EasyChair Preprint

№ 6695

Cost of Information Protection from Internal Threats for the Company's Business Process

Igor Mandritsa, Fabrizio D'Amore, Anna Fensel,
Aleksandr Zhuk, Vyacheslav Petrenko and Olga Mandritsa

September 26, 2021

COST OF INFORMATION PROTECTION FROM INTERNAL THREATS FOR THE COMPANY'S BUSINESS PROCESS

Mandritsa I.V.[1], Fabrizio d'Amore[2],Anna Fensel[3],
Zhuk A.P..[1], Petrenko V.I.[1] and Mandritsa O.V.[4]

[1] North-Caucasus Federal University, Institute of Information Technologies and Telecommunications, 1, Pushkin Street, Stavropol, 355009, 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] Russian Technological University - MIREA, Branch office, Department of regional Economics, 8, Kulakov street, Stavropol, 355035, Russia

imandritsa@ncfu.ru, damore@diag.uniroma1.it

Abstract. The article is devoted to the search for cost criteria when choosing among the information protection options of the business process of a commercial firm from internal threats. Business process scheduled in stages of business operations allows you to get a criterion for determining the cost of protecting business information and not to spend above the norm.

Keywords: Risk analysis, information security, policies.

1. Introduction

Information security is currently a critical need for all companies, worldwide. It is well known that information security is based on the fulfillment of the CIA requirements, where the three-letters acronymous stands for confidentiality, integrity and availability: other requirements, like accountability, non-repudiation etc., are not considered here, because they are not always requested for information security. However here will focus only the Russian case. For our purpose it is particularly important to address *confidentiality*, as a data breach is a successful attack to this. Attacks to confidentiality are the most frequent attacks and address unauthorized access to information. There are two main paradigms for enforcing confidentiality: data encryption and access control, one not excluding the other. However, investments for implementing such measures are significant.

Russian companies are actively investing in protection against hacker attacks. In 2018, investment in information security in IT budgets increased to 22%. The average business IT budget in the Russian Federation was $1.1 million in the next three years, there will be an increase of another 18%, due to the fact that the information technology infrastructure in companies is developing, and they need professional knowledge on cybersecurity, according to a study conducted by Kaspersky Lab [4]. Financial damage to Russian companies from data leaks has increased over the past six months. For large businesses, it was approximately $246 thousand, 2.5% more than last year, according to a study by Kaspersky Lab [ref]. For the average – it has tripled to $74 thousands; the damage caused by cyber-attacks is becoming larger, broader and more serious and includes financial and strategic losses [1]. Most likely, some cyber-attacks

are part of national or state campaigns interests. In addition, some self-serving firms may intentionally limit their investment in cybersecurity and rely on information provided by other organizations to protect themselves. This can lead to insufficient investment in cybersecurity if all participants adopt the same strategy. The urgency of the problem causes an objective need to find a rational strategy and economic model for estimating the cost of protecting business processes from penetration and threats.

2. Research goals

The subject of this research is the current business process in a commercial organization and its current economic strategy for protecting information while executing the organization's business process. The purpose of this article is to present the theoretical economy fundamentals to choose one of possible variants of economic strategy in information security process of business organizations, through a combinatorial selection of factors of the mathematical model of minimally adequate level of protection of the information assets of the organization to counter threats to the business process in the framework of the strategy of multi-level proposals for the recovery and to counter the information threats to the organization.

In turn, we will give a brief description of the role, place, and importance of current information security for the organization's business process. An important point is to determine the stages of economic operations (processes) within the framework of the client's order execution.

Today, commercial organizations in the course of their production and economic activities widely use CRM systems, in which the determining factor in describing and optimizing the current stages and tasks of business processes are correctly defined goals at each stage of customer order fulfillment, which each business has defined for itself. Companies have different approaches to the formulation of these goals and objectives.

For example, in the economic practice of business processes of enterprises, its management identifies two distinct formulations of business goals, which determine which methodology for describing business processes in the CRM environment (Microsoft Project) will be the most acceptable and most effective. Accordingly, there are two models, the content of which is as follows.

In the first model, the purpose and objectives of the organization of the entire business process of the enterprise are defined functionally, namely, it is provided that «...to solve the tasks, it is necessary to create a functional (process) model of the company that displays the structure, relationships and functions of the system, as well as the flows of information and material objects that link these functions» [business Modeling. The main approaches https://habr.com/ru/company/trinion/ blog/332772]. This approach implements an economic model such as «budget localization» or «cost budgeting» for the stages of production and sale of products and services ordered by the client.

For our study of this model, the future amount of possible damages from information security will depend on the measures and their cost, which will ensure the network infrastructure of the «data movement» between business units from the position of possible cyber-attacks by competitors in order to stop or disrupt the entire business process, create «temporary damage» to stop the business process.

