Information Technology of Risk Assessment for Automated Control Systems of Printing Production

Lubomir Sikora[1], Natalia Lysa[1], Rostislav Tkachuk[2], Volodymyr Sabat[3] and Olga Fedevych[1]

[1] *Lviv Polytechnic National University, 12, Bandera str., Lviv, 79013, Ukraine*
[2]*Lviv State University of Life Safety, 35, Kleparivska str., Lviv, 79007, Ukraine*
[3] *Ukrainian academy of printing, 19 Pid Goloskom str., Lviv, 79020, Ukraine*

Abstract

The article considers construction methods of risk assessment information technology for automated control systems of printing production (ACSPP) on the basis of detection of threats and vulnerabilities of the company assets. It is substantiated that ACSPP is one of the production assets and the risk assessment problems in the security system are reduced to determining ACSPP threats and vulnerabilities levels and countermeasures to counter possible attacks on production. In addition to the above-mentioned ACAPP security problems related to the threats and vulnerabilities inherent in most IS, a number of organizational and psychological issues should also be noted. In particular, weak awareness of the information importance and its protection by the management staff and employees of printing companies. Accordingly, the management staff is reluctant to invest in information protection and make any organizational decisions on this issue, and the employees show misunderstanding and failure to take most protection measures, which leads to negligence, and then complete disregard for protection measures. This attitude to the information security can cause significant losses to the company, which will be simply disproportionate to the cost of information security in their values. Another important problem is the imperfection of Ukrainian legislation in the information protection area and almost complete absence of domestic standards in this area. In order to achieve the required level of ACSPP protection, it is necessary to reduce the risks level to an acceptable one or eliminate the risks altogether. This can be achieved by reducing the criticality, probability and/or frequency of threats.

Keywords

System, information, assets, risks, threats, vulnerabilities, management, printing production.

1. Introduction

The main security purpose is to protect the company assets from attacks due to existing threats. Threats are assessed according to the amount of damage that may be caused to the company as a

CITRisk'2021: 2nd International Workshop on Computational & Information Technologies for Risk-Informed Systems, September 16–17, 2021, Kherson, Ukraine

EMAIL: lssikora@gmail.com (L.Sikora); lysa.nataly@gmail.com (N.Lysa); rlvtk@ukr.net (R.Tkachuk); v_sabat@ukr.net (V.Sabat); olha.y.fedevych@lpnu.ua (O.Fedevych)
ORCID: 0000-0002-7446-1980 lssikora@gmail.com (L.Sikora); 0000-0001-5513-9614 (N.Lysa); 0000-0001-9137-1891 (R.Tkachuk); 0000-0001-8130-7837 (V.Sabat); 0000-0002-8170-3001 (O.Fedevych)

result of the attacks. Losses can consist of loss of public trust or decrease in the company image in a society, responsibility before the law, threat to the personnel safety, etc. However, in the end they are somehow reduced to financial losses. The ability to implement a threat is characterized by the risk level, which in turn is directly proportional to the system vulnerability. That is, to protect the company assets it is necessary to reduce its vulnerability to an acceptable level. At the same time, the cost of measures aimed at reducing the assets vulnerability should not exceed the amount of damage that may be caused by threats to this asset as a result of attacks.

In this case, automated control systems of printing production (ACSPP) is considered as one of the company assets. In turn, ACSPP also consists of other assets. Therefore, in order to achieve the required protection level of ACSPP, it is sufficient to achieve the required protection level of its main assets: personnel, information component and hardware of the management process, goals and strategies.

The aim of study. The development of the information technology, based on the system analysis, to assess the functional dependencies between the company assets to create risk management systems in ACSPP under threat.

