

INNOVATION SCIENCE AND TECHNOLOGY

ISSUE 7, PART 1 / JULY 2026

 Acceptance of papers



**Acceptance of
papers**

Published monthly



Topics

economics,
technology, social
sciences



EDITOR-IN-CHIEF:

Mirzaliyev Sanjar Makhmatjon ugli

DEPUTY EDITOR-IN-CHIEF:

Makhmudov Nosir Makhmudovich
DSc., Prof., Academician

DEPUTY EDITOR-IN-CHIEF:

Ochilov Bobur Bakhtiyor ugli – Senior
lecturer at TSUI

THE SCIENTIFIC-POPULAR ELECTRONIC
JOURNAL **"INNOVATION SCIENCE AND
TECHNOLOGY"** HAS BEEN REGISTERED
UNDER THE NUMBER **C-5669633** BY THE
AGENCY FOR INFORMATION AND MASS
COMMUNICATIONS (AOKA) OF THE
REPUBLIC OF UZBEKISTAN, EFFECTIVE
FROM OCTOBER 9, 2024.

CONTACTS

Phone: **+998 50 737 87 88**

Website: <https://ist-journal.uz>

Email: innovationist2025@gmail.com

The scientific electronic journal "Innovation Science and Technology" has been included in the list of scientific publications recommended for the publication of main scientific results of dissertations for the award of PhD and DSc degrees in economics and technical sciences, in accordance with the Resolution No. 370 of the Presidium of the Higher Attestation Commission of the Republic of Uzbekistan, dated May 8, 2025.

Editorial board:



Sharipov Kongiratbay Avezimbetovich,
Doctor of Technical Sciences (DSc), Professor



Abdurakhmanova Gulnora Kalandarovna, Doctor of
Economic Sciences (DSc), Professor



Cham Tat Huei,
Doctor of Philosophy (PhD), Professor (Malaysia)



Muhammad Imran Sadiq
Doctor of Philosophy in Economics (PhD), Professor,
Malaysia



Ahmed Aziz Ismail
Doctor of Technical Sciences (DSc),
Professor (Egypt)



Lee Chin
Doctor of Philosophy in Economics (PhD), (Malaysia)



Asongu Simplice
Doctor of Philosophy in Economics (PhD), Cameroon



Rui Dang
Doctor of Chemistry (DSc), Professor, China



Zahoor Ahmed
Doctor of Philosophy in Economics (PhD), Turkey



Shujaat Abbas
Doctor of Philosophy in Economics (PhD), Russia



Tina A Coffelt
Doctor of Philosophy in Educational Sciences (PhD),
USA



Abdikarimova Dinara Rustamxanovna
Doctor of Economic Sciences (DSc), Professor

Kurbonbekova Mohichehra Turobjonovna
Doctor of Economic Sciences (DSc), Professor

Alimardonov Ilkhom Muzrabshokovich
Doctor of Economic Sciences (DSc), Professor



Razakova Barno Sayfiyeva
Doctor of Philosophy in Economics (PhD)



Khasanov Sarvar Ulugbek ugli
Doctor of Philosophy in Economics (PhD)



Kholikova Rukhsora Sanjarovna
Associate Professor (PhD)