The second model describes the setting of goals and tasks in different way and proceeds from the fact that «... descriptions of algorithms (scenarios) for the execution of processes in the form of its participants are necessary. In which, first of all, employees and cause-and-effect relationships, time sequences of their performance of economic actions, are defined as an ordered combination of events and functions of employees» [Diagram of use-cases in the software development process https://habr.com/ru/company/luxoft/blog/312188/]. In this case, the emphasis is on describing the sequence of actions of employees participating in the business process, determining the timing of initial and final events, identifying participants, performers, material and documentary flows and the cost of the business process by its stages. For the purpose of ensuring information security of the second model of conducting a step-by-step business process, it will be important to determine the localization of information flows between employees of the organization by stages of work when executing a client's order in the existing software. This model of business process organization is more susceptible to cyber fraud. Cyber fraudsters (hackers) made it as difficult as possible and even reset the information between the stages of the business

process of production and sale of products and services by introducing chaos, disorienting the company's employees, and violating the integrity of information on client contracts in the software that elaborates the business process of the enterprise. The total amount of possible damage will depend on the time spent by the specialist on restoring the document flow system between employees, as well as the time spent on restoring financial flows between the client and the order execution departments. Due to the existing problems of ensuring information security in the organization of a business process based on software, it is necessary to create an economic model for evaluating the protection of the business process, which is the purpose of further research.

3. Results and discussion

Existing approaches to describing business processes, as well as existing software, with rare exceptions, are specialized and poorly suited for solving those tasks for which they were not originally intended [1, 4]. Figure 1 below provides a detailed description of the business task by business process entities, using the example of a conditional commercial organization, in the form of a customer order project (business task) in the Microsoft Project environment.

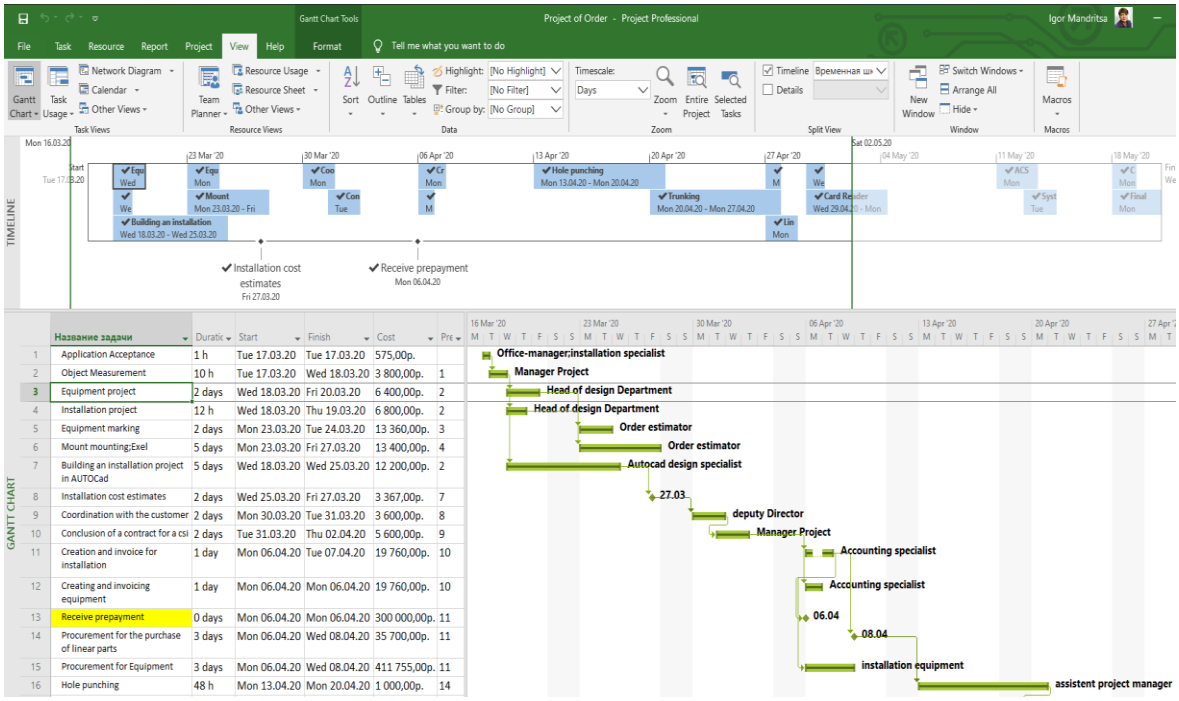

Figure 1 - Stages of the business process "Customer-ordered project implementation" in the environment Microsoft Project

The information security specialist must, first, secure the business process itself in the form of forming a plan of protective measures as an estimate of protection measures within the framework of the current information security standards in the Russian Federation adopted by the FSTEC of the Russian Federation:

- GOST R ISO / IEC 15408-1-2008 «Information technology-security Methods - criteria for evaluating it security-Part 1: Introduction and General model (IDT)» [2]; - GOST R ISO / IEC 27007-2014 identical to the international standard ISO / IEC 27007:2011 «Information technology. Security method. Guidelines for audit of information security management systems»; - ISO/IEC 27002:2013 (E) «Information technology. Method of protection. A set of recommended rules for managing information security».

