УДК 336.6

VULNERABILITY FACTORS AND CLASSIFICATION OF THREATS TO FINANCIAL SECURITY

Gao Dongze, PhD Student,
Polessky State University

Abstract. *The article presents criteria for distinguishing between vulnerability factors and threats to an organization's financial security. It also proposes an original classification of financial security threats, which encompasses the full spectrum of potential risks and can serve as a checklist for identifying an organization's specific threats*

Keywords*: threats, vulnerability factors, financial security, external and internal conditions*

In the practice of managing financial security, it is important to distinguish between vulnerability factors and threats, as the approaches to managing these categories differ. Vulnerability factors are addressed through decisions concerning the structure of an enterprise - such as its capital, client portfolio, or operational systems–with the effects of these measures often taking time to manifest. Threats, by contrast, are identified and monitored, prompting the development of a response - a process that is typically more immediate. An assessment reflecting only the level of vulnerability provides management with an understanding of the enterprise's exposure to risk, but it does not indicate whether any active forces are currently impacting the organization.

Therefore, a vulnerability factor is a property of an enterprise or its environment that increases the likelihood of damage or the severity of its impact, whereas a threat consists of a set of conditions capable of causing such damage to materialize.

It is customary to distinguish between external and internal factors, which are of a different nature and, consequently, require specific mechanisms for their management. External vulnerability factors are those over which an enterprise has no control - it can only anticipate them. It is precisely because of these factors that two enterprises with identical financial positions may have vastly different prospects, and an assessment method calibrated for one period may lead to erroneous conclusions in another. These include: exchange rate and monetary conditions, conditions of demand, conditions of supply, credit and settlement conditions, regulatory and tax conditions, industry conditions.

Internal factors are those that an enterprise can change - though not always quickly - including factors related to capital structure, liquidity status, profitability, cash flows, and information infrastructure.

Existing classifications categorize economic threats - which encompass threats to financial security - based on two criteria: their source (external or internal) [1] and their functional domain (operational, investment, financial, etc.) [2]. While both approaches are useful for assigning responsibility, they share a common drawback: neither accounts for information-related threats, except perhaps as a "residual" category. In classifica-

tions based on source, a cyber threat is defined as either external or internal depending on the entity behind it - without specifying what exactly is being threatened. In classifications based on functional domains, information-related threats do not fit into any of the established categories (as they are not directly linked to operational, investment, or financial activities); consequently, they are merely appended to the list rather than integrated into the system itself.

The classification proposed here categorizes threats along two axes that characterize the threat itself, rather than the organizational structure of the enterprise. The first axis is the object of the threat - that is, what the threat is directed toward. The object may be either the enterprise's financial resources (cash balances, accounts receivable, access to credit) or the information infrastructure used to manage and account for these resources. The distinction here is not between financial and technical aspects, but rather between two ways in which an enterprise's financial position can be harmed: a threat to financial resources leads to a direct loss of value, whereas a threat to the information infrastructure deprives the enterprise of the ability to conduct its operations or verify its financial standing (in this case, a loss of value may be one possible consequence, but it is not the defining characteristic).

The second axis is the origin of the threat - whether it arises outside or within the boundaries of the enterprise. An external threat is one that originates from a source beyond the enterprise's control, while an internal threat stems from the enterprise's own personnel, processes, or systems. The combination of these two axes allows for the identification of four distinct, equivalent classes of threats.

Class A: Threats to financial resources originating from outside the organization. Examples include the withdrawal of a credit line, fluctuations in exchange rates that increase the burden of foreign-currency-denominated liabilities, or the insolvency of a counterparty holding the enterprise's funds. This class of threats is the most extensively covered in existing literature and is typically factored into the calculation of financial ratios.

Class B: Threats to financial resources originating from within the organization. These arise from the enterprise's own decisions or actions that damage its financial position - for instance, accumulating liabilities with maturity dates that do not align with cash inflows; extending loans to affiliated entities on terms that fail to account for the associated risks; or maintaining a client portfolio or product mix with a high level of concentration, which leaves the enterprise vulnerable to decisions made by third parties. In the literature, this category is addressed within the context of internal threats.

