Journal homepage: https://itce.vn.ua/en

Information Technologies and Computer Engineering **Vol. 22, No. 3. 2025**

Article's History: Received: 08.07.2025 Revised: 15.10.2025 Accepted: 23.12.2025

UDC 004.8:005.8 DOI: 10.31649/vitce/3.2025.125

Integrated assessment of system privacy: Formalisation, normalisation and differential privacy

Dmytro Prokopovych-Tkachenko*

PhD in Technical Sciences, Associate Professor
University of Customs and Finance
49000, 2/4 Volodymyra Vernadskoho Str., Dnipro, Ukraine
https://orcid.org/0000-0002-6590-3898

Liudmyla Rybalchenko

PhD in Economics, Associate Professor
University of Customs and Finance
49000, 2/4 Volodymyra Vernadskoho Str., Dnipro, Ukraine
https://orcid.org/0000-0003-0413-8296

Volodymyr Zvieriev

PhD in Technical Sciences, Associate Professor
State University of Trade and Economics
02156, 19 Kyoto Str., Kyiv, Ukraine
https://orcid.org/0000-0002-0907-0705

Borys Khrushkov

Postgraduate Student
University of Customs and Finance
49000, 2/4 Volodymyra Vernadskoho Str., Dnipro, Ukraine
https://orcid.org/0009-0002-3978-5012

Valerii Bushkov

Postgraduate Student
State University of Trade and Economics
02156, 19 Kyoto Str., Kyiv, Ukraine
https://orcid.org/0009-0005-5097-2689

Abstract. Requirements for confidentiality and greater data privacy are constantly growing. The aim of this work was to develop a formalised approach to assessing the privacy of information systems based on a vector representation of a set of parameters. In the proposed approach, each parameter has a numerical value within a defined range that reflects the degree of its implementation or importance. For convenience and structure, the parameters were divided into several categories (access control, encryption, logging, key management, risk management, and incident management) covering the main aspects of information security. The overall privacy indicator of the system was calculated using a weighted sum, where the weighting coefficients were refined depending on the criticality of each parameter. To unify the scales and ensure correct further analysis, normalisation methods (minimax and Z-normalisation) were applied, thanks to which the obtained parameter values can be compared and effectively integrated into the general model. The proposed method used differential privacy to protect source data and enhance privacy, which was achieved by adding random noise with a normal distribution. This step complicated the process of restoring the original indicators and minimised the risk of identifying specific records, while maintaining the accuracy of aggregate statistical estimates. The developed approach consisted of several sequential stages: from initial data categorisation and normalisation to the

Suggested Citation:
Prokopovych-Tkachenko, D., Rybalchenko, L., Zvieriev, V., Khrushkov, B., & Bushkov, V. (2025). Integrated assessment of system privacy: Formalisation, normalisation and differential privacy. *Information Technologies and Computer Engineering*, 22(3), 125-135. doi: 10.31649/vitce/3.2025.125

*Corresponding author

implementation of differential privacy and data analysis in a neural network. An important advantage was the ability to integrate various aspects of data protection into a single coherent system. This multidimensional concept promoted flexibility and allowed the solution to be quickly adapted to updated requirements or new threats. The presented model is particularly relevant in areas where sensitive data is processed: healthcare, banking and finance, as well as public administration and information security. The proposed approach lays the foundation for the development and scaling of secure and transparent systems that meet modern privacy standards

Keywords: information protection; secure neural networks; vector data normalisation; access to information; security assessment parameters; statistical noise; adaptive machine learning

Introduction

In the modern era of rapid digital transformation, the volume of data generated, transmitted and processed by information systems is growing so quickly that traditional protection approaches can no longer reliably meet confidentiality and privacy requirements. This issue is particularly pressing in areas where sensitive data are processed, such as healthcare, the financial sector, public administration and systems dealing with the security of critical information. In such contexts, it is crucial to choose comprehensive protection methods and integrate them into a unified system, taking into account the diversity of confidentiality parameters that affect the overall security level, as well as the fast-changing nature of threats and new regulatory requirements. Given the dynamics of technologies and threats, there is a need for methods capable not only of analysing current security conditions but also of adapting flexibly to the emergence of new challenges.

Among the key trends in ensuring confidentiality is the combination of deep learning methods with neuro-symbolic artificial intelligence. Thus, A. Piplai *et al*. (2023) described an innovative approach that integrates knowledge graphs and deep learning to enhance the interpretability of models in the field of cybersecurity. The integration of neural networks represents knowledge of the relevant subject area and allows artificial intelligence (AI) systems to reason, learn, and generalise in a way that is understandable to experts.

Among Ukrainian sources, O.M. Gumen & K.O. Rachek (2023) are noteworthy for their use of machine learning to predict space weather while ensuring privacy. This article discusses models for predicting the Dst index. One of the models uses a precision of 83.47%. Another model, Dst Transformer (DSTT), is designed for short-term forecasting and uses Bayesian inference. The DSTT model shows high accuracy and takes into account two types of uncertainties in the data. I. Grinko *et al*. (2023) presented an overview of quantum convolutional networks for interdisciplinary use, particularly in socio-economic systems. Modelling and forecasting complex natural processes has demonstrated their effectiveness in studying complex molecular structures. It has been established that quantum convolutional neural networks can provide more accurate and faster results compared to conventional data processing methods. The work of N. Zaplatynskyi *et al*. (2024) emphasised that the growth in data volumes and the increasing complexity of information flows require comprehensive approaches to their processing and protection, including the use of AI, and that confidentiality must be integrated at the system architecture level.

