КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

UDC 004.056.5:004.7 https://doi.org/10.32515/2664-262X.2025.12(43).2.62-68

Orest Polotai[1], Assoc. Prof., PhD tech. sci., **Oleksandr Dorenskyi**[2], Assoc. Prof., PhD tech. sci., **Anastasiia Kovalenko**[2], **Kostiantyn Buravchenko**[2], Assoc. Prof., PhD tech. sci.
[1]*Lviv State University of Life Safety, Lviv, Ukraine*
[2]*Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine*
e-mail: orest.polotaj@gmail.com, dorenskyiop@kntu.kr.ua

STRIDE-based threat Modeling of Cybersecurity Risks in Local Computer Networks

The article examines the problem of ensuring LAN cybersecurity under conditions of increasing threat volume and complexity. Accordingly, the study focuses on developing a generalised adaptive method for threat modelling in LANs based on the STRIDE framework. To this end, the paper analyses current scientific sources on the application of STRIDE in the field of information security and identifies a gap between theoretical threat models and their practical implementation in the context of local networks. Based on a constructed DFD model, a structured representation of typical LAN components, external entities, network processes and data flows is formed. The STRIDE threat classification is applied to each model element, enabling the systematisation of potential risks and the development of a threat matrix for further analysis. An adaptive threat-modelling method is formulated, comprising network architecture analysis, automated generation of a threat list, selection of relevant countermeasures, modelling of a secure network architecture, and verification in a simulation environment. The effectiveness of the method is evaluated according to criteria such as completeness of threat coverage, adaptability, practical feasibility, and the degree of automation. The research findings demonstrate that the use of STRIDE in combination with DFD modelling enhances the structural consistency of cybersecurity analysis and provides a systematic approach to designing a LAN protection model.
cybersecurity, LAN, STRIDE, threat modelling, network protection, system vulnerability, risk analysis

Problem Statement. In the current era of digital transformation, local area networks (LANs) constitute a critically important component of the information infrastructure of enterprises, institutions, government agencies and other organisations. At the same time, both the number and complexity of cyber threats continue to grow. Ensuring an adequate level of LAN security therefore requires not only the deployment of technical safeguards, but also the application of effective threat-modelling and risk-analysis methods. One such approach is the STRIDE framework, which enables the systematic classification of potential threats based on a trust model. However, the practical use of STRIDE for analysing the security of local computer networks remains insufficiently explored. This is largely due to the difficulty of adapting the model to the specific characteristics of LANs, including topology, communication protocols, user privilege levels and the structure of interactions between network nodes. These factors highlight the need for a critical analysis of how STRIDE can be applied effectively in addressing LAN security tasks.

Analysis of Recent Research and Publications. The STRIDE framework enables a systematic analysis of system components (including LAN elements) for vulnerabilities across all defined threat categories. At present, STRIDE is widely discussed in the scientific literature as an effective tool for classifying threats in information systems. Publications [1, 2] consider STRIDE as a foundation for constructing threat models with a clear distinction between its six categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. These studies primarily focus on applying the method

in a general information security context, without a detailed consideration of the specific characteristics of local computer networks.

Scientific publications devoted to computer network security and information security (in particular, [3–5, 7]) emphasise vulnerability detection, analysis of data leakage channels, and methods for protecting information across different layers of network architecture. However, most of these works lack the application of formalised threat models, which limits the ability to adopt a systematic approach to risk assessment.

Some researchers (e.g., [6, 5]) propose simplified practical guidelines for building threat models using STRIDE. Nonetheless, these approaches require adaptation to real-world LAN scenarios, where numerous internal interactions, specific access restrictions, and non-standard topologies are present. Publication [2] describes the use of STRIDE in cloud environments, IoT infrastructures, and web applications. However, the issue of adapting this approach to security modelling specifically within local networks remains insufficiently addressed. Individual researchers, such as [7], highlight the importance of context-aware threat modelling, yet applied methodologies for LANs remain fragmented.

