UDK 658
JEL Classification: G32, C15, M15, D81
DOI: 10.15587/2706-5448.2026.352430

Anton Ostapets,
Iryna Parasii-Verhunenko,
Kostiantyn Bezverkhyi,
Mykola Matiukha,
Oleksandr Yurchenko

THE DEVELOPMENT OF ANALYSIS METHODOLOGY OF FINANCIAL RISKS OF PROJECTS IN IT SPHERE

The object of research is methodology for analysis of the financial risks of IT projects related to organizations' compliance with the General Data Protection Regulation (GDPR).

In this article, the authors assess the financial risks of two projects that can be considered and analyzed by organizational management to bring existing software and processes into compliance with the aforementioned GDPR requirements. The first project considered by the organization involves the development of appropriate software for users' personal data storage, protection and processing by a dedicated internal team of specialists, with the possibility of further commercialization of the developed product by selling a ready-to-use software and services package to partners and other clients. The second solution considered is a project in which the responsibility for personal data processing, storage and protection is transferred to a third party, and the organization purchases a ready-to-use package of software and related services from them.

The results of the financial risk analysis of these projects indicate that the in-house software development project is less risky and more reasonable in the long-term perspective. This is due to the fact that it provides a 231 times lower probability of exceeding the planned budget benchmark compared to the alternative project.

The risk analysis model described in the article can be used to assess financial risks of projects not only within the IT industry but also, after certain adaptations, in other business entities.

Keywords: *risk analysis, general data protection regulation (GDPR), IT project, Monte-Carlo method, financial analysis.*

Received: 11.12.2025
Received in revised form: 26.01.2026
Accepted: 17.02.2026
Published: 28.02.2026

How to cite
Ostapets, A., Parasii-Verhunenko, I., Bezverkhyi, K., Matiukha, M., Yurchenko, O. (2026). The development of analysis methodology of financial risks of projects in IT sphere. Technology Audit and Production Reserves, 1 (4 (87)), 6–20. https://doi.org/10.15587/2706-5448.2026.352430

1. Introduction

In recent years, compliance with the General Data Protection Regulation (GDPR) has become a critical imperative for enterprises operating within the European Union market or those engaged in the processing of personal data of EU residents. Given the extraterritorial jurisdiction of the GDPR, which mandates compliance for any organization processing the personal data of EU subjects regardless of the entity's legal domicile, adherence to these regulatory standards is obligatory. Consequently, any software product developed by an organization must incorporate data protection principles from its inception or be retrofitted to meet these stringent requirements if such measures were omitted during the initial development phase.

A fundamental requirement for contemporary software systems is that data protection must be embedded into the core of the product and integrated throughout the software development life cycle. This approach prioritizes data minimization, ensuring that only the essential volume of user data is collected and processed. In instances where data protection mechanisms were not integrated at the nascent stage, organizations are compelled to implement remedial measures to ensure regulatory alignment.

This research provides a comprehensive analysis and financial risk assessment of two distinct strategic approaches: the development of proprietary software designed to bring existing systems into full compliance with GDPR mandates and the acquisition of a ready-to-use solution from a third-party provider.

Risk analysis of different projects has become a very important subject for different modern scientific research. Such analysis becomes crucial in the context of digital transformation, technological complexity, uncertainties of external environment of IT companies. In scientific literature, project risk has a concept of a multidimensional phenomenon encompassing financial, technological, organizational, behavioral, and external factors that can adversely affect project cost, schedule, and overall performance.

The analysis of IT project effectiveness performed on the basis of risk-oriented approach is examined in the works of both foreign and domestic researchers. The paper [1] presents a holistic overview of financial risk management in public-private partnership projects, emphasizing the continuous identification, assessment, and monitoring of risks throughout the entire project lifecycle. Similarly, in study [2] that project portfolio risk analysis must account for the interdependence between projects, as neglecting such links can lead to biased risk assessments and suboptimal decision-making.

Financial and analytical dimensions of risk assessment are further expanded through the integration of financial and non-financial information. The role of analytical audit procedures applied to integrated reporting as a tool for the comprehensive analysis of corporate activity is emphasized in article [3].

Financial risks and risks associated with the value chain are widely utilized in the literature. The publication [4] demonstrates that supply chain risks have both direct and indirect impacts on a project's financial performance, which is particularly relevant for IT companies operating in global digital ecosystems. Specifically, the article [5] introduces dependency modelling approaches for assessing cost and time risks in large-scale projects, allowing for a more accurate reflection of cumulative risk effects. At the same time, a group of researchers in their publications [6, 7] highlight the influence of cognitive biases and the limitations of expected value-based contingency reserve calculations when evaluating project risks.

When it comes to IT projects, there are specific characteristics involved, which are confirmed by both empirical and methodological studies. Key factors that determine the success of risk management in IT projects within Romanian companies: methodological agility, stakeholder engagement, and the use of information systems for decision support are identified in study [8]. Learning methods for forecasting investment risks in IT companies are analyzed in research [9]. Furthermore, machine learning models are utilized in study [10] to assess investment risks in virtual IT firms, demonstrating the rapidly growing role of data-driven risk analytics.

Modern research increasingly focuses on risk interdependence and complex non-linear interactions between risk factors. At the same time, the study [11] proposes a simulation-based risk interdependence network model that captures cascading risk effects within projects. Concurrently, in article [12] the decision-making process under risk is expanded by integrating regret theory into three-way decision models with interval values for project resource allocation. Furthermore, in research [13] it is demonstrated that coordinated stakeholder actions in uncertain environments significantly enhance risk management effectiveness in collaborative innovation projects, which is particularly relevant for IT project ecosystems.

Organizational and human dimensions of risk management are also highlighted in scientific and practical literature. Concurrently, few sources [14, 15] demonstrate that adaptive and resource-efficient risk management frameworks are especially suitable for small and medium-sized enterprises (SMEs), including IT companies. Meanwhile, research [16] links project risk management practices with occupational health and productivity, emphasizing the socio-organizational consequences of managing them.

In the context of sustainable development and digital transformation, authors increasingly integrate risk management with sustainability-oriented approaches. Risk management models based on the life cycle and sustainability principles are proposed in articles [17, 18]. At the same time, a group of scientists [19] utilize fuzzy synthetic evaluation methods to analyze project risks in green building projects, offering methodological insights that can be adapted for green IT projects. Simultaneously, several researchers in their study [20] make further contributions by developing hybrid management decision support systems for risk-based strategic assessment.

The growing application of advanced digital technologies in project risk analysis represents another important research direction. Meanwhile, the work [21] explores whether generative artificial intelligence, such as ChatGPT, can outperform human experts in construction project risk management, providing insights into AI-assisted decision-making. Simultaneously, a group of scientific enthusiasts [22] conduct a bibliometric and systematic literature review on AI in project risk management, while in study [23] the potential of quantum computing to enhance risk forecasting accuracy for IT companies is examined.

Notably, the work [24] proposes and validates methods of multifactor correlation and regression analysis to assess the impact of individual factors on a company's operating profit. The authors constructed a mathematical model that allows for evaluating the degree of influence of indicators, such as the share of material current resources in the structure of current assets, the turnover ratio of material current resources, the share of own working capital, and its profitability, on the company's financial results.

In paper [25], methodological approaches to comparative analysis of the efficiency of enterprises' resource potential use were developed based on correlation and regression analysis. According to the methodology proposed by the scholars, resource use efficiency is evaluated by comparing the actual profit values of trading enterprises with calculated values obtained through regression models. This approach expands the possibilities of using econometric models in financial and strategic analysis of corporate performance efficiency.

The research [26] considers critical risk management strategies for the functioning of public-private partnerships. At the same time, political risk management of foreign direct investment in infrastructure projects is studied in [27]. Concurrently, the contribution of social media to risk management strategies for British IT companies is evaluated in paper [28]. Risk assessment in infrastructure project construction using artificial neural networks is performed in study [29]. Meanwhile, a group of scientists [30] conduct volatility measurements of selected IT companies within the national stock exchange context and assess risk factors from an investor's perspective. In [31], a group of foreign authors uses smart data and business analytics for recycling risk management in megaprojects. Simultaneously, the scientific work [32] investigates project risks, efficiency, and business success in the financial services sector.

In conclusion, the reviewed literature offers a solid theoretical and methodological foundation for project risk analysis. However, despite the breadth of existing research, a scientific gap remains in the development of integrated models adapted specifically for IT companies, models that simultaneously account for technological, organizational, and financial risks while considering their interdependencies and leveraging advanced analytical and intelligent technologies. This gap underscores the relevance and necessity of further research in the field of project risk analysis for IT companies.

The methodology for analysis of GDPR compliance related IT projects' financial risks are *the object of research* conducted in this article.

The aim of research is development of a methodological framework used for IT projects financial risks analysis and identification of the most financially sustainable project for long term perspective.

To reach the aim of research, it is necessary to perform the following objectives:

1. To develop an algorithm used to forecast penalties for violating GDPR requirements based on the financial performance indicators of IT companies, in order to form budgets for projects designed to minimize the risk of personal data breaches.

2. To improve the methodic of IT-projects financial risks analysis using scenario analysis and Monte Carlo method.

2. Materials and Methods

2.1. The structure of the research

The conducted research is structured into seven primary stages:

– data collection and calculation of financial performance indicators for the organization;

– data aggregation and investment volume calculation required for the development of proprietary software for user personal data processing, storage, and protection. The primary output of this stage is the expenditure component of the input data for the Monte Carlo simulation;

– collection and calculation of the required investment for a project involving the transfer of responsibility for personal data storage, processing, and protection to a third party (outsourcing);

– establishment of tariff rates, sales forecasting, and profit calculation derived from the implementation of the developed software;

ISSN-L 2664-9969; E-ISSN 2706-5448

– quantitative risk analysis of the proprietary software development project based on Monte Carlo simulation;
– quantitative analysis of the third-party outsourcing project using the Monte Carlo method;
– formulation of conclusions based on the calculations performed and providing recommendations for selecting the most viable strategy regarding cost levels.