In response to growing privacy requirements in distributed data processing environments, integrated information security assessment is actively used in training. R. Shokri *et al*. (2017) demonstrated the danger of training models without privacy mechanisms. The CYBRIA development, presented by P. Thantharate & T. Anurag (2023), allows models to be trained without sharing raw data, which significantly reduces the risk of information leakage. This article describes how eco-symbolic AI can be useful in the fields of cybersecurity and privacy – two of the most demanding areas where AI must be understandable and at the same time highly accurate in complex conditions. A similar approach is taken in the study by S. Sav *et al*. (2023), which demonstrated the effectiveness of federated recurrent networks with privacy in mind. The researchers pay particular attention to differential privacy as a means of protecting personal data. H. Lee *et al.* (2023) proved the effectiveness of adding Gaussian noise in industrial data processing tasks. The MNP method has shown significant potential for making production systems both intelligent and secure, eliminating the risk of data leakage while maintaining the quality of AI models.

The feasibility of a comprehensive study of cybersecurity issues was presented in the work of O. Chubukova *et al*. (2020), which applies machine learning algorithms and risk identification features that occur in the banking sector, namely through the use of data science to detect fraud and model risks for investment institutions. The analysis of problem areas was investigated by V. Ivanichenko *et al.* (2021). The work uses machine learning in cybersecurity to implement important issues of creating a self-learning model for reliable protection in information security decision-making. O. Semenenko *et a*l. (2024) proved that integrated computer technologies increase the level of cybersecurity in the defence sector by ensuring the detection of and response to cyber threats. Regarding the prevention of security breaches, M.A. Fathullah *et al*. (2023) proposed cloud computing mechanisms using IT projects to control and prevent risks, threats, vulnerabilities, probabilities, consequences, and control procedures, which are

classified into separate risk classes for further management decision-making.

Thus, the issue of risk reduction and data privacy remains relevant, attracting increased interest from scientists and software developers. Consequently, there was still a need to develop a methodology based on a mathematical model that involves preliminary data normalisation using a multi-layer neural network for classification. The aim of the current study was to develop a formalised model for the integrated assessment of information system confidentiality, combining a mathematical representation of security parameters, multi-level normalisation, differential privacy mechanisms and the use of neural networks to ensure the protection of sensitive data in the context of modern cyber threats.

Materials and Methods

The study was conducted using a general methodology for building privacy assessment systems adapted to modern data protection challenges. The methodology included the sequential implementation of four stages. The first stage involved categorising parameters that reflect the main areas of confidentiality assurance: access control, encryption, logging, key management, risk and incident management, etc. This approach made it possible to systematically structure the characteristics of the system and identify critical areas. The second stage involved assessing the weighting coefficients of the parameters, taking into account industry criticality, the probability of threats being realised, and the consequences of their impact. An approach consistent with risk management practices in cloud environments was applied, as well as basic approaches to weighted analysis. In the third stage, data normalisation was performed using minimax and Z-transformation, which allowed the parameters to be standardised for further calculation and analysis. This ensured data compatibility for use in intelligent models. The fourth stage involved the implementation of differential privacy mechanisms. To do this, Gaussian or Laplace noise components were added to the normalised data, in accordance with current personal data protection practices.

In the final stage, a multilayer perceptron neural network (MLP) was used as the base model for classifying the confidentiality level of systems. This type of neural network is a classic form of a deep feedforward neural network, which consists of:

- an input layer that accepts vectorised privacy parameters;
- one or more hidden layers that implement nonlinear transformations;
- an output layer that forms the final assessment of the privacy level or classification (e.g., “low,” “medium,” “high” level).

The reasons for choosing MLP were: adaptability to different types of data after normalisation; compatibility with differential privacy mechanisms (especially when using DP-SGD); high accuracy in classification tasks under noise conditions. The use of this approach made it possible to form a consistent privacy assessment system with adaptive properties and compliance with privacy requirements in the fields of healthcare, finance, information risk management, and recommendation systems.

Mathematical representation and formalisation of confidentiality parameters

The differential concept of system confidentiality is defined by a set of parameters, which can be denoted as:

$$P = \{p_1, p_2, p_3, \ldots, p_n\} \tag{1}$$

Then these parameters can be represented as a vector:

$$P = [p_1, p_2, p_3, \ldots, p_n]. \tag{2}$$

Each parameter p_i may take a numerical value within a defined interval (for example, [0; 1]), reflecting the degree of its implementation or importance.

Parameter categories. For convenience, the entire set can be divided into subsets (categories), for example: P_1 = {Access Control}, P_2 = {Encryption}, P_3 = {Logging}. Then the overall set of parameters is:

$$P = P_1 \cup P_2 \cup P_3 \cup \cdots \cup P_m. \tag{3}$$

The overall privacy assessment function $F(p)$ evaluates the level of system privacy based on the parameter vector p. The overall assessment can then be expressed as a weighted sum of all parameters:

$$F(p) = w_1 \cdot p_1 + w_2 \cdot p_2 + \ldots + w_n \cdot p_n, \tag{4}$$

where w_i – the weighting coefficient reflecting the importance of the corresponding parameter p_i.

Data normalisation for training. Before input data are fed into the neural network, all parameters p_i are normalised. This means that each parameter value is brought to a common scale, for example to the interval [0; 1], to ensure correct processing in the model and to improve its convergence during training:

$$p_i^{norm} = \frac{p_i - p_i^{min}}{p_i^{max} - p_i^{min}}. \tag{5}$$

This makes the values comparable and improves convergence during training.

Differential privacy (optional). To protect privacy during training, noise may be added:

$$p_i^{dp} = p_i + \mathcal{N}(0, \sigma^2), \tag{6}$$

where $N(0, \sigma^2)$ – is noise distributed according to a normal (Gaussian) distribution with mean 0 and variance σ^2.