2. References analysis

The main analysis of ACSPP in the domestic market is presented in [1, 2], which indicates the advantages and disadvantages of certain control systems and their functions in the printing industry. Since the purpose of ACSPP is important for the organization of its activities, it requires a detailed risk analysis. The monograph [3] highlights the fundamentals of information technology of the formation of methods and models for determining the security level of technological processes in the printing industry on the basis of risk assessment. Scientific works [4, 5] cover conceptual aspects of risk – a qualitative and quantitative risk analysis, the system of indicators of its quantitative assessment, basic approaches to modelling, management and methods of risk reduction, and in [6] a functional scheme of risk management for automated document management systems is presented, which can also be used for ACSPP. In [7], much attention is paid to the coverage of risk management tools and their consideration in making management decisions in conditions of uncertainty and risk. A typical regulation on the information protection service in the automated system is presented in the Normative documents of the information technical protection system [8–10]. In [11, 12] a novel extensible Multi-hazard Risk Assessment Framework that is a skeleton containing the multihazard risk assessment toolkit dealing with threat/danger, vulnerability, damage, coping capacity, risk, and multi-risk are presented. The risk scenarios within this framework can describe multi-hazards as a multitude of spatially distributed dynamic processes influenced by various drivers. The implementation of the proposed models and framework is also considered. The proposed event-based scenario representation model provides sufficient detailization in space and time and can properly represent multi-hazards, including compound events, cascading effects, and risk-related processes driven by environmental and societal changes. In [13] construction methods of information technology of formation and decision-making under risk conditions are considered for management of technogenic systems with use of cognitive model of operator activity. In [14] the problem of decision-making in the risk conditions and conflict situations in the presence of terminal restrictions is considered at the time of resolving the crisis in the complex system management structure.

Problem setting. Risk assessment in automated control systems of the company is a basic task in the development of protection systems with an appropriate level that would meet the optimal security requirements of the company in the process of its operation. This task is solved by determining the features of technical and information processes that are performed at the company during its operation, threats and vulnerabilities of objects and subjects of operation at each technological stage, the occurrence of emergencies after external attacks or other negative incidents. Therefore, to solve the problems of risk management in the company, it is necessary to determine its assets and functional features in detail. This process should be done according to the functional scheme shown in Figure 1. The detailed risk analysis for ACSPP involves the identification of all possible risks and assessment of their level [6].

3. Presentation of the main research material

3.1. Method of defining possible limits to assess the risks, losses and failures of complex systems under threat

Defining possible limits for risk assessment aims to clearly determine which of the resources should be taken into account when considering the results of risk analysis. When considering ACSPP risks it is necessary to take into account the following factors:

– the information technology assets (hardware, information support, information), as they make the software and hardware base for ACSPP operation;

– the personnel of the organization (who works with ACSPP and maintains it) as a source of possible threats;

– he conditions for carrying out the production activities, as they affect ACSPP proper operation;

– the business activity, which is the main purpose of ACSPP [1].

ACSPP operation is not possible if at least one of its components is not functioning, i.e. the failure of the proper operation of at least one of them will cause the failure of the other components and the system as a whole. Each of the components of ACSPP is considered in more detail – Figure 1.

