Міністерство освіти і науки України
Черкаський державний технологічний університет
Черкаська обласна державна адміністрація
Департамент цивільного захисту, оборонної роботи та взаємодії з правоохоронними органами Черкаської обласної державної адміністрації
Національний університет цивільного захисту України
Національний університет «Чернігівська політехніка»
Національний університет кораблебудування імені адмірала Макарова
Український державний університет науки і технологій
Черкаська медична академія
Черкаський науково-дослідний експертно-криміналістичний центр МВС України
Черкаська обласна організація Товариства Червоного Хреста України
Громадська організація «Асоціація цивільного захисту»
Громадська спілка «Пожежні-рятувальники України»
ТОВ «ЦЕНТР СЛУЖБИ КРОВІ «БІОФАРМА ПЛАЗМА»»
Німецьке товариство міжнародного співробітництва (GIZ), Федеративна Республіка Німеччина
Пожежна рада міста Гамбург, Федеративна Республіка Німеччина
Об'єднана платформа «Пошук, рятування, медична та гуманітарна допомога», Турецька Республіка
Університет Східного Лондона, Сполучене Королівство Великої Британії і Північної Ірландії
Жилінський університет, Словацька Республіка
Вільнюський технічний університет ім. Гедимінаса, Литовська Республіка
Габровський технічний університет, Республіка Болгарія
Центр австрійсько-українських культурних досліджень, Австрійська Республіка

МАТЕРІАЛИ

І Міжнародної науково-практичної конференції

«ТЕХНОЛОГІЇ БЕЗПЕКИ: СУЧАСНІ ВИКЛИКИ ТА ПЕРСПЕКТИВИ»

12–13 березня 2026 року, м. Черкаси

Том 2

ТЕХНОЛОГІЇ ЗАХИСТУ У БУДІВНИЦТВІ ТА ВІДНОВЛЕННІ ІНФРАСТРУКТУРИ

СУСПІЛЬНО-ПОЛІТИЧНА, ГУМАНІТАРНО-ПРАВОВА ТА ІНФОРМАЦІЙНА БЕЗПЕКА

ЕКОЛОГІЧНА БЕЗПЕКА. ЗАХИСТ ДОВКІЛЛЯ ТА ЗДОРОВ'Я ЛЮДИНИ

Черкаси ЧДТУ 2026

УДК 614.8:351.86:004:502.1](036)
Т38

Рекомендовано вченою радою Черкаського державного технологічного університету, протокол № 11 від 16 березня 2026 р.

Відповідальний за випуск: *Цікановський В. Л.*

Т38 **Матеріали** І Міжнародної науково-практичної конференції «Технології безпеки: сучасні виклики та перспективи» : 12–13 березня 2026 року, м. Черкаси [Електронний ресурс] : у 2-х томах / упоряд. : І. Г. Маладика, В. Л. Цікановський ; М-во освіти і науки України, Черкас. держ. технол. ун-т. – Т. 2. – Черкаси : ЧДТУ, 2026. – 443 с.

Обговорення концептуальних засад і стратегічних питань врегулювання безпекової складової у сучасних умовах. Підвищення ефективності заходів цивільного захисту територіальних громад. Розгляд наукових досліджень і розробок, пов'язаних із забезпеченням цивільної, пожежної, техногенної, екологічної безпеки, створенням і підтриманням безпечних умов праці, здоров'я та життєдіяльності людини. Розгляд нових безпекових рішень у суспільно-політичній, гуманітарно-правовій та інформаційній сферах. Перспективи застосування інформаційних та геоінформаційних систем і технологій; безпілотних літальних апаратів; робототехніки; захисту об'єктів енергетики та транспорту. Технології захисту у будівництві та відновленні інфраструктури в умовах глобальних викликів.

Для науковців, студентів, аспірантів та фахівців галузі.