The applied model enabled the prediction of protection and security levels, as well as timely anomaly detection using neural networks with high data accuracy. The privacy-assessment model was implemented taking into

account a formalised parameter structure, multi-level normalisation, differential privacy mechanisms and the integration of a neural network for processing protected data. Based on predefined weighting coefficients, structured by categories, and using an adaptive multilayer perceptron architecture, an experimental evaluation of the model's effectiveness was carried out. During the analysis, particular attention was paid to prediction accuracy, sensitivity to normalisation parameters, and the impact of the noise level introduced according to differential privacy requirements. The results made it possible to assess the practical feasibility of applying the developed approach in systems operating under conditions involving the processing of sensitive or personalised information.

Results and Discussion

Summary of privacy assessment by category

Effective privacy assessment requires not only qualitative analysis of security parameters, but also a formalised approach to their structuring, weighting and processing. Thus, a structured approach to organising parameters was used, which ensured flexibility, scalability and logical integrity of the analysis process. The assessment parameters were grouped into categories (labelled as $X^{(k)}$, each of which corresponds to a separate aspect of privacy – for example, "Access Control" and so on. This division allows for a systematic coverage of all important security areas, simplifies comparisons between systems with different architectures and security policies, and creates a basis for a differentiated approach to assessment, where certain categories may be given greater weight depending on the context of application. For example, a set of parameters:

$$X = \{X^{(1)}, X^{(2)}, \ldots, X^{(C)}\}, \tag{7}$$

where C – number of main categories ("Access Control", "Encryption", "Logging", etc.)

Each category $X^{(k)}$ is itself a subset (or vector) of parameters that describe specific characteristics or security settings within that category, providing detail down to the level of individual components:

$$X^{(k)} = \left(x_1^{(k)}, x_2^{(k)}, \ldots, x_{n_k}^{(k)}\right), \tag{8}$$

where n_k – the number of parameters in category k.

This allows to introduce a separate group of weight coefficients for each category:

$$W^{(k)} = \left(w_1^{(k)}, w_2^{(k)}, \ldots, w_{n_k}^{(k)}\right), \tag{9}$$

as well as one "global" weight coefficient α_k, which reflects the importance of the entire category:

$$\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_C). \tag{10}$$

Then, at the simplest level (linear model), it can be written as:

$$f(X) = \sum_{k=1}^{C} \alpha_k \left(\sum_{i=1}^{n_k} w_i^{(k)} x_i^{(k)}\right). \tag{11}$$

This allows to take into account differences in anomalies that are possible between different groups of parameters that are important for privacy and creating reliable security, as well as to adapt the model to specific system requirements or regulatory restrictions (for example, in the banking sector, encryption may be more important than logging). This approach helps to balance detail and generalisation at the integrated assessment level. Thus, the use of a categorically structured parameter model in combination with a weighting system and multi-level normalisation provides both flexibility and formal justification for the privacy assessment process.

Normalisation and standardisation at several levels

The unification of input data makes it possible to increase the accuracy and stability of calculations, as well as to ensure the comparability of parameters coming from different sources and belonging to different privacy categories. At this stage, the parameters for further research were normalised and standardised, which was implemented at several interrelated levels. This made it possible to perform calculations to identify favourable directions for ensuring privacy.

Instead of simple standardisation $x_i' = \frac{x_i - \mu_i}{\sigma_i}$ an extended approach can be used.

1. Normalisation within a category:

$$x_i^{(k)} \mapsto \tilde{x}_i^{(k)} = \frac{x_i^{(k)} - \mu_i^{(k)}}{\sigma_i^{(k)}}, \tag{12}$$

where $\mu_i^{(k)}, \sigma_i^{(k)}$ are calculated only for category k.

2. Normalisation between categories: if there are categories in which the parameter values have different scales, additional global correction or scaling can be performed.

3. Limiting values (e.g., using a sigmoid or other nonlinear function):

$$\hat{x}_i^{(k)} = \sigma\left(\tilde{x}_i^{(k)}\right) = \frac{1}{1 + e^{-\tilde{x}_i^{(k)}}}. \tag{13}$$

This ensures that all reduced values lie in the interval [0,1].

Thus, the complicated version of the input data may be as follows:

$$\hat{X}^{(k)} = \left(\hat{x}_1^{(k)}, \hat{x}_2^{(k)}, \ldots, \hat{x}_{n_k}^{(k)}\right) \tag{14}$$

and instead of $x_i^{(k)}$ is now used in the formula $\hat{x}_1^{(k)}$.

After bringing the input parameters to a unified scale, it is necessary to take into account the relationships between them, which can significantly affect the accuracy of the privacy assessment. Simple weighting does not always reflect the real complexity of the dependencies between individual security characteristics, especially in conditions of high data density. That is why the next stage of the model was to expand the computational scheme to take into account internal and inter-category correlations.

Taking into account the correlation between parameters

Cross-correlation in the context of categories means researching and identifying the correlation between different categories. That is, determining how closely different categories are related to each other. The correlation can be either negative or positive. This makes it possible to identify the relationship between factors that influence indicators that point to dangerous manifestations and threats. If the parameters within a category or between categories influence each other, quadratic or interaction terms can be added. For example, in each category k, instead of the sum $\sum_{i=1}^{n_k} w_i^{(k)} \hat{x}_i^{(k)}$ a generalised expression can be applied:

$$\sum_{i=1}^{n_k} \sum_{j=1}^{n_k} \beta_{ij}^{(k)} \hat{x}_i^{(k)} \hat{x}_j^{(k)}, \quad (15)$$

where $\beta^{(k)}$ – a matrix of parameters (weights) that takes into account: diagonal elements $\beta_{ij}^{(k)}$ correspond to the "strength" of the influence of a single parameter; non-diagonal elements $\beta_{ij}^{(k)}$ reflect the mutual influence of a pair of parameters i, j.