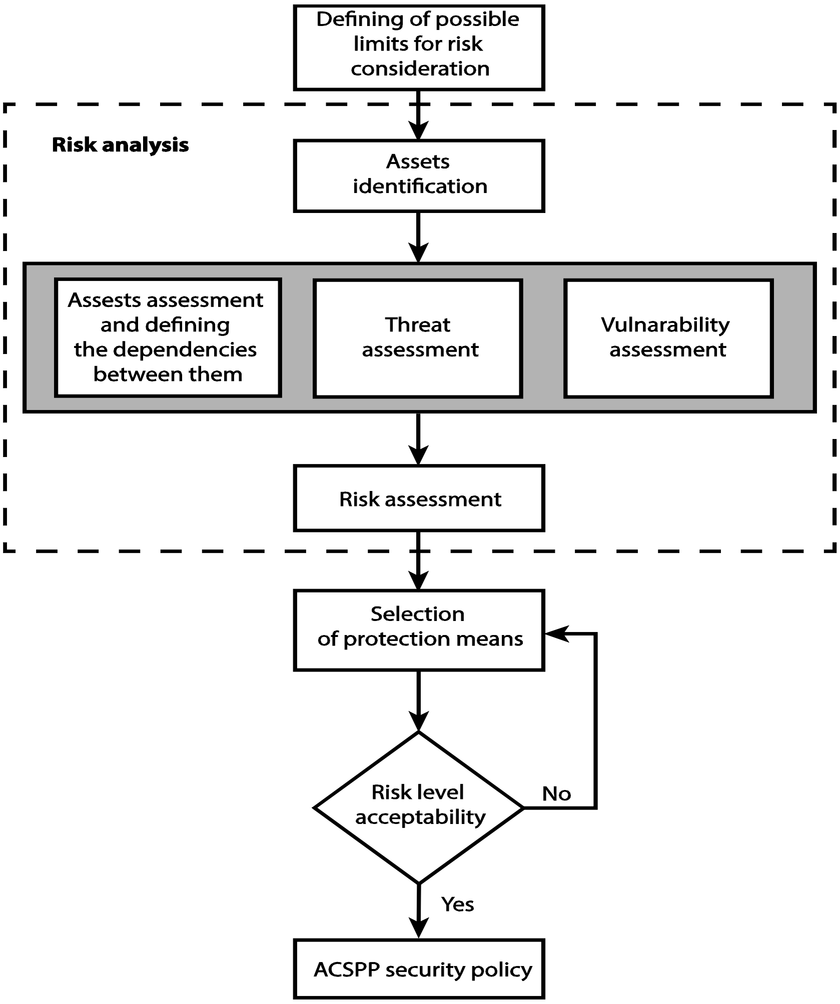
Defining of possible limits for risk consideration
Risk analysis
Assets identification
Assests assessment and defining the dependencies between them
Threat assessment
Vulnarability assessment
Risk assessment
Selection of protection means
Risk level acceptability
No
Yes
ACSPP security policy

Figure 1: Block diagram of the intelligent systems interaction (ACS-LPR)

ACSPP information component combines all the information that functions within ACSPP, as well as input and output information flows – Figure 2. The software is a separate integral part of ACSPP information component. With the help of software, the transfer and conversion of information that operates in ACSPP are carried out. The software can be divided into main and auxiliary ones.

The main software includes the software modules for processing the information that operates in ACSPP, as well as a central database (DB) – the core of ACSPP. It can store a variety of information needed in the operation process.

The auxiliary software provides the operation of the main software. These are the operating system, drivers, various utilities, etc.

According to the scheme shown in Figure 2, the operation of a typical ACSPP is as follows. The input information (customer requirements, commercial information, financial accounting data, various input documents) is processed by ACSPP software modules and entered into the central database. In the course of work, various internal company departments address to the central database through the corresponding software modules – there is an internal information exchange. In addition, during ACSPP operation, the relevant modules generate the output information (requests for materials, documents on product sales, operational accounting data). To ensure the reliability of the work, the central database information is periodically archived.

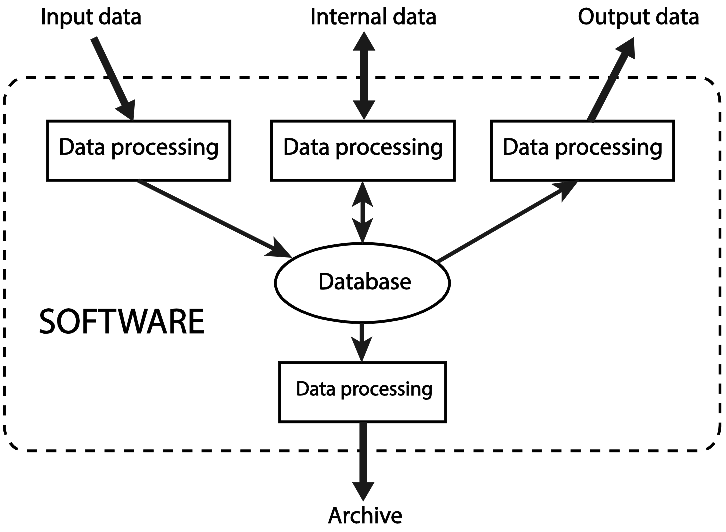

Figure 2: Information component of the automated control system of printing production

The information in ACSPP can function both in electronic non-material form and in the form of hard copies. A hard copy means a medium that contains valuable information (DVD, flash drive, paper documents, etc.).

