The Concept of Detection Internal Threats of the Company's Business Process Using API -Requests

Igor Mandritsa, Fabrizio d'Amore, Anna Fensel,
Vyacheslav Petrenko, Alexander Zhuk and Olga Mandritsa

November 16, 2021

A concept of detection internal threats of the company's business process using API requests

Mandritsa I.V.[1] [0000-0001-9911-1584], Fabrizio d'Amore[2] [0000-0002-6518-2445], Anna Fensel [3,4] [0000-0002-1391-7104], Petrenko V.I. [1] [0000-0003-4293-7013], Zhuk A.P. [1] [0000-0003-4280-7489], Mandritsa O.V.[5] [0000-0002-0364-1239],

[1] North-Caucasus Federal University, Institute of Mathematics and Information Technologies (named after Prof. Nikolay Chervyakov), 1, Pushkin Street, Stavropol, Russia
[2] SAPIENZA University, DIAG, formerly DIS - Department of Computer, Control and Management Engineering, Via Ariosto 25, I-00184 Rome, Italy
[3] University of Innsbruck, Department of Computer Science, Technikerstr. 21a, A-6020 Innsbruck, Austria,
[4] Wageningen University & Research, Netherlands
[5] Russian Technological University - MIREA, Branch office, Department of regional Economics, 8, Kulakov street, Stavropol, Russia
imandritsa@ncfu.ru, damore@diag.uniroma1.it, anna.fensel@wur.nl

Abstract. The article examines the conceptual ways and methods of using API requests for detection internal threats outgoing from participants in business processes of organizations and firms in CRM system of the company. We study the aggregate model of external and internal threats, and its important part, such as internal threats from personnel and the degree of risk of their occurrence. A threat model has been developed to protect against an internal attacker (resource - "employee" as part of a business process in a CRM system-a Microsoft project). Using a conditional example, the probabilities of risks of information leakage about the business process for an internal threat (a problem employee) are determined. The concept of a system analysis of the probability of internal threats (risks of leaks) of business information is formulated using the source code of the program using API requests based on the developed model of possible types of risks for searching for a problematic employee of a company (corporation).

Keywords: Privacy risk assessment and assurance, typology of cybersecurity internal threats, risks of internal leakage.

1 Introduction

Privacy risk assessment and assurance of the probability of implementation of information threats to the business process of the company (organization) and the associated assessment of possible economic and financial losses is the most complex and responsible part of the entire process of ensuring information security. On the one hand, the real and predictable (potential) internal and external threats are sufficiently fully identified, the degree of security of the business process of the object ultimately depends.

On the other hand, the irrational excess of the adequacy of costs for the protection of the business process, taking into account those threats, the impact of which directly on the functioning of the object is unlikely or the localization of which is impossible or ineffective, will lead to a significant overestimation of the costs of information security, and can significantly affect the actually achieved economic efficiency of information security and, as a consequence, the life cycle of the company. Consequently, the task arises to optimize the level of protection of the business process of the object from internal and external threats, which will allow to achieve maximum efficiency of the selected version of the complex of protective measures [4].

The authors of this study, as a result of discussions and empirical logic of the task, see the solution in the phased implementation of the theoretical model of "smart protection" of the information of the company's business process within the framework of systems widely used in commercial firms: ERP (Enterprise Resource Planning) and CRM (Customer Relation Management). At the same time, the authors adhere to the following standards for the creation of such "smart" automated systems: for Russian firms - GOST 34.003-90, 15971, 16504; for European firms – ISO/IEC 27001:2013 [1].