Then the model in category k will look like this:

$$g_k\left(\hat{X}^{(k)}\right) = \sum_{i=1}^{n_k} \sum_{j=1}^{n_k} \beta_{ij}^{(k)} \hat{x}_i^{(k)} \hat{x}_j^{(k)}. \quad (16)$$

And the overall estimate:

$$f(X) = \sum_{k=1}^{C} \alpha_k g_k\left(\hat{X}^{(k)}\right). \quad (17)$$

If even greater accuracy is required, cross-correlations between categories can be used:

$$\sum_{k=1}^{C} \sum_{m=1}^{C} \sum_{i=1}^{n_k} \sum_{j=1}^{n_m} \gamma_{k,m}^{(i,j)} \hat{x}_i^{(k)} \hat{x}_j^{(m)}. \quad (18)$$

This significantly increases the number of parameters to be adjusted. This means that a large data set can be used for research, which improves the quality of the research itself and the final results. Taking into account the correlation between parameters allows the model to more accurately reflect the relationships within and between categories, which is important for a comprehensive assessment of privacy. Extending the basic linear model with quadratic and cross-categorical terms allows to identify both the individual and combined effects of parameters on the overall level of security. This approach creates conditions for flexible adaptation of the model to complex information system structures.

Regularisation and restrictions on weight coefficients

For further research, it was advisable to introduce restrictions on weight coefficients. This made it possible to select from the general population those indicators that have a significant impact on the factors of privacy and to reduce the influence of insignificant factors. To avoid an "explosion" of parameters or an overestimation of the impact of specific characteristics, regularisation is often used:

1. L2 regularisation (ridge regression): adds the sum of the squares of the weights to the loss function. For example, if Θ – is the set of all $\alpha_k, w_i^{(k)}, \beta_{ij}^{(k)}$ or, $\gamma_{k,m}^{(i,j)}$ then:

$$\Omega(\Theta) = \lambda \sum_{\theta \in \Theta} \theta^2, \quad (19)$$

where λ – a hyperparameter that determines the "strength" of regularisation.

2. L1 regularisation (lasso regression): inclines some weights towards zero, which effectively cuts off insignificant parameters:

$$\Omega(\Theta) = \lambda \sum_{\theta \in \Theta} |\theta|. \quad (20)$$

This helps to obtain results for further research from those factors that have a significant impact on the indicators.

3. Weight sum constraint: it is possible to require that $\sum_{i=1}^{n_k} w_i^{(k)} = 1$ (or a similar constraint for $\beta_{ij}^{(k)}$), to ensure a certain "normality" of influence.

4. Restricting the signs of weights (e.g., $\alpha_k \geqslant 0$).

When training or calibrating a model, the total loss function (e.g., L) may contain both deviations from the desired "correct" values and regularisation:

$$L(\Theta) = Loss(\Theta) + \Omega(\Theta). \quad (21)$$

The study conducted on calculating restrictions on weight coefficients makes it possible to reduce the number of indicators selected from the total amount of data and significantly influence those factors that are closely related to the factors for assessing the confidentiality of information systems. Normalisation and limitation of weight coefficient signs ensure the interpretability and consistency of results. Confidentiality parameters, combined with weight coefficients, form a differentiated model suitable for preparing data for neural network training.

An extended approach to differential privacy

Adding noise to parameters. To ensure formal privacy guarantees during data processing and analysis, mechanisms must be implemented to reduce the risk of confidential information leaks. One of the key approaches in this area is to add random noise to input parameters or calculation results, which makes it more difficult to identify individual records. This method allows the principles of differential privacy to be implemented, ensuring a balance between model accuracy and data protection. Earlier, a simple scheme was mentioned for adding Gaussian noise to normalised $\tilde{x}_i$. However, in practice, differential privacy often uses Laplace, Gaussian, and functional mechanisms.

Laplace mechanism:

$$\tilde{x}_i = \hat{x}_i + Laplace(0, b), \quad (22)$$

where Laplace $(0, b)$ – noise from the Laplace distribution, determined by parameter b.

Gaussian mechanism:

$$\tilde{x}_i = \hat{x}_i + \mathcal{N}(0, \sigma^2), \quad (23)$$

where σ selected to ensure (ε, δ) – differential privacy.

Functional mechanism: if it is not the vector X, itself that is calculated, but the result of some function $f(X)$, noise is added directly to the output of the function:

$$f(X) \mapsto f(X) + \eta, \quad (24)$$

where η selected from the desired distribution, depending on the sensitivity of f.

Adding noise at the gradient stage (DP-SGD) – an effective method for ensuring differential privacy during neural network training. The idea is to modify the standard stochastic gradient descent (SGD) algorithm and add random Gaussian noise. If weights Θ (e.g., α_k, $\beta_{ij}^{(k)}$ etc.) are trained using stochastic gradient descent, differential privacy can be implemented through the "Clip Noise" mechanism by introducing two key mechanisms: gradient $\nabla L(\Theta)$ clipping (each gradient reduced to a limited norm, for example, $\|\nabla L(\Theta)\| \leqslant k$) and adding random Gaussian noise:

$$\nabla L(\Theta) \mapsto \nabla L(\Theta) + \mathcal{N}(0, \sigma^2 k^2). \quad (25)$$

This noise prevents the accurate reconstruction of individual data contributions to the gradient, providing a formal guarantee of differential privacy. The combination of these two steps allows to control the balance between training quality (model accuracy) and privacy protection. Increasing the parameter σ improves protection but may reduce model performance, requiring careful tuning. Thus, the approach to differential privacy can be more complex than simply "adding noise to the parameters".

Example of a generalised formula for privacy assessment. Taking all of the above into account, the sequence of the "extended" privacy assessment takes the following form:

1. Normalisation (preliminary step at the category level):

$$\hat{x}_i^{(k)} = NonlinearNorm\left(x_i^{(k)}\right), \quad (26)$$

where *NonlinearNorm* – a composite scaling procedure.