3.2. Hardware means of the automated control system

ACSPP hardware part. ACSPP hardware part includes the devices that provide the information exchange between the components within ACSPP, as well as between ACSPP and the external environment. That is, ACSPP hardware can include:

– resources: servers, workstations, mobile computers;
– peripherals: printers, scanners, barcode readers, etc.;
– communication equipment: networks and network equipment;
– devices for communication with production equipment: controllers.

A server is a resource which contains valuable information and to which remote access is possible. Accordingly, a workstation is a resource that contains valuable information and to which only local access is possible, a mobile computer is a resource that contains valuable information and can be carried by the user outside the organization.

Personnel. The term "personnel" is understood as people who maintain ACSPP (such as system administrators) and those who work directly with it (users).

Method of the system assets identification

An asset of an information technology system is a component or part of the overall system in which the organization directly invests material and information resources, and which, accordingly, requires protection by the organization. The following groups of assets can be distinguished as a typical ACSPP:

1. Information/data. This category includes the central database, internal data, output files, archives, as well as information on hard copies.

2. Software: ACSPP software modules and auxiliary software (OS, drivers, utilities, etc.);

3. Hardware resources: servers, workstations, mobile PCs.

4. Communication equipment: networks.

5. Services: information and production ones.

6. Prestige (image) of the organization [5].

3.3. Hardware means of the automated control system

For certain ACSPP assets, it is possible to define functional dependencies between them within the printing company – Figure 3.

The proper operation of the software and the information part of the assets depends on the operation of the hardware component. Since ACSPP in most cases is located on several resources, the information exchange between them will depend entirely on the network equipment. For a typical ACSPP, it is standard to have one or more servers for centralized management of information processes. In this case, the operation of workstations and mobile PCs as a part of ACSPP will depend on the proper operation of the servers.

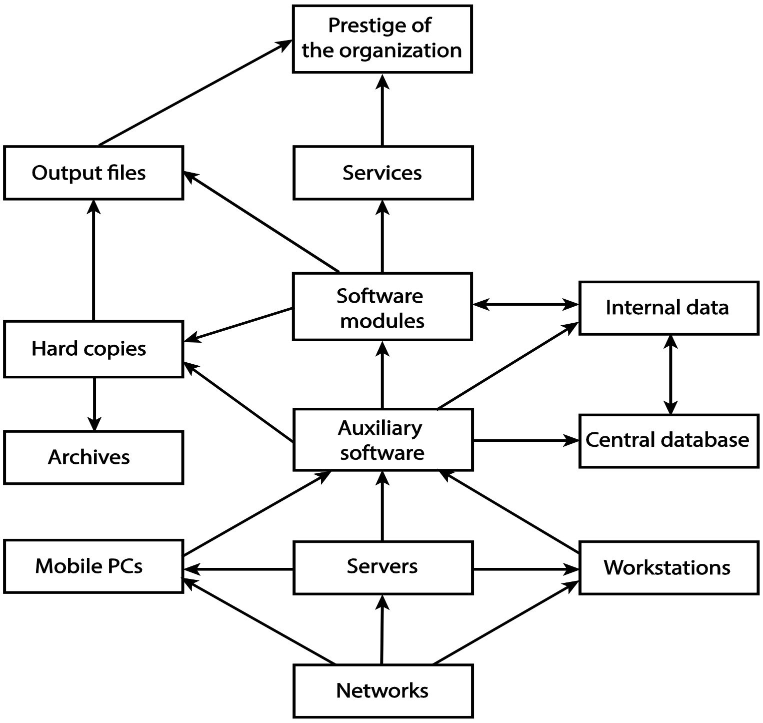

Figure 3: Functional dependencies between the information components of ACSPP structure

The operation of ACSPP information part will completely depend on the proper operation of the auxiliary software, which forms the internal information environment of ACSPP together with the software modules and provides the communication of the information part with the hardware. That is, the proper operation of the auxiliary software will depend on the operation of ACSPP software modules, the correctness of ACSPP internal data, the operation of the central database, as well as the information correctness on hard copies.

