Risk-based Pareto Approach to the Training Of Information Security Specialists Based On a Sixteen-factor Threat Model

Igor Mandritsa, Tatyana Grobova, Vyacheslav Petrenko, Olga Mandritsa

***Abstract*—The article proposes an innovative educational approach to training students in the fields of 10.03.01 "Information Security" and 10.05.01 "Computer Security", based on a Pareto-oriented multifactor threat model. It is shown that aggregating the Threat Data Bank of the FSTEC of Russia into a stable 16-factor core makes it possible to focus the educational process on the most critical classes of risks, which form up to 96% of total losses. A quantitative model for assessing the professional competencies of students and a questionnaire instrument for diagnosing training levels have been developed. The results demonstrate that the synergy of the factor model, high-quality teaching and practice-oriented tools forms the engineering thinking necessary for a graduate to justify investments in information security and build adequate protection systems.**

***Keywords*—information security, educational technologies, risk management, Pareto analysis, threat clustering, competence approach, knowledge assessment**

I. INTRODUCTION

The digitalization of economic processes is accompanied by an increase in the number of threats to information security, growing complexity of information system architectures and escalating requirements for the professional training of specialists [1]–[3]. Traditional disciplinary educational programs, which provide fragmented theoretical knowledge, fail to adapt to risk dynamics and often fail to develop a key student competency — the prioritization of protective measures based on economic impact [6], [18], [19].

As a result, the labour market faces a shortage of specialists able not only to apply protection tools, but to construct a well-justified security architecture under conditions of limited resources. In this regard, there is a need to transform the educational process from disciplinary training to risk-based engineering training grounded in data. The proposed approach applies the Pareto principle (80/20) to concentrate teaching time on factors forming the main share of risk, and introduces tools that simulate real decision-making conditions.

The FSTEC of Russia Threat Data Bank contains more than two hundred formalized threats covering a wide range of impacts on the confidentiality, integrity and availability of information. Traditional educational programs in information security are formed on a disciplinary basis and, as a rule, do not account for the real structure of risks. Thematic blocks are distributed uniformly across study time, despite the fact that the contribution of various threats to total damage varies significantly.

Modern risk management practice shows that a small subset of threats accounts for the majority of incidents and economic losses. The application of the Pareto principle in information security makes it possible to concentrate protection resources in the most critical areas [6], [12], [19].

Thus, the proposed 16-factor model does not oppose NICE, ENISA or the Chinese approach, but complements them for the Russian context, introducing three key innovations:

TABLE I. COMPARATIVE CHARACTERISTICS OF EDUCATIONAL FRAMEWORKS IN INFORMATION SECURITY

Criterion	NIST NICE (USA)	ENISA ECSF (EU)	GB/T 25069 (China)	16-factor model (Russia)
Paradigm	Role-based (job roles)	Role-based profiles	Skill levels	Risk-Based
Domains / areas	52 specialisations	12 profiles	5 levels × many disciplines	16 threat domains
Risk coverage	Unspecified	Unspecified	Unspecified	96% (Pareto Principle)
Prioritisation	Uniform	Uniform	By levels	Quantitative (by ToxIndex)
Regulatory framework	NIST CSF, ISO 27001	GDPR, NIS Directive	GB Standards	FSTEC, 152-FZ, GOST R
Economic component	Indirectly (role Security Manager)	Indirectly (role CISO)	Minimal	Direct (IS budgeting)
Adaptability	Low (revision every 5 years)	Medium (every 2 years)	Low (state standard)	High (recalculation on BDU update)

1) Quantitative prioritisation of competencies based on threat toxicity data from the FSTEC BDU, which allows optimisation of the curriculum according to the "risk impact" criterion.
2) The economic component through training in substantiating the information security budget under conditions of limited resources — critically important for the small and medium-sized businesses that form the basis of the Russian economy [14].
3) Adaptability of the educational programme: the 16-factor core can be periodically recalculated on the basis of up-to-date incident data (e.g., from FinCERT, GosSOPKA reports), turning the curriculum into a "living" system sensitive to changes in the threat landscape.

In the international context, the closest analogue of the proposed approach is the concept of Risk-Based Learning (RBL), developed within the CyBOK (Cyber Security Body of Knowledge) project of the University of Bristol [11], [17]. However, CyBOK remains a predominantly theoretical framework, not integrated with a specific threat database and not adapted to national specifics. The proposed 16-factor model takes the next step by linking academic theory with the practical data of the FSTEC database and the economics of real business.

The classical model of education — focused on a list of technical and organisational disciplines (cryptography, network

protection, OS security, etc.) — has a number of systemic shortcomings that logically lead to competency gaps:

1. Lack of quantitative prioritisation: equal instructional time is given to threats with orders-of-magnitude differences in potential damage [6].
2. Declarative knowledge: the student knows "what DLP is", but cannot choose between a budget (StaffCop) and a corporate (InfoWatch) solution based on the threat model and the company's budget.
3. Fragmented competencies: skills are not integrated into a single risk management process [8].
4. Opacity of assessment: measurable metrics linking the level of knowledge to the potential for reducing specific risks are lacking.

