DOI: 10.19192/wsfip.sj4.2016.11

Paweł SITEK*

SAFETY AND RISK ANALYSIS OF A BANKING FACILITY

Summary
From the objective point of view, safety of a banking facility is nothing more than organized opposition against any threats caused by human actions, force of nature as well as shortcomings in the civilization and threats in the bank continuity as a whole and individual elements of its material and non-material structure. The basic determinant of such approach is to maintain management continuity of a bank facility at any time and in any circumstances of its operation. The basis for that is the shape and quality of legal and organizational solutions as well as reliable and substantive assessment of the security risks of a bank facility including all the aspects of these threats. The main purpose of the research was to make a theoretical assessment of a bank facility safety in terms of potential threats.

Key words: *bank, banking facility, the risk of bank building, threat for a bank building*

INTRODUCTION

Uncertain international situation, armed conflicts, social disputes, crime, accidents and natural disasters force state authorities and individual organizations, particularly those with scattered organizational structure, to take remedial steps often without proper preparation. Dangerous situations are difficult to be predicted as they are sudden and violent. The purpose of the paper is to discuss a bank's safety in the situation where potential threats may occur. The aim of the research was to assess the safety of a banking facility in terms of potential threats.

The main research problem is included in the question: 'what does bank security look like in the context of current formal and legal regulations?' which means:

* Paweł Sitek – adjunct University of Finance and management in Warsaw, pawel.sit@wp.pl

- whether applicable provisions of law (and inner regulations) form the conditions to shape bank safety at acceptable level?;
- whether legal status – defined by inner bank legislation is satisfactory and regulates the issues related to creating management structure in emergency situation?;
- and finally, is it enough to implement tools such as detailed procedures, rules and directives?.

The methodology of threats analysis is applied in the research process, which is based on well-known in literature, methods of threats and risk analysis[1] adjusted to the specialty of the banking facility. This methodology is based on three essential elements such as safety risk, the consequences and the probability related to the three key factors: the banking service, safety areas defined as persons, property and information protection. The analysis aims at determining the size of each element, for every security areas, for each type of protection tools considering the threats related to the specified facility and specified protection measures. The final effect is to define the level of risk to safety for every Polish bank between 1 to 100 points. It is assumed that certain risks are acceptable if they adopt value below 50 points. The risk value greater than or equal to 50 points means that the risk is impossible to be accepted and in such cases it is necessary to take actions which allow to decrease the value of the current risk.

It was also important to analyze protective measures against potential threats for which the banking facility is exposed to. The characterized protective measures are directly related to persons and property protection, carried out in the form of direct physical protection (permanent or temporary) which includes constant supervision of the signals transmitted, collected and processed in the electronic devices and alarm systems as well as application of security technology.

[1] Mazaras &Gerard - *MARION- audit methods and risk assessment*, practice material for the National Bank of Poland 1997, Methodology *CRAMM* - practice materials of Inner Security Agencies.

1. Characteristics of threats and their impact on security of a banking facility in European Union (the ECB)

The threat level of a typical crime has persisted in the European Union countries for several years on the medium level and the situation is quite stable. In Europe, since the end of 2014, there have not been any serious incidents as well as new/untypical ways of criminal actions. Yet, in some countries there is high risk of terrorism. An alarming issue is the fact that a large number of EU citizens has joined the Islamic State and the possibility of their homecoming to their respective countries[2].

The information given during the meeting of a working group '*Security Inspectors Group (SIG) and its Liaison Members Frankfurt 2015*'[3] paid attention, inter alia, that the Netherlands has seized, during the last two years, 22 thousand firearms including a large number of AK-47 rifles, automatic and machinery weapon. Quite often there are incidents of using guns but mainly in context of settling a score between people from the criminal underworld and they are mostly the victims of violence. Therefore, due to high level of risk in the Netherlands the police force was reorganized and a single National Police, out of 25 regional police corps, was formed. A new challenge, for the European Central Bank, is a different kind of protest and demonstration against them. The most noteworthy example might be the attack on the President Mr. Mario Draghi during the conference at the headquarters of the European Central Bank in April 2015[4]. During his speech an activist from Femen group burst into the lectern, shouting 'stop ECB dictatorship'. Fortunately, apart from scattering confetti on President Draghi, she did not take any other forms of violence and she was quickly neutralized by security personnel. A month earlier, just before the opening of the new ECB's premises in Frankfurt, anti-capitalism manifestation was organized. It gathered, in front of the bank headquarters, about 10 thousand people with the slogans 'stop austerity policy' and although it was supposed to be a peaceful event it turned into a riot. Fights with the police lasted throughout the day and as a result

[2] A. Zięba, *Terroryzm w Unii Europejskiej na początku XXI wieku: wnioski dla Polski*, http://www.inp.uw.edu.pl/files/publikacje/TerroryzmUEAZieba.pdf (4 June 2016).
[3] Information based on the report from the meeting of working group Security Inspectors Group (SIG) and its Liaison Members Frankfurt 2015.
[4] *Atak na szefa EBC,* http://wiadomosci.dziennik.pl/swiat (4 May 2016).

several radio-dispatched cars were burned, about 150 police officers were injured and more than 500 people were detained. The police managed to foil the attempt of intrusion by the demonstrators to the new ECB's headquarter. It was not the first case of aggression against central banks and in the recent years there were similar incidents in Italy and Greece. That is why, nowadays, central banks start to change the policy of the access to their facilities to make it difficult to enter on their area by force.