2. Interactions and weights (within category):

$$g_k\left(\hat{X}^{(k)}\right) = \sum_{i=1}^{n_k} \sum_{j=1}^{n_k} \beta_{ij}^{(k)} \hat{x}_i^{(k)} \hat{x}_j^{(k)}. \quad (27)$$

3. Global weight of category α_k.

4. Intercategory term (optional):

$$h(X) = \sum_{k=1}^{C} \sum_{m=k+1}^{C} \sum_{i=1}^{n_k} \sum_{j=1}^{n_m} \gamma_{k,m}^{(i,j)} \hat{x}_i^{(k)} \hat{x}_j^{(m)}. \quad (28)$$

5. Conclusion:

$$f(X) = \underbrace{\sum_{k=1}^{C} \alpha_k g_k\left(\hat{X}^{(k)}\right)}_{\text{intra-category interactions}} + \underbrace{h(X)}_{\text{inter-category interactions}} + \varepsilon_{noise}, \quad (29)$$

where ε_{noise} – random noise that can be added: directly to $f(X)$ (Laplace/Gaussian mechanism); during the training of β, α, γ (via DP-SGD).

6. Regularisation (etc.) added to the loss function during training or calibration $\alpha_k, \beta_{ij}^{(k)}, \gamma_{k,m}^{(i,j)}$.

Thus, unlike the basic linear combination with normalisation, the "extended" scheme contains:

- grouping of parameters into categories with their own coefficients, plus global coefficients for the entire block;
- non-linear transformations and multi-level normalisation (internal and global);
- accounting for cross-influences: through additional matrices β, γ;
- regularisation to prevent overfitting and inadequately large weights;
- differential privacy (through noise in the data, in the output function, or in the gradient during training).

All this increases the complexity of calculations and the number of parameters, but allows for more flexible modelling of dependencies between security/privacy factors and, if necessary, protects the privacy of final data or intermediate results. Below is an example of a simple block diagram (Fig. 1) that shows the main categories of privacy parameters (access control, encryption, logging) and how they are combined into a general evaluation function. The diagram demonstrates the process of processing confidential parameters aimed at ensuring data privacy and improving data security. The visualisation shows a multi-stage approach to information processing: from data categorisation to normalisation, ensuring differential privacy and further analysis using a neural network. This approach allows different aspects of data protection to be integrated into a single structure that takes into account the requirements of modern confidential information processing systems.

The described block diagram is an important tool for developers and analysts, as it helps visualise and understand complex processes involved in handling confidential information. It allows potential vulnerabilities and weak points within the system to be easily identified, as well as helping to optimise data-protection strategies. The block diagram serves not only as an internal tool during the development process but also as a means of communication with clients and other stakeholders, helping to understand the importance of privacy and data security in the modern digital environment.

All input data is divided into categories that reflect key aspects of information security. Access control ensures that data access rights are verified. Encryption implements mechanisms to protect information from unauthorised access. Logging is responsible for collecting and storing data about events in the system. Key management includes operations for storing, processing, and rotating encryption keys. Risk management assesses and monitors potential threats. Incident management focuses on detecting and responding to security incidents. After collecting data from

different categories, it is combined into a single metric using a weighted sum. Weighting coefficients reflect the importance of each parameter, and the parameter values are combined in formula (9). The resulting metric is normalised to bring it to a single scale. Min-max normalisation is used, which brings the values to a range from minimum to maximum, or Z-normalisation, which is based on the mean and standard deviation. To ensure privacy, random noise is added to the normalised values according to the normal distribution law. This makes it difficult to recover the original data, protecting privacy and compliance with differential privacy requirements. In the final stage, the processed data is fed into a neural network, which is used for prediction, classification, or other data analysis tasks.

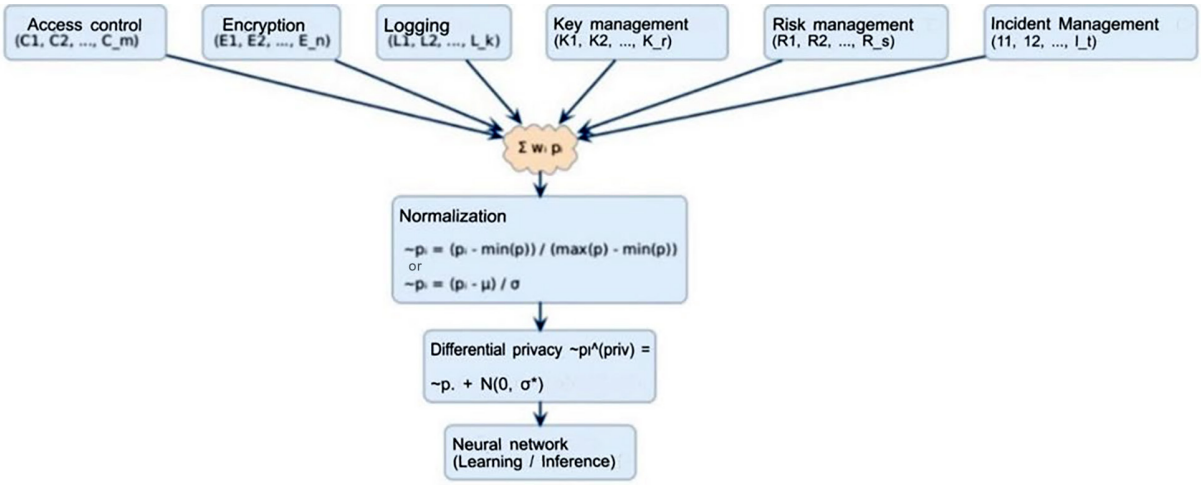

Figure 1. Block diagram of the privacy-parameter category
Source: constructed based on data from the authors

This scheme reflects an integrated approach to the processing of confidential data that can be applied in systems focused on the protection of personal information, including in the fields of healthcare, finance, and information security. The described privacy parameters, together with weighting coefficients, allow to construct a differential concept of privacy. Such formalisation will be useful when preparing and normalising data for further training of neural networks or other machine learning methods.