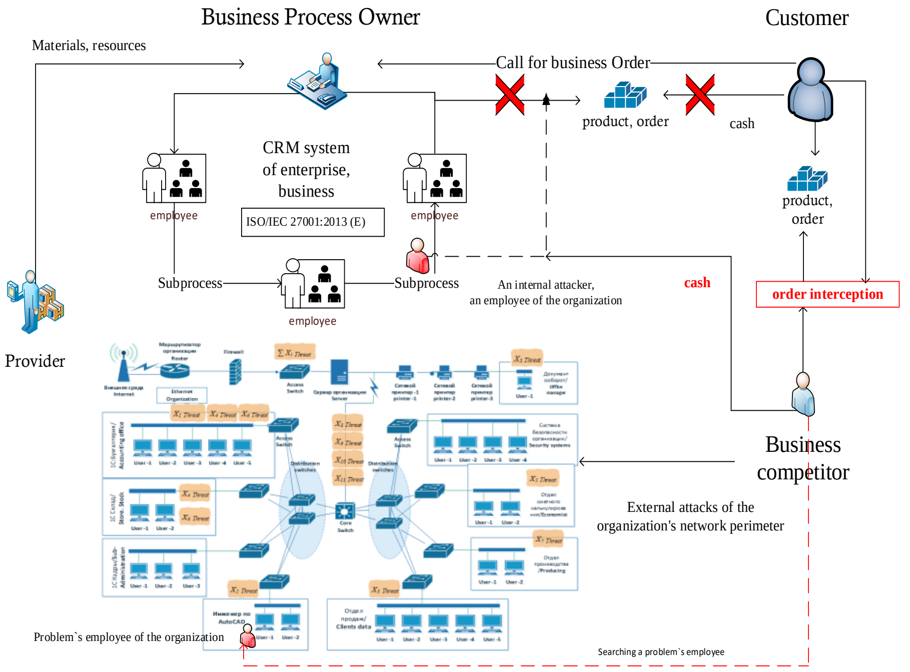


Fig. 1. The emergence of information threats to the business process of the company (external threats not the subject of this paper)

2 Internal problem employee threat model

Exploring the problem of risk of threats, loss of business information from the perspective discussed in Russia of the draft of the standard for information protection (Technical Committee for standardization of «information protection» (TC 362) from 07 February 2020), the authors made an attempt to identify unique aspects of the threats of cybersecurity for the business process of a commercial organization and its constituent elements, in particular [5]:

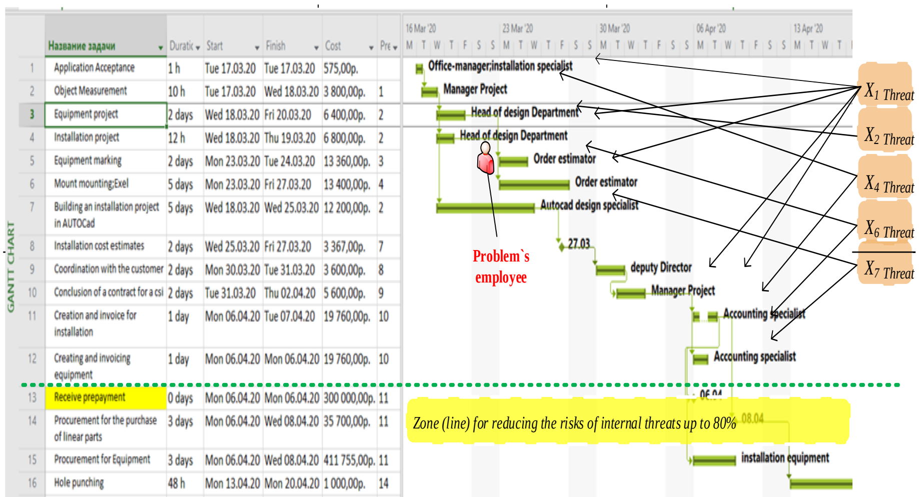
- information security on the stages of the business process,
- information security for the participants of the business process,
- determining the cost-effectiveness threshold for protecting an organization's critical information infrastructure.

At the current moment of development of the science of information technology, in terms of information security and risk assessment, the authors believe that the part of the theory – risk assessment and methods of their assessment – is not sufficiently developed and presented. Cybercrime today creates threats coming from the cyberspace to an organization (firm) and that part of its information that fills this space with benefit, utility or economy, as well as this is called cost. Thus, not all information has a value.

The authors and many experts believe that only information about the business process creates this kind of asset that will bring future benefits to the organization (in the form of income, profit) and can actually be called business information. The loss of such information at various stages is a real (physical and material) damage to the organization. Thus, from the moment when all the information in the turnover of a firm or organization, including business information, begins to bring some income to its owner, the question arises about its rational (optimal) protection from cybercrime (persons who violate the Criminal Code). So according to the Russian criminal code, article 237, theft (copy) information containing business information is one of the types of enrichment, or «pure» profit kidnapper, both at the level of individuals and at a higher level of economic inclusion criminal individuals in this type of activity. The value of business process information is not only in documented words, numbers, and images: knowledge, concepts, ideas, and brands are examples of intangible forms of information.