Considering new trends and threats such as the last recorded attack on cash processing centres made by organized criminal groups with the use of explosive material and machinery weapon, or attack from the air using the helicopter, new project of building cash processing centres has been introduced.

The centres has been located in such a way to provide outside security passage with a width of at least 25 meters from the first outside fence to the main building. The new building has been designed in such a form to provide security case of using explosive materials, airstrike or all-out outside attack. It was considered that even in such situations the building should 'protect itself' for at least 30 minutes, thanks to the use of technological and organizational solutions. For that reason, apart from location and obstacles preventing entrance into the main building, the following solutions have been used:

- activities related to the support for EURO is inside of the building and administrative, office and subsidiary functions are in the outside zones,
- special roofing construction above the building has been designed, on one hand it provides access to the light and air to the inside court but on the other, it limits the possibility of air strike,
- to protect treasury space a double wall with similar resistance to burglary was made: the treasury walls were designed in the same form to prolong time needed to gain access to the values even with the use of explosive materials.

Another issue connected with the protection is the air freight of EURO[5] banknotes. A huge problem, especially for central banks in small countries which organized annually only a few air freights, is the

[5] European Central Bank directives dated 20 July 2012 related to the data exchange connected with the cash services ECB/2012/16 (Journal of Laws UE. L. 2012. 245. 3).

cooperation with the airlines servicing cargo freights. For carriers the problems related to the issues such as: checking and verification of personal crew warehouse, special procedures of loading and unloading of the airport operations, the duration of such operations, etc. cause that the carriers are reluctant to undertake such orders. The quality of cooperation with the National Bank, which is the key business partner for the carrier, is generally unsatisfactory. Therefore, it is recommended to attempt creation of a single central contract, for example, by the ECB in order to increase the negotiation possibilities and above all forming standard requirements which the carrier would have to meet to apply for such an order. This idea met with sceptical approach by the ECB representatives who pointed to the difficulty in providing the same flexibility as national banks have today, at the level of one central contract.

In addition, the issues of procedural nature were also discussed in the meeting. The participants discussed when and in what circumstances should real acknowledgement of receipt for the collection of the air freight be notified and how the bank, the receiver, the courier, and the sender should protect the valuables. The point is that often during the airport operations, the couriers lose the possibility of full control over the pallets with the banknotes and the moment of formal takeover of the value removes from the couriers the responsibility for the assigned property.

The next problem is the protection of cargo freights with the EURO banknotes especially their monitoring in the realization process. The ECB has attempted to engage NATO to this undertaking as it has the possibility of full control of air space over the member states. Nowadays such flights are covered by standard procedures deriving from the regulations of civil aviation. However, in case of the plane crash of Malaysian Airlines flight MH370 in 2014 (flight from Kuala Lumpur to Peking), standard-based solution for civil control flights were insufficient. So far we do not know the place where the crash occurred or the route which the plane followed a few hours before the crash. Unfortunately the ECB's request was denied and in the justification NATO pointed to technical possibilities that are currently available in

civil applications. These solutions are currently the subject of in-depth analysis by ECB's experts[6].

2. Characteristics of threats and their impact on the security of a banking facility in Poland

In order to identify the threats and their impact on the security of a banking facility it is necessary to diagnose and understand deeply all kinds of threats with their time, space and environmental conditions of their formation and occurrence. For this purpose the following classification of the threats made for determining the security risk of a banking facility can be used.

According to the criterion of causality, threats have been divided into random and intended. According to the criterion of place, threats have been divided into external and internal. According to the nature of the crime: criminal, economic and financial as well as the threats of computer and IT nature were identified. According to the coverage of risk, for extensive and local.

Random threats: these are threats resulting from forces of nature (the elements), they are not directly related to the intended action of a man. Of course in some cases the boundary between the random threats and the dangers resulting from man actions is not precise. It can be the case, for example, that a man in a conscious or unconscious way will trigger the forces of the nature. The randomness of these events can also be described in some framework by using statistics or even probability taking into account the input of the nature phenomenon that are likely to occur or occur in specific area (mine damage, flood, droughts, storms and hurricane). The most common threat from this group is fire. This is a random threat although it usually results from neglecting certain regulations by human beings[7].

Intended threats: are these which are caused by a man. The source of these threats is a man's action or lack of it. Their diversity is as huge as unlimited human imagination. In practice, however, it depends on the complexity of the function that represents the subject of the threats. In

[6] Information based on the report from the meeting of working group *Security Inspectors Group (SIG) and its Laison Members Frankfurt 2015*.

[7] J. Jędrasik – Jankowska, *Pojęcia i konstrukcje prawne ubezpieczenia społecznego*, Wolters Kluwer 2016, pp. 103 – 127.

our case this subject is a bank with a wide range of services and statutory functions. Therefore, the amount of threats here is enormous. Another characteristic feature of the described threat is illegality- in other words- the intended threats are caused by illegal actions. The next characteristic feature is the actual character. So these are real threats. Therefore, to classify the event as an intended threat it must be done by a specific person, in specific time and purpose and it must be illegal. In legal terminology such an event is defined as an offence. For this reason the intended threat is often a potential crime[8].