CONTENTS

PLATFORM MIDDLEWARE-MANAGEMENT: FROM RESOURCE CONTROL TO INTERACTION COORDINATION IN DIGITAL SERVICE ECOSYSTEMS.....	8
Ilgor Abdullayev	
APPROACHES TO IMPROVING KNOWLEDGE EXCHANGE PROCESSES IN INDUSTRIAL CLUSTERS.....	16
Mamadaliyev Anaxxon Ziyodillayevich	
IMPROVING EXPENDITURE ACCOUNTING IN HIGHER EDUCATION INSTITUTIONS	21
Islom Ergash ugli Khonimqulov	
MANAGEMENT OF FOREIGN EXCHANGE AND CONCENTRATION RISKS IN THE OPERATIONS OF COMMERCIAL BANKS	26
Qurbonov Ilhom Jumaqulovich	
WAYS TO IMPROVE THE USE OF NATURAL RESOURCES IN THE DEVELOPMENT OF HEALTH SERVICES.	29
Sobirov Kayum Xamraevich	
REGIONAL BANKING MARKET TRENDS FOR RETAIL DEVELOPMENT	33
Salamov Islom Tashqazaqovich	
REFORMS UNDERTAKEN IN THE REPUBLIC TO INCREASE PRODUCTION CAPACITY AT FOOD INDUSTRY ENTERPRISES	37
Gulmatov Sunnatillo Nurillayevich	
PROSPECTS FOR USING ISLAMIC FINTECH TECHNOLOGIES IN SMALL BUSINESS FINANCING IN UZBEKISTAN	44
Toshxo'jayev Abduqodirxon Abdulmansurxon ugli	
ADAPTIVE CONCEPT OF HUMAN CAPITAL MANAGEMENT: A NEW PARADIGM FOR SUSTAINABLE ECONOMIC GROWTH	51
Dinora Qudrat qizi Yusubboyeva	
MECHANISMS FOR ENHANCING EDUCATION SERVICE QUALITY IN DEVELOPING YOUTH ENTREPRENEURSHIP IN THE ARAL SEA REGION.....	58
Raxmanov Raxmanbergan Abdullayevich	
CONCEPTUAL FOUNDATIONS OF IMPLEMENTING AGILE MANAGEMENT IN PUBLIC ADMINISTRATION	62
Sayfiyev Jasur Ravshanovich	
SCIENTIFIC PERSPECTIVES OF WORLD, EUROPEAN, AND CIS SCHOLARS ON ENTREPRENEURSHIP DEVELOPMENT AND FINANCIAL SUPPORT: A COMPARATIVE ANALYSIS	70
Inobatov Abror Boshlarovich	
SUSTAINABILITY REPORTING AND ESG AUDITING: EMERGING TRENDS IN CORPORATE ACCOUNTABILITY.....	84
Turabekov Bekali, Eshpulatova Zaynab	
ИНДИКАТОРЫ ОЦЕНКИ И МОНИТОРИНГА РАЗВИТИЯ ЖЕНСКОГО ПРЕДПРИНИМАТЕЛЬСТВА В УЗБЕКИСТАНЕ	91
Хусанова Зулфия Рахматуллаевна	
A METHODOLOGICAL APPROACH TO DIGITALIZING INTERNAL AUDIT IN COMMERCIAL BANKS BASED ON THE CONTINUOUS AUDITING CONCEPT	95
Narziyev Xayotjon Azamatovich	
AN AUTHOR'S APPROACH TO THE CLASSIFICATION OF FINANCIAL INVESTMENTS BY MEASUREMENT BASIS FOR ACCOUNTING AND AUDITING PURPOSES	102
Jumamurodov To'libay Yeldashbayevich	
ENHANCING THE CONTINUOUS MONITORING PROCEDURE FOR IDENTIFYING IMPAIRMENT INDICATORS OF NON-CURRENT ASSETS IN JOINT-STOCK COMPANIES.....	107
Fayzullayev Begzod Baxtiyor o'g'li	