The stages of research are highlighted in Fig. 1.

2.2. Materials

During the initial stage of the research, a calculation of financial indicators was performed for an organization specializing in the sale of software for processing user inquiries (helpdesk/ticketing systems); notably, the software is marketed to clients within the EU. Consequently, the product must comply with the requirements of the European General Data Protection Regulation (GDPR). The following indicators were used for subsequent calculations [33, 34]:

– total headcount (number of employees);
– number of clients;
– cost of tariff packages;
– average employee salary categorized by grade;
– foreign exchange rate (USD);
– applicable corporate tax rate;
– facility rental costs.

In the subsequent stage, the following parameters are employed for calculation [35–44]:

– salary ranges for employees in relevant positions;
– costs of ISO 27001 certification;
– technical documentation development costs;
– estimated software audit costs;
– workstation acquisition costs;
– server equipment costs;
– costs of additional software licenses.

The third stage involves estimating the investment volume and ongoing expenditures required for the acquisition of a ready-to-use set of products and services from a third-party provider, based on the following metrics [45–52]:

– cloud storage (10 TB/USD per year);
– maintenance and data transfer costs (USD);
– DLP (data loss prevention) platform and compliance solutions (USD for 500 employees);
– compliance management platform (for end-users of the sold product), calculated for 200000 users;
– DPO (data protection officer) salary;
– integration and implementation costs (one-time fees);
– employee training expenses.

The fourth stage consists of calculating core business metrics. The following indicators are used for these calculations:

– subscription plan pricing (value proposition);
– opening customer base for each tariff at the start of the period;
– customer churn rate;
– sales volume (number of units sold);
– integration service fees;
– employee training fees.

The fifth stage involves Monte Carlo simulation. The primary inputs for this modeling include the results from the second stage (development costs) and the fourth stage (revenue/business metrics).

The penultimate stage is a Monte Carlo simulation designed to determine the cost distribution for acquiring third-party services, factoring in a 2-year outlook.

The final stage involves formulating conclusions based on the simulation results and selecting the optimal solution (proprietary development versus third-party acquisition).

2.3. Methods

At the first stage, the organization's profit is calculated based on the total sales revenue and the total expenses incurred during the accounting period, using the following formula

$$Profit = TI - TE, \quad (1)$$

where TI represents the company's total income from product and service sales, and TE denotes the total expenses incurred during the specified time period

$$TI = \Sigma P_i S_i, \quad (2)$$

where total income is calculated based on P_i (the price of a specific tariff plan in USD) and S_i (the number of active users for that plan).

To calculate the tax component of the expenditures, the corresponding income value in foreign currency must be multiplied by the current exchange rate

$$TIuah = TI \cdot CER, \quad (3)$$

where CER – the USD-to-UAH currency exchange rate.

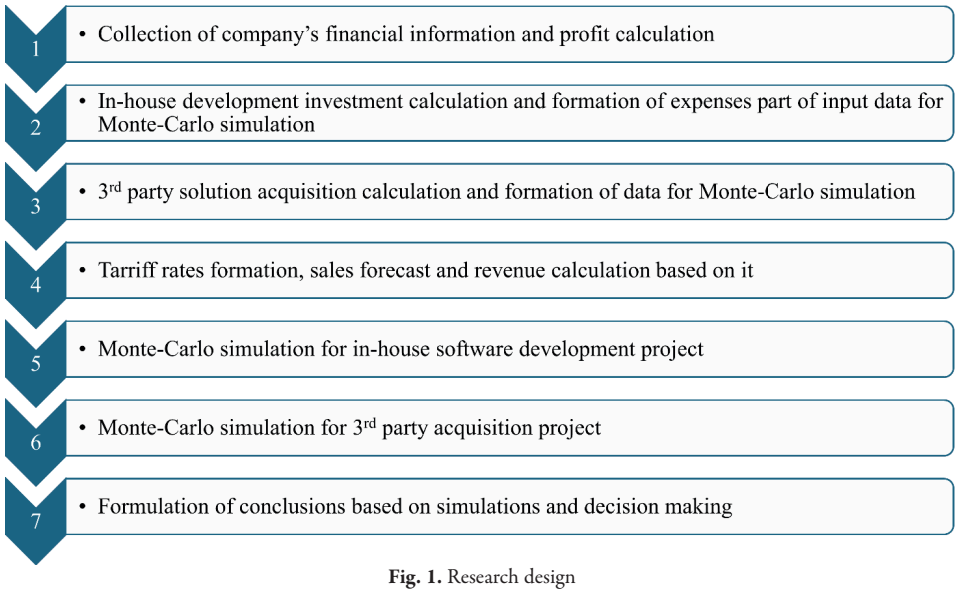

Fig. 1. Research design

Consequently, the total expenses are calculated using the following formula

$$TE = TAX_{tot} + OE, \quad (4)$$

where TAX_{tot} – the total amount of taxes paid by the organization, and OE (operating expenses) represents the total costs for office rent, equipment, and other cumulative expenditures.

The unified social contribution (ESC), personal income tax (PIT), and military tax are calculated based on the number of employees within specific grades and the average salary per grade

$$TAX_i = (TP \cdot NE_x \cdot AS_x)/100, \quad (5)$$

where TP – the tax percentage, NE_x – the number of employees in a specific grade x, x – the grade level, and AS_x – the average salary for that grade.

The preliminary calculations in the second and third stages of the research are straightforward and are computed as the sum of the company's expenses or investments based on the indicators mentioned above. Notably, in the case of proprietary development, expenditures in the second year will be lower than in the first due to the absence of costs for tangible assets such as workstations, server, and networking equipment.

Calculations in the fourth stage are based on assumptions regarding potential sales volumes.

The organization's cost simulations using the Monte Carlo method are performed using built-in functions in Microsoft Excel, such as = = RAND() and = NORMINV(probability; mean; st_dev). The arguments for these functions include probability, the mean value, and the standard deviation, assuming a normal distribution as the governing law.

To perform the calculations and simulations in this research, Microsoft Excel (Microsoft Corporation, USA) with the StatPlus add-on was utilized.

3. Results and Discussion

3.1. The development of GDPR violation penalties forecast algorithm and formation of GDPR compliance project budget based on company's financial performance indicators

The organization under study employs 483 individuals. For the purpose of simplifying subsequent calculations, it is assumed that all employees are officially registered in accordance with labor legislation and are included on the company's payroll. While salary payments and tax contributions are processed in Ukrainian Hryvnia (UAH), the base salary is pegged to the US Dollar (USD). For the following calculations, an exchange rate of 40 UAH per 1 USD has been used.

The baseline values for calculating the revenue component of the company's operations are presented in Table 1.

Additionally, the company has implemented a general grading strategy to determine employee compensation, where Grade 1 represents entry-level staff with minimal experience and qualifications, and Grade 6 comprises the executive management team.

The distribution of employees by grade and the calculation of payroll taxes are conducted based on the following statutory tax rates:

– Personal income tax (PIT) – 18%;

– Military eax – 1.5%;

– Unified social contribution (USC) – 22%.

The USC calculation follows specific regulatory guidelines: if the monthly salary exceeds 160000 UAH, the calculation base is capped at this amount. Consequently, the maximum USC contribution is fixed at 35200 UAH per person.

The results of these calculations are presented in Table 2.

The annual tax liabilities of the company, calculated as the sum of monthly contributions multiplied by the fiscal year, are summarized in Table 3.

Table 1

Calculation of company revenue from software product sales

Tariff name	Active user count	Service cost (USD/month)	Minimum users	Maximum users	Annual revenue (incl. VAT), USD	Annual revenue (incl. VAT), UAH	Annual revenue (excl. VAT), USD
Base	110000–130000	10	110000	130000	13200000–15600000	528000000–624000000	11000000–13000000
Medium	25000–35000	25	25000	35000	7500000–10500000	300000000–420000000	6250000–8750000
Maximum	15000–20000	50	15000	20000	9000000–12000000	360000000–480000000	7500000–10000000
Professional	10000–15000	100	10000	15000	12000000–18000000	480000000–720000000	10000000–15000000
TOTAL	–	–	160000	200000	41700000–56100000	1668000000–2244000000	34750000–46750000

Table 2

Monthly payroll tax calculation by employee grade

Grade	Number of employees	Average salary (USD)	Average salary (UAH)	USC per employee (UAH)	Total USC (UAH)	Total PIT (UAH)	Total military tax (UAH)
G1 (trainee)	195	800	32000	7040	1372800	1123200	93600
G2 (junior)	87	1200	48000	10560	918720	751680	62640
G3 (middle)	65	1800	72000	15840	1029600	842400	70200
G4 (senior)	43	2500	100000	22000	946000	774000	64500
G5 (expert, manager)	55	5444	217760	35200	1936000	2155824	179652
G6 (top-management)	38	10884	435360	35200	1337600	2977862	248155.2

Table 3

Calculation of total annual tax liabilities

Tax category	Rate (%)	Total amount (UAH)	Total amount (USD)
Corporate income tax	18	113108183.42–199508183.42	2827704.59–4987704.59
Unified social contribution (USC)	22	90488640	2262216
Personal income tax (PIT)	18	103499596.8	2587489.92
Military tax	1.5	8624966.4	215624.16
TOTAL	–	308376816–394776816	7893034.67–10053034.67

ISSN-L 2664-9969; E-ISSN 2706-5448

Based on the calculations provided above, it becomes possible to determine the company's net profit. The pre-tax income ranges from 628378796.8 to 1117003763.2 UAH. After deducting operational expenses and taxes, the company's net profit stands between 515270613.38 and 917495579.78 UAH (approximately 12881765.33–22937389.49 USD).

To calculate potential GDPR fine the algorithm shown in Fig. 2 is used.

Each violation is reviewed by the responsible commission on an individual basis, and the administrative fines are adaptive. However, in the event of a decision to apply the maximum penalty under GDPR, the organization must pay a fine of 20 million EUR or up to 4% of its global annual turnover, whichever is higher [33].