The aim of the assault can be a bank's client who is doing financial transaction or who is using safety deposit box. The assault is so distinctive that it takes a short time. The other places in the bank are less exposed to this type of threat but they cannot be completely excluded. The next threat of a criminal character can be **burglary**. The aim of this crime is generally stealing the money or equipment. It can also be a preliminary stage to a planned financial, economic or computer-IT crime. Nowadays and for sure in the near future, the burglary will be one of the steps on the way to espionage and sabotage. So it can be seen that the risk of burglary can occur in almost every place and its aim does not necessarily have to be stealing money. We can even say that stealing money from the bank, as the act of burglary, is the source of the biggest losses. A successful burglary allows to commit other crimes, as a result of which losses may be far larger and are not able to be estimated or sorted out in a real time.

Another threat from this group is caused by **theft**. The characteristic for this crime is the fact that the perpetrator entered the building without violating the law. The perpetrators of these crimes may be, in theory, bank employees as well as the bank's clients. Their aim is to steal the property in a direct way.

The literature mostly says about: economic, financial and computer threats. Recent years in Europe and in the world have contributed to the development of global information technology. For that reason computer-IT threats have become the most recent threat and they mostly threaten the integrity and confidentiality of the stored and processed information in the bank or transmitted in an information network - internal and

[8] P. Sienkiewicz, Analiza ryzyka w zarządzaniu projektami systemów, AON 2005, pp. 9 – 12.

external. This is a new and extremely dangerous form of threat. It includes direct theft on unlimited scale, economic espionage and sabotage. The area of occurrence of this threat is mostly strategic places in the bank: places with computer equipment and the information network.

The computer-IT threats include all these criminal groups which attempt to 'burgle' to the information network or to reach the bank computers in order to steal, to change or to delete the information. Potential criminals can be the bank's employees as well as people from the outside. The occurrence of such threat is not limited to bank working hours but it exists constantly when the computers are working or they can be turned on[9]. The dynamic development of the information technology, observed in recent years, and its extensive and widespread use in banks and financial institutions resulting in the access to an increasingly wide range of services through the network and computer systems, causes the formation of new and extension of existing threats.

These threats, in the area of information technology and telecommunication, are associated mainly with the fact of disobeying safety systems for development of new information technologies as well as not paying the proper attention to the safety aspects in earlier periods of information systems formation. The fast development of information systems forces to constant development of IT infrastructure and it also imposes a number of new tasks[10]. In banks, customer service is conducted by means of electronic information processing which involves a number of threats. On the basis of the above characteristics for banking facility the catalogue of the threats have been generated. These are: fire, flood[11], burglary, theft[12], assault, terrorism attack, disclosure of confidential information to unauthorized people, disclosure of sensitive information[13], wiretap, preview[14], property destruction or damage,

[9] A. Suchaczewska , *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Oficyna Wolters Kluwer business, Warszawa 2010, pp. 48 – 54.
[10] Ibidem, pp. 57 – 60.
[11] *The flood in face of the threat*, Government Security Centre Office analysis 2013, pp. 3 – 12.
[12] J. Kupczyński, B. Rydz, *Strategia działania współczesnego włamywacza*, Central Forensic Police Laboratory, Warszawa 2015, pp. 15 – 20.
[13] Z. T. Nowicki, *Alarm o przestępstwie*, TNOiK, Toruń 1997, p. 222.

breakdown of equipment and devices that are part of a system[15], sabotage[16], employees disloyalty, bribery, kidnapping for extortion, unauthorized duplication, forgery, staff policy in terms of security aspect, employees incompetence, failure to comply with formal and legal provisions in terms of persons and property protection, lack or inappropriate formal legal rules.

3. Methodology of threat analysis for a banking facility

Methodology, on which the threats analysis of the protected banking facility is based, was created on well-known specialized methodologies of threats analysis and the risks adjusted to a specific banking facility and it covers three essential elements[17]:

- safety risk: understood as risk arising due to lack or existence of inadequate solutions in the field of banking facility protection against unauthorized, harmful or criminal action of the employees or a third party or, as a result, of interference by majeure force, thus negatively affecting the performance of the important tasks necessary to achieve the bank objectives.
- results: understood as undesirable, negative effect of the occurrence of particular threats,
- probability: understood as the noticeable and measurable possibility of the occurrence of a particular threat as a result of favourable environmental conditions (surrounding) and as the result of the revealed 'weakness' in protections measures relating to three key areas identified as bank security: persons protection (PP) understood as the action aimed at ensuring life and health safety and personal integrity, property protection (PP) understood as the actions preventing the offences against property and against damage resulting from these threats as well as banning the access of unauthorized

[14] R. Radziejewski, S. J. Siudalski, *Ochrona Osób i Mienia*, Electronic Systems Institute, Electronics Department of Technical Military Academy, Warszawa 2013, pp. 19 – 20.
[15] Z. T. Nowicki, *Alarm o przestępstwie*, TNOiK, Toruń 1997, p. 204.
[16] Ibidem, p. 123.
[17] M. Szulim, M. Kuchta , *Metoda analizy skuteczności systemu bezpieczeństwa obiektu*, Biuletyn WAT Vol. LIX, Nr 4, 2010, pp. 112 – 114.

persons to the protected area[18]; information protection (PI) understood as the action using individual protection measures to prevent the disclosure of the legal protected and sensitive information and sensitive as well as preventing unauthorized access to it[19].

The analysis is based on defined size of each element, for each security areas, each type of measures protection considering the threats relating to specific facility and particular protection measures. The final effect is to determine the level of security risk for every banking facility according to the criteria provided in the table below[20].