The Figure 2, «Threat model for protection against an internal attacker», presents a typology of threats to participants in business processes of organizations and firms as part of the internal threats to the business process of the firm in CRM system [4].

As shown in Figure 2, the presented threat model from an internal attacker consists of $\sum Xi$ threats - types of threats (leaks) of information about the client (buyer); i.e., his personal data. This business information is the future income of the company. If you assess the risk of loss is the business information for the stages of the business process before receiving your advance payment from the buyer, the risk of its leakage disproportionate to the stage of obtaining an advance payment from the buyer. Since the probability after the pre-financial part of the business process is already significantly reduced and it is unlikely that the buyer will change the company-seller (manufacturer of services, goods or works) and the risks of leakage of business information will be reduced to minimal values.



	Название задачи	Duratic	Start	Finish	Cost	Pre
1	Application Acceptance	1 h	Tue 17.03.20	Tue 17.03.20	575,00р.	
2	Object Measurement	10 h	Tue 17.03.20	Wed 18.03.20	3 800,00р.	1
3	Equipment project	2 days	Wed 18.03.20	Fri 20.03.20	6 400,00р.	2
4	Installation project	12 h	Wed 18.03.20	Thu 19.03.20	6 800,00р.	2
5	Equipment marking	2 days	Mon 23.03.20	Tue 24.03.20	13 360,00р.	3
6	Mount mounting;Exel	5 days	Mon 23.03.20	Fri 27.03.20	13 400,00р.	4
7	Building an installation project in AUTOCad	5 days	Wed 18.03.20	Wed 25.03.20	12 200,00р.	2
8	Installation cost estimates	2 days	Wed 25.03.20	Fri 27.03.20	3 367,00р.	7
9	Coordination with the customer	2 days	Mon 30.03.20	Tue 31.03.20	3 600,00р.	8
10	Conclusion of a contract for a csi	2 days	Tue 31.03.20	Thu 02.04.20	5 600,00р.	9
11	Creation and invoice for installation	1 day	Mon 06.04.20	Tue 07.04.20	19 760,00р.	10
12	Creating and invoicing equipment	1 day	Mon 06.04.20	Mon 06.04.20	19 760,00р.	10
13	Receive prepayment	0 days	Mon 06.04.20	Mon 06.04.20	300 000,00р.	11
14	Procurement for the purchase of linear parts	3 days	Mon 06.04.20	Wed 08.04.20	35 700,00р.	11
15	Procurement for Equipment	3 days	Mon 06.04.20	Wed 08.04.20	411 755,00р.	11
16	Hole punching	48 h	Mon 13.04.20	Mon 20.04.20	1 000,00р.	14

Fig. 2. Threat`s model for protection against an internal attacker (resource - «problem`s employee» as part of a business process in CRM system – Microsoft Project)

Further, after Figure 2, Table 1 examines the aggregate risk model from external and internal threats to business information loss, and its important part is internal threats from personnel and the degree of risk of their occurrence This (conditional) calculation will be presented below. It should be noted that today the standards of the Russian Federation with the numbers of the range 27003:27005 contain recommendations for the protection of business information. They specifically indicate that such features of « business information - from the authors, in correlation with the international standard ISO/IEC 27002: 2013, include [3]:

- probable threat zone (for business information),
- the type of information asset that will be exposed to the threat,
- type of impacting threat factor (on business information),
- indicators (processes, participants, and stages) of the organization's business process that will be exposed to the threat.

3 Results and discussion.

According to this methodology (which has no Russian counterpart), organizations of all types and sizes (including the public and private sector, commercial and non-commercial) accumulate, process, store and transmit information in various forms, including electronic, physical and oral (for example, interviews and presentations). Presented in Figure 1, we list the internal threats and reduce them to a modernized threat model for the business process of a commercial organization.