Secondly, the information security specialist will need to classify the threats to the business process and their probabilities, and then develop a modernized version of the threat model within the framework of the order of the FSTEC of the Russian Federation dated February 11, 2013 N 17, in which the protection of the client's personal data and the business process we are considering have the same features as when

drawing up a threat model in relation to the business process. These features (in correlation with the international standard ISO / IEC 27002:2013) include:

- area of probable threats by stages of the business process;
- the type of information asset that will be threatened;
- the view of this factor and threats;
- indicators of the organization's business process that will be exposed to the threat.

According to this standard (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) information.

The value of information in the business process is not only in documented terms, numbers, and images – it is knowledge, concepts, ideas, technologies, and brands as examples of intangible forms. In a real world where everything is interconnected, information and related business processes, systems that serve the business process, information networks that combine everything into a single process, and personnel who functionally carry out their operation, processing and protection – all these are information assets that, like other important business (filled with value) financial and material assets.

2. Results of goal issue

In table 1, we present the cost of business process stages for a single customer order and the probabilistic amounts of damage from information threats.

Table 1 – distribution of the cost of the order according to the stages of the business process.

Np	Title	Start	Ending	Duration	Expenses	Summ of step
1	2	3	4	5	6	7
1	Application Acceptance	Tue 17.03.20	Tue 17.03.20	1 hour	400,00 ₽	400,00 ₽
2	Object Measurement	Tue 17.03.20	Wed 18.03.20	10 h	3 800,00 ₽	4 200,00 ₽
3	Equipment project	Wed 18.03.20	Fri 20.03.20	2 days	6 400,00 ₽	10 600,00 ₽
4	Installation project	Wed 18.03.20	Thu 19.03.20	12 h	6 800,00 ₽	17 400,00 ₽
5	Equipment marking	Mon 23.03.20	Tue 24.03.20	2 days	13 360,00 ₽	30 760,00 ₽
6	Mount mounting; Exel	Mon 23.03.20	Fri 27.03.20	5 days	13 400,00 ₽	44 160,00 ₽
7	Building an installation project in AUTOCad	Wed 18.03.20	Wed 25.03.20	5 days	12 200,00 ₽	56 360,00 ₽
8	Installation cost estimates	Wed 25.03.20	Fri 27.03.20	2 days	3 367,00 ₽	59 727,00 ₽
9	Coordination with the customer	Mon 30.03.20	Tue 31.03.20	2 days	3 600,00 ₽	63 327,00 ₽
10	Conclusion of a contract for a csi	Tue 31.03.20	Thu 02.04.20	2 days	5 600,00 ₽	68 927,00 ₽
11	Creation and invoice for installation	Mon 06.04.20	Tue 07.04.20	1 day	19 760,00 ₽	88 687,00 ₽
12	Creating and invoicing equipment	Mon 06.04.20	Mon 06.04.20	1 day	19 760,00 ₽	108 447,0 ₽
13	Receive prepayment	Mon 06.04.20	Mon 06.04.20	3 days	300 000,00 ₽	
14	Procurement for the purchase of linear parts	Mon 06.04.20	Wed 08.04.20	3 days	35 700,00 ₽	144 147,0 ₽
15	Procurement for Equipment	Mon 06.04.20	Wed 08.04.20	3 days	411 755,00 ₽	555 902,0 ₽
16	Hole punching	Mon 13.04.20	Mon 20.04.20	48 h	1 000,00 ₽	556 902,0 ₽
17	Trunking	Mon 20.04.20	Mon 27.04.20	48 h	500,00 ₽	557 402,0 ₽
18	tightening wires into pipes	Mon 27.04.20	Mon 27.04.20	1 day	2 840,00 ₽	560 242,0 ₽
19	Linear Testing	Mon 27.04.20	Tue 28.04.20	2 days	4 000,00 ₽	564 242,0 ₽
20	Surrender under the Act of the linear part	Wed 29.04.20	Fri 01.05.20	2 days	3 520,00 ₽	567 762,0 ₽
21	Turnstile mounting	Wed 29.04.20	Thu 30.04.20	12 h	2 860,00 ₽	570 622,0 ₽
22	Card Reader Installation	Wed 29.04.20	Mon 04.05.20	3 days	9 720,00 ₽	580 342,0 ₽
23	Installation of CPU and other equipment	Mon 04.05.20	Thu 07.05.20	4 days	12 000,00 ₽	592 342,0 ₽
24	ACS settings	Mon 11.05.20	Wed 13.05.20	20 h	9 100,00 ₽	601 442,0 ₽

25	System testing	Tue 12.05.20	Thu 14.05.20	2 days	6 480,00 ₽	607 922,0 ₽
26	Commissioning facility	Mon 18.05.20	Tue 19.05.20	12 h	7 800,00 ₽	615 722,0 ₽
27	Final settlement for ACS	Mon 18.05.20	Wed 20.05.20	3 days	₽ 615,722.00	

Next table 2 shows the listed threats and their amounts of probable damages to the business process of a commercial organization.