УДК 614.8:351.86:004:502.1](036)

ТЕМАТИЧНІ СЕКЦІЇ КОНФЕРЕНЦІЇ:

Секція 1 Цивільний захист, пожежна і техногенна безпека та охорона праці.
Секція 2 Технології захисту у будівництві та відновленні інфраструктури.
Секція 3 Суспільно-політична, гуманітарно-правова та інформаційна безпека.
Секція 4 Екологічна безпека. Захист довкілля та здоров'я людини.

Матеріали збірника представлені мовою оригіналу. Кожен автор несе повну відповідальність за зміст своїх публікацій, достовірність фактів, цитат, власних імен та інших даних, точність і коректність посилань, дотримання засад академічної доброчесності.

ОРГКОМІТЕТ КОНФЕРЕНЦІЇ

ГРИГОР	***голова оргкомітету,***
Олег Олександрович	*ректор Черкаського державного технологічного університету, д-р політ. наук, професор*
ТАБУРЕЦЬ	***співголова організаційного комітету,***
Ігор Іванович	*канд. екон. наук, доцент, начальник Черкаської обласної військової адміністрації*
ШАМРАЙ	***заступник голови організаційного комітету,***
Олександр Григорович	*канд. іст. наук, доцент, заступник голови Черкаської обласної державної адміністрації*
ЦАРЮК	***заступник голови організаційного комітету,***
Антон Олександрович	*заступник голови Черкаської обласної державної адміністраціїї*
ДАНИЛЕВСЬКИЙ	***заступник голови організаційного комітету,***
Валерій Вікторович	*канд. іст. наук, доцент, начальник Управління освіти і науки Черкаської обласної державної адміністрації*
ЛАЗУРЕНКО	***заступник голови організаційного комітету,***
Валентин Миколайович	*д-р іст. наук, професор, проректор з гуманітарно-виховних питань Черкаського державного технологічного університету, заслужений працівник освіти України, голова Черкаської обласної організації Національної спілки краєзнавців України*
ФАУРЕ	***заступник голови організаційного комітету,***
Еміль Віталійович	*д-р техн. наук, професор, проректор з науково-дослідної роботи та міжнародних зв'язків Черкаського державного технологічного університету*
МАЛАДИКА	***заступник голови організаційного комітету,***
Ігор Григорович	*канд. техн. наук, доцент, завідувач кафедри геодезії, землеустрою, будівельних конструкцій та безпеки життєдіяльності Черкаського державного технологічного університету*
ЦІКАНОВСЬКИЙ	***секретар організаційного комітету,***
Володимир Леонідович	*старший викладач кафедри геодезії, землеустрою, будівельних конструкцій та безпеки життєдіяльності Черкаського державного технологічного університету*

С. Сванстрема (S. Swanström, 2022), виданій Інститутом політики безпеки та розвитку (Стокгольм): «Китай та Росія – час стримування!» [13, с. 33].