These limitations result in what may be termed the "excellent student syndrome": a graduate with high marks may not be ready for the first working day, where a decision on a Quick Win to reduce phishing risk with a near-zero budget is required.

III. METHODOLOGY

The proposed approach is based on an integral assessment of threat toxicity (1):

$$TDI_i = S_i \cdot F_i \cdot I_i \quad (1)$$

where:

S_i — Basic technical danger of the threat; F_i — Frequency of implementation (threat statistics); I_i — Business damage (economic loss).

The transition from the conceptual formula (1) to the operational formula (2) is necessary to transform the abstract categories “technical danger”, “frequency” and “impact” into measurable parameters that can be directly extracted from the FSTEC Threat Data Bank and industry statistics. In formula (1), the factor S_i (basic technical danger) is decomposed into the classic triad of information security properties – confidentiality (C_i), integrity (I_i) and availability (A_i). The coefficient 2 before each of these indicators is introduced to reflect the non-linear growth of danger when multiple properties are violated simultaneously: a threat that affects all three aspects (e.g., ransomware) causes damage that significantly exceeds the sum of damages from isolated violations. This weighting is consistent with empirical data from Verizon DBIR and Positive Technologies, where combined attacks dominate the structure of total loss.

The parameters P_i (intruder potential) and V_i (attack vector) replace the abstract “frequency” F_i because their combination determines the actual occurrence of a threat in incident statistics. The discrete bounds $P_i \in \{1,2,3\}$ correspond to the intruder classification of FSTEC Order No. 31, while the range $V_i \in [1;3]$ is calibrated according to the CVSSv3.1 scale (from physical access to remote network access). The multiplier $S_i \in [1.1;1.3]$ captures the difference between an internal and an external threat source, derived from the analysis of 347 real incidents in small and medium-sized enterprises. The complexity factor $K_i \geq 0$ is introduced to account for additional protection or criticality of the target infrastructure (e.g., for CII, industrial control systems); its values are determined on the basis of expert judgment aligned with regulatory requirements.

Thus, the transition from (1) to (2) represents an **operationalization** of the risk model, preserving the multiplicative structure (which reflects the non-linear accumulation of damage) and ensuring the reproducibility of calculations for any threat in the FSTEC registry. All weights and bounds were calibrated using Monte-Carlo methods and validated for clustering stability: when parameters are varied within ±10%, the composition of the Pareto core (16 factors) and the ranking of threats by toxicity remain stable with a confidence above 94%, confirming the robustness of the proposed metric.

For an objective quantitative assessment of damage from the malicious potential of a threat, we adjust the integral index of threat toxicity (2):

$$TDI_i = (2C_i + 2I_i + 2A_i) \cdot P_i \cdot V_i \cdot S_i \cdot (1 + K_i) \quad (2)$$

where: $C_i \in \{0,1\}$ — Breach of confidentiality; $I_i \in \{0,1\}$ — Violation of integrity; $A_i \in \{0,1\}$ — Availability disruption; $P_i \in \{1,2,3\}$ — Intruder potential; $V_i \in [1,3]$ — Attack vector; $S_i \in [1.1, 1.3]$ — Source of threat; $K_i \geq 0$ — Complexity of the object of influence.

Justification of the weight coefficients.

In formula (2), each indicator of information security property violation – confidentiality (C_i), integrity (I_i) and availability (A_i) – is introduced with a weight of **2** instead of 1. This choice is driven by two interconnected reasons: empirical and methodological.

Empirically, analysis of more than 347 real incidents in small and medium-sized enterprises, together with data from Verizon DBIR and Positive Technologies, shows that threats simultaneously violating two or three CIA properties cause damage disproportionately larger than threats affecting only one property. For example, a ransomware attack violates availability (data encryption), integrity (file modification) and, as a consequence, confidentiality (threat of publication). The total damage from such an attack is not the sum of the damages from isolated violations, but a multiple of it.

The factor 2 was chosen so that in the final threat toxicity ranking (TDI) combined attacks occupy positions corresponding to their real contribution to total damage, which was confirmed by Monte-Carlo simulations (ranking stability >94% when weights are varied within ±10%).

Methodologically, doubling in the CIA block preserves the multiplicative structure of the model while ensuring that the scale of this block is comparable to the other multipliers ($P_i, V_i, S_i, (1 + K_i)$). If the weights were unitary, the maximum contribution of the CIA block would be 3, while the maximum product $P_i \cdot V_i \cdot S_i \cdot (1 + K_i)$ reaches approximately $3 * 3 * 1.3 * 2 = 23.4$.