Therefore, a gap exists between the theoretical foundation of STRIDE and its practical application in securing local area networks. This gap underscores the relevance, novelty, and scientific value of the present study.

Tasks Statement. The aim of this study is to develop a generalised STRIDE-based approach (an adaptive method) for analysing the security model of a local area network. To achieve this aim, the following research objectives must be addressed: 1) identify the typical components and data flows within a local network; 2) apply the STRIDE method to the constructed trust model; 3) develop a method (approach) for identifying and mitigating threats; 4) evaluate the effectiveness of the proposed method.

Main Results. The process of applying STRIDE typically begins with constructing a system model in the form of a Data Flow Diagram (DFD), which serves as the key artefact in STRIDE-based threat modelling. The diagram identifies processes, data stores, external entities and information flows. Each system element is then analysed through the lens of the six STRIDE threat categories, allowing specific risks to be identified for each component.

To construct a threat model for a local area network, a DFD is used that incorporates user nodes, servers, access points and external interactions. This diagram functions as a security model of the LAN, taking into account the key components that ensure secure information exchange between external sources and internal resources. The external source is represented by an abstract “external entity” that communicates with the network via the Internet. At the boundary of the LAN is a firewall, which performs packet filtering for inbound and outbound traffic, blocking unwanted or potentially malicious connections.

Once traffic passes through the firewall, it reaches the router, which routes packets according to the internal network configuration. The router directs data along two possible paths: one towards the internal network, where the resources accessed by users are located, and the other towards the Network Intrusion Detection System (NIDS), which analyses traffic to identify anomalous or malicious activity.

The intrusion detection system, in turn, also interacts with the internal network and sends the results of its operation to a log storage repository, where the data are preserved for further analysis, auditing or incident response. The final participant in the internal network is the user, who interacts with the resources within the system, and whose activity may also be monitored to detect potential threats. Overall, this diagram illustrates a typical secure LAN architecture based on a multilayered approach to threat detection and prevention, in which each component performs a specific role in ensuring information security.

After the DFD is constructed, the process proceeds to threat identification, which is presented in Table 1.

Table 1 – Identification of Threats in the Local Network

Name	Description
Spoofing	the possibility of spoofing IP addresses or MAC identifiers
Tampering	modification of data within network packets
Repudiation	users denying actions performed due to lack of proper logging
Information Disclosure	information leakage through unencrypted channels
Denial of Service	flooding attacks or ARP spoofing
Elevation of Privilege	escalation to administrative privileges via exploits

Source: developed on the basis of [10]

Based on this classification, a risk matrix (Table 2) is constructed and subsequently used for the development of the protection algorithm.

Table 2 – Risk Matrix and Threats of the Local Network

STRIDE Category	Threat	Potential Target Component	Risk Level	Countermeasures
S	IP/MAC address spoofing	Workstations, gateways	High	MAC filtering, DHCP snooping, 802.1X
T	Traffic modification (MITM)	Switches, routers	High	Encryption (IPSec), access control (ACL)
R	Repudiation of actior (logging disabled)	Servers, guest terminals	Medium	System logging, digital signatures
I	Interception of unencrypted data	Wi-Fi access points	High	SSL/TLS, WPA3, VPN
D	Traffic flooding, ARP-based attacks	Servers, routers	High	Traffic limiting, IDS/IPS, QoS
E	Obtaining administrative privileges	Nodes with software or OS vulnerabilities	High	Software updates, RBAC, multi-factor authentication

Source: developed on the basis of [8, 9]

Thus, the presented matrix serves as the analytical foundation for constructing an adaptive protection algorithm for a local network, taking into account contemporary threats.

The method involves the following stages (tasks):

– analysis of the DFD model;

– automated generation of a list of threats using STRIDE;

– development of countermeasure recommendations (authentication, encryption, traffic monitoring, etc.);

– verification within a simulation environment (e.g., Cisco Packet Tracer or GNS3).

The method (adaptive approach) for protecting a local computer network in light of identified threats is structured according to the UML Sequence Diagram shown in Fig. 1.