The formula for calculating possible damages (column 6) is equal to the total amount of the client's order 615,722 thousand rubles minus the cost of the business process stage. From table 2, we can see that the amount of damage falls to zero by the end of the business process itself, which suggests that as the client's order is completed, the firm can also reduce future information security costs. The client did not refuse our contractor, and the order will bring the company a margin (profit) from its execution.

Table 2 - Amounts of probable damages to the organization's business process by process stage

Npp	Title	Duration	Expenses	Summ Damage of step	Summ Damage for full process
1	2	3	4	5	6
one	Application Acceptance	1 hour	400,00 ₽	400,00 ₽	615722
2	Object Measurement	10 h	3 800,00 ₽	4 200,00 ₽	615322
3	Equipment project	2 days	6 400,00 ₽	10 600,00 ₽	611122
4	Installation project	12 h	6 800,00 ₽	17 400,00 ₽	600522
5	Equipment marking	2 days	13 360,00 ₽	30 760,00 ₽	583122
6	Mount mounting; Exel	5 days	13 400,00 ₽	44 160,00 ₽	552362
7	Building an installation project in AUTOCad	5 days	12 200,00 ₽	56 360,00 ₽	508202
8	Installation cost estimates	2 days	3 367,00 ₽	59 727,00 ₽	451842
9	Coordination with the customer	2 days	3 600,00 ₽	63 327,00 ₽	392115
10	Conclusion of a contract for a csi	2 days	5 600,00 ₽	68 927,00 ₽	328788
11	Creation and invoice for installation	1 day	19 760,00 ₽	88 687,00 ₽	259861
12	Creating and invoicing equipment	1 day	19 760,00 ₽	108 447,00 ₽	171174
13	Receive prepayment	3 days	300 000,0 ₽		
14	Procurement for the purchase of linear parts	3 days	35 700,00 ₽	144 147,00 ₽	59820
15	Procurement for Equipment	3 days	411 755,0 ₽	555 902,00 ₽	58820
16	Hole punching	48 h	1 000,00 ₽	556 902,00 ₽	58320
17	Trunking	48 h	500,00 ₽	557 402,00 ₽	55480
18	tightening wires into pipes	1 day	2 840,00 ₽	560 242,00 ₽	51480
19	Linear Testing	2 days	4 000,00 ₽	564 242,00 ₽	47960
20	Surrender under the Act of the linear part	2 days	3 520,00 ₽	567 762,00 ₽	45100
21	Turnstile mounting	12 h	2 860,00 ₽	570 622,00 ₽	35380
22	Card Reader Installation	3 days	9 720,00 ₽	580 342,00 ₽	23380
23	Installation of CPU and other equipment	4 days	12 000,00 ₽	592 342,00 ₽	14280
24	ACS settings	20 h	9 100,00 ₽	601 442,00 ₽	7800
25	System testing	2 days	6 480,00 ₽	607 922,00 ₽	6600
26	Commissioning facility	12 h	7 800,00 ₽	615 722,00 ₽	0
27	Final settlement for ACS	3 days	615,722.00		615722

The cost of completing the order will be paid by the client, and the revenue will be received by the company. However, the most important issue is the rational amount of costs at the first stages – when the client appears at the company, receiving his personal data, which is especially important for competitors

(in case of possible «poaching»), and accordingly all stages of pre – «processing» the order, when our company will spend its resources (assets) and competence (visiting the customer, measurements, and development of a sketch of the future order, cost calculation, order approval and cost coordination, etc. types of work) that will be performed before the first receipt of an advance amount equal to half the cost of the order [6]. We believe that the rationality of information security will be calculated as a certain threshold for reducing the probability of losing a client and, accordingly, not receiving the amounts of income (revenue) and compensating our company for the costs incurred at the first stages of the business process.

In table 2, these amounts are shown in positions 1 through 12. In the position 13 we consider the information security threshold for the given example of a business process, when the probability of subsequent damages is reduced by half.

Table 3 and 4 present calculations of the required amounts for information security for 3 levels of information security when a firm hires specialists of various competencies who will provide these levels of security in accordance with the firm's own understanding of the probability that their firm will be attacked by an information attack to poach a client or other probabilistic information problems for the firm.