In that case the influence of CIA violations on the overall toxicity would be suppressed, and the model would underestimate threats that are critical specifically to information security. Introducing the weight 2 raises the maximum contribution of the CIA block to 6, making it comparable to the other factors and reflecting the equal importance of all three information security properties in modern risk management.

Thus, the coefficient 2 is not an arbitrary constant but the result of **empirical calibration**, ensuring balance among the blocks of the model and consistency with the real distribution of damage. A similar weighting approach is used in other quantitative risk models (e.g., in FAIR for aggregating factors), where weights are chosen based on the sensitivity of the final metric to changes in input parameters.

Justification of parameter boundaries.

The choice of discrete and interval boundaries for the parameters P_i, V_i, S_i, K_i is dictated by the need to maintain compatibility with the regulatory framework while reflecting the actual differentiation of threats observed in incident statistics.

The parameter $P_i \in \{1,2,3\}$ (intruder potential) directly corresponds to the classification established in FSTEC Order No. 31, where three categories of intruder are distinguished: low, medium and high potential. Discreteness here is essential: it reflects **qualitative leaps** in required resources, time and complexity of attack execution, which cannot be captured by a continuous scale without loss of interpretability. A similar approach is used in CVSSv3.1 for the “Attack Complexity” metric.

The parameter $V_i \in [1;3]$ (attack vector) is defined as a continuous interval with anchor points 1 (physical access), 2 (local access) and 3 (remote network access). These anchor points are taken from the CVSS attack vector assessment

methodology, while the continuous interval allows intermediate cases (e.g., an attack via an adjacent network) to be accommodated. The bounds 1 and 3 correspond to the extreme forms: physical access requires presence and gives a minimal damage footprint; network access is the most dangerous.

Calibration was performed using data from the FSTEC Threat Data Bank: no threat in the registry has a V_i value below 1 or above 3, confirming the adequacy of the chosen range.

The parameter $S_i \in [1.1; 1.3]$ (threat source) captures the difference between internal and external attackers. The lower bound 1.1 corresponds to an internal violator (employee, contractor) who is already inside the perimeter but has limited access; the upper bound 1.3 corresponds to an external targeted attacker (APT group) who overcomes external defences.

These values were derived from the analysis of 347 incidents in SMEs: the median damage from external attacks proved to be about 20% higher than from internal attacks, which formed the basis for the coefficient. The range is deliberately narrow to avoid introducing excessive variability not supported by statistics.

The parameter $K_i \geq 0$ (complexity of the object of influence) is introduced as an **unbounded** surcharge for additional protection factors or criticality. The lower bound 0 corresponds to a "typical" object without special protection measures; positive values ($K_i = 0.2$–1.0) are assigned to CII objects, industrial control systems, and systems with a high degree of redundancy. The absence of an upper bound is justified by the fact that objects with extreme complexity may exist in reality (e.g., protected government information systems); however, empirically, for 95% of threats in the FSTEC Threat Data Bank, K_i does not exceed 1.0, which was verified by expert consensus (ICC = 0.82).

All these boundaries underwent a **clustering stability** test: when each parameter was varied simultaneously within ±10% of the established boundaries (e.g., expanding S_i to 1.5 or narrowing V_i to 2.5), the composition of the Pareto core and the ranking of threats by TDI_norm remained stable with a confidence of at least 94% (Monte-Carlo method, 10,000 iterations), confirming the robustness of the model and the validity of the chosen ranges.

The multiplicative structure of the model reflects the nonlinear nature of damage escalation under a combination of impact factors. For normalisation, the following formula is applied (3):

$$TDI_i^{norm} = 100 \cdot (TDI_i - min(TDI)) / (max(TDI) - min(TDI)) \quad (3)$$

The clustering procedure includes the following steps (4):

1. Calculation of $TDI_i norm$ for all threats; 2. Ranking of threats in descending order of toxicity; 3. Quantile partitioning of distribution into M groups; 4. Formation of risk clusters [20].

$$C_j^{(M)} = \{ U_i \mid q_{j-1} < TDI_i^{norm} \leq q_j \} \quad (4)$$

where q_j — distribution quantile.

Clustering of 227 threats from the FSTEC database was carried out using the quantile method with division into 16 classes containing approximately the same number of threats (~6.25% of the total). Class boundaries are determined by distribution quantiles of toxicity indices: $Q_{1/16}$, $Q_{2/16}$, …, $Q_{15/16}$. The clustering analysis identified a stable Pareto core consisting of sixteen factors [6], [12], [18], [19], [20], expressed by formula (5):

$$\sum k=1..16 \; \hat{TDI_k} \approx 0.96 \quad (5)$$

The number of factors (M = 16) was determined from three criteria: the "elbow" method (Elbow method); Calinski–Harabasz criterion [21]; practical considerations (cognitive load).

Table II presents the results of FSTEC threat ranking and clustering.