In this case, the company's annual revenue ranges from 34750000 to 46750000 USD, which equates to 29956896–40301724 EUR (assuming an exchange rate of 1 EUR = 1.16 USD). Since 4% of this amount is only 1198276–1612068 EUR, the statutory fine of 20 million EUR would be applied as it is the greater value.

Given that the organization's net profit is 12881765.33–22937389.49 USD (11104970.11–19773611.63 EUR), the occurrence of a data leak resulting in the maximum fine would cause the loss of 22 months' net profit (under minimum profit conditions) or approximately one full year of profit (under maximum profit conditions).

Consequently, management has decided to invest 3% of the annual net profit into risk mitigation. This corresponds to a range of 386453–688121 USD, with a mean value of 537287 USD. This minimal yearly figure will serve as the baseline for the upcoming financial risk assessment.

3.2. Method of GDPR compliance IT-projects' financial risks analysis using scenario analysis and Monte Carlo method

The input data for calculating the cost of proprietary software development (to ensure GDPR compliance) includes employee salaries, hardware and software procurement, and the costs associated with mandatory audits and certifications.

To execute the in-house development project, the following core specialized personnel are required:

– project manager/product owner: responsible for coordination, stakeholder communication, and requirement engineering;
– software developers (full-stack or frontend and backend): responsible for programming and core functional implementation;
– security engineer/DevOps: focused on security infrastructure, CI/CD pipelines, hashing, and encryption;
– QA/test engineer: responsible for product testing, security audits, penetration testing, and leak detection testing.

Important notice: It is considered that personnel is hired for 2-year contract with possibility of further prolongation after testing and 1st year sales stage is finished. Hypothesis of research and modelling includes that there are no other risks (such as HR, legal, social, technological) that can create an impact of projects.

The labor costs for the personnel required for software creation are detailed in Table 4.

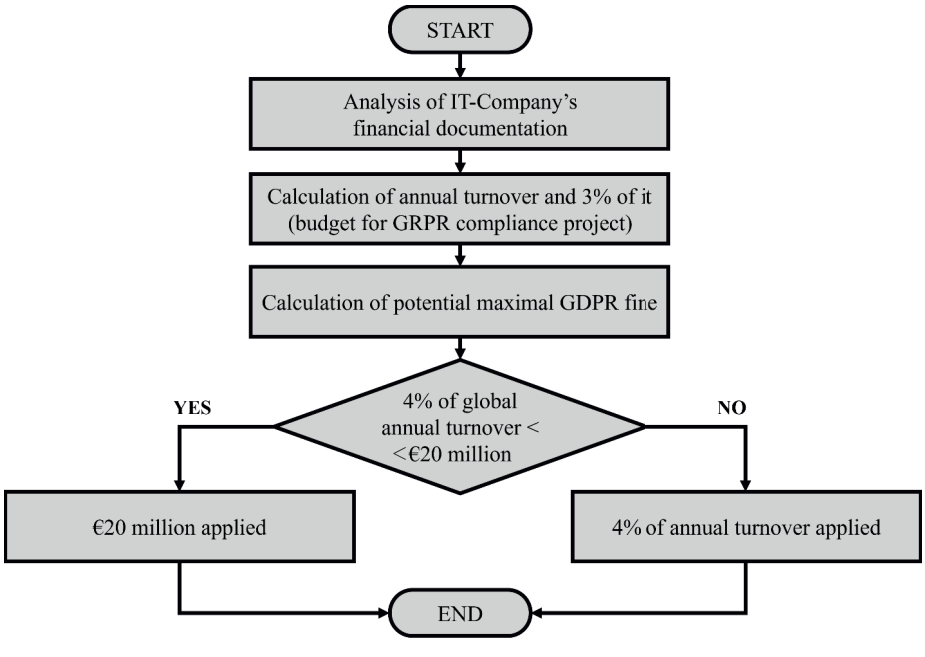

Fig. 2. GDPR fine calculation algorithm

Table 4

Salary of employees involved in project

Position	Required headcount	Qualification level (seniority)	Min. salary (USD)	Max. salary (USD)	Min. salary (UAH)	Max. salary (UAH)
Project manager/Product owner	1	Senior	3500	4000	140000	160000
Software developers (full-stack or frontend and backend)	2–3	1 Senior	5000	6250	200000	250000
		2 Middle	3000	3500	120000	140000
Security engineer/DevOps	1	Senior	5500	7500	220000	300000
QA/Test Engineer	1	Middle	2000	2800	80000	112000
TOTAL	5–6	–	22000	–	880000	962000

Annual payroll tax liabilities for the personnel assigned to the project, calculated based on current statutory rates, are summarized in Table 5 [37–41].

The next category of required expenditures includes the minimum necessary set of equipment, software, services, and relevant licenses. The calculations for these costs are presented in Table 6 [42–44, 46].

In addition to equipment and software expenditures, it is essential to obtain certification according to ISO 27001, conduct software audits, and ensure the creation and regular updating of documentation. The breakdown of these costs is provided in Table 7 [44, 45].

Given the factors mentioned above, specifically that the company risks losing two years of profit if the maximum GDPR fine is imposed, it is appropriate to calculate expenditures for this period (where the first year is dedicated to development, and the second year to refinement and implementation).

The expenditures for the second research year are presented in Table 8.

To simplify subsequent calculations, it is appropriate to aggregate expenditures into the following groups: personnel costs, payroll taxes, equipment and software, and additional expenses. Furthermore, to conduct the Monte Carlo simulation, it is necessary to calculate the mean (average) values and the standard deviation for each category group. The standard deviation is calculated assuming a 90% confidence interval.

Table 5

Annual payroll tax calculation for project personnel

Position	Number of employees	Min. PIT (UAH)	Max. PIT (UAH)	Min. military tax (UAH)	Max. military tax (UAH)	Min. USC (UAH)	Max. USC (UAH)
Project manager/Product owner	1	302400	345600	25200	28800	422400	422400
Software developers (full-stack or frontend and backend)	2–3	432000	540000	36000	45000	422400	422400
		518400	302400	21600	25200	422400	422400
Security engineer/DevOps	1	475200	648000	39600	54000	422400	422400
QA/Test engineer	1	172800	241920	14400	20160	211200	422400
TOTAL	5–6	1900800	2077920	136800	173160	1900800	2112000

Table 6

Expenditures for equipment and software

Expenditure category	Min cost (USD)	Max cost (USD)	Min cost (UAH)	Max cost (UAH)
Workstations (laptops for 6 employees)	6000	9000	240000	360000
Server equipment and annual cloud resource fees	4000	7500	160000	300000
Networking equipment (routers, VPN servers, etc.)	1500	3000	60000	120000
Software (licenses for IDE, version control, CI/CD, DBs, testing tools) per year	3000	4500	120000	180000
Security and encryption systems per year	1600	2900	64000	116000
Data backup and recovery systems per year	700	1300	28000	52000
TOTAL	16800	28200	672000	1128000

Table 7

Additional expenditures

Expenditure category	Min cost (USD)	Max cost (USD)	Min cost (UAH)	Max cost (UAH)
Certification and audits (ISO 27001:2022, ISO 27701)	20000	25000	800000	1000000
Documentation development and staff training	1500	2500	60000	100000
Other audits and consulting services	12000	20000	480000	800000
TOTAL	33500	47500	1340000	1900000

Table 8

Project expenditures for the second year

Expenditure category	Min costs (UAH)	Max costs (UAH)
Employee salaries	10560000	11544000
Payroll taxes	3938400	4363080
Server equipment and cloud service fees	160000	300000
Software	120000	180000
Security and encryption systems	64000	116000
Data backup and recovery systems	28000	52000
Audits and consulting	240000	400000
TOTAL	15110400	16955080

ISSN-L 2664-9969; E-ISSN 2706-5448

The corresponding values for the Monte Carlo simulation for the first and second years of the study are presented in Table 9.

Before conducting the Monte Carlo simulation for the in-house development project, it is essential to perform a comparative cost analysis for the outsourcing model. This involves delegating the storage, processing, and protection of personal data to third-party providers.

Furthermore, these calculations serve as the foundation for the sales department's pricing strategy. Since the company's long-term strategy includes the commercial sale of its proprietary software starting in the second year, the potential revenue from these sales will be factored into the Monte Carlo simulation results for the in-house project.

The baseline tools and measures required for an outsourcing-based approach to data protection include:

– *Cloud storage*: secure environments for data retention;

– *Data loss prevention (DLP) platform*: Tools to monitor and prevent unauthorized data transfers;

– *Compliance management platform*: software to ensure ongoing adherence to GDPR and other regulations;

– *Data protection officer (DPO) salary:* The cost of hiring a specialized professional to oversee data privacy;

– *Implementation and transition costs:* expenses related to integration, employee training, and the secure migration of data.

The estimated costs for these items are summarized in Table 10 [46–52].

The results of the calculations for the mean values and standard deviations for each of the expenditure categories mentioned above are presented in Table 11.

At this stage, the calculated mean expenditures for each category are utilized to develop a strategic commercial pricing proposal. This serves two purposes: it benchmarks the company's internal costs and establishes a competitive market entry price for the proprietary software starting in Year 2. Year 2 is considered as a testing phase of sales and as a period of software updates. The results of 2nd year become a basis for further changes in investment volumes and necessity project extension.

The breakdown of average annual costs per user/employee is as follows:

– *Cloud storage*: with an average annual cost of 2100 USD for 200000 users, the monthly cost per user is 2100 USD/200000/12 = = 0.000875 USD (rounded to 0.1 cents);

– *Data exchange and maintenance:* the monthly cost per user is 4800 USD/200000/12 = 0.002 USD;

– *DLP and compliance (internal):* the monthly cost per employee for internal security is 120000 USD/500/12 = 12.00 USD;

– *User compliance platform:* the monthly cost per user is 45000 USD/200000/12 = 0.01875 USD (rounded to 2 cents).

The average total integration cost is approximately 110000 USD (0.06 USD per user), and training costs included into the tariff are roughly 17500 (0.7 cents per user) out of a total expenditure of 455400 USD.

