outstripped time and its product became convenient for all professions and segments of the population, including pensioners.[1] One of the authors of this article (A.A. Berdyugin) witnessed these innovations, since he was born and lived in Neryungri from 1988 to 2010 before he moved to Moscow. The gradual abandonment of cash is a consequence of the active introduction of electronic banking technologies (EBT)[2] in the banking business [4] and provides an opportunity (opposite to the risk) for cybercriminals.

Along with the EBT obvious advantages, profiles of typical banking risks have significantly expanded, including operational risk (OpR). A world leading developer of the methodology for assessing banking risks, the Basel Committee on Banking Supervision has issued several documents on improving banking supervision. It recommends that credit institutions create a reserve for operational risk, which includes a reserve for cyber risk (see Basel II, III and Basel IV).[3]

According to the Committee, commercial banks have to reserve funds for OpR, considering active development and use of information technologies (fintech or techfin [1, 2]).

OpR means the risk of direct and indirect losses as a result of:

- low efficiency or erroneous internal business processes of a commercial bank;
- actions of the staff and third parties;
- violations and shortcomings in the operation of information, technological and other systems;
- external events.

OpR includes legal risks, but excludes strategic and reputational risks. It also includes various risks depending on the types of processes:

- the risk of insufficient information security;
- the risk associated with deficiencies in the construction of information systems in a particular organization;
- the project risk as a consequence of OpR;
- the risk of violation of control procedures, which may include compliance risk or risk of internal control deficiencies;
- the risk of errors in the processes of development, verification, adaptation, acceptance of methods and quantitative models for assessing assets and risks (model risk as a consequence of OpR);
- the risk associated with erroneous actions of the personnel.

[1] The art of survival: what helped CFT overcome all financial crises. URL: https://www.rbc.ru/magazine/2016/12/582c40a29a7947079b45fdce (accessed on 26.05.2020).

[2] EBT are based on PC-banking (management of bank accounts and cards from a computer via the Internet and a Web browser online) and mobile banking (SMS-banking, as well as management of bank accounts and cards via a special application from smartphones, tablets and smart watches). EBT also include ATMs and self-service banking terminals.

[3] The content of these documents, as well as various articles by leading experts in the field of banking supervision, are here www.bis.org.

Fig. 1. **Building an operational risk management system in the context of electronic banking technologies**

Source: complied by the authors based on [5].

In general, OpR control system in the context of EBT may look as follows (*Fig. 1*) [5]. We will adapt the generally accepted term "risk of information security breach" and consider OpR in the fuel and energy balance.

Definition 1. By risk of cyberattacks (RCa) we understand a quantitative expression of a likely increase in typical banking risks influenced by insider and hacker threats, in case of disruptions to the automated banking system, as well as expression of the magnitude of negative consequences (financial costs, reduced reputation, loss of liquidity) caused by the threat. The concept of RCa in EBT was used by the authors in [3, 6, 7].

The key is the software package that ensures the functioning of the operational risk management system in EBT. The EBT susceptible to cyberattacks can be classified by way of providing financial remote services:

- PC-banking;
- Telephone/SMS banking;
- Terminal banking;
- Mobile banking.

Testing for penetration into the protected perimeter of commercial banks, carried out by experts from Positive Technologies, showed that seven out of eight organizations have a local network not protected from penetration from the global network. The security of the corporate infrastructure of most considered credit and financial institutions from internal cyberattacks was assessed by the company as extremely low.[4] Commercial banks reimbursed their clients only 15% (935 million roubles, or every sev-

[4] Penetration testing in organizations of the credit and financial sector. URL: https://www.ptsecurity.com/ru-ru/research/analytics/pentest-finance-2020/ (accessed on 27.06.2020).

enth stolen rouble), and explained this by a high proportion of social engineering: clients themselves disclose confidential information.[5]

Thus, cyberattacks cause significant damage to banks and become the reason for typical banking risks (credit, operational, legal, reputational, strategic risks and liquidity risk), whose characteristics are provided in the letter of the Bank of Russia No. 70-T "On typical banking risks").