The described scheme is an important step towards ensuring data privacy and security in the modern world, where information is a critically valuable resource. The use of such data processing methods not only protects personal information from unauthorised access but also ensures compliance with legal requirements and ethical standards. The developed methodology can be adapted and used in various fields where confidential data processing is required, contributing to an increase in user confidence in information processing systems and ensuring the stability and security of their operation.

Differential privacy is one of the most effective approaches to data privacy protection, particularly in areas where sensitive information is processed. Its basic principle is to add random noise to data or calculation results, making it impossible to recover the original values. Formally, differential privacy is achieved by adding noise that has a normal or Laplace distribution. For example, for a normalised parameter x_i, the following is applied:

$$x_i' = x_i + \mathcal{N}(0, \sigma^2), \tag{30}$$

where $N(0, \sigma^2)$ – random noise with normal distribution, parameter σ controls the level of data blurring.

In recommendation systems for search and streaming services, algorithms analyse user preferences. Based on formula (22), adding noise to the output data is provided by the following formula:

$$r' = r + Lap(\lambda), \tag{31}$$

where $Lap(\lambda)$ – Laplace noise with parameter λ, which determines the level of privacy.

In the financial sector, for secure analysis of transaction data, the total number of transactions can be calculated using:

$$T' = T + \mathcal{N}(0, \sigma_T^2), \tag{32}$$

where T – the actual number of transactions, and σ_T^2 controls the level of differential privacy.

To reduce the impact of noise on the accuracy of the analysis, adaptive mechanisms can be used to adjust the privacy parameters. For example, the gradient noise mechanism (*DP-SGD*):

$$\tilde{g}_i = clip(g_i, C) + \mathcal{N}\left(0, \sigma_g^2\right), \tag{33}$$

where g_i – the gradient of the loss function; C – the threshold value (clipping); $N(0, \sigma^{g2})$ – additional Gaussian noise.

Thus, the integration of differential privacy allows for secure information analysis algorithms. It is important

to note that differential privacy does not guarantee the absolute impossibility of identifying an individual, but it makes this process extremely difficult and minimises the risk of confidential information leakage. It is for this reason that differential privacy is a powerful tool for protecting personal data in the modern digital world, where the processing of large amounts of information is the norm (Dwork & Roth, 2014).

Differential privacy is one of the most effective approaches to protecting data confidentiality, especially in areas where sensitive information is processed. Its basic principle is to add random noise to the input data or to the results of calculations, making it impossible to accurately recover the original values. This allows aggregated data to be used for analysis while maintaining the anonymity of individual records. One of the most common methods of ensuring differential privacy is the use of random noise, which can have a normal or Laplace distribution. For example, when analysing normalised parameters, a random component distributed according to a specific law is added to their values. The degree of data blurring is determined by the corresponding distribution parameters, which control the level of confidentiality.

In recommendation systems used in search and streaming services, algorithms analyse user preferences to improve personalised recommendations. Adding random noise to records of user interactions with content ensures privacy with little impact on system performance. Thus, the confidentiality of personal preferences is preserved without significantly reducing the effectiveness of the algorithm. In the financial sector, differential privacy is used to analyse transaction data, allowing banks to identify suspicious transactions without revealing information about specific customers. This is achieved by modifying aggregate metrics, such as the total number of transactions over a given period, by adding random noise. Since adding noise can affect the accuracy of the analysis results, it is important to choose adaptive mechanisms that allow the level of privacy to be adjusted according to specific needs. For example, when using neural networks, methods of regulating gradient weight updates can be applied by adding random noise during the model training stage. This reduces the risk of recovering the original data from intermediate results, with little impact on the performance of the algorithm.

This study uses a multilayer neural network as a baseline model for classifying the privacy level of systems, indicating its effectiveness for data protection. These results are also confirmed by studies that used other approaches. In particular, S. Tyshchenko & E. Kuznetsov (2024) described the use of neural networks in image classification. The authors solved the problem based on the task of entering an image into a neural network and assigning any label to the image. A time-efficient dataset was used to build the training model, which depended on the size and quality of the dataset. A. Rutkas & V. Shtanko (2024) raised a philosophical question about the importance of using artificial neural networks for interaction between humans and artificial systems. This idea has been technically developed in the current study, as the integration of differential privacy not only provides a technical level of security but also increases user confidence in automated data analysis systems.

In some publications, the authors focused on the applied economic use of artificial neural networks: N. Savka *et al*. (2020) analyse the forecasting of business activity using radial basis networks. The performance indicators of an enterprise depend on the specifics of its marketing policy, which is especially important for enterprises involved in product sales. Most existing methods for modelling enterprise activity are based on statistical and mathematical methods. Similarly, the proposed current methodology has demonstrated flexibility, allowing the model to be adapted to the specifics of specific domains – from finance to healthcare. H. Liavynets *et al*. (2024) investigated the application of neural network models in the hotel and restaurant industry for processing and analysing large amounts of data, which makes it possible to forecast information for strategic management decisions in the hotel and restaurant business.

The work of Y. Terpilovskyi (2024) explores bioinformatics and the representation of *k*-mer DNA data. The first method used by the author employs a vector of binary features, where each possible *k*-mer corresponds to a binary feature, resulting in high-dimensional and sparse feature vectors. The second method was based on the Conway-Bromage-Lyndon (CBL) structure, which introduces a compressed and dynamic representation of k-mers. In the proposed study, the problem of sparsity and multidimensionality is solved by normalising parameters and introducing noise mechanisms, which allows confidentiality to be maintained without losing informativeness.