Table 9

Input data for Monte Carlo simulation (proprietary software development project)

Year	Aggregate expenditure category	Min. cost (UAH)	Max. cost (UAH)	Mean cost (UAH)	Z-value (for 90% CI)	Interval width	Standard deviation (UAH)
Year 1	Personnel	10560000	11544000	11052000	1.64	3.29	299114.76
	Equipment and software	672000	1128000	900000	1.64	3.29	138614.16
	Payroll taxes	3938400	4363080	4150740	1.64	3.29	129093.55
	Additional expenses	1340000	1900000	1620000	1.64	3.29	170227.91
Year 2	Personnel	10560000	11544000	11052000	1.64	3.29	299114.76
	Equipment and software	372000	648000	510000	1.64	3.29	83898.04
	Payroll taxes	3938400	4363080	4150740	1.64	3.29	129093.55
	Additional expenses	240000	400000	320000	1.64	3.29	48636.55

Table 10

Estimated costs for implementing third-party solutions (outsourcing)

Expense category	Monthly fee (USD)		Annual costs (USD) Min		Two-year period total (USD)	
	Min	Max	Min	Max	Min	Max
Cloud environment (10 TB subscription)	150	200	1800	2400	3600	4800
Data storage and exchange fees	300	500	3600	6000	7200	12000
DLP and compliance platform (for 500 employees)	7500	12500	90000	150000	180000	300000
Compliance management (for 200k users)	3000	4500	36000	54000	72000	108000
DPO salary (contract-based)	10000	16000	120000	192000	240000	384000
Integration and implementation (one-time fee)	–	–	100000	120000	100000	120000
Staff training	–	–	15000	20000	30000	40000
TOTAL	–	–	366400	544400	632800	968800

Table 11

Input data for Monte Carlo simulation (third-party solution)

Expenditure category	Min. cost (USD)	Max. cost (USD)	Mean cost (USD)	Z-value (90% CI)	Interval width (Z-spread)	Standard deviation (USD)
Cloud environment (10 TB)	3600	4800	4200	1.64	3.29	364.77
Data storage and exchange	7200	12000	9600	1.64	3.29	1459.1
DLP and compliance platform (for 500 employees)	180000	300000	240000	1.64	3.29	36477.41
Compliance management platform (for 200000 users)	72000	108000	90000	1.64	3.29	10943.22
DPO salary (contract-based)	240000	384000	312000	1.64	3.29	43772.89
Integration and implementation	100000	120000	110000	1.64	3.29	6079.57
Staff training	30000	40000	35000	1.64	3.29	3039.78

When analyzing these figures against the total cost structure: integration and Implementation account for approximately 25% of total expenditures, staff training accounts for approximately 4% of total expenditures.

By averaging these values, the baseline cost per user for the software service is estimated at approximately 0.023 USD.

Based on current market structures and competitor offerings, the following subscription tiers have been developed. These tiers are differentiated by the number of protected employees and the volume of external users:

– *Package S*: up to 25 employees and 50000 users;
– *Package M*: 26–50 employees and up to 100000 users;
– *Package L*: 51–75 employees and up to 250000 users;
– *Package XL*: 76–125 employees and up to 500000 users.

Note: for clients exceeding 125 employees or 500000 users, individual enterprise solutions will be offered and are excluded from this general forecast.

The maximum cost for each tariff is calculated assuming full utilization of the employee and user quotas. The calculation prioritizes the number of employees as the primary value driver, acknowledging that companies with 25+ staff may not always reach the user maximum (e. g., 100000 users).

By multiplying the capacity limits of each tier by the average unit costs calculated above, it is possible to derive the maximum monthly and annual values for each package. The calculation of maximum tariff values is given in Table 12.

It is also expedient to calculate the minimum potential tariff value based on the following assumptions: the minimum number of employees for Package S is set at 5, while for other packages; it is the lowest possible number within the respective range. The minimum number of users is assumed to be 5000 for Packages S and M, and 50000 for Packages L and XL.

These calculations help establish the "lower bound" of potential revenue, accounting for companies that may have the required staff but have not yet scaled their user base to the maximum limit of the tier.

The results of these calculations are presented in Table 13.

The penultimate step before determining the final pricing proposal for each package is to calculate the weighted average cost based on a sample of 100 clients. This calculation is built upon the following distribution assumptions regarding service utilization:

– 50% of clients utilize the minimum volume of services;
– 35% of clients utilize the average volume (the mean between minimum and maximum values);
– 15% of clients utilize the maximum volume of services.

This weighted approach provides a more realistic revenue forecast than simple averaging, as it accounts the market reality that a majority of subscribers often occupy the lower end of a tier's capacity. The results of these calculations are presented in Table 14.

Table 12

Calculation of maximum tariff values

Package name	Max. number of employees	Max. number of users	Price based on employees (USD)	Price based on users (USD)	Total price (USD)
S	25	50000	500	1150	1650
M	50	100000	1000	2300	3300
L	75	250000	1500	5750	7250
XL	125	500000	2500	11500	14000

Table 13

Calculation of minimum tariff values

Package name	Min. number of employees	Min. number of users	Price based on employees (USD)	Price based on users (USD)	Total price (USD)
S	5	5000	100	115	215
M	26	5000	520	115	635
L	51	50000	1020	1150	2170
XL	76	50000	1520	1150	2670

Table 14

Calculation of service costs per tariff

Package name	Utilization assumption	Percentage of clients	Number of clients (per 100)	Total category Value (USD)
S	min	50%	50	10750
	mid	35%	35	32638
	max	15%	15	24750
	Average monthly revenue per client (ARPU): 681 USD			
M	min	50%	50	31750
	mid	35%	35	68863
	max	15%	15	49500
	Average monthly revenue per client (ARPU): 1501 USD			
L	min	50%	50	108500
	mid	35%	35	164850
	max	15%	15	108750
	Average monthly revenue per client (ARPU): 3821 USD			
XL	min	50%	50	133500
	mid	35%	35	291725
	max	15%	15	210000
	Average monthly revenue per client (ARPU): 6352 USD			

ISSN-L 2664-9969; E-ISSN 2706-5448

By applying a 30% profit margin and performing minor rounding, the calculated baseline costs for the tariffs are established. However, to ensure these prices are competitive and marketing-attractive, they have been rounded up to the nearest logical threshold. Market price is given in Table 15. To calculate the total margin and one-time fees (integration and training), the following market penetration distribution is assumed for the sales forecast:

– *Package S:* 75% of total sales;
– *Package M:* 15% of total sales;
– *Package L:* 7% of total sales;
– *Package XL:* 3% of total sales.

Results of margin, integration costs and staff training costs calculation are given in Table 16.

Once the tariff plan pricing is finalized and the integration and training costs are calculated, the sales department proceeds to forecast the number of potential deals to be signed over the next three years. This forecast also accounts for a potential churn rate of 0.1% per annum, representing the expected loss of customers over time.

The sales forecast is illustrated in Fig. 3.

Based on the forecast provided above, it is now possible to calculate the client base and profit. The results of these calculations are graphically represented in Fig. 4.

Table 15

Formulation of tariff price

Package name	Calculated cost (+30% margin)	Final market price (monthly)
S	885 USD	1000 USD
M	1951 USD	2000 USD
L	4967 USD	5000 USD
XL	8258 USD	8500 USD

Table 16

Calculation of margin, integration costs, and staff training

Package name	Tariff cost basis (USD)	Rounded price (USD)	Rounded margin (%)	Sales share (%)	Integration cost (USD)	Staff training cost (USD)
S	681	1000	32%	75%	3000	480
M	1501	2000	25%	15%	6000	960
L	3821	5000	24%	7%	15000	2400
XL	6352	8500	25%	3%	25500	4080