The generalised (adaptive) method for LAN protection follows the following sequence of actions: 'Start Event' – 'Tasks': Analyse DFD Model, Identify Model Elements, Generate Threat List (STRIDE), Select Countermeasure, Model Secure Network, Verify via Simulation – 'Exclusive Gateway (XOR)': Threat Identified? Is Analysis Completed? – 'End Event'.

The method begins with the initiation of the analysis of the network structure. The first step is the examination of the DFD, which serves as the basis for identifying the main components and data flows within the local network. This is followed by the identification of model elements (external entities, processes, data stores and the data flows between them). The next step is to check whether threats have been identified for each element of the model. If a threat has not yet been detected, a list of threats is generated using the STRIDE framework (the six threat categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege).

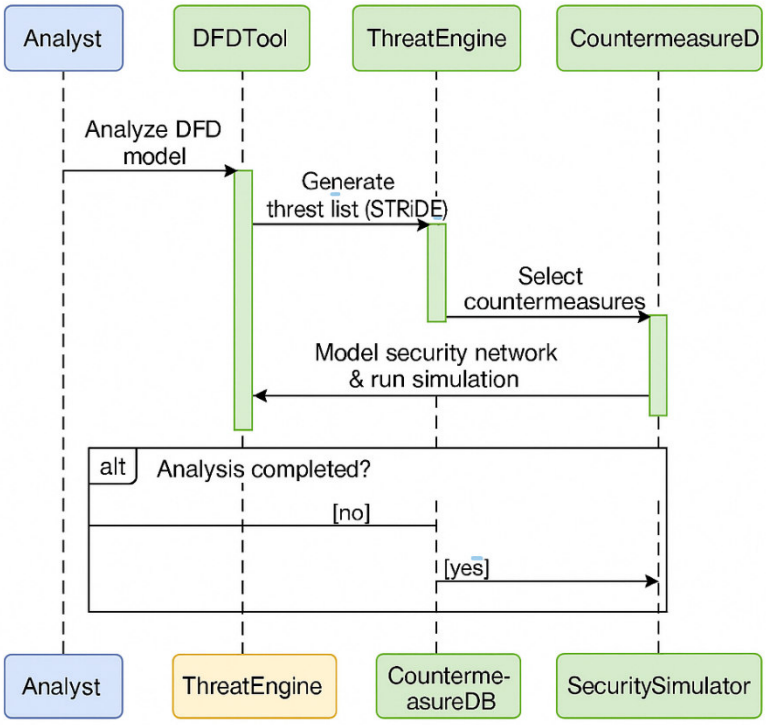

Figure 1 – Sequence Diagram of LAN Protection

Source: developed by the authors

Once the threat list has been produced, appropriate countermeasures are selected, ensuring they correspond to the specific threat type. For example, authentication is applied against spoofing, while encryption mitigates information disclosure. The next stage involves modelling a secure network architecture that incorporates these countermeasures. This step enables the creation of a solution design that accounts for the protection of all critical components.

The subsequent stage of the method is the verification of the model within a simulation environment. This allows the effectiveness of the proposed security architecture to be tested under conditions close to real-world operation. If the verification is successful (and the analysis is complete), the process reaches the final stage—completion. At this point, the security model is deemed ready for implementation. If vulnerabilities or ineffective measures

are discovered during simulation, the cycle is repeated starting from the analysis stage, until an optimal security configuration is achieved.

The effectiveness of the STRIDE-based LAN protection algorithm can be assessed according to several key criteria: completeness of threat coverage, adaptability to changes, practical feasibility of implementation, level of automation and the ability to verify the model (Table 3).

In summary, the following key points should be emphasised. The identification of typical components and data flows within a local network made it possible to construct a basic trust model in which nodes (servers, workstations, network devices), users and the directions of information exchange between them are clearly defined. This approach enabled the specific characteristics of LAN operation within typical organisational structures to be taken into account.