ACSPP software modules are used to convert the information and are also an intermediate link between the users and the central database. That is, the condition of the central database and internal data will depend on the correct operation of ACSPP software modules, which in turn will also affect the operation of ACSPP software modules. In addition, through ACSPP software modules the information is exported both in electronic form (output files) and in hard copies. Almost the whole range of information and production services provided by the company, and hence the company prestige, will also depend on the operation of ACSPP software modules.

In ACSPP working process, the information is periodically archived on hard discs, the condition of which will depend on the condition of the archives.

3.4. Component assessment of the company assets under threat

The asset value is determined by its importance to the business activities of the organization, and the assessment level of business activities may be based on security considerations, i.e. how much the business activities of the organization and other IS assets may suffer from leakage, distortion, unavailability and destruction of information. Thus, the assets identification and the assessment, based on the business interests of the organization, is a key factor in the risk determining. The asset value also depends on the cost of the asset formation and maintaining. The identified assets are valuable to the organization. However, it is not possible to directly determine the financial value of each of them. It is also necessary to determine the value or degree of importance of the asset to the organization in non-profit activities. Otherwise, it will be difficult to determine the protection level required and the amount of funds that organizations should spend on protection measures [3–4].

To assess the assets, a three-level scale is selected: 1 – low asset value; 2 – average asset value; 3 – high asset value – Table 1. It should be noted that some assets cannot be valued on a material scale. In addition, not all assets are subject to replacement, so its value cannot be assessed. The overall asset assessment is determined by the highest assessment – the total value assigned to one of the assessment scales.

Table 1

Component assessment of assets

№	Name of the asset	Material assessment	Non-material assessment	Replacement cost	Total assessment
1	Prestige of the organization	—	3	—	3
2	Services	—	3	—	3
3	Output files	—	3	1	3
4	Archives	1	1	—	1
5	Hard copies	1	1	1	1
6	Internal data	—	3	—	3
7	Central database	—	3	—	3
8	Auxiliary software	2	3	1	3
9	ACSPP software modules	2	3	1	3

10	Workstations	2	2	2	2
11	Mobile PCs	2	2	2	2
12	Servers	3	3	3	3
13	Networks	1	3	2	3

As mentioned above, the material assessment may not be determined for all assets, as it is difficult to assess the value of such assets as the prestige of the organization, services, output files, internal data, central database, in monetary terms. The cost of archives and hard copies is assessed at the cost of media. The cost of ACSPP software and modules is not high compared to the value of other company assets (e.g. premises, printing equipment), but it is not as low as the cost of media. The same can be said for the assessment of workstations and mobile PCs. The cost of the server equipment is usually higher than the cost of other computer equipment, so it is rated "high". At the same time, the cost of networks per workplace will be quite low.

Non-material assessment is necessary in order to assess the criticality of a particular asset for the company proper operation From this point of view, most assets are critical because they are interconnected. However, the criticality of assets such as archives and hard copies will be relatively low, provided that the remaining assets function properly. The criticality of mobile PCs and workstations is rated as "average", because the failure of these assets will only lead to some slowdown in the company activity, as all important information is stored on servers.

When assessing the cost of replacing assets, both the material assessment of assets and the cost of replacing the asset are taken into account. In particular, the replacement of information assets (output files, auxiliary software, ACSPP software modules) will not require high costs. Some assets, such as the prestige of the organization, services, archives, internal data, central database, are not subject to replacement.