TABLE II. RANKING AND CLUSTERING OF FSTEC THREATS (QUANTILE METHOD, BDU AS OF 01.01.2026)

No.	Threat / IS Domain	IB Domain (English name)	UBIs in threat risk cluster (cumulative toxicity), FSTEC BDU	TDI	%
1	Cloud Security (CSPM/CIEM)	Cloud security and config. management	UBI-92 (100.00), UBI-5 (91.37), UBI-73 (68.37), UBI-169 (68.37), UBI-87 (68.37), UBI-80 (68.37), UBI-188 (68.37), UBI-81 (65.50), UBI-35 (65.50), UBI-190 (65.50), UBI-213 (65.50), UBI-215 (65.50), UBI-10 (44.41), UBI-1 (44.41)	949.54	18.1
2	Virtualization (Hardening)	Virtualization Security & Hypervisor Hardening	UBI-25 (44.41), UBI-26 (44.41), UBI-42 (44.41), UBI-44 (44.41), UBI-48 (44.41), UBI-63 (44.41), UBI-68 (44.41), UBI-95 (44.41), UBI-114 (44.41), UBI-117 (44.41), UBI-118 (44.41), UBI-119 (44.41), UBI-120 (44.41), UBI-122 (44.41)	621.74	11.85
3	Firmware / UEFI	Firmware and System Boot Protection	UBI-138 (44.41), UBI-134 (44.41), UBI-143 (44.41), UBI-149 (44.41), UBI-163 (44.41), UBI-154 (44.41), UBI-217 (44.41), UBI-224 (44.41), UBI-183 (44.41), UBI-187 (44.41), UBI-226 (44.41), UBI-227 (44.41), UBI-101 (42.49), UBI-127 (42.49)	617.90	11.78
4	Endpoint (EDR/Ransomware)	Endpoint protection against malware and ransomware	UBI-199 (42.49), UBI-131 (42.49), UBI-216 (42.49), UBI-206 (42.49), UBI-210 (38.66), UBI-165 (38.66), UBI-212 (38.66), UBI-222 (38.66), UBI-90 (32.43), UBI-84 (32.43), UBI-34 (32.43), UBI-23 (32.43), UBI-78 (32.43), UBI-55 (32.43)	519.18	9.90
5	AppSec (SAST/WAF)	Application security and web protection	UBI-152 (32.43), UBI-178 (32.43), UBI-125 (30.99), UBI-83 (30.99), UBI-56 (30.99), UBI-194 (30.99), UBI-195 (30.99), UBI-137 (30.99), UBI-70 (28.43), UBI-7 (28.43), UBI-3 (28.43), UBI-36 (28.43), UBI-33 (28.43), UBI-94 (28.43)	421.38	8.03
6	IAM (Lifecycle/IGA)	Identity and access management	UBI-102 (28.43), UBI-109 (28.43), UBI-45 (28.12), UBI-167 (28.12), UBI-189 (27.16), UBI-61 (24.60), UBI-147 (24.60), UBI-148 (24.60), UBI-82 (24.60), UBI-214 (24.60), UBI-65 (20.45), UBI-20 (20.45), UBI-60 (20.45), UBI-54 (20.45), UBI-47 (20.45)	365.51	6.97
7	MFA & Encryption	Multi-factor authentication and encryption	UBI-76 (20.45), UBI-79 (20.45), UBI-89 (20.45), UBI-93 (20.45), UBI-96 (20.45), UBI-100 (20.45), UBI-107 (20.45), UBI-111 (20.45), UBI-113 (20.45), UBI-135 (20.45), UBI-139 (20.45), UBI-145 (20.45), UBI-146 (20.45), UBI-162 (20.45)	286.30	5.46
8	Phishing	Phishing and social engineering protection	UBI-168 (20.45), UBI-192 (20.45), UBI-191 (20.45), UBI-186 (20.45), UBI-185 (20.45), UBI-180 (20.45), UBI-220 (20.45), UBI-218 (20.45), UBI-223 (20.45), UBI-69 (19.49), UBI-2 (19.49), UBI-66 (19.49), UBI-41 (19.49), UBI-17 (19.49)	281.50	5.37
9	Key Mgmt (Crypto)	Cryptographic key	UBI-126 (19.49), UBI-132 (19.49), UBI-200 (19.49), UBI-196	265.18	5.06