Category C: Threats to information infrastructure originating from outside the organization. These include the initiation of fraudulent payments by third parties; service disruptions at external providers of payment, cloud, or software solutions; and the disclosure of the enterprise's financial information to third parties who might exploit it for their own benefit.

Category D: Threats to information infrastructure originating from within the organization. These are linked to the actions or omissions of personnel and the specific nature of the enterprise's internal processes - such as concentrating the authority to authorize payments among a small group of individuals, failing to segregate duties between the person who initiates a payment and the person who approves it, or neglecting to revoke access rights in a timely manner when an employee leaves the organization. Of the four categories listed, this one is the least explored: literature on information security focuses

primarily on external attacks, while literature on financial security concentrates on threats of a directly financial nature.

This classification possesses three properties absent from existing categorization systems, each of which serves as an argument in favor of its adoption. First, each class corresponds to specific components of the assessment framework (Table 1). Within the information security domain, distinctions are drawn based on the source of the threat, which in turn dictates the choice of countermeasures: access controls are applied against external threats, while measures related to process organization and the segregation of duties are used against internal ones. This alignment allows for a unified assessment framework to be applied to both types of indicators, ensuring that the information security component does not become an isolated, "alien" add-on.

Second, this classification distinguishes between the object of a threat and its source, enabling them to be evaluated both individually and collectively. An enterprise might be well-protected against external intrusion yet suffer from significant internal flaws - or vice versa. If threats were classified solely by their source, both scenarios would simply characterize the enterprise as being exposed to both internal and external threats, without specifying where the vulnerability actually lies.

Third, this classification is both exhaustive and self-contained. Every threat necessarily involves an object (the resources or the infrastructure used to manage them) and a location (inside or outside the enterprise). Consequently, the four defined classes encompass the entire spectrum of potential threats; a threat register compiled using this classification ensures that no threat goes unnoticed simply because it does not "fit" into the established framework. Furthermore, the classification can serve as a checklist, allowing an enterprise to analyze the specific threats it faces within each class. If no threats have been recorded for a particular class, this does not constitute an answer; rather, it serves as a prompt to raise the question.

Table – Classes of threats and the blocks of the assessment system to which they correspond

Class	Blocks of the assessment system	Principal indicators
A – financial resources, external	Solvency; liquidity; cash flow	Current liquidity ratio; quick and absolute liquidity ratios; receivables turnover period; share of overdue payables
B – financial resources, internal	Capital structure; profitability; cash flow	Autonomy ratio; debt-to-equity ratio; interest coverage; return on assets; volatility of return on sales; free cash flow
C – information infrastructure, external	Information security	Share of transactions through protected channels; fraud losses as a share of revenue; mean time to detect and contain; concentration with a single external provider
D – information infrastructure, internal	Information security	Concentration of payment authority; segregation of duties; tested recovery arrangements; incidents affecting financial processes

It should be noted that the correspondence presented in Table 1 is not perfectly precise for every indicator. Two indicators within the "cash flows" category - the accounts

receivable turnover period and the share of overdue accounts payable- respond to threats from both Class A and Class B. For instance, an increase in the accounts receivable turnover period could result either from the actions of counterparties or from a deliberate decision by the enterprise to grant them extended payment terms in order to preserve business relationships. Meanwhile, the "information security" category encompasses indicators related to threats in Classes C and D. Thus, a "many-to-many" relationship exists at the periphery of the system; this is an inherent characteristic of the subject being classified, not a flaw in the classification itself. Since threats are not confined strictly to the enterprise or its external environment, any classification that artificially imposed such boundaries would lead to a distorted view of the organization's risk exposure.

Thus, categorizing financial security threats into specific groups–internal and external threats to financial resources, and internal and external threats to an organization’s information infrastructure–allows for a clear distinction between the object of a threat and its source. This enables an assessment of these threats both individually and collectively, facilitating a well-founded approach to selecting countermeasures.

Список использованных источников

1. Никулин, Р.Ю. Классификация угроз экономической безопасности предприятия / Р.Ю. Никулин // Стратегии бизнеса. - 2022. - Т. 10, № 7. - С. 167-171.

2. Кузнецова, І.О. Класифікація загроз економічній безпеці підприємства / І.О. Кузнецова, О.О. Кюне // Вісник соціально-економічних досліджень. - 2015. - Вип. 3 (58). - С. 120-28.