SOFTWARE IMPLEMENTATION OF ASSESSMENT METHOD OF RCa IN EBT

According to the Federal Law of the Russian Federation No. 184-FZ "On Technical Regulation", risk is the likelihood of damage to the life or health of citizens, property of individuals or legal entities, state or municipal property, the environment, life or health of animals and plants, considering the severity of this damage [6]. *Table 1* shows a comparative characteristic of cyberattack risk assessment tools.

Domestic software for risk assessment is presented only by "GRIF 2006", not supported by the manufacturer. Therefore, we automate the method of quantitative assessment of RCa management in EBT, described in [3, 6], in the high-level language Borland Delphi (*Fig. 2* shows the user-friendly interface and a ready-made example) using [9–11].

1. First, the risk analyst selects a demand from the drop-down list and assesses it by four radio buttons ([3, 6] provide approximate requirements for the RCa control system), thereby setting the initial data:

```
…
Cells[1, Row]:=
IntToStr(RadioGroup.ItemIndex +
1);
…
```

2. After the cells are filled with demands and are assessed on a 4-point scale, we determine the quantitative value of the probability of an unfavorable outcome when implementing RCa by pressing "Probability of RCa" button:

```
procedure TRiskForm.
ProbabilityButtonClick(Sender:
TObject);
var
 znam, j: Integer;
begin
 znam:= 0;
 for j:= 1 to ConditionOfBank-
 StringGrid.rowCount do
  if ConditionOfBankStringGrid.
  Cells[1, j] <> '' then
 begin
  znam:= znam + StrToInt(Condi
  tionOfBankStringGrid.Cells[1,
  j]); // Cells[Col, Row]
  ProbabilityLabel.Caption:=
  FloatToStr(SimpleRoundTo(100 *
  j / znam,—2)) + '%';
  RadioGroup.ItemIndex:= -1;
  // to remove the radio buttons
 end;
end;
```

Meeting the requirement (positive answer) reduces the probability of RCa and vice versa.

3. For further work, requirements and calculations can be saved into a Microsoft Excel report by clicking on the appropriate button:

```
…
 with ConditionOfBankStringGrid
 do
 begin
  for i:= 0 to ColCount — 1 do
   for j:= 0 to RowCount — 1 do
   Excel.Sheets[1]. Cells [j + 1,
   i + 1]:= Cells [i, j]; // "To
   link" Excel and Delphi
 end;
  Excel.Sheets[1]. Cells [1, 7]:=
 'Result: '; {Write down the
  percentage of RCa}
```

[5] Report of the Bank of Russia "Review of transactions performed without the consent of clients of financial institutions in 2019". URL: http://www.cbr.ru/Content/Document/File/103609/Review_of_transactions_2019.pdf (accessed on 28.06.2020).

Table 1

Comparative characteristics of cyberattack risk assessment tools

Product	CRAMM (Central Computer Telecommunications Agency, UK)	RiskWatch, Riskwatch International (USA)	GRIF 2006, Digital Security Office (Russia)	Microsoft Security Assessment Tool
Support:	Provided	Provided	Absent	Provided
User friendly:	Requires special training and high qualifications of an auditor	Requires special training and high qualifications of an auditor	The program interface is focused on IT managers and executives. Requires specialized knowledge of information security	The program interface is focused on IT managers and executives. Requires specialized knowledge of information security
Cost:	License cost from 2 thousand to 5 thousand dollars per one workplace	License cost from 10 thousand dollars per one workplace	License cost from 1 thousand dollars per one workplace	Free
Entry data:	– Resources; – value of resources; – threats; – system vulnerabilities; – selection of adequate measures	– Type of information system; – basic safety requirements; – resources; – losses; – threats; – vulnerabilities; – protective measures; – value of resources; – frequency of threats; – selection of countermeasures	– Resources; – network hardware; – types of information; – group of users; – protection; – threats; – vulnerabilities; – selection of countermeasures	Formed based on user responses
Options / content of the report:	– Risk analysis report; – general report on risk analysis; – detailed report on risk analysis	– Brief summary; – report on the cost of protected resources and expected losses from the implementation of threats; – report on threats and countermeasures; – business loss report; – security audit report	– Inventory of resources; – risks by types of information; – resource risks; – the ratio of damage from RCa and resource; – selected countermeasures; – expert recommendations	– Detailed guidance; – recommendations for reducing RCa; – links to industry guidelines; – banking risk profile; – deep protection index
Quantitative or qualitative method:	Qualitative assessment	Quantitative assessment	Qualitative and quantitative assessment	Qualitative assessment
Availability of a network solution:	Absent	Absent	Corporate version	Absent

Source: compiled based on the works of the authors [8].