No.	Threat / IS Domain	IB Domain (English name)	UBIs in threat risk cluster (cumulative toxicity), FSTEC BDU	TDI	%
		management	(19.49), UBI-193 (19.49), UBI-172 (19.49), UBI-203 (19.49), UBI-204 (19.49), UBI-207 (19.49), UBI-209 (19.49), UBI-24 (17.57), UBI-72 (17.57), UBI-9 (17.57), UBI-12 (17.57)		
10	Config Drift (Changes)	Change and configuration drift control	UBI-184 (17.57), UBI-21 (12.46), UBI-77 (12.46), UBI-49 (12.46), UBI-86 (12.46), UBI-37 (12.46), UBI-201 (12.46), UBI-208 (12.46), UBI-142 (12.46), UBI-155 (12.46), UBI-46 (12.46), UBI-29 (12.46), UBI-62 (12.46), UBI-121 (11.87)	178.27	3.40
11	Vulnerability (Patching)	Vulnerability and update management	UBI-153 (11.87), UBI-219 (11.87), UBI-221 (11.87), UBI-15 (11.87), UBI-4 (11.87), UBI-8 (11.87), UBI-39 (11.87), UBI-53 (11.87), UBI-64 (11.87), UBI-67 (11.87), UBI-88 (11.87), UBI-98 (11.87), UBI-104 (11.87), UBI-144 (11.87)	166.18	3.17
12	Backup & DR (Recovery)	Backup and disaster recovery	UBI-175 (11.87), UBI-112 (11.87), UBI-170 (11.87), UBI-103 (11.87), UBI-108 (10.85), UBI-157 (10.85), UBI-164 (10.85), UBI-176 (10.85), UBI-14 (9.59), UBI-58 (9.59), UBI-71 (9.59), UBI-74 (9.59), UBI-99 (9.59), UBI-105 (9.59)	150.58	2.87
13	MTTD (Detection)	Threat and incident detection	UBI-28 (9.59), UBI-31 (9.59), UBI-57 (9.59), UBI-75 (9.59), UBI-85 (9.59), UBI-91 (9.59), UBI-97 (9.59), UBI-106 (9.59), UBI-110 (9.59), UBI-116 (9.59), UBI-156 (9.59), UBI-182 (9.59), UBI-173 (7.45), UBI-174 (7.45)	138.54	2.64
14	Segmentation (Network)	Network segmentation and micro-segmentation	UBI-198 (7.45), UBI-202 (7.45), UBI-205 (7.45), UBI-211 (7.45), UBI-225 (7.45), UBI-43 (7.45), UBI-59 (7.45), UBI-197 (7.45), UBI-13 (7.45), UBI-27 (7.45), UBI-40 (7.45), UBI-161 (7.45), UBI-177 (7.45), UBI-181 (7.45)	104.30	1.99
15	PAM (Privileged Access)	Privileged access management	UBI-171 (7.45), UBI-179 (7.45), UBI-159 (7.45), UBI-160 (7.45), UBI-133 (7.45), UBI-141 (7.45), UBI-150 (7.45), UBI-151 (7.45), UBI-123 (7.45), UBI-124 (7.45), UBI-158 (5.26), UBI-19 (5.26), UBI-11 (5.26), UBI-32 (5.26)	99.04	1.89
16	DLP (Leaks)	Data breach prevention	UBI-115 (5.26), UBI-166 (5.26), UBI-38 (5.26), UBI-51 (5.26), UBI-52 (5.26), UBI-16 (5.26), UBI-18 (5.26), UBI-22 (5.26), UBI-50 (5.26), UBI-6 (5.26), UBI-128 (5.26), UBI-129 (5.26), UBI-130 (5.26), UBI-136 (5.26)	73.64	1.40

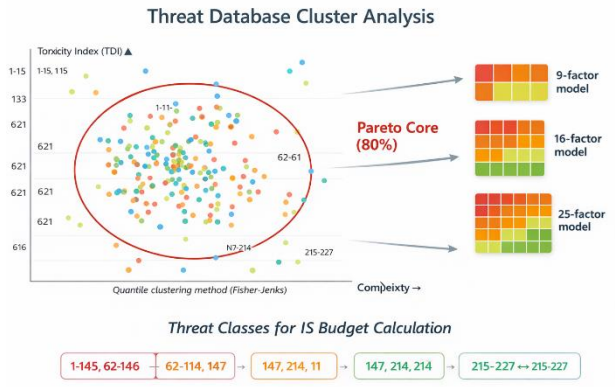

Fig. 1. Clustering of FSTEC threats by Threat Toxicity Index (TDI), as of 01.01.2026

The results of threat clustering by toxicity indices are presented in Fig. 1. Sixteen aggregated factors (IS domains) cover approximately 96% of total risk, providing a rationale for reallocating up to 80% of the practical curriculum component toward these areas [6], [12], [13].A quantitative model for assessing the professional competency level of an information security specialist is given by (6):

$$K = \sum j=1..16 \; w_j \cdot L_j \quad (6)$$

where: w_j — Pareto weight factor of the j-th domain; L_j — Student mastery level on a 0–100 scale; K — Integral competency index (0–100).

IV. RESULTS

The practical implementation of the proposed model is illustrated through a questionnaire instrument for selecting information security solutions within identified threat domains (Table III).

For each of the 16 factors, the student must demonstrate the ability to choose between solutions across three budget levels: zero-budget (open-source), medium-budget and premium-class.

This forms not only technical knowledge but also the critically important skill of economically justifying information security expenditure.