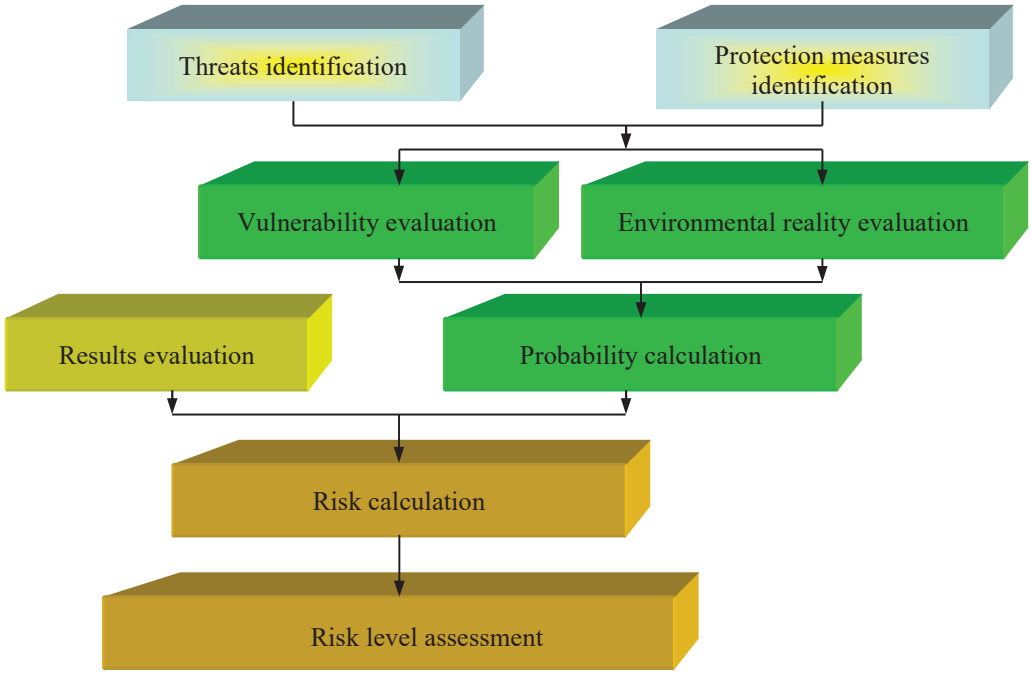
Table no. 2. Criteria defining the level of security risk for the banking facility

No.	Level of security risk	The number of points
1	Low risk	0 - 30
2	Medium risk	30,1 - 60
3	High risk	60,1 - 90
4	Very high risk	90,1 - 100

Source: The criteria is based on 'Methodology of threats analysis and risk protection in banking facility in the field of safety measures use for persons and property protection'. Own elaboration of the Polish National Bank

[18] The Act of 22 August 1997 for persons and property protection (Journal of Laws of 1997, no. 114, item 740).
[19] The Act of 5 August 2010 for protection of classified information (Journal of Laws of 2010, no. 182, item 1228).
[20] Methodology of threats analysis and risk protection in banking facility in the field of safety measures use for persons and property protection. Own elaboration of the Polish National Bank.

Figure no. 1. Methodology flow chart



The source: Criteria based on Methodology of threats analysis and risk protection in banking facility in the field of safety measures use for persons and property protection. Own elaboration of the Polish National Bank

The analysis process boils down to obtain the answers to the following questions:

- whether in real conditions the "x" threat can occur or not?,
- which area and place in the bank can the "x" threat be connected with?,
- whether the "x" threat may have its source outside or inside of the bank structure?,
- what assets *(information, devices, space, valu*e) of the bank can the "x" be?,
- what is the nature of the potential "x" threat?,
- what the duration period of bank operation can the "x" threat relate to?,
- what technical and organizational measures are able to neutralize the "x" threat and whether such measures are available?

These answers are the basis in the assessment of the current level of the facility safety and the choice of the security measures adequate to the existing threats as well as developing the plan for their implementation and possible modernization. In addition, it may help to detect these areas, in technical security systems and physical protection, where the risk exceeds the acceptable level. There is an increase in awareness of the threats existence and the high level of the banking facility safety.

These analyses allow the security managers to determine and identify the necessary measures in the field of protection measures applied in the bank. In addition, they provide the data on which we can base decisions regarding the choice of the priorities and relationship between the technical security and other protection measures.

For proper execution of these range of activities related to carrying out the threats and risk analysis, it is necessary to identify and understand time and spatial threats as well as their formation in environmental condition. The key point to identify and understand all the threats, which the banking facility is exposed to in the areas of persons, property and information protection, is the classification of these threats. On the basis of the above classification, we can determine what threats can occur in a particular banking facility and these identified threats are the subject to further analysis. To conduct a valid assessment there are meetings with a competent representative of external institutions such as the Police or Fire Extinguishing Service responsible for security in the area of banking facility[21].

Their task is to provide the information related to the level of these threats. Opinions and assessments are related to the banking facility on the basis of its location. To be more objective and to make average ratings, the level is defined in following categories: 'low', 'medium', 'high', and 'extremely high' for the four threat groups classified as 'random threats', 'criminal threats', 'organizational threats' and 'information protection threats' group. Each category is assigned to a threshold. This classification of the threshold is the supporting elements to determine further value of the rating points of the individual features 'vulnerability' and 'environmental reality'.

[21] *Facility protection plan related to mandatory protection*, www.zabezpieczenia.com.pl/publicystyka/plan-ochrony-obiektu-podlegajacego-obowiazkowej-ochronie (7 June 2016).