Table 1 presents the conditional probability of occurrence of such threats from external and internal intruders, for example, the order of access control systems from the buyer conditional on the data of the manufacturer of access control systems (notional value). The following Table 1 shows the implementation of the conceptual approach of fixing the values of the risks of a problematic employee of the company according to the specified API requests according to Figure 3.

Table 1. Probability of leak risks for the internal threat model (conditional example).

№	Name of the stage of the business process / FULL name of the resource-employee of the company	Probability of threats via technical channels / (from an external attack) ∑R_i(CSINT)	The probability of threats from the staff / (by the number of problems) after API-request (to the specified API-request according to Fig 3. ∑R_i(OSINT)	The total probability of the threat of loss of information (external + internal probability) ∑R_i
1	Application acceptance /FULL name	0	0,3*	0,3
2	Object measurement	0,01	0,04	0,05
3	Equipment project	0,01	0,29*	0,3
4	Installation project	0,01	0	0,01
5	Preparation of estimates for equipment (problem`s employee)	0,01	0,8*	0,81
6	Preparation of estimates for installation; Microsoft Excel	0,01	0	0,01
7	Building a mounting project in AutoCAD	0,01	0,19	0,2
8	Building an installation estimate	0,01	0,04	0,05
9	Agreement with the customer	0,01	0,29*	0,3
10	Conclusion of a contract for CISS (Comprehensive information security system)	0,01	0,09	0,1
11	Creating and issuing an invoice for installation	0,01	0,09	0,1
12	Create and issue an invoice for equipment	0,01	0	0,01
13	Receiving a prepayment for a customer order	0	0	0

The relevance of the search for internal threats (in terms of the number of problems an employee meets) is beyond doubt. The maximum probability for the model of threats from internal intruders (employees-insiders) will be in four zones (marked with a *) and, accordingly, the security department needs to take countermeasures to protect against these types of threats. The authors propose a method of determining the threshold of rationality (optimality) as the amount of expenses for the cost of countermeasures (as an estimate of the events) in this case, count on the basis of the value of the likely amounts of damages for each of the stages of the business process, with the position of the maximum amount of possible damage from the loss of the buyer (the client) in Microsoft Project the full amount of the order, which is the income (revenue) from the client. Accordingly, we get the maximum amount of damage from the types of threats presented in Figure 2, and the amount of the costs of information protection measures for the developed measures to face both external and internal threats.

At the same time, the main focus of the information security specialist will be a new model for building a personnel management system at the stages of the business process and, accordingly, the amounts of possible damage to these stages. For a more detailed analysis of the risks to a participant in the business process of becoming an insider of a competitor company, the authors developed a concept for studying the internal threats of business information leakage from insider personnel, based on its metadata related to the external environment, as shown in Figure 3.