ЛІТЕРАТУРА

1. Alexandrescu M. & Stoica M. S. Authoritarian demand in East-Central Europe post-pandemic and amid neighbouring war. *Politics and Governance*, 2024. Vol. 12, article 8594. 14 p. URL: https://doi.org/10.17645/pag.8594
2. Ballard-Rosa C., Malik M. A., Rickard S. J., Scheve K. The economic origins of authoritarian values: evidence from local trade shocks in the United Kingdom. *Comparative Political Studies*, 2021. Vol. 54, iss. 13. P. 2321–2353. URL: https://doi.org/10.1177/00104140211024296
3. Cottiero C. Understanding and interrupting modern day authoritarian collaboration: suggestions for the democracy support community. International Foundation for Electoral System, Arlington, April 2024. 31 p. URL: https://www.gla.ac.uk/media/Media_1182164_smxx.pdf
4. Crepaz M. M. L. & Naoufal P. Authoritarianism, economic threat, and the limits of multiculturalism in post-migration crisis Germany. *Social Science Quarterly*, 2022. Vol. 103, iss. 2. P. 425–438. URL: https://doi.org/10.1111/ssqu.13144
5. Diamond L. Democracy's arc from resurgent to imperiled. *Journal of Democracy*, 2022. Vol. 33, no. 1. P. 163–179. URL: https://doi.org/10.1353/jod.2022.0012
6. Dziundziuk B. A comparative analysis of the impact of authoritarian and democratic political systems on addressing global challenges. *Foreign Affairs*, 2024. Vol. 34, no. 6. P. 47–56. URL: https://doi.org/10.59214/ua.fa/6.2024.47
7. Ekiert G. Democracy and authoritarianism in the 21st Century: a sketch. *Policy briefs series*. A publication of the: Ash Center for Democratic Governance and Innovation Harvard Kennedy School, December 2023. 16 p. URL: https://ash.harvard.edu/wp-content/uploads/2023/12/democracy_and_authoritarianism_in_the_21st_century-_a_sketch.pdf
8. Ficek R. Authoritarianism as a «wicked problem» in contemporary international relations. *UR journal of humanities and social sciences*, 2022. Vol. 3, iss. 24. P. 95–115. URL: https://doi.org/10.15584/johass.2022.3.6
9. Kasım M. The authoritarian rise of China and its geopolitical dilemma. *Current Research in Social Sciences*, 2025. Vol. 11, iss. 1. P. 65–85. URL: http://dx.doi.org/10.30613/curesosc.1423847
10. Khoma N. & Nikolayeva M. Neoauthoritarianism as a challenge to global security. *Przegląd Strategiczny*, 2023. Iss. 16. P. 63–75. URL: https://doi.org/10.14746/ps.2023.1.5
11. McLean E. V. Chapter 16. Economic coercion. – In: J. C. W. Pevehouse & L. Seabrooke (eds). The Oxford handbook of international political economy. Publisher: Oxford University Press, 2021. P. 254–275. https://doi.org/10.1093/oxfordhb/9780198793519.013.2
12. Salajan F. D. & Jules T. D. The global resurgence of authoritarianism and its existential threats to education: implications for scholarship in comparative and international education *Comparative Education Review,* 2024. Vol. 68, iss. 3. P. 319–344. URL: https://doi.org/10.1086/732119
13. Swanström S. (ed.) Collective economic self-defense against authoritarianism: lessons for EU. *Special paper*, February 2022. Institute for Security and Development Policy, Stockholm. 102 p. URL: https://www.isdp.eu//wp-content/uploads/2022/02/Collective-Self-Defense-Against-Authoritarianism-24.02.2022.pdf

УДК 81'276:351.86:005.334

LANGUAGE AS A SECURITY FACTOR: WHY TERMINOLOGY MATTERS FOR PROTECTION, RISK MANAGEMENT AND INSTITUTIONAL RESILIENCE

Yuliia NENKO,
Doctor of Pedagogical Sciences, Professor,
National University of Civil Protection of Ukraine

When we speak about security, we usually imagine visible or technical measures: surveillance cameras, access cards, alarm systems, firewalls, background checks, or emergency plans. However, before any of these mechanisms can function effectively, there must be a shared understanding of what exactly is being protected, from whom, and by which means. This shared understanding is built through language. The terms we use – such as «risk», «threat», «vulnerability», «incident», or «resilience» – shape how security is perceived, discussed, and implemented. In this sense, language is not simply a tool for describing security; it is one of its fundamental components.

Scholars have repeatedly noted that the field of security lacks consistent and harmonised terminology [2; 4; 7]. Different standards, organisations, and professional communities define key concepts in slightly different ways. While these differences may appear minor, they can significantly affect interpretation and practice. For example, if one department defines «risk» as the probability of an unwanted event, while another defines it as a combination of probability and impact, their assessments and priorities may differ. According to ISO 31000, risk is defined as the «effect of uncertainty on objectives» [5]. Even this definition requires interpretation: what counts as an objective, and how is «effect» measured? These interpretive processes are linguistic in nature.