4. Component method for assessing the risks of system failure under active threat

To select adequate protection measures, it is necessary to assess the risk level. [7, 8] The risk level depends on the asset value, the threat criticality, the threat probability and frequency. The risk level will be determined by the formula:

$$R_{j,i} = V_j \times K_{j,i} \times P_{j,i} \times W_{j,i} \times T_i^{\Sigma},$$

where V_j – is the value of the *j*-th asset;

$K_{j,i}$ – is the criticality of the *i*-th threat for the *j*- th asset;

$P_{j,i}$ – is the probability of occurrence of the *i*-th threat for the *j*-th asset;

$W_{j,i}$ – is the frequency of occurrence of the *i*-th threat for the *j*-th asset during a year;

T_i^{Σ} – is the total value, obtained by assessing vulnerabilities for the *i*-th threat. It is calculated by the formula:

$$T_i^{\Sigma} = \sum_{q=1}^{n} P_q^T,$$

where P_q^T – is the probability of occurrence of vulnerability *q* for the *i*-th threat;

n – is a number of vulnerabilities used by the *i*-th threat.

The total risk value for the *i*-th threat:

$$R_i^{\Sigma} = \sum_{j=1}^{k} R_{j,i},$$

where k – is a total number of assets.

The probability of the *j*-th asset to the risk is calculated by the formula:

$$R_j^{\Sigma} = \sum_{i=1}^{s} R_{j,i},$$

where s – is a total number of threats.

The results of the risk assessment are presented in Table 2.

Table 2

Identification and assessment of risks of losses under threat

Threat	Risk value R for the asset j													
	Networks	Servers	Mobile PCs	Workstations	ACSPP software modules	Auxiliary software	Central database	Internal data	Hard copies	Archives	Output files	Services	Prestige of the organization	Total risk
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Human physical threats aimed at IS resource														
Unauthorized use of equipment	0	234	156	702	1053	1053	1053	1053	351	0	1053	1053	1053	8814
Disclosure, transfer or loss of access delimitation attributes	0	729	486	486	729	729	729	729	243	0	729	729	729	7047
Human physical threats aimed at IS communication channel														
Cable damage	513	0	0	0	114	114	114	114	0	0	513	513	513	2508
Local physical threats aimed at IS														
Fire	144	144	96	96	0	0	0	0	48	48	144	144	144	1008
Cross-reference	270	45	30	30	0	0	0	0	60	20	45	45	45	590
Failure of external energy sources	729	729	486	486	0	0	0	0	0	0	0	729	729	3888
Failure of internal (reserve) energy sources	972	972	648	648	0	0	0	0	0	0	0	972	972	5184

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Sharp voltage fluctuations in the power grid	729	729	486	486	0	0	0	0	0	0	0	729	729	3888
Physical threats related to equipment failure														
Loss of information as a result of media failure	0	243	324	324	486	486	243	486	108	36	216	486	486	3924
Defective media	0	162	216	216	324	324	162	324	72	24	144	324	324	2616
Decreased equipment reliability after its expiration date	108	108	72	72	0	0	0	0	72	36	0	108	108	684
Data loss or system malfunction due to overflow of storage devices	0	432	288	288	192	432	216	192	0	0	192	432	432	3096
Local logical threats aimed at OS														
Running files with viruses that attack OS	0	0	0	0	324	729	729	729	108	0	324	729	729	4401
Running OS from external media	0	0	0	0	264	594	594	594	88	0	264	594	594	3586
Modification of OS components	0	0	0	0	360	810	810	810	120	0	360	810	810	4890
Refusal to service OS	0	0	0	0	264	594	594	594	88	0	264	594	594	3586
Local logical threats aimed at software														
Opening files with macro viruses	0	0	0	0	288	648	648	648	96	0	288	648	648	3912
Modification of application software	0	0	0	0	396	891	891	891	132	0	396	891	891	5379

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Refusal to service application software	0	0	0	0	360	1215	1215	1215	120	0	360	1215	1215	6915
Local logical threats aimed at the information, stored and processed at the resource														
Unauthorized modification of information in the database stored on the resource	0	0	0	0	0	0	891	891	297	0	891	891	891	4752
Unauthorized modification of electronic documents containing valuable information	0	0	0	0	0	0	0	1377	459	459	1377	1377	1377	6426
Loss or violation of the integrity of information stored on the resource due to improper operation of the software	0	0	0	0	0	0	729	729	243	0	729	729	729	3888
Deletion of valuable information stored in the database by the violator	0	0	0	0	0	0	729	729	108	0	324	729	729	3348
Deletion of electronic documents containing valuable information by the violator	0	0	0	0	0	0	324	729	243	0	729	729	729	3483