Table 3 - Parameters of labor costs for information security specialists (when hiring them for 1 month)

Cost of defence approach	Strong level	Middle level	Ligth level
1	2	3	4
Salary of an information security specialist according to the choice of security level (Rouble/Hour) * 300 hours for full complex defence work for task	1500	940	220
Salary of an information security specialist according to the choice of security level (Rouble/Month) 160 hours a month	240000	150000	35000
Coefficient of competence for task of defence work (at light level)	0.3	0.6	1.0

At the same time, we assume (as of the current date of writing this article) that specialists differ not only in the level of remuneration for their work, but also in the time they need for a standard set of information and support actions to ensure a decent level of security.

A particularly important part of the business process for each organization is a block-a link known as «settlement and cash services» and its possible «damage», such as the downtime of receiving an advance or the total income from completing a business task [8]. From the point of view of information cyber threats, at the moment 01-03-2020, any target virus that has penetrated the company's systems at the entry points, namely, any company's equipment can be potentially vulnerable, can cause both denial of service of cash systems, and illegitimate transfer of funds to the «fake accounts» of the attacker [6]. At the same time, the stage known in the business process of any organization as the approval of the design layout of the customer's project and any target virus that has penetrated the company's systems at the entry points will lead to downtime for calculating and approving the start of installation work under this client agreement.

The main reason will be a denial of service after a local target attack on the company's information system, which allows replacing a legitimate project (accepted for execution in the business process of the organization) with a false one. Also known as the «calculation» stage of the business process, after a local target attack on the company's information system, the customer will fail to fulfill the contract for the order, in the form of downtime at the stages of installation, installation of equipment, for calculating and approving the start of installation work [9].

Here, information security is no less important from attacks on intermediary companies or suppliers, through the introduction of «fake-contracts» into the organization's information system and into the business process of the organization. It is also necessary to highlight possible forced production

downtime from third parties (power supply, lack of components, etc.) when commissioning a customer's order, through local DDoS attacks on IP telephony [7].

Table 4 - Calculations of the company's expenses for the types of information work of an information security specialist (when hiring him for 1 month), taking into account his competence coefficient

№	Cost of defence approach	Strong level	Middle level	Ligth level
1	2	3	4	5
All departure	Salary of an information security specialist according to the choice of security level (Rouble/Hour) * 300 hours	1500	940	220
All departure	Microsoft Windows Server 2016 Standard 64-bit Russian 1pk DSP OEI DVD 16 Core ~70000 roubles.)	70000	70000	70000
Office-manager	Installing access control (Rouble/Hour) * 30 hours	13500	16920	6600
Office-manager	Adequate security policy (Rouble/Hour) * 20 hours	9000	11280	4400
Office-manager	Creating a threat model (Rouble/Hour) * 20 hours	9000	11280	4400
Accounting office	Installing access control (Rouble/Hour) * 150 hours	67500	84600	33000
Accounting office	Adequate security policy (Rouble/Hour) * 100 hours	45000	56400	22000
Accounting office	Creating a threat model (Rouble/Hour) * 50 hours	22500	28200	11000
Clients Data	Installing access control (Rouble/Hour) * 50 hours	22500	28200	11000
Clients Data	Adequate security policy (Rouble/Hour) * 30 hours	13500	16920	6600
Clients Data	Creating a threat model (Rouble/Hour) * 20 hours	9000	11280	4400
AutoCad desiner	Installing access control (Rouble/Hour) * 100 hours	45000	56400	22000
AutoCad desiner	Adequate security policy (Rouble/Hour) * 50 hours	22500	28200	11000
AutoCad desiner	Creating a threat model (Rouble/Hour) * 25 hours	11250	14100	5500
Stock (manager)	Installing access control (Rouble/Hour) * 100 hours	45000	56400	22000
Stock (manager)	Adequate security policy (Rouble/Hour) * 50 hours	22500	28200	11000
Stock (manager)	Creating a threat model (Rouble/Hour) * 20 hours	9000	11280	4400
Production	Installing access control (Rouble/Hour) * 50 hours	22500	28200	11000
Production	Adequate security policy (Rouble/Hour) * 30 hours	13500	16920	6600
Production	Creating a threat model (Rouble/Hour) * 20 hours	9000	11280	4400
Service of firm	Installing access control (Rouble/Hour) * 20 hours	9000	11280	4400
Service of firm	Adequate security policy (Rouble/Hour) * 10 hours	4500	5640	2200
Service of firm	Creating a threat model (Rouble/Hour) * 5 hours	2250	2820	1100

Next table 5 shows the results of the cost of information security specialists according to the list of works to protect the company's business process.