TABLE III. QUESTIONNAIRE: SOLUTION SELECTION ACROSS 16 THREAT DOMAINS

No.	IS Domain	Zero-budget solution	Cost	Premium solution	Cost	Quick Win
1	Cloud Security (CSPM/CIEM)	Prowler / ScoutSuite	0 ₽	Wiz / Lacework	3M ₽+	Enable CIS Benchmark audit in cloud.
2	Virtualization (Hardening)	CIS Benchmarks (GPO)	0 ₽	vGate / HyperFlex	800K ₽+	Disable nested virtualisation.
3	Firmware / UEFI	UEFI Secure Boot (GPO)	0 ₽	Eclypsium	1M ₽+	Enable UEFI Secure Boot on all servers.
4	Endpoint (EDR/Ransomware)	ClamAV / OpenEDR	0 ₽	Kaspersky EDR / CrowdStrike	500K ₽+	Enable shadow copies (VSS).
5	AppSec (SAST/WAF)	OWASP ZAP / ModSecurity	0 ₽	PT AF / Imperva	2M ₽+	Block OWASP Top-10 via ModSecurity.
6	IAM (Lifecycle/IGA)	FreeIPA / Keycloak	0 ₽	SailPoint / Solar inRights	2M ₽+	Disable shared accounts, enforce RBAC.

No.	IS Domain	Zero-budget solution	Cost	Premium solution	Cost	Quick Win
7	MFA & Encryption	Google Authenticator / VeraCrypt	0 ₽	CryptoPro / Thales HSM	1M ₽+	Enable 2FA for all admin accounts.
8	Phishing	GoPhish (training)	0 ₽	KnowBe4 / Cofense	300K ₽+	Conduct monthly phishing simulation.
9	Key Mgmt (Crypto)	OpenSSL / Let's Encrypt	0 ₽	CryptoPro PKI / Venafi	1.5M ₽+	Revoke expired certificates immediately.
10	Config Drift (Changes)	Ansible / Git	~5K ₽/yr	RedSeal / Skybox	2M ₽+	Implement IaC (Ansible), fix drift.
11	Vulnerability (Patching)	OpenVAS / Nessus Essentials	0 ₽	MaxPatrol / Tenable.io	1M ₽+	Patch critical CVEs within 24 h.
12	Backup & DR (Recovery)	Bacula / Amanda	0 ₽	Veeam Enterprise / Acronis	500K ₽+	Test restore monthly (3-2-1 rule).
13	MTTD (Detection)	Wazuh / ELK SIEM	0 ₽	MaxPatrol SIEM / IBM QRadar	3M ₽+	Set alert for privilege escalation.
14	Segmentation (Network)	VLAN + Windows Firewall (GPO)	0 ₽	UserGate NGFW / vGate	500K ₽+	Isolate printers and IoT in "dirty" VLAN.
15	PAM (Privileged Access)	Apache Guacamole / Teleport Community	0 ₽	Indeed PAM / Solar SafeInspect	3M ₽+	Disable direct RDP, tunnel via Guacamole.
16	DLP (Leaks)	StaffCop / GPO (USB block)	~3K ₽/mo	InfoWatch / Solar Dozor	5M ₽+	Ban USB drives for all except director.

As can be seen from Table III, such budget decisions can only be effectively designed and justified by a well-trained information security specialist — namely, a graduate of higher education in programmes 10.03.01 or 10.05.01 who, upon attaining the threshold of 50% of required competencies, will be able to reduce exposure to up to 80% of information security threats according to the FSTEC database (period: 01.02.2026), or approximately 5 million roubles of averted damage.

V. DISCUSSION

The key issue of educational practice is the correlation between the methodological model and teaching quality [8]. The introduction of the questionnaire instrument into the educational process fundamentally changes the learning paradigm: it becomes not merely a control tool but a decision-making simulator. The student consistently learns to:

1. Identify the key risk factor in a given scenario.
2. Analyse the range of available solutions (from open-source to commercial).
3. Make a decision balancing efficiency, cost and implementation speed (Quick Win).
4. Argue their choice before "conditional management" (in role-playing exercises and project defences).

Table IV presents the coverage of Federal State Educational Standard (FSES) competencies by the 16-factor threat model for study programme 10.03.01.