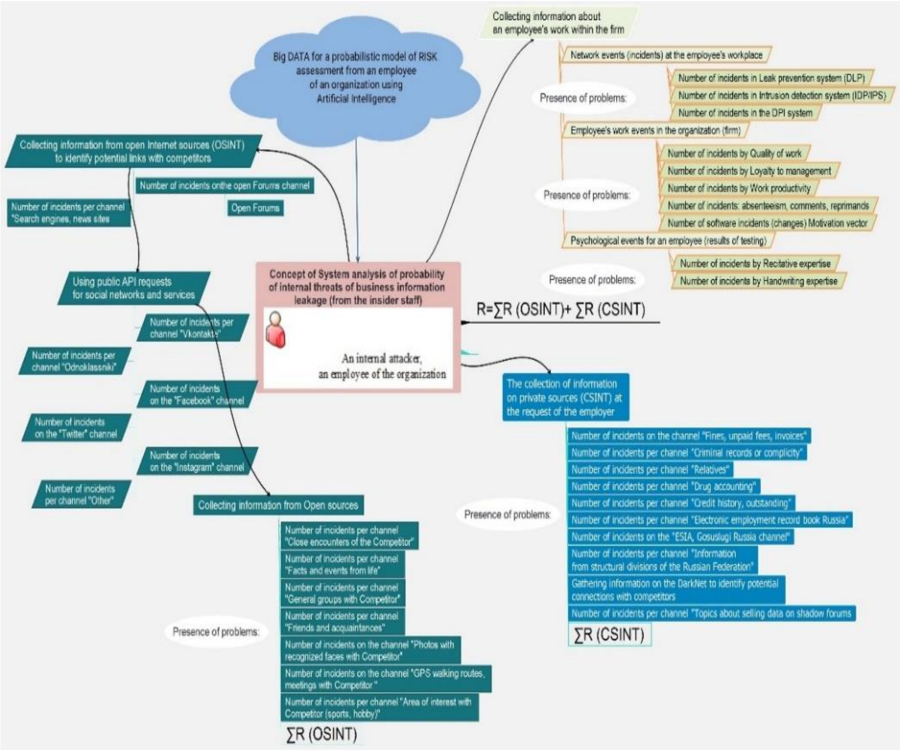

Big DATA for a probabilistic model of RISK assessment from an employee of an organization using Artificial Intelligence
Collecting information about an employee's work within the firm
Network events (incidents) at the employee's workplace
Presence of problems:
Number of incidents in Leak prevention system (DLP)
Number of incidents in Intrusion detection system (IDP/IPS)
Number of incidents in the DPI system
Employee's work events in the organization (firm)
Presence of problems:
Number of incidents by Quality of work
Number of incidents by Loyalty to management
Number of incidents by Work productivity
Number of incidents: absenteeism, comments, reprimands
Number of software incidents (changes) Motivation vector
Psychological events for an employee (results of testing)
Presence of problems:
Number of incidents by Recitative expertise
Number of incidents by Handwriting expertise
Collecting information from open Internet sources (OSINT) to identify potential links with competitors
Number of incidents onthe open Forums channel
Open Forums
Number of incidents per channel "Search engines, news sites
Using public API requests for social networks and services
Number of incidents per channel "Vkontakte"
Number of incidents per channel "Odnoklassniki"
Number of incidents on the "Facebook" channel
Number of incidents on the "Twitter" channel
Number of incidents on the "Instagram" channel
Number of incidents per channel "Other"
Concept of System analysis of probability of internal threats of business information leakage (from the insider staff)
An internal attacker, an employee of the organization
R=∑R (OSINT)+ ∑R (CSINT)
The collection of information on private sources (CSINT) at the request of the employer
Presence of problems:
Number of incidents on the channel "Fines, unpaid fees, invoices"
Number of incidents per channel "Criminal records or complicity"
Number of incidents per channel "Relatives"
Number of incidents per channel "Drug accounting"
Number of incidents per channel "Credit history, outstanding"
Number of incidents per channel "Electronic employment record book Russia"
Number of incidents on the "ESIA, Gosuslugi Russia channel"
Number of incidents per channel "Information from structural divisions of the Russian Federation"
Gathering information on the DarkNet to identify potential connections with competitors
Number of incidents per channel "Topics about selling data on shadow forums
∑R (CSINT)
Collecting information from Open sources
Presence of problems:
Number of incidents per channel "Close encounters of the Competitor"
Number of incidents per channel "Facts and events from life"
Number of incidents per channel "General groups with Competitor"
Number of incidents per channel "Friends and acquaintances"
Number of incidents on the channel "Photos with recognized faces with Competitor"
Number of incidents on the channel "GPS walking routes, meetings with Competitor "
Number of incidents per channel "Area of interest with Competitor (sports, hobby)"
∑R (OSINT)

Fig.3. A concept of System analysis of probability of internal threats (risks of leaks) of business information

As it can be seen from Figure 3, the concept describes three types of collected information about a participant to a business process:

- information about the work of an employee within the company;
- information from closed sources (CSINT);
- information from open sources (OSINT).

Each type of information collection combines a group of search aspects that should be emphasized when identifying the threat of internal leakage of information from personnel. Thus, the authors distinguish between two types of risks - (∑R(CSINT) and ∑R(OSINT) that are subject to a scientifically based measurement method, for the purpose of early detection of risks from an internal insider [7, 8, 9]. As a result, the sum of all risks according to the typology Figure 3 for each employee with access to commercial information will have the form (1), which will automatically fill table 1 with data:

$$\sum R_i = ((\sum_{n=1} R_i \left(CSINT\right) + \sum_{m=1} R_i \left(CSINT\right)) \qquad (1)$$

There is a set of tools for programs to interact with each other, called the API (Application Programming Interface), with which it is possible to get information about the participants of the business process using the data of an application. As mentioned above, business information can be information about the business process of the company, as well as data about the participants in this business process, especially customers who bring income (benefit).