Then, individually for each protection measure applied in the banking facility, the potential results in the occurrence of every identified threat are estimated. Estimation is carried out in relation to all previously motioned key areas of security it means: **persons protection, property protection and information protection** and they reflect the direct and indirect damages in the banking facility which can occur as a result of a threat relating to the analyzed protection measure. The estimation results are defined by the use of a point scale within the range from 1 to 10 points. Where point 1 means that the threat does not result in any effect or that the effects would be minimal, whereas 10 points mean maximum level of the effects.

3.1. Risk assessment of a banking facility

Assessment of the individual vulnerability is related to identification and evaluation of the vulnerability in individual protection measures. It is defined as the identification of the 'weak point' and ease evaluation of protection measure where the 'damage' can be caused. The vulnerability itself does not cause the damage, it may be only the opportunity which may allow the attackers to cause the damage. First of all these vulnerabilities related to the threats, are analyzed considering the changes occurred in the environment and existing protection. The total value of the vulnerability level is in the range from 0,5 to 5,0 points[22].

The next step is to determine the indicator of the real level in environmental threats that means the real occurrence of the specified threat in existing environmental (region, country, city, district). The estimation refers to the opinions of the local services responsible for the security. The level of individual probability is the sum of the level of individual vulnerability and environmental reality.

[22] P. Sienkiewicz, Analiza ryzyka w zarządzaniu projektami systemów, AON 2005.

Formula no. 1 Individual probability.

$$P_J = p_J + r_J$$

where:
P_J – individual probability,
p_J - individual vulnerability,
r_J – individual reality[23].

The size of probability ranges from 1 to 10 points, where point 1 corresponds to 0,1 probability and 10 points to 1,0 probability expressed in the values corresponding to mathematical formula of probability. The methodology assumes that the level of **individual risk** is the function of the effects which can arise in a banking facility if a specific threat occurs and the probability of this threat occurrence, expressed as the product of these components that means:

Formula no. 2 Individual risk.

$$R_J = S_J \times P_J$$

where:
R_J – individual risk,
S_J – individual results,
P_J – individual probability[24].

Then individual risks are summed and the risk related to the particular protection measure (**Rs**) is calculated as the average risk which is the result of the sum quotient of the individual risk ($\mathbf{R_J}$) specified for the adopted threats and the number of accepted risks (**Z**).
Formula no. 3 Average risk.

$$R_S = \frac{\sum R_J}{Z}$$ [25]

[23] The formula of individual probability defined in Methodology of threats analysis and risk protection in banking facility in the field of safety measures use for persons and property protection. Own elaboration of the Polish National Bank
[24] Formula for individual risk defined in Methodology of threats analysis and risk protection in banking facility in the field of safety measures use for persons and property protection. Own elaboration of the Polish National Bank
[25] Formula for average risk defined in Methodology of threats analysis and risk protection in banking facility in the field of safety measures use for persons and property protection. Own elaboration of the Polish National Bank.

For each of the protection measure safety risk matrix will be filled, presented in the table below.

Table no. 3. Safety risk matrix

No.	Threats*)	Results S_J			Probability P_J			Individual risk R_J		
		OO	**OM**	**OI**	**OO**	**OM**	**OI**	**OO**	**OM**	**OI**
1.	Threat no. 1									
2.	Threat on. 2									
3.	Threat no. 3									
4.	…									
Average risk size - R_S										

In the table above the abbreviations are related to:(OO) – persons protection, (OM) – property protection, (OI) – information protection.
**) The list of the potential threats was presented in chapter 2.3. 'Threats characteristic and their impact on security of a banking facility in Poland'*

Source: The table was defined on the basis of Methodology of threats analysis and risk protection in banking facility in the field of safety measures use for persons and property protection. Own elaboration of the Polish National Bank.

The risk level accepts the values from 1 to 100. The lowest value is obtained when small potential effects of specified threat meet with the minimum probability of the threat. High risk value occurs when the effects of the specific threat are serious and the probability of the threat is high.

After filling the risk matrix for all protection measures the individual average risks **(Rs)** are compiled in the table of safety facility risk and the **risk of facility safety (R_O)** is calculated as the quotient of the average risk sum (**R_S)** for individual protection measures and number of the protection measure (**$Ś_O$**), for which the risk has been identified.

Formula no. 4 The risk of facility safety.

$$R_O = \frac{\sum R_S}{\acute{S}_O} \quad 26$$

Table no. 4. The risk of the facility safety.

No.	Specification of the protection measures(ŚO) *)	Average risk (RS)		
		OO	OM	OI
1.	Protection measure no. 1			
2	Protection measure no. 2			
3	Protection measure no. 3			
4	…			
The risk of facility safety (RO)				

In the table above the abbreviations are related to:(OO) – persons protection, (OM) – property protection, (OI) – information protection.
**) The list of the potential threats was presented in chapter 4. 'Protection measures against the potential threats of the banking facility'.*

Source: The table was defined on the basis of Methodology of threats analysis and risk protection in banking facility in the field of safety measures use for persons and property protection. Own elaboration of the Polish National Bank.

For banking facility particular risks are acceptable if they adopt the value:

$$R \langle 50\, pkt.* \quad 27$$

) it applies to all risks including average risk* *(RS)*** *and individual risk* ***(RJ).*** *The risk values higher or equal 50 points mean unacceptable risk (in these cases it is necessary to take actions to reduce the risk size)*

In order to illustrate the analysis process as the additional element there should be summary of safety risks in banking facility within the

[26] Formula for facility safety defined in Methodology of threats analysis and risk protection in banking facility in the field of safety measures use for persons and property protection. Own elaboration of the Polish National Bank.
[27] The level of acceptable facility risk defined in Methodology of threats analysis and risk protection in banking facility in the field of safety measures use for persons and property protection. Own elaboration of the Polish National Bank.

protection measures applied to protect persons and property. The following table presents the formula of the summary.