Language influences security at several levels. First, it shapes perception. The way a problem is named affects how seriously it is taken. For instance, describing an event as a «minor technical issue» rather than a «security breach» changes the perceived urgency of response. Research in risk communication shows that terminology strongly affects stakeholder reactions and decision-making processes [3]. Thus, language is not neutral; it frames reality.

Second, language structures analysis. Risk assessment frameworks depend on clearly defined concepts. Terms such as «threat», «hazard», «vulnerability», and «exposure» are often used interchangeably in everyday speech, yet in professional contexts they refer to distinct elements of risk models [1]. If these distinctions are blurred, analytical clarity decreases. Inconsistent terminology can lead to double counting of risks or, conversely, to gaps in analysis.

Third, language enables coordination. Modern security challenges rarely fall within a single domain. Universities, for example, must address physical security (protection of facilities), information security (data protection), and

personnel security (background checks, ethical conduct). Each of these areas has developed its own professional vocabulary. However, when incidents occur – such as data breaches combined with unauthorised physical access – coordination between units becomes essential. If the units operate with different conceptual frameworks, misunderstandings can arise.

Studies of security ontologies highlight precisely this issue. Researchers have shown that security-related terms are often defined inconsistently across standards and academic literature [2; 7]. The absence of a shared conceptual model makes integration difficult. A harmonised terminology does not eliminate disciplinary diversity, but it provides a common reference point. It functions similarly to a shared protocol in digital communication: without agreed meanings, interaction becomes unreliable.

The distinction between security and resilience illustrates how language clarifies institutional priorities. These two terms are frequently used together, sometimes as if they were interchangeable. However, they refer to different aspects of organisational capacity. Security is primarily concerned with preventing unwanted events. It includes measures that aim to protect assets before an incident occurs. Resilience, by contrast, refers to the ability of a system to respond, recover, and adapt after disruption [3]. When institutions fail to differentiate clearly between these concepts, they may focus excessively on prevention while neglecting recovery planning, or vice versa. Clear terminology helps allocate resources more rationally.

Language also plays a crucial role in governance. Security governance involves setting priorities, defining responsibilities, and establishing acceptable levels of risk. These processes are fundamentally discursive. Policies are written texts; procedures are formulated in language; training materials rely on shared definitions. If key concepts are interpreted differently by administrators, IT specialists, and academic staff, institutional coherence weakens. Governance becomes fragmented not because of technical failure but because of semantic misalignment.

In university settings, this issue is particularly relevant. Universities combine educational, research, administrative, and technological functions. They host diverse communities with varying levels of security awareness. Terms such as «data protection», «confidential information», or «critical infrastructure» may carry different meanings for researchers, IT personnel, and management. Without clear definitions, expectations remain ambiguous. Ambiguity can create unintentional non-compliance or inconsistent practices.

Language is equally important in crisis communication [6]. During emergencies, clarity and precision are essential. Ambiguous instructions can delay response or create panic. Research in crisis management emphasises that effective communication depends on shared understanding of terminology and procedures [3]. If staff members interpret key terms differently, coordinated action becomes more difficult.

Moreover, terminology influences professional identity. Fields that are widely recognised as mature professions – such as medicine, engineering, or emergency services – rely on clearly defined conceptual frameworks [6]. Shared vocabulary supports training, certification, and ethical standards. Security, as a developing professional field, faces the challenge of establishing comparable coherence. M.Donner already argued for the development of a security ontology to strengthen the discipline [4]. Later reviews confirmed that fragmentation remains a significant issue [2; 7].

The growing complexity of security environments further increases the importance of linguistic clarity. Digital transformation has blurred boundaries between physical and cyber domains. Remote work, cloud storage, and online learning platforms have introduced new forms of vulnerability. In such hybrid environments, security measures must be integrated. Integration requires a shared conceptual language. Without it, policies may overlap or contradict each other.

Importantly, improving security language does not mean making terminology more complicated. On the contrary, effective security communication often requires simplification and clarification. Definitions should be precise but understandable. Overly technical language can create distance between security specialists and other staff members. A balance must be found between accuracy and accessibility.