Table 3 – Criteria for Assessing the Effectiveness of LAN Protection

Effect	Description
Completeness of threat coverage	STRIDE provides a comprehensive approach to threat classification, covering six primary attack vectors: spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege. As a result, the developed algorithm enables the identification of critical risks at all levels of interaction between elements within the DFD model.
Adaptability	The algorithm is flexible and suitable for application across various network structures, ranging from small office environments to large corporate infrastructures. It supports iterative re-analysis in cases where shortcomings are identified or new threats emerge.
Practical feasibility of implementation	The use of DFD diagrams, the STRIDE methodology and simulation tools (such as GNS3 and Cisco Packet Tracer) makes the algorithm applicable both in educational contexts and real-world projects. Each stage is logically justified and grounded in solid technical principles.
Level of automation	The algorithm can be partially automated — including threat generation based on the model, selection of countermeasures and creation of policies. This enables integration into CI/CD pipelines or information security management systems.
Verification	The final stage involves testing the model in a simulation environment. This not only verifies the correctness of the implemented security measures but also helps identify potential conflicts or shortcomings prior to deployment in a production network.

Source: developed by the authors

An algorithm for identifying and eliminating threats was developed, based on the application of STRIDE principles to real-world LAN operation scenarios. The algorithm considers user context, communication protocol, and trust level associated with each node, allowing not only the identification of threats but also the formulation of appropriate recommendations for their mitigation (for example, the implementation of authentication, encryption, access auditing, and so forth).

Conclusions. The article presents the results of developing a STRIDE-based adaptive threat-modelling method for the cybersecurity of local computer networks. Specifically, the study identifies typical LAN components and data flows; applies STRIDE to the trust model;

develops an approach for identifying and mitigating threats; and evaluates the effectiveness of the generalised (adaptive) STRIDE-based method for LAN cybersecurity threat modelling. Thus, the research objectives have been achieved, confirming the effectiveness of a systematic approach to identifying and classifying threats within a networked environment while taking into account the specific interactions between its components.

The application of STRIDE to the trust model enabled the systematisation of threats across the categories of Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege. This approach made it possible to identify potential vulnerabilities in each direction of data exchange and for every object within the model.

The effectiveness of the proposed method was assessed through expert evaluation using a hypothetical corporate LAN. The results demonstrated that the model is capable of identifying most common threats that are often overlooked in traditional security assessments. The structured and adaptive nature of the algorithm confirms its practical applicability.

Thus, the findings of this study indicate the feasibility and value of using STRIDE as a tool for developing LAN protection models. Future research may focus on automating the modelling process and developing software tools for integrating STRIDE into the information security policies of organisations, institutions and enterprises. Furthermore, practical results from studies [11, 12] suggest the potential for exploring the integration of artificial intelligence capabilities into the proposed method, which may significantly enhance the cybersecurity of LAN environments.