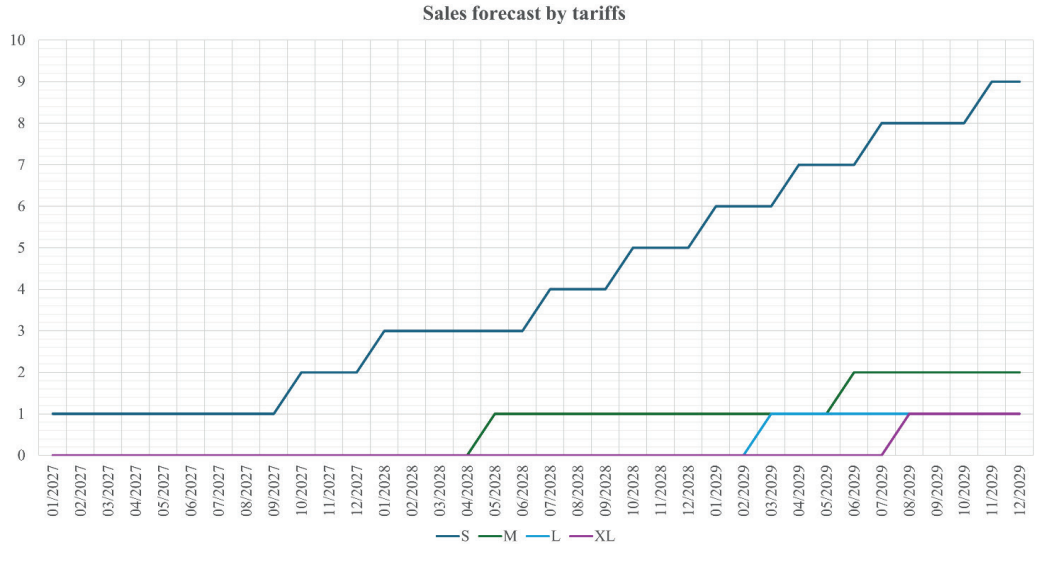

Fig. 3. Sales forecast by tariff tiers

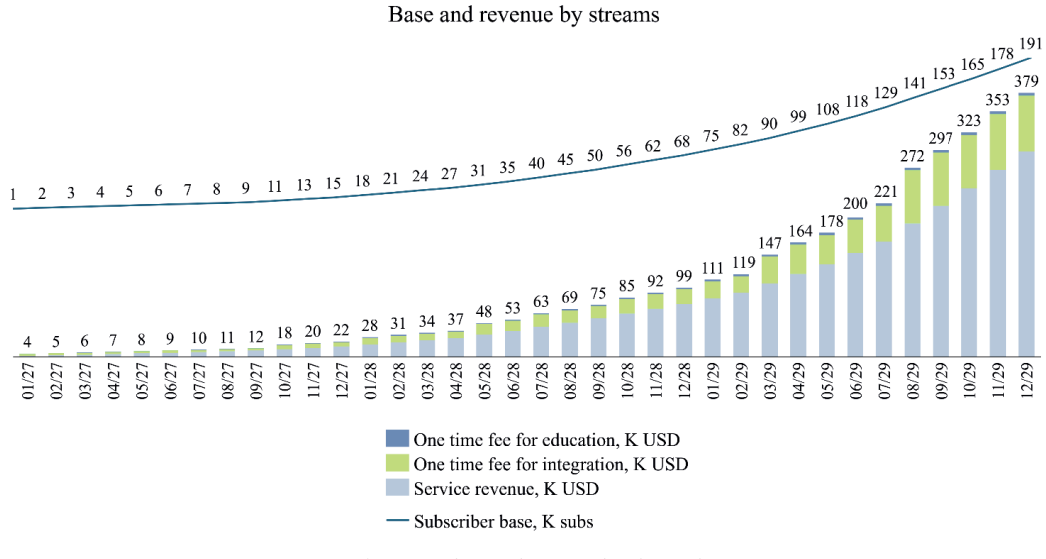

Fig. 4. Total customer base and revenue distribution by streams

Based on the projections, the calculation of revenue streams distributed by year is presented in Table 17.

The 2027 profit amount, excluding VAT, will be subsequently factored into the Monte Carlo simulation for the in-house development scenario. Based on the calculations performed, it is now possible to conduct a Monte Carlo simulation for the in-house development scenario. To achieve a more accurate distribution of costs, it is advisable to run 2000 or more simulations. A portion of the cost values for one of the iterations (noting that cost values change constantly after any document updates, which is a specific feature of the RANDOM() function in Microsoft Excel) is presented in Table 18.

Table 17

Calculation of revenue by streams

Revenue category	2027	2028	2029
Service revenue (subscription), USD	84000	513000	2063500
Service revenue, UAH	3360000	20520000	82540000
Service revenue (excl. VAT), UAH	2800000	17100000	68783333
One-time integration revenue, USD	45000	183000	658500
One-time integration revenue, UAH	1800000	7320000	26340000
One-time integration revenue (Excl. VAT), UAH	1500000	6100000	21950000
One-time training revenue, USD	7200	29280	105360
One-time training revenue, UAH	288000	1171200	4214400
One-time training revenue (excl. VAT), UAH	240000	976000	3512000
TOTAL REVENUE, USD	136200	725280	2827360
TOTAL REVENUE (Excl. VAT), USD	113500	604400	2356133
TOTAL REVENUE, UAH	5448000	29011200	113094400
TOTAL REVENUE (Excl. VAT), UAH	4540000	24176000	94245333

Table 18

Results of a Monte Carlo simulation iteration for the in-house development scenario

SCN	2027 expenditures (UAH)				TOT EXP, USD	2028 expenditures (UAH)				TOT EXP, USD	REV, USD	TOT, USD
	PER	EQP	TAX	ADD		PER	EQP	TAX	ADD			
1	2	3	4	5	6	7	8	9	10	11	12	13
1	11328217	1100479	4274999	1475396	454477	11514233	581865	4111832	279818	412194	113500	753171
2	11295543	1052986	4159015	1690740	454957	11088367	559085	4398018	334683	409504	113500	750961
3	11180929	893672	4138003	1649425	446551	11312117	515640	3996589	305112	403236	113500	736287
4	10487774	698470	4164338	1168711	412982	11160171	590825	4292781	215179	406474	113500	705956
5	11496839	1116522	4251727	1928523	469840	10878201	320534	4007906	266084	386818	113500	743158
6	10564671	741293	4267415	1524197	427439	11235179	557767	4017579	365180	404393	113500	718332
7	10938033	937170	4209405	1543237	440696	10992098	492054	3928507	317495	393254	113500	720450
8	10863134	1001943	4193633	1673990	443318	10766526	512107	4101260	260515	391010	113500	720828
9	11018719	839443	4227452	1681897	444188	11015816	497910	4471531	223018	405207	113500	735895
10	10933439	894648	3919557	1597034	433617	11001586	413808	4238675	433664	402193	113500	722310
11	11101855	827568	4108602	1894369	448310	11375461	413330	4272079	379313	411005	113500	745814
12	11425594	985824	4162025	1678151	456290	11025341	482263	4419400	311811	405970	113500	748760
13	10992747	878428	4324127	1565610	444023	11340496	439045	3963286	294359	400930	113500	731452
14	11034287	1069860	4006815	1416435	438185	10742329	458418	4090797	304579	389903	113500	714588
15	10933569	1027754	4109573	1610716	442040	11187372	485716	4449373	368924	412285	113500	740825
16	11258102	1250451	4150947	1746182	460142	10794383	506179	4017990	332047	391265	113500	737907
17	10696241	986440	4016731	1480067	429487	11104915	664232	4247903	307633	408117	113500	724104
18	11283045	1028241	4177807	1689718	454470	11211982	430228	4056392	370014	401715	113500	742686
19	10660129	808149	4087330	1632353	429699	10743710	424938	4061850	354712	389630	113500	705829
20	11413051	876972	4209050	1485875	449624	10926324	551985	4117883	244165	396009	113500	732133
1981	11272347	905056	4231033	1636260	451117	11372986	476982	4077859	345937	406844	113500	744461
1982	10842839	786282	4061997	1423029	427854	10399766	559805	4275360	254491	387236	113500	701589
1983	10741640	684456	4000845	1430646	421440	10791203	370925	4380121	321726	396599	113500	704539
1984	11393271	874222	4040624	1562623	446768	11667169	546781	3915394	354055	412085	113500	745353
1985	11140539	625219	4062970	1378470	430180	10877047	496401	4558703	338661	406770	113500	723450
1986	11589562	588858	4284043	1579383	451046	10991975	576631	4435188	336016	408495	113500	746041
1987	10942672	471921	4372143	1649504	435906	10924117	427752	3896970	265801	387866	113500	710272
1988	10516145	1009833	4104181	1565220	429884	10612868	621096	4487876	342483	401608	113500	717993
1989	10746803	730319	4172833	1695767	433643	11163711	594341	4161946	456603	409415	113500	729558
1990	10741312	858936	4078542	1782805	436540	11118806	382034	4108088	384657	399840	113500	722880
1991	10911715	961002	4062336	1543772	436971	11271986	707806	4373685	281864	415884	113500	739354
1992	10884312	1044349	3937189	1486758	433815	11266283	571390	4196977	197578	405806	113500	726121
1993	10915255	786180	4004971	1754141	436514	11277879	728773	4157153	337560	412534	113500	735548
1994	10935556	988056	4270413	1531674	443142	10972742	499674	4163416	266981	397570	113500	727213
1995	10986672	673396	4217028	1725571	440067	11645608	575659	4083693	389173	417353	113500	743920
1996	10550817	734191	4303321	1336398	423118	11040583	596666	4144605	382969	404121	113500	713739
1997	10727979	924368	4282509	1539807	436867	10761989	526589	4384575	335799	400224	113500	723590
1998	11046979	766000	4253760	1708284	444376	11458357	474978	4194038	262702	409752	113500	740627
1999	10615716	744909	4019481	1516022	422403	11005819	472192	4122212	389455	399742	113500	708645
2000	11272791	1087537	4056881	1709075	453157	11037359	634270	4086242	297331	401380	113500	741037

Notes: SCN – number of scenario, PER – expense for personnel, UAH; EQP – expenses for hardware and software, UAH; TAX – taxes for personnel, UAH; ADD – additional expenses, UAH; TOT EXP – total of expenses, USD; REV – revenue without VAT, USD; TOT – total expenses for 2-year period

ISSN-L 2664-9969; E-ISSN 2706-5448

Based on the results of the 2000 simulations, it is now possible to construct a histogram representing the distribution of total project costs over the two-year period. This distribution is illustrated in Fig. 5.

According to the conducted simulation, it is possible to observe that the most probable costs fall within the range of 725000–730000 USD.

The next step is to perform a corresponding cost simulation for the risk transfer scenario (outsourcing or purchasing a ready-made solution).

The results of one iteration of the two-year cost simulation are presented in Table 19.