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Threats related to unintentional actions of the personnel														
Violation of information confidentiality due to unintentional actions	0	0	0	0	0	891	891	891	0	0	891	891	891	5346
Unintentional violation of information integrity	0	0	0	0	972	972	972	972	324	0	972	972	972	7128
Unintentional deletion of critical information	0	0	0	0	972	972	972	972	324	324	972	972	972	7452
Risk propensity of assets	3465	4527	3288	3834	7098	11454	13506	15669	3704	947	12177	19035	19035	—

As a result of risk assessment, a certain number is obtained for each threat, which characterizes the risk level caused by this threat. Thus, it is possible to rank threats in order to reduce the risk caused by them – Table 3. This is necessary for the correct choice of adequate protection measures.

Table 3
List of ACSPP main threats in risk descending order

№	Threat	Total risk
1	2	3
1	Unauthorized use of equipment	8814
2	Unintentional deletion of critical information	7452
3	Unintentional violation of information integrity	7128
4	Disclosure, transfer or loss of access delimitation attributes	7047
5	Refusal to service application software	6915
6	Unauthorized modification of electronic documents containing valuable information	6426
7	Modification of application software	5379
8	Violation of information confidentiality due to unintentional actions	5346
9	Failure of internal (reserve) energy sources	5184
10	Modification of OS components	4890
11	Unauthorized modification of information in the database stored on the resource	4752
12	Running files with viruses that attack OS	4401
13	Loss of information as a result of media failure	3924
14	Opening files with macro viruses	3912

15	Failure of external energy sources	3888
16	Sharp voltage fluctuations in the power grid	3888
17	Loss or violation of the integrity of information stored on the resource due to improper operation of the software	3888
18	Running OS from external media	3586
19	Refusal to service OS	3586
20	Deletion of electronic documents containing valuable information by the violator	3483
21	Deletion of valuable information stored in the database by the violator	3348
22	Data loss or system malfunction due to overflow of storage devices	3096
23	Defective media	2616
24	Cable damage	2508
25	Fire	1008
26	Decreased equipment reliability after its expiration date	684
27	Cross-reference	590

The risk propensity of assets shows how vulnerable an asset is. Its level will affect the selection of protection measures and means for the asset, as well as the priority of their implementation. The list of assets in their risk propensity descending order is presented in Table 4.

Table 4
List of assets in their risk propensity descending order

№	Asset	Risk propensity
1	Prestige of the organization	19035
2	Services	19035
3	Internal data	15669
4	Central database	13506
5	Output files	12177
6	Auxiliary software	11454
7	ACSPP software modules	7098
8	Servers	4527
9	Workstations	3834
10	Hard copies	3704
11	Networks	3465
12	Mobile PCs	3288
13	Archives	947

In addition to the above-mentioned ACAPP security problems related to the threats and vulnerabilities inherent in most IS, a number of organizational and psychological issues should also be noted. In particular, weak awareness of the information importance and its protection by the management staff and employees of printing companies. Accordingly, the management staff is reluctant to invest in information protection and make any organizational decisions on this issue, and the employees show misunderstanding and failure to take most protection measures, which leads to negligence, and then complete disregard for protection measures. This attitude to the information security can cause significant losses to the company, which will be simply disproportionate to the cost of information security in their values.

Another important problem is the imperfection of Ukrainian legislation in the information protection area and almost complete absence of domestic standards in this area.

In order to achieve the required level of ACSPP protection, it is necessary to reduce the risks level to an acceptable one or eliminate the risks altogether. This can be achieved by reducing the criticality, probability and/or frequency of threats. One can also reduce the probability of vulnerabilities to this threat or eliminate them altogether. This is achieved by implementing appropriate protection measures.

5. Conclusion

The functional scheme of risk management for ACSPP is constructed with a detailed definition of various risk components. The assets identification and the analysis of their functional dependency are carried out. A three-level scale is selected to assess ACSPP assets and, accordingly, the risks.