List of References

1. Shostack, A. Threat Modeling: Designing for Security. Wiley, Hoboken. *Scientific research*: URL: www.scirp.org/reference/referencespapers?referenceid=3746452 (дата звернення: 22.06.2025).
2. OWASP. *Application Threat Modeling*: Веб сайт. URL: www.owasp.org/index.php/Threat_Risk_Modeling (дата звернення: 22.06.2025).
3. Khalil S. M., Bahsi H., Dola H., Korõtko T., McLaughlin K., Kotkas V. Threat Modeling of Cyber-Physical Systems: A Case Study of a Microgrid System. *Computers & Security*. Vol. 124, 2023. Pp. 102950.
4. Khan S. A. A STRIDE Model based Threat Modelling using Unified and-Or Fuzzy Operator for Computer Network Security. *International Journal of Computing and Network Technology*. Vol. 5, 1, 2017. Pp. 13-20.
5. Доренський О.П., Улічев О.С., Задорожний К.О., Коваленко А.С., Дрєєва Г.М. Концептуальна модель системи інформаційного протиборства координаційного центру з питань національної безпеки і оборони. *Центральноукраїнський науковий вісник. Технічні науки.* 2024. Вип. 10(41). Ч. 2. С. 23-31. https://doi.org/10.32515/2664-262X.2024.10(41).2.23-31.
6. Agile Modeling. *Security Threat Models: An Agile Introduction*: Веб сайт. URL: http://www.agilemodeling.com/artifacts/securityThreatModel.htm (дата звернення: 22.06.2025).
7. Kizza, J. M. Guide to Computer Network Security. Springer 2019.
8. Гапон А.О., Федорченко В.М., Поляков А.О. Підходи до побудови моделі загроз для аналізу безпеки відкритого програмного кода. *Системи обробки інформації*. 2020. Вип. 1. С. 128-135. DOI: 10.30748/soi.2020.160.17.
9. Полотай О.І., Пузир А.О. Аналіз та впровадження засобів запобігання витоку конфіденційної інформації на підприємствах, на прикладі системи DLP. *Вісник Львівського державного університету безпеки життєдіяльності*. 2024. № 30. С. 134-144. DOI: 10.32447/20784643.30.2024.13.
10. Полотай О.І., Фединець Н.І., Кухарська Н.П. Дослідження загроз інформаційної безпеки та способів їх вирішення в комп'ютерних мережах на канальному рівні. *Вісник Львівського державного університету безпеки життєдіяльності.* 2024. № 29. С. 65-71. DOI: 10.32447/20784643.29.2024.07.
11. Шелехов І.В., Прилепа Д.В., Хібовська Ю.О., Шамонін К.Є., Доренський О.П. Інформаційно-екстремальна технологія інтелектуального аналізу якості освітнього контенту в закладах вищої освіти. *Центральноукраїнський науковий вісник. Технічні науки.* 2025. Вип. 12(43), ч. 1. С. 58-72. DOI: https://doi.org/10.32515/2664-262X.2025.12(43).1.58-72.
12. Korniienko O., Kozub N., Dorenskyi O. Method and Technological Solution of an AI-Based Adaptive Investor Survey Service for Determining an Individual Risk Profile. *Central Ukrainian Scientific Bulletin. Technical Sciences*. 2025. Issue 11(42), Part II. P. 3-10. DOI: 10.32515/2664-262X.2025.11(42).1.3-10.

References

1. Shostack, A. (2014). Threat Modeling: Designing for Security. Wiley, Hoboken. Scientific research: URL: www.scirp.org/reference/referencespapers?referenceid=3746452 (accessed: 22.06.2025).
2. OWASP. Application Threat Modeling: Веб сайт. URL: www.owasp.org/index.php/Threat_Risk_Modeling (accessed: 22.06.2025).
3. Khalil, S. M., Bahsi, H., Dola, H., Korõtko, T., McLaughlin, K., & Kotkas, V. (2023). Threat Modeling of Cyber Physical Systems: A Case Study of a Microgrid System. *Computers & Security*, 124, 102950.
4. Khan, S. A. (2017). A STRIDE Model based Threat Modelling using Unified and Or Fuzzy Operator for Computer Network Security. *International Journal of Computing and Network Technology*, 5(1), 13–20.
5. Dorenskyi, O. P., Ulichev, O. S., Zadorozhnyi, K. O., Kovalenko, A. S., & Drieieva, H. M. (2024). Conceptual model of the system of information confrontation of the coordination center for national security and defence. *Tsentralnoukrainskyi naukovyi visnyk. Tekhnichni nauky*, 10(41) II, 23–31. https://doi.org/10.32515/2664-262X.2024.10(41).2.23-31 [in Ukrainian].
6. Agile Modeling. Security Threat Models: An Agile Introduction: Веб сайт. URL: http://www.agilemodeling.com/artifacts/securityThreatModel.htm (accessed: 22.06.2025).
7. Kizza, J. M. (2019). Guide to Computer Network Security. Springer.
8. Hapon, A. O., Fedorchenko, V. M., & Polyakov, A. O. (2020). Approaches to building a threat model for open source code security analysis. *Systemy obrobky informatsii*, 1, 128–135. https://doi.org/10.30748/soi.2020.160.17 [in Ukrainian].
9. Polotai, O. I., & Puzyr, A. O. (2024). Analysis and implementation of DLP systems to prevent confidential data leakage at enterprises. *Visnyk Lvivskoho derzhavnoho universytetu bezpeky zhyttiediialnosti*, 30, 134–144. https://doi.org/10.32447/20784643.30.2024.13 [in Ukrainian].
10. Polotai, O. I., Fedynets, N. I., & Kukharska, N. P. (2024). Research of cybersecurity threats and ways to counter them at the data-link layer of computer networks. *Visnyk Lvivskoho derzhavnoho universytetu bezpeky zhyttiediialnosti*, 29, 65–71. https://doi.org/10.32447/20784643.29.2024.07 [in Ukrainian].
11. Shelekhov, I. V., Prylepa, D. V., Khibovska, Yu. O., Shamonin, K. Ye., & Dorenskyi, O. P. (2025). Information-extreme technology for intelligent analysis of educational content quality in universities. *Tsentralnoukrainskyi naukovyi visnyk. Tekhnichni nauky*, 12(43) I, 58–72. https://doi.org/10.32515/2664-262X.2025.12(43).1.58-72 [in Ukrainian].
12. Korniienko, O., Kozub, N., & Dorenskyi, O. (2025). Method and technological solution of an AI-based adaptive investor survey service for determining individual risk profile. *Central Ukrainian Scientific Bulletin. Technical Sciences*, 11(42) II, 3–10. https://doi.org/10.32515/2664-262X.2025.11(42).1.3-10.