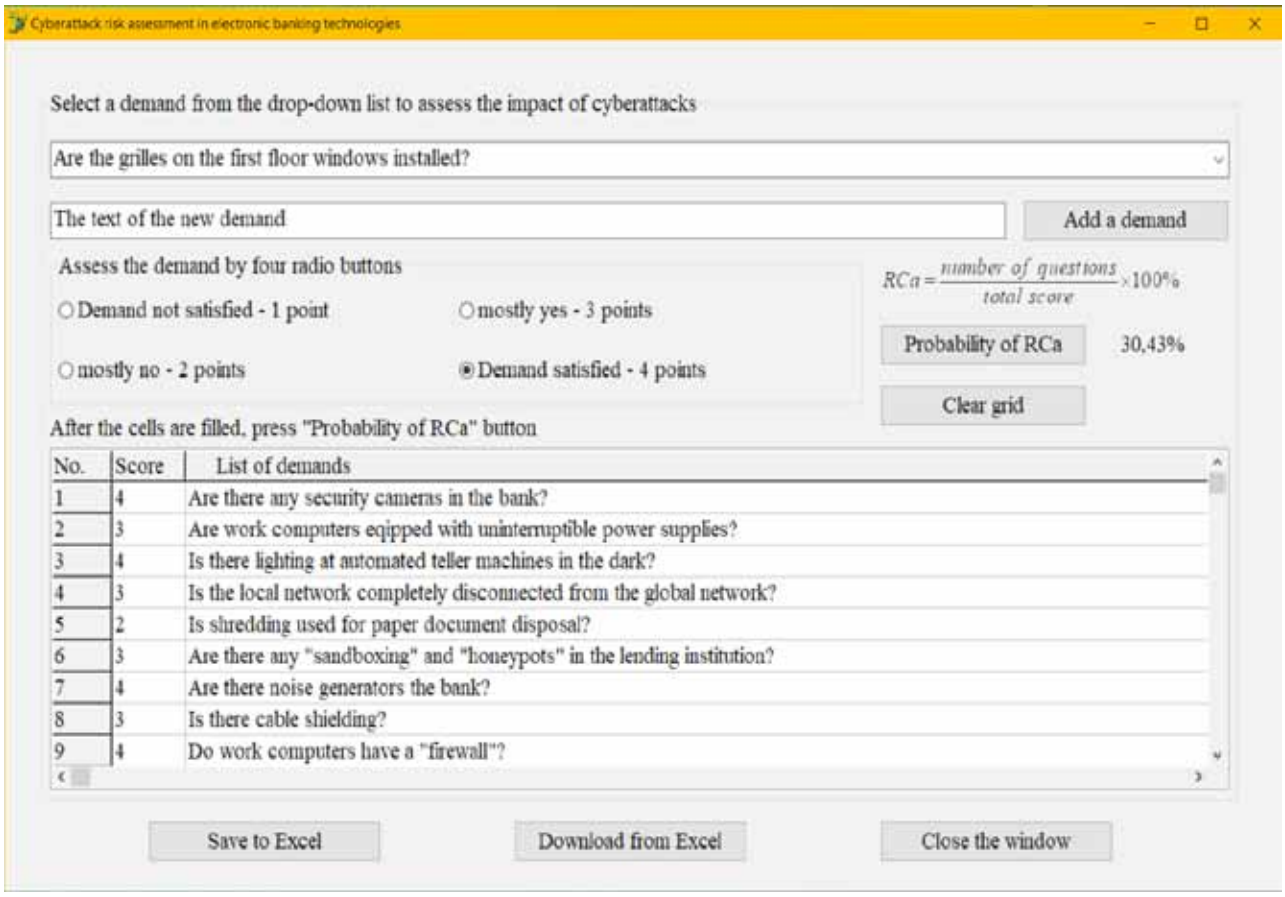

Fig. 2. **Example of using the program that assesses the risks of cyberattacks**

Source: developed by the authors in the high-level language Borland Delphi.

```
Excel.Sheets[1]. Cells [1, 8]:=
ProbabilityLabel.Caption;
Excel.DisplayAlerts:= False;
// Switch off Excel notifica-
tions
if SaveDialog.Execute then
// If you started the save win-
dow, then
try
 Excel.ActiveWorkbook.
 SaveAs(SaveDialog.FileName);
 ShowMessage ('Saved to file: '
 + #10 + SaveDialog.FileName);
except
 ShowMessage ('The file can-
 not be saved, it is open for
 writing or read-only.'
 + #10 + ' Try to save the file
 under a different name.');
end;
...
```

4. The existing list of requirements and assessments can be downloaded from the Excel database:

```
...
 Excel:= CreateOleObject ('Excel.
 Application');
 Excel.Workbooks.Open(OpenDialog.
 FileName);
 with ConditionOfBankStringGrid
 do
 begin
  for i:= 2 to Excel.ActiveSheet.
  UsedRange.Rows.Count do
  for j:= 1 to ColCount do
  begin
   {Make the number of rows of
   StringGrid equal to the num-
   ber …}
   RowCount:= Excel.ActiveSheet.
   UsedRange.Rows.Count; {…
   filled Excel rows}
```

```
    Cells [j-1, i-1]:= Excel.
    Sheets[1]. Cells [i, j];
    {Load from Excel to Delphi}
  end;
end;
```

…

The list of demands was developed by the authors empirically and is based on the analysis of the relevant literature. The revision is possible when exploiting the program.

5. The program works when the corresponding modules are connected:

```
uses
…
  Math {connect the module for
  mathematical functions},
  ComObj {connect the module for
  Microsoft COM objects};
…
var
  RiskForm: TRiskForm;
  Excel: OleVariant; {Declaring
  object OleVariant with a Micro-
  soft Excel name}
…
```

Note. The program provides that the probability of the risk realization was not zero, since there is no absolute protection. A distinctive feature of the Borland Delphi is the need to disable Delphi's reaction to exceptions (try — except — end): in the system menu Tools → Debugger Options → Language Exceptions → disable Stop on Delphi Exceptions.[6]