In the study by A. Volokyta & M. Melenchukov (2024), neural networks are used to detect attacks in distributed systems. In this context, the proposed methodology demonstrates potential in the field of cyber security, especially given its scalability and applicability in public administration systems and financial infrastructure. In the current study, a neural network is used to enhance data protection confidentiality. Equally revealing is the analysis by M.S. Ahsan & A.-S.K. Pathan (2025), who draw attention to the security issues of the Internet of Things. One of the key issues is the identification of potential vulnerabilities and access control, which determines the overall security of Internet of Things systems. These tasks are also solved using the developed approach thanks to a multi-level risk assessment structure. A distinctive feature of the current study was the use of a protection prediction model for the timely detection of anomalies, which uses neural networks with high data accuracy.

Thus, the study highlighted the growing role of comprehensive approaches to privacy assessment that combine mathematical formalisation, adaptive data processing methods, and differential privacy. Analysis of the literature confirmed that effective protection of information systems requires interdisciplinary integration of technical, organisational, and ethical solutions. In summary, the results

demonstrate that combining neural network models with differential privacy mechanisms is a promising direction for creating robust and reliable data protection systems.

Conclusions

This study developed a formalised approach to the integrated assessment of information system privacy, taking into account the multi-component structure of risks and modern requirements for data privacy. The proposed methodology is based on the mathematical representation of parameters in the form of vectors, subsequent data normalisation, the application of weighting coefficients, and the implementation of differential privacy. Within the scope of the study, confidentiality parameters were structured by category, multi-level normalisation was performed, noise addition mechanisms were implemented at the processing and training stages, and a multi-layer neural network was used for classification. The results confirm the effectiveness of the developed model in maintaining a balance between the accuracy of analytical forecasts and the level of protection of confidential information.

The method provides flexibility in configuring the structure of weight coefficients, allows taking into account both the criticality of individual parameters and their categorical significance, and also allows scaling the system for different application domains. The inclusion of differential privacy mechanisms, in particular the addition of noise (Laplace, Gaussian, functional mechanism) and the use of DP-SGD during training, increases the level of privacy and makes the approach relevant for modern automated information protection systems. The developed block diagram, which reflects the process of categorisation, normalisation, differential privacy and further analysis of parameters, demonstrates the practical applicability of the proposed approach for developers and analysts. It facilitates the identification of potential vulnerabilities, the optimisation of protection strategies and communication with all interested parties.

The approach proposed in the study is relevant for use in healthcare, the financial sector, public administration systems, recommendation systems, and other areas where the secure processing of personalised data is important. The results conceptualise the possibility of creating unified privacy assessment systems based on quantitative criteria and modern artificial intelligence algorithms. This highlights the practical significance of the approach for building reliable, transparent, and ethical information systems that meet digital security and regulatory compliance requirements. This approach allows maintaining a balance between data security and the ability to perform financial analysis.

Thus, the integration of differential privacy into data analysis systems ensures their security and compliance with modern confidentiality requirements. The use of methods for adding random noise, adaptive privacy level control, and algorithm parameter adjustment allows for the creation of effective information processing mechanisms without the risk of sensitive data disclosure. Promising areas for further research include expanding the model to take into account context-oriented risk parameters, integration with behavioural analysis systems, and optimisation of adaptive privacy level control mechanisms depending on the user profile and the type of data being processed. Modifying aggregate indicators by adding random noise allows maintaining a balance between data security and the ability to perform analysis.

Acknowledgements

None.

Funding

The study was not funded.

Conflict of Interest

None.

References

[1] Ahsan, M.S., & Pathan, A.-S.K. (2025). A comprehensive survey on the requirements, applications, and future challenges for access control models in IoT: The state of the art. *IoT*, 6(1), article number 9. doi: 10.3390/iot6010009.

[2] Chubukova, O., Ponomarenko, I., & Domantovych, O. (2020). Using data science to risk assessment. *Market Infrastructure*, 47, 129-132. doi: 10.32843/infrastruct47-24.

[3] Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science*, 9(3-4), 211-407. doi: 10.1561/0400000042.

[4] Fathullah, M.A., Subbarao, A., & Muthaiyah, S. (2023). A systematic review: Risk management of cloud computing projects in healthcare. *International Journal of Management, Finance and Accounting*, 4(2), 83-115. doi: 10.33093/ijomfa.2023.4.2.5.

[5] Grinko, I., Skrypnyk, T., & Barmak, O. (2023). Quantum convolutional neural networks: Features of implementation in technical, natural and socio-economic systems. *Herald of Khmelnytskyi National University. Technical Sciences*, 323(4), 87-94. doi: 10.31891/2307-5732-2023-323-4-87-94.

[6] Gumen, O.M., & Rachek, K.O. (2023). Neural networks and machine learning in data processing for space weather forecasting. *Applied Questions of Mathematical Modeling*, 6(2), 19-23. doi: 10.32782/mathematical-modelling/2023-6-2-2.

[7] Ivanichenko, V., Sablina, M., & Kravchuk, K. (2021). Use of machine learning in cyber security. *Cybersecurity: Education, Science, Technology*, 4(12), 132-142. doi: 10.28925/2663-4023.2021.12.132142.