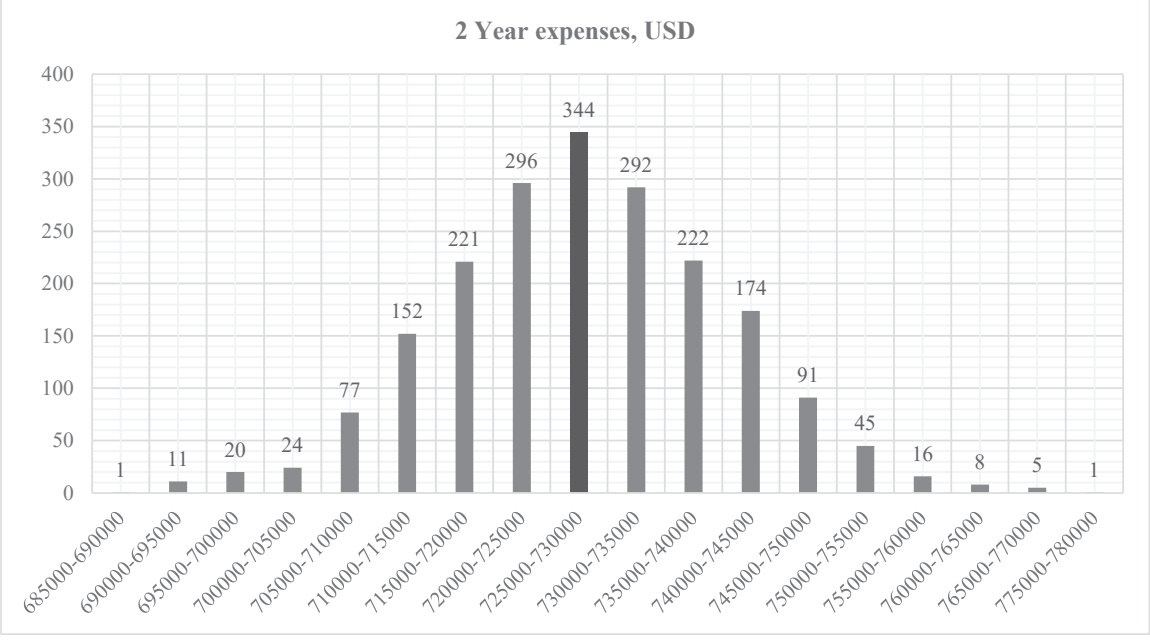

Fig. 5. Two-year expenditures for the in-house software development project

Table 19

Results of a Monte Carlo simulation iteration for the third-party solution acquisition project

SCN	CS	S&D	DLP	CMP	DPO	I&I	TRN	TOTAL USD
1	2	3	4	5	6	7	8	9
1	4305	6957	206519	75866	338159	110557	29993	772356
2	4717	10295	283669	95504	326529	123606	32415	876734
3	4034	6736	238457	102650	256432	105935	36126	750371
4	4106	11315	263086	91383	327387	110366	36723	844367
5	4132	13250	209523	97652	335574	118464	37405	816000
6	4605	10702	250701	78749	314019	108104	31827	798707
7	4243	9670	235499	82601	310391	111020	38476	791900
8	4148	10626	288957	68611	373190	110520	36571	892624
9	4242	10512	156352	78705	362335	107548	35937	755630
10	4474	10323	211660	97109	335981	113479	28298	801325
11	4905	9010	282941	76790	263975	110061	34130	781812
12	4030	10283	268898	90429	295053	109066	35819	813578
13	4250	11527	264133	92897	297260	107419	35186	812672
14	4214	10351	271023	84462	273964	110873	39705	794592
15	4565	6055	267783	100859	318008	108872	31085	837228
16	4122	8648	223159	100514	390717	116901	27464	871524
17	3813	6646	271865	98294	301195	119520	39198	840531
18	4127	8232	304033	76113	365878	115042	34953	908379
19	4929	9834	259375	101051	371829	103513	35804	886336
20	4537	11873	265095	103922	297133	107511	34770	824840
1981	4182	8047	219254	100712	310141	108271	33038	783645
1982	4613	9051	245841	98203	281537	116047	35230	790523
1983	4079	7778	277295	93052	368093	112873	30203	893373

Continuation of Table 19

1	2	3	4	5	6	7	8	9
1984	3845	10449	207271	92517	292365	111715	35518	753679
1985	4193	10243	205720	88738	255340	107547	33257	705039
1986	4052	9408	285346	92502	241744	107662	31847	772560
1987	4207	9805	186226	97312	239886	98003	36283	671722
1988	4485	8201	269670	92209	260999	114487	34774	784825
1989	4165	10250	277733	74291	388157	107898	35849	898342
1990	4296	10616	270987	100318	280728	112872	32559	812376
1991	4192	8370	219712	85875	323628	108583	32806	783165
1992	3835	7287	188066	87643	319037	109545	37294	752706
1993	4336	8323	252232	83276	348179	105845	31976	834167
1994	4191	10706	214788	85415	369622	112284	31331	828338
1995	4135	9104	286328	83598	377386	115662	43512	919725
1996	4607	11130	234029	94143	260777	112946	34723	752356
1997	4004	8138	215384	82592	249868	112734	34805	707525
1998	4695	7951	313872	107208	294343	96595	30203	854867
1999	5048	8548	193250	110861	268923	107239	42588	736457
2000	4176	9398	291914	88007	226599	112561	38603	771259

Notes: SCN – number of scenario, CS – cloud storage expenses, USD; S&D – data transfer and storage subscription, USD; DLP – DLP platform subscription price, USD; CMP – compliance platform price, USD; DPO – data protection officer salary, USD; I&I – price for integration and implementation, USD; TRN – training price, USD; TOTAL – total expenses, USD

The corresponding histogram of the simulation results distribution is shown in Fig. 6.

According to the conducted simulation, the most probable amount of expenditures will fall within the range of 800000 to 810000 USD.

Considering the profit percentage previously determined by management that can be invested in personal data protection tools, and the minimum annual investment amount (386453 USD), the total minimum investment over a two-year period will amount to 772906 USD. This sum serves as the benchmark for calculating the probability of the project's budget overrun risk.

Based on the simulation results and accounting for the potential revenue from selling proprietary software, the organization will not incur additional losses to implement the project: actual costs will be approximately 43000–48000 USD less than the projected minimum investment (resulting in a savings of 5.5–6.2% of the investment amount). Simultaneously, the probability that costs will exceed 770000 USD is only 0.3%. A significant advantage of in-house development is that the initial investments (first-year costs) of 425000–430000 USD will be recouped in September 2028, specifically 21 months after the start of sales.

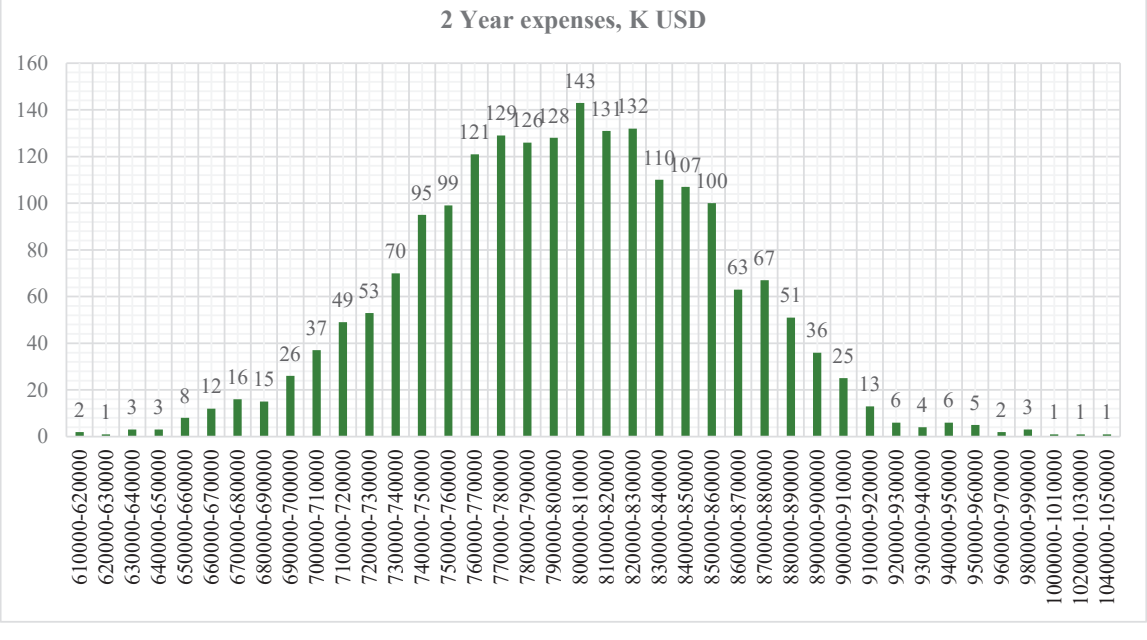

Fig. 6. Cost distribution over a two-year period for the project of acquiring ready-made solutions from a third party

ISSN-L 2664-9969; E-ISSN 2706-5448

In the case of purchasing software and services from a third party (outsourcing), the most likely expenditure will be 800000–810000 USD, which exceeds the allocated budget by 27000–37000 USD (or by 3.4–4.8%). The overall probability that the expenditure for this scenario will exceed the 770000 USD limit is approximately 69.5%. This probability is critically high. If the strategy of purchasing a ready-made product is chosen, management must decide either to abandon the project or to increase the share of investment in data protection to 3.5–4% of the organization's net profit.

3.3. Discussion

The research conducted by the authors shifts the conventional understanding of risk management approaches. Unlike the studies mentioned above [1, 2], risks are considered here not as isolated variables but as a complex of interconnected factors. The volatility of technology, the constant need for adaptation of the company's structure and corporate culture, and the influence of the external environment significantly impact project outcomes and, consequently, the organization's financial performance. Risks in the digital technology world, to which the IT industry belongs, are highly sensitive to environmental changes that can occur at lightning speed and pose a threat to business continuity. Furthermore, a vital aspect of conducting business in the IT sector is the necessity to keep pace with technological advancements and continuously monitor changes in regulatory documents, as a missed stage of development or a neglected recommendation can lead to significant financial and reputational losses.

The modern way of doing business in the IT industry relies not only on financial reports but also on intellectual capital, innovation, corporate culture, and data protection. Ignoring these factors can lead to incorrect strategic decisions. Research [3] proves that considering both financial and non-financial information provides a more realistic picture of existing risks. For many IT companies, intangible assets are the dominant factor in business existence, as they encompass unique ideas and approaches to specific solutions. An approach that accounts for intangible assets is an effective way not only to save costs but also to preserve reputation, protect intellectual property, and counteract disruptions and cyber threats. It is also worth noting that the results of this research align with the opinions of other experts regarding the necessity of considering the impact of one risk on another. Studies [2, 11] have proven the feasibility of an integrated approach to risk analysis and control, accounting for their interconnections, as viewing each risk in isolation can lead to improper prioritization of their mitigation. Consequently, under modern circumstances, a standard risk register will be insufficient for organizational management; therefore, it is necessary to create more advanced reports and dashboards that account for the interconnections between risks.