Language training can therefore be considered part of security culture. When staff members understand what terms such as «incident», «breach», or «escalation» mean within their institution, they are more likely to respond appropriately. A shared glossary or terminology guide can serve as a practical tool. Such measures may seem minor compared to technological investments, but they contribute to institutional coherence.

In conclusion, security is not only a technical or organisational matter; it is also a linguistic one. Language shapes perception, structures analysis, supports coordination, and underpins governance. Inconsistent terminology can create hidden vulnerabilities, while harmonised language strengthens resilience and cooperation. For universities and other institutions, attention to security-related terminology is therefore a practical necessity rather than an abstract theoretical concern. By investing in conceptual clarity and shared understanding, institutions reinforce the foundations upon which all other security measures depend.

REFERENCES

1. Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, 253(1), 1–13.
2. Blanco, C., Lasheras, J., Valencia-García, R., Fernández-Medina, E., Toval, A., & Piattini, M. (2008). A systematic review and comparison of security ontologies. *Information and Software Technology*, 50(9–10), 819–832.

3. Boin, A., ’t Hart, P., Stern, E., & Sundelius, B. (2017). *The politics of crisis management: Public leadership under pressure* (2nd ed.). Cambridge University Press.
4. Donner, M. (2003). Toward a security ontology. *IEEE Security & Privacy*, 1(3), 6–7.
5. ISO. (2009). *ISO 31000: Risk management — Principles and guidelines*. International Organization for Standardization.
6. Nenko, Y., Yaryhina, V., Vorona, V. Examining officer readiness for foreign language intercourse in international operations. *Revista Praxis Educational*, v.17, n.46, p. 1-23, JUL./SET.| 2021. https://doi.org/10.22481/praxisedu.v17i46.8816
7. Souag, A., Salinesi, C., & Wattiau, I. (2012). Ontologies for security requirements: A literature survey. *Requirements Engineering*, 17(3), 169–185.

УДК 7.05:339.1]:502.1

FASHION-ІНДУСТРІЯ В КОНТЕКСТІ ЕКОЛОГІЧНОЇ БЕЗПЕКИ

***Олександра КОВБАСА**, викладач кафедри графічного дизайну, моди та стилю (ГДМС),*
***Іванна СТРЕЛЬБА**, студентка кафедри ГДМС*
Черкаський державний технологічний університет

Сучасний етап розвитку підприємництва відзначається багатовимірністю та суперечливістю впливу на суспільні процеси. Це виступає водночас рушійною силою економічного зростання і джерелом підвищеного антропогенного навантаження на довкілля. У цьому контексті індустрія моди є показовим прикладом трансформації креативного сектору в масштабну глобалізовану систему виробництва. Якщо раніше вона асоціювалася переважно з художнім самовираженням і культурними тенденціями, то нині функціонує за принципами високої оборотності товарів та мінімізації витрат. Такі зміни зумовили суттєве зростання екологічного навантаження, пов’язаного з використанням водних ресурсів, енергії, синтетичних матеріалів і хімічних реагентів.

Загострення екопроблем у другій половині XX – на початку XXI століття є наслідком активізації промислового виробництва, глобалізації ринків і зростання споживання. Антропогенне навантаження на довкілля проявляється у зміні клімату, втраті біорізноманіття, виснаженні земельних ресурсів, дефіциті прісної води та накопиченні відходів. Сучасна модель економічного розвитку, орієнтована на постійне зростання обсягів виробництва, спричиняє перевищення відновлювальної здатності природних екосистем і формує системні екологічні ризики глобального масштабу [1].

Феномен швидкої моди (fast fashion) характерний скороченнями виробничих циклів, високою частотою оновлення асортименту та орієнтацією на цінову доступність для масового споживача. Незважаючи на розширення доступу до актуальних модних тенденцій, ця модель супроводжується істотними екологічними наслідками: активізацією