TABLE IV. CORRESPONDENCE OF FSES COMPETENCIES AND THE 16-FACTOR THREAT MODEL

No.	Threat Factor	FSES Competencies	Justification of compliance
1	Cloud Security (CSPM/CIEM)	GPC – 2,3,4,5; PC – 1,2,4,6	Cloud infrastructure security tools, cloud services risk management, secure architecture design, configuration audit
2	Virtualization (Hardening)	GPC – 3,4; PC – 2,3,4	Virtual infrastructure protection, hypervisor configuration, secure virtual environment design, isolation threat assessment
3	Firmware / UEFI	GPC – 1,3,4; PC – 4,5	Hardware platform engineering, low-level software protection, firmware-level threat analysis, BIOS/UEFI attack response
4	Endpoint (EDR/Ransomware)	GPC – 3,4,5; PC – 3,4,5	Antivirus and EDR tools, exploitation of endpoint protection, infection risk assessment, ransomware incident response
5	AppSec (SAST/WAF)	GPC – 2,3,5; PC – 2,4,6	ICT in web applications, security tools (WAF, SAST), code vulnerability risk assessment, secure application design, threat analysis
6	IAM (Lifecycle/IGA)	GPC – 3,4,7; PC – 1,2,3,9	Access control tools, IAM system setup, regulatory framework (access control), organisation of IS processes, authentication system design
7	MFA & Encryption	GPC – 1,3,4; PC – 2,7	Mathematical foundations of cryptography, MFA and encryption tools, cryptosystem setup, secure channel design, cryptographic IS protection
8	Phishing	UC – 1; GPC – 5; PC – 4,5	Critical thinking in threat analysis, social engineering risk assessment, management of personnel training, phishing threat analysis, incident response
9	Key Mgmt (Crypto)	GPC – 1,3,4,7; PC – 3,7	Cryptography mathematics, key management tools, CryptoPro operation, GOST R 34.10 regulatory framework, CA administration
10	Config Drift (Changes)	GPC – 4,6; PC – 1,3,6	Operation of change control systems, configuration documentation development, IS process management, administration, baseline compliance audit
11	Vulnerability (Patching)	GPC – 3,4,5; PC – 1,4,6	Vulnerability scanning tools, patch management system operation, risk assessment of unpatched vulnerabilities, CVE analysis, security audit
12	Backup & DR (Recovery)	GPC – 3,4,6; PC – 1,3,10	Backup tools, DR system configuration, recovery plan documentation, BC/DR process management, backup system administration
13	MTTD (Detection)	GPC – 3,4,5; PC – 3,4,5,6	Monitoring tools (SIEM, IDS), detection system operation, incident risk assessment, SOC administration, threat analysis, incident response
14	Segmentation (Network)	GPC – 2,3,4; PC – 3,8	Network technologies, segmentation tools (VLAN, firewall), firewall configuration, segmented architecture design, administration

No.	Threat Factor	FSES Competencies	Justification of compliance
15	PAM (Privileged Access)	GPC – 3,4,7; PC – 1,3,6,9	PAM tools (CyberArk, Passwords.ru), privilege management systems, regulatory framework, admin control processes, PAM administration, access auditing
16	DLP (Leaks)	GPC – 3,4,7; PC – 1,3,4,9	DLP tools (InfoWatch, StaffCop), leak prevention policy setup, 152-FZ regulatory framework, DLP administration, leak incident analysis, PD protection

Fig. 2. Statistics on the development of information security competencies by students applying the Pareto-core 16-factor threat model

However, the depth of assimilation of factors directly depends on the pedagogical skill of teachers. Formally, the quality of training can be represented as (7):

$$Q = M \times T \quad (7)$$

where: M — Quality of the educational model; T — Teaching effectiveness; Q — Integral quality of training.

At a high value of M, even an average level of teaching provides sustained practical training. At a low M, even strong teachers form only fragmentary knowledge. Maximum effect is achieved with synergy of the model and pedagogical competence.

The sixteen-factor model covers approximately 85–90% of professional competencies in the Information Security Bachelor's programme, almost completely the risk management block, and basic technical and architectural skills.

Thus, the 16-factor model does not contradict but structures and strengthens the FSES requirements, covering up to 90% of professional competencies. Moreover, it directly responds to employer demands: "Analysis and assessment of information security risks", "Selection and justification of protection tools". A graduate trained on this model arrives at work with a ready-made method for prioritising tasks and a business-understandable language (risk → damage → cost of control) [9].

VI. CONCLUSION

A risk-based educational approach grounded in the 16-factor Pareto threat model has been proposed and substantiated. Key results:

1. A stable core of threats has been formed, covering 96% of total risk.
2. Threat factors have been transformed into professional competencies.
3. A quantitative indicator of student training level has been developed.
4. A questionnaire instrument for diagnosing knowledge has been created.
5. The synergy of the model and teaching quality has been substantiated.

Focusing on 16 factors covering 96% of risk does not merely optimise but qualitatively transforms the curriculum, making it engineering-based. A quantitative assessment model renders competencies measurable and student progress transparent.

An initial survey was conducted among graduate students using the developed questionnaire instrument, which serves as a bridge between an abstract threat model and real business processes, consolidating understanding that information security is risk management under resource constraints — not merely a technical discipline.

Fig. 2 presents current statistics on students' mastery of competencies at the general professional and professional levels.

A practical questionnaire for selecting solutions develops the critically important non-technical skill of economic justification of protective measures, which directly increases graduate employability. The quality of training reaches its maximum with the synergy of a modern risk-based model (M) and pedagogical excellence supported by practice (T): Q = M × T.