If such information is publicly available on the Internet, for example, in social networks, it is possible to find, structure, and analyze such information through the use of API technology (whether an employee has problems).

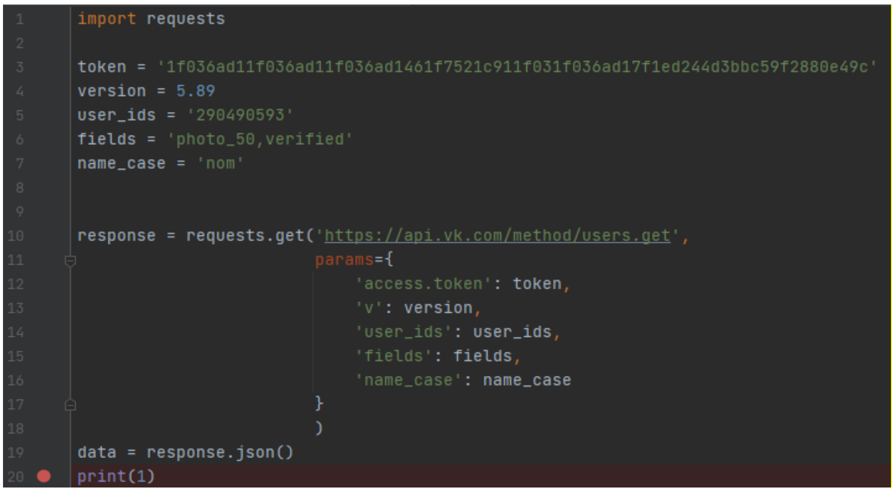
As a result of the implementation of this concept, the security department of the company will be able to change the security policy for a problem employee of the company who has access to commercial information in the event of a sudden increase in the risk indicator of its problem (according to the conditional example in Table 1 - this is line 5 – risk value – 0,81) in order to avoid leakage of commercial information.

Thus, the concept proposed by the authors reacts much earlier in time than all known information protection systems will work on the principle of registering leakage incidents.

4 Methods detection of problem`s employee

The APIs, that are a technology, an architectural style focused on using the HTTP protocol as a transport protocol when generating requests to the server and responses returned by this server. If the information about the participants of the business process is located, for example, in a social network, then it can be likely obtained from the servers used by this social network via its API - leakage (from the insider staff) for column 4 in table 1.

An example is shown in Figure 4.



```
import requests

token = '1f036ad11f036ad11f036ad1461f7521c911f031f036ad17f1ed244d3bbc59f2880e49c'
version = 5.89
user_ids = '290490593'
fields = 'photo_50,verified'
name_case = 'nom'


response = requests.get('https://api.vk.com/method/users.get',
                        params={
                            'access.token': token,
                            'v': version,
                            'user_ids': user_ids,
                            'fields': fields,
                            'name_case': name_case
                        }
                        )
data = response.json()
print(1)
```

Fig.4. Program source code using the API requests to find problem`s employee

As a result, you can get a response of this type:

["response":[{"first name": "**Igor**", "id":290490593, "last name": "**Mandritsa**", "can access closed": true, "is closed": false]

Fig.5. Sample response to an API requests to find problem`s employee

The authors also believe that threats to a commercial organization can, in principle, be divided into two main types: external and internal). The task of any criminal (as an attacker inside the company or a cyber fraudster from the external environment of the company) will be to «complicate» or «reset» the business information of the company between its stages of production and sale of products or services by introducing chaos, disorienting the employees of the company, violating the integrity of the aggregate information that discusses the entire business process.

In turn, the amount of damages will depend on the recovery time or slow motion «information flow» between employees, and also the time of the financial flows between the client and the departments of the executors of the order, from the perspective of possible cyber-attacks aiming at «losing», «bankrupting», «resetting» the transaction itself and creating a «direct financial» damage from subsequent alterations, or claims (return receipts) on the client side in the form of deviations from the approved parameters of the business process.