Table 5 - Calculations of the company's costs for the types of information work of an information security specialist by links (participants) of the business process

Departure of enterprises	Strong level	Middle level	Ligth level
1	2	3	4
Office-manager	31500	39480	15400
Accounting office	135000	169200	66000
Clients Data	45000	56400	22000
AutoCad desiner	78750	98700	38500
Stock (manager)	76500	95880	37400
Production	45000	56400	22000
Service of firm	15750	19740	7700
All departure	70000	70000	70000
Summ	497500	605800	279000

It is also likely that there will be no access to the component database, changes to its contents, or a sudden failure to provide components, and as a result, a delay in the start of installation or commissioning of the order.

Table 6 - Probability of leakage risks for threat model of the business process

№	Business process phase	Likelihood of threats through technical channels	Likelihood of threats from staff	Total probability
1	2	3	4	5
1	Accepting the buyer's application	0	0,3	0,3
2	Froze the order object	0,01	0,04	0,05
3	Order equipment project	0,01	0,29	0,3
4	Order mounting project	0,01	0	0,01
5	Making estimates for equipment	0,01	0,8	0,81
6	Making estimates for installation; Microsoft Excel	0,01	0	0,01
7	Building a montage project in AUTOCad	0,01	0,19	0,2
8	Building an estimate of the installation	0,01	0,04	0,05
9	Reconciling with the customer	0,01	0,29	0,3
10	Conclusion of a contract on information security	0,01	0,09	0,1
11	Create and bill for installation	0,01	0,09	0,1
12	Create and invoice for equipment	0,01	0	0,01
13	Receiving prepayment from the buyer	0	0	0

Next, figure 2 and 3 shows the localization of information threats to the business process of organizations that perform the task «Implementing a project on the client's order» with the indication of the risk zones of malicious penetration.

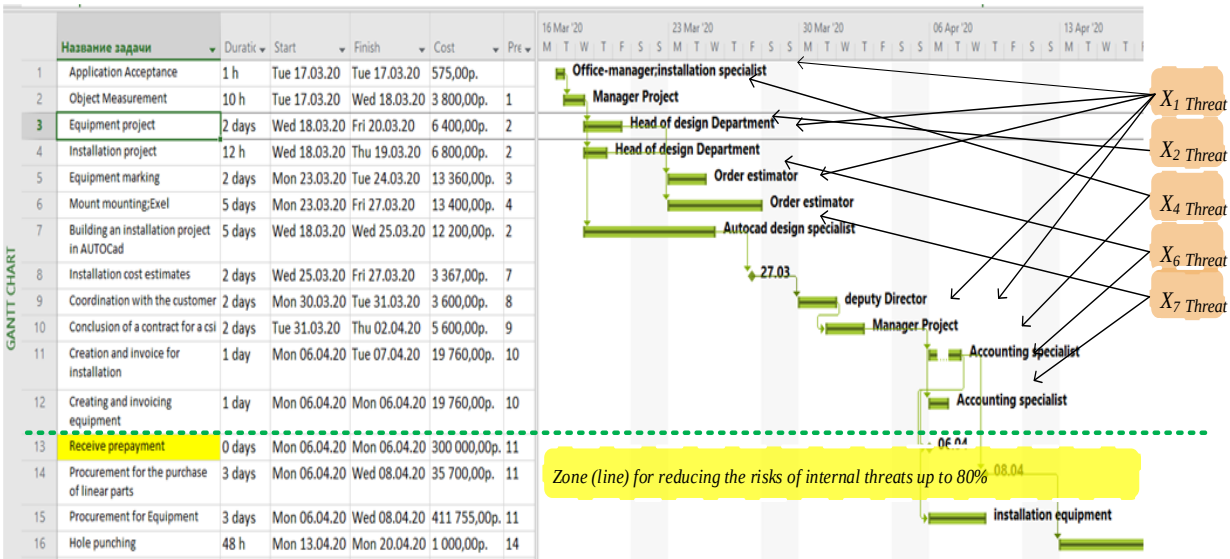

Figure 3 - Information security internal risk Zones of a business task (as part of a business process)