Table no 5. The summary of safety risks in banking facility (within the protection measures applied to protect persons and property)

No.	Threats*)	Protection measure no. 1			Protection measure no. 2			Protection measure no. 3			…			Safety risk of the facility calculated for specified threats		
		OO	OM	OI	OO	OM	OI	OO	OM	OI	OO	OM	OI	OO	OM	OI
1.	Threat no. 1															
2.	Threat no 2															
3.	Threat no 3															
4.	…															
5.	Average risk size Rs calculated for specific protection measures															

In the table above the abbreviations are related to:(OO) – persons protection, (OM) – property protection, (OI) – information protection.
**) The list of the potential threats was presented in chapter 2.3. 'Threats characteristic and their impact on the banking facility safety in Poland'.*

Source: The table was defined on the basis of Methodology of threats analysis and risk protection in banking facility in the field of safety measures use for persons and property protection. Own elaboration of the Polish National Bank.

4. Protection measures against potential threats which banking facilities are exposed to

4.1. Physical protection of persons and property

Physical protection of persons and property as Specialist Protective Armed Formation organized in form of Internal Security (Banking Guard) or in the form of Commercial Specialist Protective Armed Formation within the scope of direct, permanent or ad hoc physical protection related to constant supervision of the signals transmitted, collected and processed in electronic devices and alarm systems as well

as the conveyance of monetary value and other valuable and dangerous objects[28].

The basic duties of physical protection employees is to obey the law, to implement precisely the tasks arising from protection system and follow the internal and external formal-legal regulations. They are also obliged to constant vigilance and attention span on the protective activities, to keep the register of service record and to notify superiors about any noticed irregularities which may influence the condition of security facility and in case of emergency, taking immediate intervention to dead off the danger. The intervention must be commensurate to the degree of the risk including the time, enemy forces, forces of own security personnel and the place of intervention. In addition, every employee of physical protection is obliged to keep confidentially all the data related to the protected facility and take care of proper condition of equipment used to carry out the tasks. Facilities protection may be implemented 'stationary' as the constant or ad hoc protection on the site and 'mobile' by the intervention or protective groups.

4.2. Technical systems of persons and property security

Equipment and technical systems of persons and banking facility property protection are nowadays fast developing technology. Their application covers all areas of social life. Along with the improvement of living conditions and prosperity of the society we can observe the increase in personal and property threats both for private property and banking facilities. For the technical protection systems, in terms of complex security system, the following protection measures are applied: 'systems and devices of property protection'. These are intrusion alarm systems - used to detect and indicate the presence, entry or the attempt to enter the protected facility, separated security zone or separately protected space. CCTV surveillance systems consist of such elements as camera kits, control devices, devices for transfer, register, archive and control. Access control systems as the group of identification, detection, decision-making and regulation devices cooperate according to the defined algorithm which together with organizational activities allow for controlled entry and leaving from the area supervised by the system.

[28] The Act of 22 August 1997 for persons and property protection (Journal of Laws of 1997, no. 114, item 740).

Within these systems there can be separated subsystem supporting the organizational tasks in terms of management of parking space on the internal and external courtyards, parking lots and garages[29].

Particularly important in this area are the alarm transmission systems as the devices or network used for automatic transition of the information concerning the condition of one or more alarm systems to one or more alarm receiving centres. The systems can contain several independent links which use different alarm transmission devices (wire or wireless).

The supporting systems are: car alarm systems as the signalling systems of the trial to enter inside the vehicle used for the transport of monetary value (for example door opening, clumping etc.), monitoring systems of value transport implemented as the systems which allow - with the use of necessary technical and organizational measures - to supervise constantly and remotely the vehicles used for value transport (these systems use car alarm systems and wireless alarm transmission systems). Supporting elements can be electronic devices for sealing the cabinet and space - the devices recording the unauthorized opening of the cabinet or space.

Information protection systems and devices are another group of measures used as a part of complex system of banking facility security. The information protection devices are the devices detecting the installed transmitters used for wiretap (operating and stand-guarding) – there are mostly meters of the radioactive energy made by the devices in terms of electromagnetic waves or devices for detecting physical presence of the electronic elements hidden in building constructions or the objects which equipped the space.

These are also devices to jammer the internal and external wiretap - mostly in the form of sound waves generators or electromagnetic which distort the information outside the room or derange the work of the constituent element in the wiretap which is installed in the room. The systems and methods of protection against electromagnetic wiretap (capturing electromagnetic emission) - mainly in the form of passive or active methods of distorting emitted electromagnetic waves or limiting

[29] M. Szustakowski, W. Ciurapiński, *Techniczne systemy zabezpiecznia mienia i infrastruktury krytycznej*, Institute of Optoelectronics at Technical Military Academy, Warszawa 2006, pp. 1 – 5.

the emission from the devices processing sensitive information to the level considered safe by authorized body[30].

Additional group consists of devices against preview - mainly in the form of curtains, blinds, shutters, etc. to prevent remote image registration, the devices for cryptographic information protection - according to separate studies and information devices with the reduced emission (mainly computers, printers, monitors covers to prevent disclosing emission).