From a methodological standpoint, the study conducted by the authors aligns precisely with the modern trend in risk management. The proposed methodologies can be enhanced through artificial intelligence, machine learning, and big data technologies. Positive examples from authors [9, 10] prove that new technologies – provided there is a critical approach from management and tolerance toward implementing changes in organizational processes – help to better identify and forecast project and investment risks. This approach is also supported by study [6]. It is also important to note that risk management in the modern era must be part of the corporate culture and the decision-making approach. Additionally, it is crucial that any analysis conducted by artificial intelligence requires a critical approach to the evaluation and interpretation of the data obtained, which can only be performed by qualified specialists.

The modern digital economy disrupts older, more conservative management principles, such as ESG, which were primarily used in construction and infrastructure [17, 18], where projects are viewed over long timeframes (years). It forces organizations to transition into the digital sphere, where changes are tracked much faster, allowing for more rapid measures to prevent negative consequences.

In modern conditions, organizations face new risks, such as data protection, the energy efficiency and environmental friendliness of data centers, the ethics of using artificial intelligence, and digital equity. An incorrect approach to controlling such risks can lead to monetary sanctions, multi-million-dollar lawsuits, and a loss of organizational reputation.

The information technology industry is one of the most dynamic in its development; accordingly, project requirements and the projects themselves can change weekly, necessitating the constant adaptation of business models to a shifting environment. Therefore, creating a universal approach to risk management is a complex task. The integration of artificial intelligence into risk management processes does not simplify the situation, as the quantity and quality of input data are vital for its use. Another important aspect of using AI tools is the need for staff training to create correct and relevant queries and input appropriate data. In light of these aspects, a large gap is forming between large and small companies.

It is precisely such difficulties that compel researchers and practitioners from various fields to seek flexible tools that can be relatively easily adapted for each company. Thus, risk management will become more accessible and effective for organizations of various scales. Therefore, the search for better technological solutions, the flexibility of strategic vision, and the refinement of the decision-making and problem-response processes constitute the essence of this research. Accounting for the aforementioned factors is the key to successful business conduct in the field of information technology.

The methodology proposed in this research has several limitations, which include the following:

– the results of the calculations directly depend on the quality and relevance of the input data, which include sensitive commercial confidential information and data from internal reports; therefore, this type of analysis can only be performed by specialists or departments with a high level of access to corporate financial information acting under NDA;

– the proposed methodology for IT projects financial risks analysis is based on retrospective data; however, because IT projects are characterized by a high level of innovation, short product life cycles, and dependence on technological trends, it becomes difficult to use such data for costs forecasting.

Future research should include a wider application of Monte Carlo simulations within general risk management processes, allowing for the analysis of risks beyond those related to GDPR or compliance.

Additionally, it is possible to expand the volume of input data for more detailed analysis and to apply this approach to projects outside the field of software development.

Another direction for future research is the integration of sales forecasting, sales monitoring tools, and CRM systems with Monte Carlo simulations, which will facilitate the live analysis of project risks involving the sale of products and services.

Furthermore, the integration of Monte Carlo simulations with Big Data technologies represents a promising perspective for future research, as this can support the creation of real-time risk management dashboards for stakeholders.

4. Conclusions

1. In the process of the research performed by authors, an algorithm of GDPR violation penalties forecast based on the financial performance indicators of IT companies was developed. The developed algorithm serves to facilitate the budgeting of projects addressed to minimize the risk of personal data breaches. According to calculation of the organization's financial indicators, it was revealed that in the event

of a personal data breach and application of maximum sanctions for violation of GDPR-requirements, the organization would face a fine of 20 million EUR. Such penalty can lead to a potential loss of profit for over a 22-month period (assuming minimum profit levels). Additionally, it was determined that projected budget for GDPR compliance projects should be approximately 770 thousand USD (for a two-year planning horizon).

2. The research improves the methodology of financial risks of IT-projects analysis by integrating scenario analysis and Monte Carlo method. This approach allowed to justify the choice of optimal decision aimed to minimize financial losses of IT projects. The following indicators are the results of conducted analysis: the most probable cost range (considering potential profit) for an in-house development project is between 725000 and 730000 USD, while the alternative project of third-party package acquisition shows costs between 800000 and 810000 USD. According to conducted modelling, the project of in-house development remains withing the planned investment volumes and has a critically low risk (0.3%) of budget overrun. Furthermore, according to sales predictions, the maximum payback period for initial investments is around 21 months with a transition to profit starting from third year from the date when development started. Monte Carlo modelling for third-party solutions acquisition shown extremely high probability (69.5%) of budget overrun. In this case, such high risk of budget overrun can motivate the company's management to search for alternative solutions as probability of remaining within planned budget is only 30.5% while the probability of exceeding the volume of planned investments by more than 100000 USD is 11%. Such high risk is no acceptable for company's long-term strategy.

Conflict of interest

The authors declare that there are no conflicts of interest regarding this research, including financial, personal, authorship, or any other factors that could have influenced the research or the results presented in this work.

Funding

This research was conducted without external financial support.

Data availability

All data are available in numerical or graphical form within the main body of the manuscript.

Use of artificial intelligence

The authors state that generative artificial intelligence tools were used exclusively for language editing, grammar checking of the manuscript under full human control.

Tool used: Gemini (Google Gemini 3).

The authors bear full responsibility for the final manuscript.

Declaration is submitted by Anton Ostapets.

Authors' contributions

Anton Ostapets: Resources, Formal analysis, Visualization, Data curation, Writing – original draft; ***Iryna Parasii-Verhunenko*:** Conceptualization, Methodology, Investigation, Writing – original draft; ***Kostiantyn Bezverkhyi:*** Writing – review and editing, Validation, Supervision, Project administration; ***Mykola Matiukha:*** Funding acquisition, Data curation, Writing – review and editing; ***Oleksandr Yurchenko:*** Funding acquisition, Visualization.

References

1. Akomea-Frimpong, I., Jin, X., Osei-Kyei, R. (2020). A holistic review of research studies on financial risk management in public–private partnership projects. *Engineering, Construction and Architectural Management, 28 (9),* 2549–2569. https://doi.org/10.1108/ecam-02-2020-0103
2. Bai, L., Shi, H., Kang, S., Zhang, B. (2021). Project portfolio risk analysis with the consideration of project interdependencies. *Engineering, Construction and Architectural Management, 30 (2),* 647–670. https://doi.org/10.1108/ecam-06-2021-0555
3. Bezverkhyi, K., Hnylytska, L., Yurchenko, O., Poddubna, N. (2023). Analytical procedures of the audit of integrated reporting of corporate enterprises. *Financial and Credit Activity Problems of Theory and Practice, 3 (50),* 87–101. https://doi.org/10.55643/fcaptp.3.50.2023.4045
4. Chen, H. L. (2023). Influence of supply chain risks on project financial performance. *International Journal of Production Economics, 260,* 108870. https://doi.org/10.1016/j.ijpe.2023.108870
5. Kim, B.-C. (2023). Dependence Modeling for Large-scale Project Cost and Time Risk Assessment: Additive Risk Factor Approaches. *IEEE Transactions on Engineering Management, 70 (2),* 417–436. https://doi.org/10.1109/tem.2020.3046542
6. Love, P. E. D., Ika, L. A., Matthews, J., Fang, W. (2024). Risk and Uncertainty in the Cost Contingency of Transport Projects: Accommodating Bias or Heuristics, or Both? *IEEE Transactions on Engineering Management, 71,* 205–219. https://doi.org/10.1109/tem.2021.3119064
7. Vegas-Fernández, F. (2022). Project Risk Costs: Estimation Overruns Caused When Using Only Expected Value for Contingency Calculations. *Journal of Management in Engineering, 38 (5).* https://doi.org/10.1061/(asce)me.1943-5479.0001064
8. Otniel, D., Claudiu, B., Lorena, B., Felician, A. (2019). Characteristics of Effective IT Project Risk Management in Romanian IT Companies. *Economic Computation and Economic Cybernetics Studies and Research, 53 (4/2019),* 177–193. https://doi.org/10.24818/18423264/53.4.19.11
9. Singh, B., Henge, S. K. (2021). Access Risk Management for Arabian IT Company for Investing Based on Prediction of Supervised Learning. *Journal of Risk Analysis and Crisis Response, 11 (3).* https://doi.org/10.54560/jracr.v11i3.300
10. Lipyanina, H., Maksymovych, V., Sachenko, A., Lendyuk, T., Fomenko, A., Kit, I. (2020). Assessing the Investment Risk of Virtual IT Company Based on Machine Learning. *Data Stream Mining & Processing,* 167–187. https://doi.org/10.1007/978-3-030-61656-4_11
11. Guan, L., Abbasi, A., Ryan, M. J. (2021). A simulation-based risk interdependency network model for project risk assessment. *Decision Support Systems, 148,* 113602. https://doi.org/10.1016/j.dss.2021.113602
12. Liang, D., Wang, M., Xu, Z., Chen, X. (2019). Risk interval-valued three-way decisions model with regret theory and its application to project resource allocation. *Journal of the Operational Research Society, 72 (1),* 180–199. https://doi.org/10.1080/01605682.2019.1654939
13. Liu, Z., Ding, R., Wang, L., Song, R., Song, X. (2023). Cooperation in an uncertain environment: The impact of stakeholders' concerted action on collaborative innovation projects risk management. *Technological Forecasting and Social Change, 196,* 122804. https://doi.org/10.1016/j.techfore.2023.122804
14. Ferreira de Araújo Lima, P., Marcelino-Sadaba, S., Verbano, C. (2021). Successful implementation of project risk management in small and medium enterprises: a cross-case analysis. *International Journal of Managing Projects in Business, 14 (4),* 1023–1045. https://doi.org/10.1108/ijmpb-06-2020-0203
15. Testorelli, R., Ferreira de Araújo Lima, P., Verbano, C. (2020). Fostering project risk management in SMEs: an emergent framework from a literature review. *Production Planning & Control, 33 (13),* 1304–1318. https://doi.org/10.1080/09537287.2020.1859633
16. Dhande, J., Rane, P., Dhande, H. (2025). Influence of Project Risk Management in Micro and Small-Scale Industries on Workers' Occupational Health to Enhance Productivity: An Ergonomic Approach. *International Journal of Industrial Engineering and Management, 16 (1),* 52–63. https://doi.org/10.24867/ijiem-370
17. Elseknidy, M., Al-Mhdawi, M. K. S., Qazi, A., Ojiako, U., Mahammedi, C., Rahimian, F. P. (2025). Developing a sustainability-driven risk management framework for green building projects: A literature review. *Journal of Cleaner Production, 519,* 145891. https://doi.org/10.1016/j.jclepro.2025.145891
18. Koc, K., Kunkcu, H., Gurgun, A. P. (2023). A Life Cycle Risk Management Framework for Green Building Project Stakeholders. *Journal of Management in Engineering, 39 (4).* https://doi.org/10.1061/jmenea.meeng-5361
19. Nguyen, H. D., Macchion, L. (2022). A comprehensive risk assessment model based on a fuzzy synthetic evaluation approach for green building projects: the case of Vietnam. *Engineering, Construction and Architectural Management, 30 (7),* 2837–2861. https://doi.org/10.1108/ecam-09-2021-0824