Regular application of the program for ensuring the cybersecurity of a commercial bank will allow monitoring the effectiveness of measures aimed at leveling the negative consequences of implementing RCa in the context of EBT. The final assessment of the likelihood of RCa presents an idea of the corporate infrastructure security of a credit institution. In the introduction, we describe the security of most banks as extremely low (see above the results of Positive Technologies on penetration testing). Using this program to assess RCa in the context of EBT will allow for effective management of the overall risk management system in a credit institution.

DEVELOPING A PROBABILISTIC MODEL TO ASSESS RCa IN EBT

Stealing large sums of electronic money includes not only stealing the numbers and PIN-codes of bank cards or passwords to access bank accounts, but also developing a mechanism to withdraw stolen money to "safe" accounts (the so-called money laundering). This is done in various ways: through a sequence of electronic transfers in the victim's EBT to the accounts of the attacker through figureheads or by purchasing goods in online stores with later resale at reduced prices [12–14].

Testing for penetration into the protected perimeter of commercial banks, carried out by experts from Positive Technologies, showed that seven out of eight organizations have a local network not protected from penetration from the global network.

For a more detailed analysis, we have developed a method where the number of checks of risk factors[7] contributing to theft and withdrawal of funds, with total number n of negative factors, can be reduced several times as follows:

1. Estimated money losses are grouped according to k factors of RCa $(k < n)$.

[6] Codecall Programming Forum. Community Forum Software by IP.Board. URL: http://forum.codecall.net (accessed on 10.07.2020).

[7] By risk factors we understand a quantitative expression of the fulfillment of the demands from the previous section.

2. Possible losses falling within the range of insignificant or acceptable risks imply the end of the cycle.

3. Possible losses falling within the range of critical or catastrophic risks require an individual consideration of each n factor. Then, for k factors of RCa $k+1$ check is required.

Proof. We will build a probabilistic model to assess RCa in EBT that can become the basis for the methods developed in [15]. Let the probability of critical or catastrophic losses be equal to p and be the same for each of n factors. Losses from implementing RCa in EBT are independent for each factor. The elements of the probabilistic model constitute a sequence of Bernoulli distributions for n tests with probability p.