One of the most important systems and devices for persons protection is an **alarm system signalling an attack.** This system allows discreetly and immediately to give the information about the attack. It can be supported by the reserve system of operating room observation (RSOS) which discreetly enables to monitor remotely and wiretap of the operation room. The employees control systems of Internal Protection Services or commercial companies performing patrol function is also a supportive system of security personnel. For personal protection specialized devices, portable or stationary, allowing to detect threat specific for terrorist attack may be used.

For the proper functioning of personal and property protection **communication systems** are used. These are systems for alarm purposes, wire and wireless systems of two-way voice communication which enable effective communication within the banking facility. These systems can be supported by the system of registration of telephone conversation to record sensitive conversations for example terrorist threats, extortion or blackmail.

There are also **integrated systems** in the banking facilities. The integrated systems as technical protection in the banking facility are dedicated to commercial software which equips the service and management workplace. They allow, at the level of common desktop, to observe and analyze the condition of work of autonomous technical security systems, implement alarming procedure and distribute the information in accordance with a specified algorithm. The simplest integrated system is the system which monitors technical security in the

[30] J. Krawiec, G. Ożarek, *Systemy zarządzania bezpieczeństwem informacji w praktyce. Zabezpieczenie*, Polish Standardisation Committee, Warszawa 2014, pp. 7 – 9.

banking facilities and allows to observe and analyze the working condition of the technical security systems[31].

4.3. Mechanical security devices

Among technical security systems of personal and property protection it is worth considering the mechanical security devices (MUZ) defined as 'the devices with appropriate certificates and nameplates identifying the resistance category to burglary, issued by the Precision Mechanic Institute or other qualified certification body accredited by the Polish Accreditation Centre'.[32]

The basic function of the Mechanical Security Devices is to 'resist' and prevent access to the protected resources for the period necessary to take an effective action by the security personnel. The use of Mechanical Security Devices is the oldest way to protect the property, facilities and areas. Since prehistoric times people have been developing mechanical security solutions. Nowadays mechanical and construction security is connected with the resistance of walls, floors, rooms, holes security, windows, doors and the storage value equipment: cabinets, safes, treasury rooms – confidential chancellery for storage the documents, information as well as stores and warehouses, areas, airports and marine, military units, enterprises etc.

4.4. Fire alarm signalling systems

Fire alarm signalling systems (SAP) are systems to detect and indicate the location of the threat or fire implemented as the electric installation:

- fixed fire fighting systems - devices permanently associated with the facility containing own supply of fire-extinguishing, equipped with the system for its storage and automatically run in the early stage of the fire, used for extinguishing materials and equipment by completely filling the space or partial activities,

[31] M. Szustakowski, W. Ciurapiński, *Techniczne systemy zabezpiecznia mienia i infrastruktury krytycznej*, Institute of Optoelectronics at Technical Military Academy, Warszawa, pp. 6 - 11.
[32] The Act of 3 April 1993 on research and certification (Journal of Laws 199 , no. 55, item 250).

- smoke and ventilation systems - the devices permanently associated with the facility which in case of the fire must provide reduction of the concentration of toxic gases, maintain the necessary oxygen level, remove heat excess and combustion products formed during the fire as well as to provide sufficient visibility to evacuate,
- individual (local) fire fighting equipment - other, not previously mentioned, stationary and portable devices for fire protection for example handheld, portable and transportable fire extinguishers, water tanks, fire fighting etc.[33].

Some of the banking facilities are subjected to the requirements of Regulation of the Ministry of Internal Affairs and Administration dated 21 April 2006 on fire protection of buildings and other facilities and the areas of installation audible warning systems (DSO). These are warning systems (alarm broadcast systems) which, after fire alarm signalling, should clearly notify the people in the danger zone about the threat and indicate the evacuation way[34]. Organization of facility protection - as the instructions, procedures, rules results from the Directives of the Polish National Bank dated 2014[35].

Conclusions

The analyses conducted on the basis of the above characterized methodology, show that banking facilities protection is applied correctly. The level of protection and security is sufficient. However, one must consider the possibility of potential threats that may be initiated by criminal or diversionary elements which aim could be to get legal tender or disorganization of currency flow. The role of banking facilities and their location results in the possibility of the threat in form of the robbery. What is more, the robbery is a specific form of the terrorist aggression which can be pointed out in all areas of the bank operations. The place most exposed to this type of threats, is operating room where there is the direct contact of the bank employee with the client. Regarding the availability to the operating room for the third party and

[33] W. Frankowski, B. Zaleski, *Skrypt Inspektora Ochrony Przeciwpożarowej*, Fire Extinguishing Technology Centre, Warszawa 2014, pp. 197 – 202.
[34] Ibidem, p. 203.
[35] Directives of the Polish National Bank from 2014: Technical security standards used in protection of persons and property'.

the fact of storing money in the bank counter, the above threat should be assessed as very probable.

Regarding personal resources, it is generally assumed that the greatest damage for the bank can be caused by the bank's employees, employees from external companies doing repair, maintenance and service activities as well as lack of restriction of the organizational rules. Despite the fact that requirement is carried out due to obligatory legal rules, one could not be sure who is really employed. Whether the potential candidate in his/her private life, does not have connection to a criminal organization. Or whether the desire to work in the bank is not caused by the desire to misappropriate the property or information which are owned by the bank.