О. І. Полотай[1], доц., канд. техн. наук, **О. П. Доренський**[2], доц., канд. техн. наук, **А. С. Коваленко**[2], **К. О. Буравченко**[2], доц., канд. техн. наук

[1]*Львівський державний університет безпеки життєдіяльності, Львів, Україна*

[2]*Центральноукраїнський національний технічний університет, м. Кропивницький, Україна,*

STRIDE-моделювання загроз кібербезпеці локальних комп'ютерних мереж

Праця присвячена проблемі забезпечення кібербезпеки LAN в умовах зростання кількості та складності загроз, для вирішення якої сформувано узагальнений адаптивний спосіб моделювання загроз LAN на основі STRIDE. За результатами дослідження визначено наявний розрив між теоретичними моделями загроз і їх практичною реалізацією у контексті локальних комп'ютерних мереж. На основі побудови моделі DFD сформовано структуроване представлення типових компонент LAN, зовнішні сутності, мережеві процеси та потоки даних. До кожного елементу моделі застосовано класифікацію загроз STRIDE, що дозволило систематизувати потенційні ризики, сформувати матрицю загроз для подальшого аналізу.

Адаптивний метод моделювання загроз включає процеси аналізу архітектури мережі, автоматизованого формування переліку загроз, вибору релевантних контрзаходів, моделювання захищеної мережі, верифікації в симуляційному середовищі. Оцінювання його ефективності здійснено за критеріями повноти покриття загроз, адаптивності, практичності впровадження та можливості автоматизації.

Результати дослідження показали, що застосування STRIDE у поєднанні з DFD-моделюванням дозволяє підвищити рівень структурованості аналізу кіберзагроз, реалізувати системний підхід до формування моделі захисту локальної мережі. Це дає можливість ідентифікувати потенційні вразливості, які часто залишаються поза увагою при традиційних підходах. Перспективами подальших розвідок є розроблення програмних засобів для автоматизації STRIDE-моделювання та інтеграція інструментів штучного інтелекту для підвищення ефективності захисту LAN.

кібербезпека, локальна мережа, STRIDE, моделювання загроз, захист мережі, вразливість, аналіз ризиків

Одержано (Received) 09.09.2025 *Прорецензовано (Reviewed) 01.10.2025*
Прийнято до друку (Approved) 28.10.2025