[8] Lee, H., Finke, D.C., & Yang, H. (2023). Privacy-preserving neural networks for smart manufacturing. *Journal of Computing and Information Science in Engineering*, 24(7), article number 071002. doi: 10.1115/1.4063728.
[9] Liavynets, H., Liulka, O., & Tkachuk, Y. (2024). Shallow artificial neural networks in management hotel and restaurant business. *Economy and Society*, 68. doi: 10.32782/2524-0072/2024-68-46.
[10] Piplai, A., Kotal, A., Mohseni, S., Gaur, M., Mittal, S., & Joshi, A. (2023). Knowledge-enhanced neurosymbolic artificial intelligence for cybersecurity and privacy. *IEEE Internet Computing*, 27(5), 43-48. doi: 10.1109/MIC.2023.3299435.
[11] Rutkas, A., & Shtanko, V. (2024). Artificial neural networks: A tool or a partner of the human mind. *Grail of Science*, 47, 652-659. doi: 10.36074/grail-of-science.20.12.2024.099.
[12] Sav, S., Diaa, A., Pyrgelis, A., Bossuat, J.-P., & Hubaux, J.-P. (2023). Privacy-preserving federated recurrent neural networks. *Proceedings on Privacy Enhancing Technologies*, 2023(4), 500-521. doi: 10.56553/popets-2023-0122.
[13] Savka, N., Vasylkiv, N., Dubchak, L., & Mudryk, I. (2020). Radial-basis neural networks for enterprises activity prediction. *European Science*, 3(sge17-03), 42-48. doi: 10.30890/2709-2313.2023-17-03-012.
[14] Semenenko, O., Kirsanov, S., Movchan, A., Ihnatiev, M., & Dobrovolskyi, U. (2024). Impact of computer-integrated technologies on cybersecurity in the defence sector. *Machinery & Energetics*, 15(2), 118-129. doi: 10.31548/machinery/2.2024.118.
[15] Shokri, R., Stronati, M., Song, C., & Shmatikov, V. (2017). Membership inference attacks against machine learning models. In *IEEE symposium on security and privacy* (pp. 3-18). San Jose: IEEE. doi: 10.1109/SP.2017.41.
[16] Terpilovskyi, Y. (2024). Comparison of DNA k-mer data representations for classification via neural networks. *International Scientific Technical Journal "Problems of Control and Informatics"*, 69(6), 61-69. doi: 10.34229/1028-0979-2024-6-5.
[17] Thantharate, P., & Anurag, T. (2023). CYBRIA – Pioneering federated learning for privacy aware cybersecurity. In *IEEE 20th international conference on smart communities: Improving quality of life using AI, robotics and IoT (HONET)* (pp. 56-61). Boca Raton: IEEE. doi: 10.1109/honet59747.2023.10374608.
[18] Tyshchenko, S., & Kuznetsov, E. (2024). Neural networks for the problem of image classification. *Science and Technology Today*, 3(31). doi: 10.52058/2786-6025-2024-3(31)-705-718.
[19] Volokyta, A., & Melenchukov, M. (2024). Neural networks in detecting attacks on distributed systems. *Technical Sciences and Technologies*, 1(35), 135-145. doi: 10.25140/2411-5363-2024-1(35)-135-145.
[20] Zaplatynskyi, N., Lub, P., & Zaporozhtsev, S. (2024). Improving cybersecurity with artificial intelligence. *Bulletin of Cherkasy State Technological University*, 29(4), 53-61. doi: 10.62660/bcstu/4.2024.53.

Інтегрована оцінка конфіденційності систем: формалізація, нормалізація та диференційна приватність

Дмитро Прокопович-Ткаченко

Кандидат технічних наук, доцент
Університет митної справи та фінансів
49000, вул. Володимира Вернадського, 2/4, м. Дніпро, Україна
https://orcid.org/0000-0002-6590-3898

Людмила Рибальченко

Кандидат економічних наук, доцент
Університет митної справи та фінансів
49000, вул. Володимира Вернадського, 2/4, м. Дніпро, Україна
https://orcid.org/0000-0003-0413-8296

Володимир Звєрєв

Кандидат технічних наук, доцент
Державний торговельно-економічний університет
02156, вул. Кіото, 19, м. Київ, Україна
https://orcid.org/0000-0002-0907-0705

Борис Хрушков

Аспірант
Університет митної справи та фінансів
49000, вул. Володимира Вернадського, 2/4, м. Дніпро, Україна
https://orcid.org/0009-0002-3978-5012

Бушков Валерій

Аспірант
Державний торговельно-економічний університет
02156, вул. Кіото, 19, м. Київ, Україна
https://orcid.org/0009-0005-5097-2689

Анотація. Вимоги щодо конфіденційності та приватності даних дедалі більше зростають. Метою роботи було розробити формалізований підхід до оцінювання конфіденційності інформаційних систем, що базується на векторному поданні множини параметрів. У запропонованому підході кожен параметр має числове значення у визначеному інтервалі, яке відображає ступінь його реалізації або важливості. Для зручності та структурованості параметри було розділено на кілька категорій (контроль доступу, шифрування, логування, управління ключами, керування ризиками й управління інцидентами), що охоплюють основні аспекти інформаційної безпеки. Загальний показник конфіденційності системи обчислювався за допомогою зваженої суми, де вагові коефіцієнти уточнювалися залежно від критичності кожного параметра. Для уніфікації шкал і забезпечення коректного подальшого аналізу застосовано методи нормалізації (мінімаксна та Z-нормалізація), завдяки чому отримані значення параметрів можна порівнювати й ефективно інтегрувати в загальну модель. У пропонованому методі для захисту вихідних даних і підвищення приватності використовується диференційна приватність, що забезпечується додаванням випадкового шуму з нормальним розподілом. Такий крок ускладнює процес відновлення початкових показників та мінімізує ризик ідентифікації конкретних записів, зберігаючи при цьому точність сукупних статистичних оцінок. Розроблений підхід містить кілька послідовних етапів: від первинної категоризації й нормалізації даних до реалізації диференційної приватності до аналізу даних у нейронній мережі. Його важливою перевагою є можливість інтегрувати різні аспекти захисту даних у єдину узгоджену систему. Така багатовимірна концепція сприяє гнучкості рішення та дозволяє швидко адаптувати його до оновлених вимог або появи нових загроз. Представлена модель особливо актуальна в галузях, де обробляються чутливі дані: охороні здоров'я, банківському та фінансовому секторах, а також у сфері державного управління й інформаційної безпеки. Запропонований підхід закладає основу для розробки й масштабування безпечних та прозорих систем, які відповідають сучасним стандартам збереження конфіденційності

Ключові слова: захист інформації; безпекові нейронні мережі; нормалізація векторних даних; доступ до інформації; параметри оцінки безпеки; статистичний шум; адаптивне машинне навчання