As a rule, all protection measures of the banking facilities meet the current requirements of the legal provisions and inner regulations. They are regularly upgraded, maintained and serviced. However, every technical equipment can fail but its failure is low enough so it is not possible to state that the technical process of aging of operating devices significantly influences their current implementation. Every day in banking facilities there are upgrading activities aimed at adapting the systems to the new legal provisions of applicable law. There is constant technological and functional standardization of the systems in order to improve and upgrade specified solutions. The upgrade of existing procedures and instructions is carried out all the time. In case of introduction of new technical solutions new procedures must be developed in relation to these solutions. The assessment of the security level:

- highly - equipped facilities with technical devices and security systems,
- high formal qualification of the security personnel,
- high skills of practical operation of devices and technical security systems,
- correct cooperation with the Police and other services,
- employment stability.

Complex technical and organizational security systems for the facilities are based on integrated safety areas. Security and protection are treated as one of the extensive security system built on individual security subsystems keeping its own hardware and software autonomy integrated within the local monitoring position. The applied devices are

regularly replaced and upgraded and there is no need for their immediate exchange.

To define the risk level, the opinions and assessment of the people responsible for security in each facilities and opinions of the people from external companies working with the bank safety matters, were considered.

On the basis of the gained information it was found that the protection of the analyzed facilities is maintained correctly. The security and protection level is high. The applied protection measures are completed and sufficient. Nonetheless, we should consider the possibility of the threats mostly related to organized crime. We could not exclude people's actions caused by medical factors (mental illness, depression etc.).

The purpose of this article was to assess the security of banking facilities in term of potential threats what has been achieved, to a large extent, by:

- defining and presenting the methodology assumptions which are directly related to the basic functions of the bank activity;
- identifying potential threats directly relating to banking facilities;
- identifying protection measures in the field of personal and property protection which are applied in the banking facilities;
- indicating potential weakness in, broadly defined, security of the banking facilities.

The above elaborations mainly focus on the description of the most essential elements and phrases related to the safety of banking facilities what may become the starting point for further research.

Legal sources

[1.] The Constitution of the Republic of Poland (Journal of Laws of 1997, no. 78, item 483).

[2.] The Act of 3 April 1993 on research and certification (Journal of Laws of 1993, no. 55, item 250).

[3.] The Act of 22 August 1997 on persons and property protection as amended (Journal of Laws of 1997, no.114, item 740).

[4.] Bank Act of 29 August 1997 (Journal of Laws No. 140, item 939), the Polish National Bank Act of August 29, 1997 (Journal of Laws No. 140, item 938).

[5.] The Act of 5 August 2010 on classified information protection (Journal of Laws 2010, no. 182, item 1228).

[6.] European Central Bank directives of 20 July, 2012 on the exchange of the data on the cash EBC/2012/16 (Journal of Laws UE. L. 2012. 245. 3).

Literature

[1.] Information based on the report from the meeting of working group Security Inspectors Group (SIG) and its Laison Members Frankfurt 2015.

[2.] Jędrasik – Jankowska J., Pojęcia i konstrukcje prawne ubezpieczenia społecznego, Wolters Kluwer 2016.

[3.] Krawiec J., Ożarek G., *Systemy zarządzania bezpieczeństwem informacji*
w praktyce Zabezpieczenie, the Polish Standardisation Committee, Warszawa 2014.

[4.] Kupczyński J. Rydz B., *Strategia działania współczesnego włamywacza*, Central Forensic Laboratory of the Police, Warszawa 2015.

[5.] Mazaras &Gerard - MARION, Metoda audytu i oceny ryzyka, materiały szkoleniowe dla NBP rok 1997, Metodyka CRAMM - training materials of Internal Security Agency.

[6.] Metodyka analizy zagrożeń i ochrony ryzyka w obiektach bankowych w zakresie środków ochrony stosowanych do ochrony osób i mienia. 2014.

[7.] Nowicki, Z. T., *Alarm o Przestępstwie*, TNOiK, Toruń 1997.

[8.] *Powódź w obliczu zagrożenia*, the Government Centre for Security, Department of Analysis, 2013.

[9.] Radziejewski R., Siudalski S., Ochrona Osób i Mienia, Instytut Systemów Elektronicznych Wydziału Elektroniki WAT, Warszawa 2013.

[10.] Rotfeld A. D., Strategia bezpieczeństwa narodowego RP w nowych warunkach międzynarodowych: nowe wyzwania, nowe zadania, AON Scientific Journal, 2003, nr 4 (53).

[11.] Sienkiewicz P., Analiza ryzyka w zarządzaniu projektami systemów, AON 2005.

[12.] Suchaczewska A., Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem, Wolters Kluwer Business, Warszawa 2010.

[13.] Szulim M., Kuchta M., *Metoda analizy skuteczności systemu bezpieczeństwa obiektu,* Bulletin of Technical Military Academy, Vol. LIX, Nr 4, 2010.

[14.] Szustakowski M., Ciurapiński W., *Techniczne systemy zabezpiecznia mienia i infrastruktury krytycznej,* Institute of Optoelectronics at Technical Military Academy, Warszawa.

[15.] Guidelines of the National Bank of Poland: Standard of Technical Protective Solutions Applied in Personal and Property Protection, 2014.

Internet sources

[1.] http://wiadomosci.dziennik.pl/swiat (4 May 2016).

[2.] http://www.uwm.edu.pl/mkzk/download/ wprowadzenie.pdf.

[3.] http://www.zabezpieczenia.com.pl/publicystyka/plan-ochrony-obiektu-podlegajacego-obowiazkowej-ochronie (17 June 2016).

[4.] http://www.inp.uw.edu.pl/files/publikacje/TerroryzmUEAZieba.pdf (4 May 2016).