Definition 2. Bernoulli distribution models a random arbitrary experiment with a known probability of success or failure. Random variable ς has Bernoulli distribution with probability $p\left(0\le p\le 1\right)$ if its values are equal to 0 or 1 with probabilities $P\left(\varsigma=0\right)=1-p$ and $P\left(\varsigma=1\right)=p$ accordingly.

If n is divided by k, then n/k will be tested. X_j is the number of checks performed in group j, $j=1,2,\ldots,n/k$. Then

$$X_j=\begin{cases}1, \text{ with probability } P\left(X_j\right)=\left(1-p\right)^k,\\ \text{all } k \text{ factors within standard}\\ k+1, \text{ with probability } P\left(X_j\right)=1-\left(1-p\right)^k,\\ \text{with negative factors.}\end{cases}$$

Here $\left(1-p\right)^k$ is the product (combination) of events opposite to critical or catastrophic losses. Let $Z=X_1+X_2+\ldots+X_{n/k}$ be the total number of checks. Let us estimate $k_0=k_0\left(p\right)$ group size for the given value of p (the value of p can be estimated by the detection frequency of negative factors in previous tests). This $k_0=k_0\left(p\right)$ group size should minimize the value of mathematical expectation $M\left(Z\right)$. According to the definition of mathematical expectation $M\left(\xi\right)=\sum_k x_k p_k$, we have:

$$M\left(X_j\right)=1\cdot\left(1-p\right)^k+\left(k+1\right)\cdot\left[1-\left(1-p\right)^k\right]=$$
$$=k+1-k\cdot\left(1-p\right)^k.$$

According to the definition of mathematical expectation $M\left(\xi+\eta\right)=M\left(\xi\right)+M\left(\eta\right)$, we have:

$$M\left(Z\right)=M\left(X_1\right)+M\left(X_2\right)+\ldots+M\left(X_{n/k}\right)=$$
$$=\frac{n}{k}\cdot M\left(X_j\right)=n\cdot\left[1+1/k-\left(1-p\right)^k\right].$$

Further research will allow us to develop a software package for automating the identification of risk factors, which will reduce the number of checks by several times.

To determine $k_0=k_0\left(p\right)$ group size we can assume that $H\left(x\right)=1+1/x-\left(1-p\right)^x$ at $x>0$. For p values that are close to 0, function $H\left(x\right)$ will reach the minimum at x_0, which is the minimum extremum of equation $H'\left(x\right)=0$, i.e.

$$\left[1+1/x-\left(1-p\right)^x\right]'=1/x^2+\left(1-p\right)^x\cdot\ln\left(1-p\right).$$

The resulting equation relative to x is clearly not solvable. According to Newton's binomial theorem, for small p we have $\left(1-p\right)^x\approx 1-px$. Replacing

$$H\left(x\right)=1+1/x-\left(1-p\right)^x$$

with $\tilde{H}\left(x\right)=1+1/x-1+px=1/x+px$, we find the minimum point of function

$$\left(1/x+px\right)'=0\Leftrightarrow -1/x^2+p=0,$$

where $\tilde{x}_0=1/\sqrt{p}$.

Wherein $\tilde{H}(\tilde{x}_0)=\sqrt{p}+p/\sqrt{p}=2\sqrt{p}$. Let the minimum probability of critical or catastrophic losses be 1%. Then for $p=0.01$ we have:

$$\tilde{x}_0=1/\sqrt{0.01}=10,\quad \tilde{H}(\tilde{x}_0)=2\sqrt{0.01}=1/5,$$

$$M(Z)\approx n\cdot\tilde{H}(\tilde{x}_0)=n/5.$$

Expected number of loss checks $M(Z)=n/5$ (fivefold reduction). The model proposed to identify negative risk factors makes it possible to reduce by 5 times the time spent on checking monetary losses from RCa implementation. This significantly increases the effectiveness of measures to identify the most vulnerable segment that are used by information security structures of RCa management technicians.

CONCLUSIONS

Further research will allow us to develop a software package for automating the identification of risk factors, which will reduce the number of checks by several times.