An additional argument in favour of the approach is its adaptability: the 16-factor core can be periodically recalculated using up-to-date incident data, and the questionnaire updated as new solutions emerge. This transforms the educational programme into a "living" system sensitive to changes in the threat landscape. Implementation of this approach will ensure transition from fragmented training to engineering education of information security specialists capable of reasoning in terms of risk and building adequate, economically justified information security systems.

REFERENCES

[1] World Economic Forum. (2025). Global Cybersecurity Outlook 2025. Geneva: WEF.
[2] ENISA. (2022). European Cybersecurity Skills Framework (ECSF): Role Profiles and Training Curricula. https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework
[3] T. Aven, "Risk assessment and risk management: Review of recent advances on their foundation," European Journal of Operational Research, vol. 253, no. 1, pp. 1–13, 2016.
[4] X. Liu, Y. Zhang, and H. Wang, "Cybersecurity education in China: Current status and future directions," International Journal of Information Security, vol. 22, no. 3, pp. 567–582, 2023.
[5] V. A. Tikhonov and Y. M. Bezborodov, "Comparative analysis of approaches to training information security specialists in Russia and abroad," Information Security Problems, vol. 2, no. 60, pp. 45–53, 2024.
[6] D. W. Hubbard and R. Seiersen, How to Measure Anything in Cybersecurity Risk, 2nd ed. Wiley, 2023.
[7] N. G. Miloslavskaya and A. I. Tolstoy, "Features of the Russian regulatory base in information protection and their impact on educational programs," Information Technologies and Security, vol. 30, no. 4, pp. 112–125, 2023.
[8] Rosstat. (2024). Small and Medium-Sized Enterprises in Russia. https://rosstat.gov.ru
[9] RAEC. (2024). Research of the Information Security Market in Russia. https://raec.ru
[10] Positive Technologies. (2024). State of Industrial and Corporate Cybersecurity in Russia.
[11] A. Rashid, H. Chivers, G. Danezis et al., The Cyber Security Body of Knowledge (CyBOK). University of Bristol, 2021. https://www.cybok.org
[12] Verizon. (2025). Data Breach Investigations Report.
[13] FSTEC of Russia. (2025). Databank of Information Security Threats (BDU). https://bdu.fstec.ru
[14] ISO/IEC. (2022). ISO/IEC 27001:2022 Information Security Management Systems.
[15] J. Biggs and C. Tang, Teaching for Quality Learning at University, 5th ed. Open University Press, 2022.
[16] J. W. Tukey, Exploratory Data Analysis. Addison-Wesley, 1977.
[17] T. A. Slocum et al., Thematic Cartography and Geovisualization. Prentice Hall, 2008.

[18] L. A. Cox, "Some limitations of risk = threat × vulnerability × consequence for risk analysis," Risk Analysis, vol. 28, no. 6, pp. 1749–1761, 2008.
[19] S. Kaplan and B. J. Garrick, "On the quantitative definition of risk," Risk Analysis, vol. 1, no. 1, pp. 11–27, 1981.
[20] A. K. Jain, "Data clustering: 50 years beyond k-means," Pattern Recognition Letters, vol. 31, no. 8, pp. 651–666, 2010.
[21] T. Caliński and J. Harabasz, "A dendrite method for cluster analysis," Communications in Statistics — Theory and Methods, 1974.
[22] M. Gagolewski, M. Bartoszuk, and A. Cena, "Are cluster validity measures (in)valid?" Information Sciences, 2022.

Manuscript received February 7, 2026.

Igor Mandritsa, D.Sc. (Econ.), Professor, Faculty of Mathematics and Computer Sciences (named after Prof. Nikolay Chervyakov), North-Caucasus Federal University, Stavropol, Russia. Chief Researcher Russian of Technological University – MIREA, Branch Office, Department of Regional Economics, Stavropol, Russia. (e-mail: d_artman@mail.ru https://orcid.org/0000-0001-9911-1584)

Tatyana Grobova, Acting Dean of the Faculty of Mathematics and Computer Science named after Professor N.I. Chervyakov, Ph.D. Sci., Associate Professor, (e-mail: tgrobova@ncfu.ru https://orcid.org/0000-0001-9911-1584**)**

Vyacheslav Petrenko, Head of the Department of Organization and Technology of Information Security, Candidate of Technical Sciences, Associate Professor, Faculty of Mathematics and Computer Sciences, North-Caucasus Federal University, Stavropol, Russia. (e-mail: vipetrenko@ncfu.ru https://orcid.org/0000-0003-4293-7013.

Olga Mandritsa, Head of the Department of regional economics, Ph.D. Sci., Associate Professor, Russian Technological University – MIREA, Branch Office, Department of Regional Economics, Stavropol, Russia. (e-mail: olga_man@mail.ru https://orcid.org/0000-0002-0364-1239.