A particularly significant link in the threats to the business process for each organization is the block-link known as «cash and settlement services» and its possible «damage», such as the downtime of receiving an advance or the total income from completing a business task from stages 1 to 12 in Figure 1.

5 Conclusion

From the position information of cyber threats, at the moment 01.04.2021 year target of any virus infiltrated the system's entry points, namely, any equipment can be vulnerable, can cause a denial-of-service cash register systems, and the illegitimate transfer of funds to «fake accounts» of the attacker.

To this purpose we observe that it would be easy to secure the email by introducing a "close" form of PGP (free open-source software in the form of OpenPGP), where email messages get encruption and signature, and trusted public keys are only coming from a centralized source, managed by the company itself. The effect of encrypted/signed emails would be being exempted by the so-called spear phishing emails [6], that target high positions within the company.

At the same time, the stage known in the business process of any organization as the approval of the design layout of the project with the customer will be targeted by any virus (e.g., a ransomware) that has penetrated the company's information system at the entry points and will lead to downtime for the stages of calculating the order, the stages of designing the order, and approving the start of installation work under a specific client agreement.

From the perspective of external threats, the authors point out the importance of information security from an unlikely, but still possible non-ethical hacker attacks on the company itself – the object of protection, and agents of the company or its suppliers, through the implementation of an information system of the organization through Trojan viruses «false»-contracts in the business process of the organization. Also, the creation of a «clone of the customer» (or a targeted attack for a long time with the subsequent destruction of the company's assets) should be attributed to the very «unlikely», but still considered information threats to the loss of business information.

Summing up, the authors believe that cybersecurity, provided only by technical means, is limited and should be supplemented by appropriate risk analysis and procedures for controlling internal personal security using also machine learning and developing a rational (then economic) information security policy within the framework of the proposed aggregate model (from external and internal) threats to the business process of the firm (organization).

The authors of this article propose to call such information security systems "smart protection" of a company (organization), since the request API will be an embedded part (script in Microsoft Project) of CRM system and with the help of machine learning, translate the entire process of identifying a problem employee into an automated process, when the information security department of the firm will receive information automatically and immediately respond by changing the policy of access of employees of the company to the commercial information of the entire business process.

References

1. https://www.iso.org/ru/isoiec-27001-information-security.html last accessed 2021/01/11.
2. ISO/IEK 27032 2012 «Information technology. Security methods. Cybersecurity guidelines». https://www.iso.org/standard/44375.html. last accessed 2021/01/11.
3. Microsoft Dynamics CRM http://www.microsoft.com/ru-ru/dynamics/crm.aspx, last accessed 2021/01/11.
4. Mandritsa I, Peleshenko V, Mandritsa O, Fensel A, Tebueva F, Petrenko V, Solovieva I, Mecella M Defining a cybersecurity strategy of an organization: criteria, objectives and functions Integrating Research Agendas and Devising Joint Challenges. International Multidisciplinary Symposium ICT Research in Russian Federation and Europe. P 199. (2018).
5. Belov V, Pestunov A, Pestunova T On the Issue of Information Security Risks Assessment of Business Processes Actual problems of electronic instrument engineering (APEIE) - Proceedings XIV International scientific-technical conference. In 8 Volumes, P. 112. (2018)
6. FIRMEX 2021. Spear phishing: who's getting caught? https://www.firmex.com/resources/infographics/spear-phishing-whos-getting-caught/. Retrieved on March 9th.(2021).
7. Toapanta M, Mafla E, Benavides B, Huilcpi D, Approach to Mitigate the Cyber-Environment Risks of a Technology Platform, March, DOI: 10.1109/ICICT50521.2020.00069, Conference: The International Conference on Information and Computer Technologies (ICICT-2020) USA.
8. Dioubate B., Molok N., Shuhaili T., Risk assessment model for organizational information security, V. 10, P. 23, ARPN Journal of Engineering and Applied Sciences, (ARPN) (2015).
9. Suhartana M, Pardamean B, Soewito B, Modeling of Risk Factors in Determining Network Security Level, International Journal of Security and Its Applications, V.8, No.3 P. 193. (2014).