EBT introduction contributes to a significant reduction in operating expenses for credit institutions. At the same time, the bank's work in cyberspace is associated with additional sources of typical banking risks.

The paper proposes a simple method for assessing RCa, which, if necessary, can be constantly expanded by including additional control parameters and the development of new models. It can be used permanently by specialists of risk departments. The results of the RCa assessment may increase the efficiency of decisions taken by credit institutions to ensure cybersecurity in EBT.

REFERENCES

1. King B. Bank 4.0: Banking everywhere, never at a Bank. Singapore: John Wiley & Sons Ltd; 2018. 352 p.
2. Skinner C. Digital human: The fourth revolution of humanity includes everyone. Singapore: Marshall Cavendish International (Asia) Pte Ltd; 2018. 400 p.
3. Revenkov P.V., Berdyugin A.A. Method of quantifying the risk of cyberattacks in the context of electronic banking. *Bankovskoye delo = Banking*. 2020;7:32–37. (In Russ.).
4. Salihu A., Metin H., Hajrizi E., Ahmeti M. The effect of security and ease of use on reducing the problems/deficiencies of Electronic Banking Services. *IFAC-PapersOnLine*. 2019;52(25):159–163. DOI: 10.1016/j.ifacol.2019.12.465
5. Kleijmeer R., Prenio J., Yong J. Varying shades of red: How red team testing frameworks can enhance the cyber resilience of financial institutions. Financial Stability Institute. FSI Insights on Policy Implementation. 2019;(21). URL: https://www.bis.org/fsi/publ/insights21.pdf (accessed on 20.05.2020).
6. Konyavskii V.A., Revenkov P.V., Frolov D.B. et al. Cybersecurity in the conditions of electronic banking: Practical guide. Moscow: Prometei; 2020. 520 p. (In Russ.).
7. Berdyugin A.A., Revenkov P.V. Approaches to measuring the risk of cyberattacks in remote banking services of Russia. *IT Security*. 2019;26(4):83–92. DOI: 10.26583/bit.2019.4.06
8. Skorodumova O.B., Skorodumov B.I., Matronina L.F. Components of the quality of information security. *Natsional'naya bezopasnost' / nota bene = National Security / nota bene*. 2018;(2):1–9. (In Russ.).
9. Vasilieva E.V., Solyanov K.S., Konevtseva T.D. Adaptive data warehouse as the technological basis of the banking ecosystem. *Finansy: teoriya i praktika = Finance: Theory and Practice*. 2019;24(3):132–146. (In Russ.). DOI: 10.26794/2587–5671–2019–24–3–132–146
10. Flenov M.E. The Delphi Bible. St. Petersburg: BHV-Petersburg; 2011. 688 p. (in Russ.).
11. Kozminykh S.I. The use of computer simulation for staff training at the facilities of fuel and energy complex. *Informatsionnye resursy Rossii = Information Resources of Russia*. 2019;(3):2–8. (In Russ.).
12. Lee L. Cybercrime has evolved: It's time cyber security did too. *Computer Fraud & Security*. 2019;2019(6):8–11. DOI: 10.1016/S 1361–3723(19)30063–6

13. Gisin V. B., Slavin B. B. et al. Paradigms of the digital economy: Artificial intelligence technologies in finance and fintech. Moscow: Cogito-Centre; 2019. 326 p. (In Russ.).
14. Nikkel B. Fintech forensics: Criminal investigation and digital evidence in financial technologies. *Forensic Science International: Digital Investigation*. 2020;33:200908. DOI: 10.1016/j.fsidi.2020.200908
15. Krylov G. O. Improving decision-making processes when processing big data in the Federal Financial Monitoring Service. *Modern mathematics and concepts of innovative mathematical education*. 2020;7(1):143–152.

ABOUT THE AUTHORS

Aleksandr A. Berdyugin — Lecturer, Department of Information Security, Financial University, Moscow, Russia
a40546b@gmail.com

Pavel V. Revenkov — Dr. Sci (Econ.), Prof., Department of Information Security, Financial University, Moscow, Russia
pavel.revenkov@mail.ru

The article was submitted on 28.06.2020; revised on 24.08.2020 and accepted for publication on 12.09.2020.
The authors read and approved the final version of the manuscript.