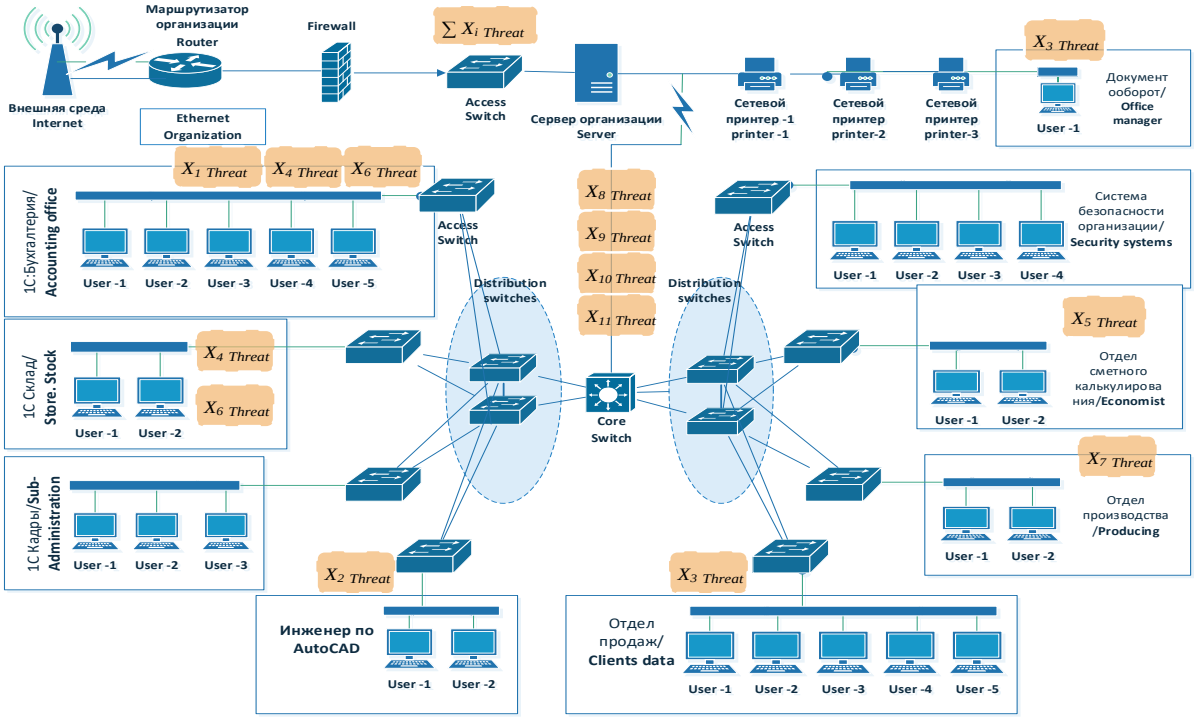

Figure 4 - Information security risk Zones of a business task (in correlation with a business process fig. 3)

Also, well-known threats to the business process of the organization are-disruption of the delivery of components for the execution of the order. We will also mention a possible technical failure (failure) of the customer's order installed after installation (dismantling time, subsequent alterations and waiting for delivery of new components) [12]. The most likely threats include infection of all information assets of the company and destruction of data (including all existing projects, documents, reports and other stages, and key factors of the business process) [10]. The least likely information threats, but quite feasible in the conditions of competition for a niche of the organization's market will be a complete violation of the information integrity of the software OR hardware of the organization, according to the well-known example of Tailored Access Operations, with the possibility of interception of management or destruction of data [11]. The creation of a «fake-counterpart of the customer» (or a targeted attack for a long time with the subsequent destruction of the company) should be attributed to completely «unrealistic», but still considered information threats [13].

We will summarize the presented classifications of information threats and reflect these factors in the modernized threat model in figure 5.

Conclusions

An organization's information assets are subject to both deliberate and accidental threats, and their associated processes, systems, networks, and people have inherent vulnerabilities.

Changes to business processes and systems or other external changes (such as new laws and regulations) may create new risks to information security.

Therefore, given the many ways in which threats of cybercriminals, using vulnerabilities of «stages» and «blocks» of the business process, can harm the organization, we can confidently say that information security risks are always present.

The information security management system (isms for short), as defined in ISO/IEC 27001 [1], provides a holistic, consistent view of the organization's information security risks in order to implement a comprehensive set of measures to ensure information security within an integrated management system.