The risk level assessment is made for each of ACSPP assets on the basis of identified threats and their vulnerabilities. As a result of risk assessment, threats are ranked in order of risk reduction and the dependency of assets on their risk propensity is revealed.

The risk assessment process for automated control systems of printing production is studied. The following results are obtained: methods of risk assessment for ACSPP are analysed, which are based on the identification and assessment of assets, threats and vulnerabilities of the printing company; the assets of a typical ACSPP are determined, the dependencies between them are defined and their assessment is carried out. For ACSPP assets, the value of which is assessed as "high", methods of providing the additional protection are suggested; the risk assessment for ACSPP is carried out, as a result of which a list of 27 main threats of ACSPP is obtained, which require the introduction of additional protection measures. It is defined that the threats to ACSPP with the greatest risk are unauthorized use of equipment, unintentional deletion of critical information, unintentional violation of the information integrity; the risk propensity of ACSPP assets is analysed. As a result, the most risk propensity assets are the prestige and services provided by the company, as well as internal data circulating in ACSPP and the central database of ACSPP.

References

[1] V. Kovaleva, Yu. Samarin, Selection of the control system of the printing company, ComputerArt. Journal for printers and publishers. №11, 2007, pp. 61–64

[2] V. Kovaleva, Yu. Samarin, Management systems of the printing company. ComputerArt. Journal for printers and publishers (2017) [Cited: 27.08.2018] Retrieved from: http://compuart.ru/article.aspx?id=18248&iid=846

[3] B. Durnyak, G. Petriashvili, V. Sabat, T. Maiba, Defining the security level of technological processes on the basis of risk assessment, Lviv, UAP, 2019

[4] V. Vitlinsky, G. Velikoivanenko, Riskology in economics and entrepreneurship, Monograph, Kyiv, KNEU, 2004

[5] T. Lashev, V. Korolev, S. Shargin, Mathematical methods for assessing the optimal parameters of risk processes. Systems and means of informatics, Moscow, IPI RAS, 2002, pp. 127–141

[6] V. Sabat, Analysis of risks in automated document management systems, Modelling and information technology. Collection of scientific works, Kyiv, IPME named after H.E. Pukhov of NAS of Ukraine, Issue 73, 2014, pp. 198–204.

[7] L. Donets, Economic risks and methods of measuring them, Tutorial, Kyiv, Centre for Educational Literature, 2006

[8] NDSTPI of the Department of Special Telecommunication Systems and Information Protection of the Security Service of Ukraine from 04.12.2012, No 805 https://tzi.com.ua/downloads/1.4-001-2000.pdf

[9] NDTPI 1.1-002-99, General instructions for the protection of information in computer systems from unauthorized access

[10] NDTPI 1.4-001-2000, Typical regulation for information protection service in an automated system

[11] V. Sherstjuk, M. Zharikova, R. Levkivskiy, V. Gusev, Density-Based Risk Assessments within Soft Safety Domains. CEUR Workshop Proceedings, 2020, vol. 2805, pp. 355–372. http://ceur-ws.org/Vol-2805/paper26.pdf

[12] V. Sherstjuk, M. Zharikova: Risk assessment framework based on the model of human-infrastructure system. CEUR Workshop Proceedings, 2020, 2740, pp. 37–52. http://ceur-ws.org/Vol-2740/20200037.pdf

[13] L. Sikora, N. Lysa, O. Fedevych, M. Navytka, R. Tkachuk, I. Dronyuk, Information technologies of formation of intellectual decision-making strategies under conditions of cognitive failures, in: Proceedings of Computational & Information Technologies for Risk-Informed Systems, CITRisk-2020, Kherson, Ukraine, 2020, pp. 233–254

[14] L. Sikora, R. Tkachuk, N. Lysa, I. Dronyuk, O. Fedevych, Information and logic cognitive technologies of decision-making in risk conditions, in: Proceedings of the 1st International Workshop on Intelligent Information Technologies & Systems of Information Security, IntellTSIS 2020, Khmelnytskyi, Vol. 2623, Ukraine, pp. 340–356