ISSN-L 2664-9969; E-ISSN 2706-5448

20. Wan, Q., Miao, X., Wang, C., Dinçer, H., Yüksel, S. (2023). A hybrid decision support system with golden cut and bipolar q-ROFSs for evaluating the risk-based strategic priorities of fintech lending for clean energy projects. *Financial Innovation, 9 (1).* https://doi.org/10.1186/s40854-022-00406-w
21. Nyqvist, R., Peltokorpi, A., Seppänen, O. (2024). Can ChatGPT exceed humans in construction project risk management? *Engineering, Construction and Architectural Management, 31 (13),* 223–243. https://doi.org/10.1108/ecam-08-2023-0819
22. Tian, K., Zhu, Z., Mbachu, J., Ghanbaripour, A., Moorhead, M. (2025). Artificial intelligence in risk management within the realm of construction projects: A bibliometric analysis and systematic literature review. *Journal of Innovation & Knowledge, 10 (3),* 100711. https://doi.org/10.1016/j.jik.2025.100711
23. Sivan, A., Priya, K. (2025). Quantum computing and risk prediction accuracy: an analysis of IT companies' risk appetite. *International Journal of Business and Systems Research, 19 (2),* 111–139. https://doi.org/10.1504/ijbsr.2025.145483
24. Nazarova, K., Bezverkhyi, K., Nezhyva, M., Hordopolov, V., Nehodenko, V. (2022). Regression analysis of operating profit of the company. *Financial and Credit Activity Problems of Theory and Practice, 4 (45),* 124–132. https://doi.org/10.55643/fcaptp.4.45.2022.3667
25. Parasii-Verhunenko, I., Yurchyshyn, Y., Bezverkhyi, K., Hryshchenko, N., Nazarova, K., Pryimak, N. (2023). Comparative analysis of efficiency and utilization completeness of resource potential in trading enterprises: methodological aspects. *Financial and Credit Activity Problems of Theory and Practice, 4 (51),* 245–260. https://doi.org/10.55643/fcaptp.4.51.2023.4099
26. Jiang, W., Jiang, J., Martek, I., Jiang, W. (2025). Critical risk management strategies for the operation of public–private partnerships: a vulnerability perspective of infrastructure projects. *Engineering, Construction and Architectural Management, 32 (7),* 4771–4795. https://doi.org/10.1108/ecam-12-2023-1292
27. Jiang, W., Martek, I., Hosseini, M. R., Chen, C. (2019). Political risk management of foreign direct investment in infrastructure projects: Bibliometric-qualitative analyses of research in developing countries. *Engineering, Construction and Architectural Management, 28 (1),* 125–153. https://doi.org/10.1108/ecam-05-2019-0270
28. Kaur, P., Askri, S., Majeed, J., Iqbal, N., Peel, R., Armosh, F. et al. (2025). Social Media's Contribution to Risk Management Strategies for UK-Based IT Companies. *Technology and Innovative Management as Drivers of Sustainable Progress,* 247–294. https://doi.org/10.4018/979-8-3373-2858-4.ch011
29. Nabawy, M., Gouda Mohamed, A. (2022). Risks assessment in the construction of infrastructure projects using artificial neural networks. *International Journal of Construction Management, 24 (4),* 361–373. https://doi.org/10.1080/15623599.2022.2156902
30. Naidu, Dr. K., Ghangare, Prof. A., Chhajer, K. (2019). Measurement of Volatility of Selected IT Companies in Context of National Stock Exchange and Assessment of Risk Factors From an Investor's Point of View. *International Journal of Recent Technology and Engineering (IJRTE), 8 (3),* 8491–8495. https://doi.org/10.35940/ijrte.c4889.098319
31. Nazarova, K., Bezverkhyi, K., Hordopolov, V., Melnyk, T., Poddubna, N. (2021). Risk analysis of companies' activities on the basis of non-financial and financial statements. *Agricultural and Resource Economics: International Scientific E-Journal, 7 (4),* 180–199. https://doi.org/10.51599/are.2021.07.04.10
32. Matthews, J., Love, P. E. D., Porter, S. R., Fang, W. (2022). Smart data and business analytics: A theoretical framework for managing rework risks in megaprojects. *International Journal of Information Management, 65,* 102495. https://doi.org/10.1016/j.ijinfomgt.2022.102495
33. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (2016). *European Union.* Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj
34. *GDPR Enforcement Tracker.* Available at: https://www.enforcementtracker.com
35. *LLC taxation in Ukraine.* Available at: https://buh.ua/en/taxation-of-llc
36. *Rynok orendy ofisnoi nerukhomosti v Ukraini (cherven 2025): tendentsii ta analityka* (2025). Available at: https://gisuvecon.com/main/105/rinok-orendi-ofisnoyi-neruhomosti-v-ukrayini-cherven-2025-tendenciyi-ta-analitika/
37. *Zarplaty menedzheriv v IT, lito 2025: yak zminylysia za piv roku* (2025). Available at: https://dou.ua/lenta/articles/salary-report-managers-summer-2025/
38. Salaries Software Engineer (Middle-Senior) (2025). *DOU.ua.* Available at: https://jobs.dou.ua/salaries/?period=2025-06&group=1&position=Software%20Engineer&title=4
39. Salaries Full Stack Software Engineer (Junior-Middle) (2025). *DOU.ua.* Available at: https://jobs.dou.ua/salaries/?period=2025-06&group=1&position=Software%20Engineer&title=3&specialization=Full%20Stack
40. Salaries Security Engineer (Senior) (2025). *DOU.ua.* Available at: https://jobs.dou.ua/salaries/?period=2025-06&group=7&position=Security%20Engineer&title=4&experience=5-10
41. Salaries Automation QA (Middle) (2025). *DOU.ua.* Available at: https://jobs.dou.ua/salaries/?period=2025-06&group=2&position=QA/QC/SDET&title=3&specialization=Automation%20QA
42. Noutbuky dlia biznesu. *TELEMART.UA* Available at: https://telemart.ua/ua/laptops/filter/for-business/?srsltid=AfmBOopsoxBVSijztL_N3NyfK-oU3q7MBuNL8HCB-jzTbq-ScW6NeilL8
43. Servery. *EServer.* Available at: https://e-server.com.ua/uk/aktivne-obladnannja/serveri
44. Software Development Costs: Your Comprehensive 2025 Guide (2025). *Fiverr International Ltd.* Available at: https://www.fiverr.com/resources/costs/software-development
45. Webb, K. (2022). How much does ISO 27001 certification cost? *Strike Graph.* Available at: https://www.strikegraph.com/blog/how-much-does-iso-2700-certification-cost
46. Gschwentner, M. (2025). Cheap Cloud Storage: Who Has the Best Value for Money? *EXPERTE.com.* Available at: https://www.experte.com/cloud-storage/cheap-cloud-storage
47. Data Loss Prevention Software Cost (2024). *Strac.* Available at: https://www.strac.io/blog/data-loss-prevention-software-cost
48. 10 Best Compliance Software for 2025: Compare Their Features, Pros, Cons and Pricing. *Scrut Automation.* Available at: https://www.scrut.io/post/best-compliance-software
49. Data protection officer salary guide Ireland. *Morgan McKinley.* Available at: https://www.morganmckinley.com/ie/salary-guide/data/data-protection-officer/ireland
50. Moore, M. *How to Become a Data Protection Officer.* Available at: https://onlinedegrees.sandiego.edu/data-protection-officer-career-guide/
51. *Internal vs. external data protection officer: Which is right for your business?* Available at: https://www.dataguard.com/en-gb/internal-vs-external-data-protection-officer/
52. Compliance automation software. *Usercentrics.* Available at: https://usercentrics.com/knowledge-hub/compliance-automation-software/

✉***Anton Ostapets,*** *PhD Student, Department of Financial Analysis and Audit, State University of Trade and Economics, Kyiv, Ukraine, ORCID: https://orcid.org/0000-0001-7048-6112, e-mail: a.ostapets@knute.edu.ua*

Iryna Parasii-Verhunenko, *Doctor of Economic Sciences, Professor, Department of Financial Analysis and Audit, State University of Trade and Economics, Kyiv, Ukraine, ORCID: https://orcid.org/0000-0001-6506-6965*

Kostiantyn Bezverkhyi, *Doctor of Economic Sciences, Associate Professor, Department of Financial Analysis and Audit, State University of Trade and Economics, Kyiv, Ukraine, ORCID: https://orcid.org/0000-0001-8785-1147*

Mykola Matiukha, *PhD, Associate Professor, Department of Economics, Kyiv National University of Technologies and Design, Kyiv, Ukraine, ORCID: https://orcid.org/0000-0002-7968-3777*

Oleksandr Yurchenko, *PhD, Department of International Economics, Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine, ORCID: https://orcid.org/0000-0002-8447-6510*

✉*Corresponding author*