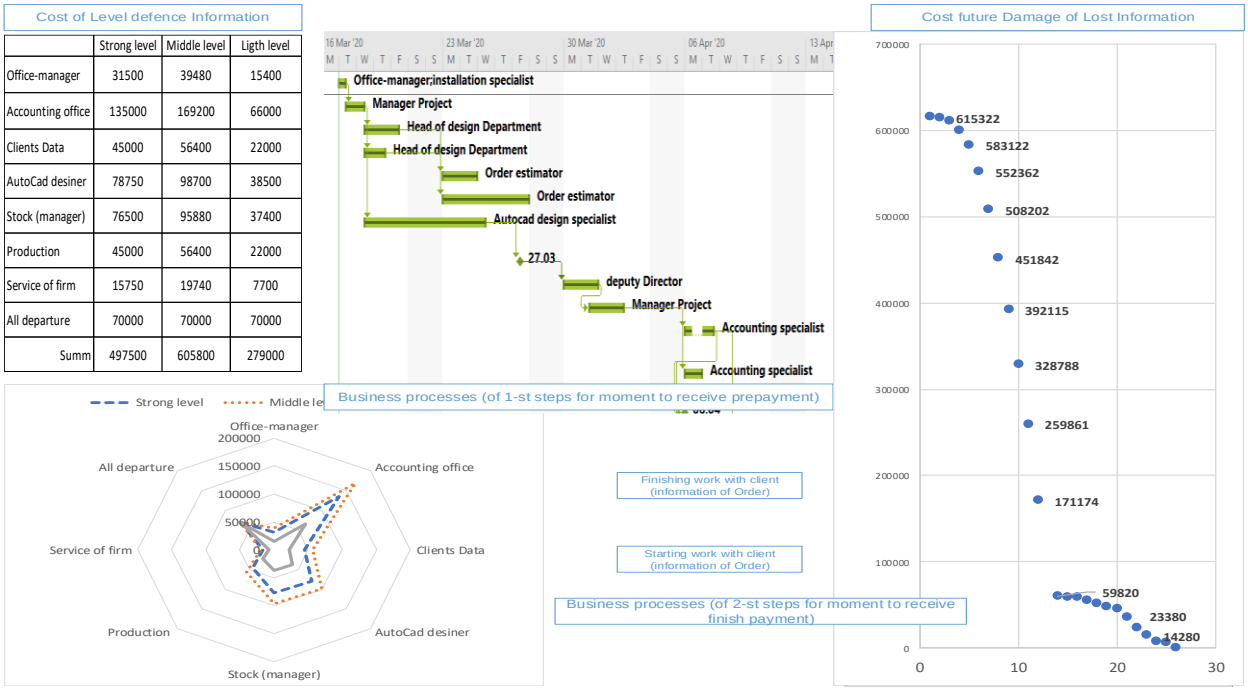

Figure 5 - Implementation of costs for information measures to protect the organization's business process (according to ISO/IEC 27001:2013 (E) and in correlation with a business process fig. 3))

Many information systems were developed without taking into account security requirements in the context of ISO / IEC 27001 and this standard. Security provided only by technical means is limited and must be supplemented by appropriate management and procedures.

Determining which tools to use in a particular case requires careful planning and attention to detail. The successful functioning of the ISMS requires the support of all employees of the organization. This may also require the participation of shareholders, suppliers, or other external parties. You may also need advice from outside experts. Thus, we can begin to develop a sufficient information security strategy within the framework of the proposed threat model for the object of research.

Source list

1. https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf
2. https://www.iso.org/ru/isoiec-27001-information-security.html
3. http://publication.businessstudio.ru/businessmodel.php?lang=ru-ru&oguid=4aab2654-145e-40cb-9372-1f64ad04651f
4. https://infowatch.com/report2018_half
5. Salnitri, M., Dalpiaz, F., Giorgini, P.: Modeling and verifying security policies in business processes. In: Bider, I., Gaaloul, K., Krogstie, J., Nurcan, S., Proper, H.A., Schmidt, R., Soffer, P. (eds.) BPMDS 2014 and EMMSAD 2014. LNBIP, vol. 175, pp. 200–214. Springer, Heidelberg (2014)
6. Mandritsa I.V., Peleshenko V.I., Mandritsa O.V., Fensel A., Tebueva F.B., Petrenko V.I., Solovieva I.V., 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. 2018. C. 199-205.*

7. Rodriguez A., Fernandez-Medina E.. Piattim M. A BPMN Extension for the Modeling of Security Requirements ш Business Processes. ШCE — Transactions on Information and Systems. Volume E90-D Issue. e 4. March 2007. Pages 745-752
8. Ahmed, N., Deriving security requirements from business process models. Ph.D. thesis. University of Tartu (2014)
9. Ahmed, N., Matulevičius, R.: Securing business processes using security risk-oriented patterns. Comput. Stand. Interfaces 36(4), 723–733 (2014)
10. Leitner, M., Miller, M., Rinderle-Ma, St.: An analysis and evaluation of security aspects in business process model and notation. In: Proceedings of the Eighth International Conference on Availability, Reliability and Security (ARES), pp. 262–267 (2013)
11. Cjaputa K.: Business process based introduction of security aspects in enterprise architecture. Master thesis, RTU (2016)
12. Belov V.M., Pestunov A.I., Pestunova T.M. On the Issue of Information Security Risks Assessment of Business Processes Actual problems of electronic instrument engineering (APEIE) - Proceedings XIV International scientifictecnical conference. In 8 Volumes, 2018
13. Gordon, L., Loeb, M.: Managing Cybersecurity Resources: A Cost-Benefit Analysis, 1st edn. McGraw-Hill, New York (2005)
14. Florêncio, D., Herley, C.: Sex, lies and cyber-crime surveys. In: Ed: Bruce Schneier (ed.) Economics of Information Security and Privacy III. Springer, New York (2013).