THE INTERRELATIONSHIP BETWEEN MATERIALITY AND AUDIT RISK IN PUBLIC-SECTOR INTERNAL AUDITING AND THEIR APPLICATION WITHIN A UNIFIED METHODOLOGICAL FRAMEWORK.....	114
Ismatillayev Baypo'lat Xushvaqtovich	
THE NATURE, DEFINITION AND CLASSIFICATION OF INTERNAL AUDIT OF PUBLIC PROCUREMENT	122
Rajabov Shukhrat Ismayilovich	
A METHODOLOGY FOR THE COMPOSITE ASSESSMENT OF THE MATURITY OF INTERNAL AUDIT FUNCTIONS IN COMMERCIAL BANKS.....	128
Ismailov Azizbek Madaminovich	
THE ECONOMIC SUBSTANCE OF THE CONCEPT OF "RISK-BASED INTERNAL AUDITING" AND THE THEORETICAL FOUNDATIONS OF ITS APPLICATION IN LIGHT INDUSTRY ENTERPRISES	136
Shahlo Mahmatmurodovna Tojiyeva	
THE INSTITUTIONAL MECHANISM FOR THE INNOVATIVE DEVELOPMENT OF THE RAILWAY NETWORK.....	143
Muradov Bakhrom Akramjanovich	
ТЕОРЕТИЧЕСКОЕ ОПРЕДЕЛЕНИЕ ОСНОВНЫХ СТАТИЧЕСКИХ ХАРАКТЕРИСТИК ОПТОЭЛЕКТРОННЫХ ДИСКРЕТНЫХ ПРЕОБРАЗОВАТЕЛЕЙ ПЕРЕМЕЩЕНИЙ С ПОЛЫМИ И ВОЛОКОННЫМИ СВЕТОВОДАМИ.....	148
Умид Садирдинович Холматов	
ИНСТИТУЦИОНАЛЬНЫЙ РАЗРЫВ В ЗАЩИТЕ ЗАЁМЩИКОВ: ЭМПИРИЧЕСКИЙ АНАЛИЗ НАЧИСЛЕНИЯ ПРОЦЕНТОВ И НЕУСТОЙКИ ПОСЛЕ СУДЕБНОГО ВЗЫСКАНИЯ В УЗБЕКИСТАНЕ..	155
Жаксымуратов Бахрам Раджович	
PROSPECTS FOR SMALL BUSINESS DEVELOPMENT IN THE CONTEXT OF THE GREEN ECONOMY.....	164
Abdurakhimov Iskandar Nodirjon o'g'li	
DIGITAL PAYMENT ADOPTION IN TOURISM: FACTORS INFLUENCING ACCEPTANCE IN SAMARKAND, UZBEKISTAN	169
Nazarova Kamola Sultonmurod qizi	
CHANGE MANAGEMENT IN THE ADOPTION OF BIM TECHNOLOGY IN UZBEKISTAN'S CONSTRUCTION PROJECTS: A CONCEPTUAL APPROACH BASED ON THE ADKAR MODEL.....	176
Shaxlo Baxtiyor qizi G'ulomova	
SMART DESTINATIONS, SMARTER JOURNEYS: SCIENCE, INNOVATION, AND THE DIGITAL TRANSFORMATION OF GLOBAL TOURISM.....	182
Sirojiddinova Shahrizoda, Nasimov Dilmurod Abdulloyevich	
SELECTION OF INPUT MAGNITUDE FOR INVESTIGATING KINEMATIC AND STRUCTURAL PARAMETERS OF VSH PTM ELLIPTICAL DRUM COTTON PICKING APPARATUS	186
Abdazimov Anvar, Ravutov Shavkat, Rajapbayev Umidjon	
BIOGAS GENERATION AND PRACTICAL IMPLEMENTATION IN UZBEKISTAN: TECHNOLOGICAL ASPECTS AND STATISTICAL ASSESSMENT	191
Eshbekov Mukhriddin, Khudoyqulov Zokir	
THE ROLE OF YOUTH ENTREPRENEURSHIP ENTITIES IN INDUSTRIAL DEVELOPMENT: AN EMPIRICAL ANALYSIS.....	198
Mirzatov Baxtiyor Toxirovich	
MODERN FORMWORK SYSTEMS FOR MONOLITHIC CONSTRUCTION: CHALLENGES AND APPLICATION POTENTIAL OF BASALT FIBER REINFORCED POLYMER COMPOSITES	202
Ali Narbabayevich Soatov, Husniddin Tolibovich Hasanov	
CREATING A PATIENT ELECTRONIC MEDICAL RECORD FROM MEDICAL CONVERSATIONS USING NATURAL LANGUAGE PROCESSING.....	209
Ibragimov Sanjarbek Salijanovich	
РАЗРАБОТКА МЕТОДОВ И АЛГОРИТМОВ ПАРАМЕТРИЧЕСКОГО 3D-МОДЕЛИРОВАНИЯ ОДЕЖДЫ С УЧЁТОМ АНТРОПОМЕТРИЧЕСКИХ ХАРАКТЕРИСТИК ФИГУРЫ ЧЕЛОВЕКА	217
Каримбердиева Мохинур Шерзод кизи	
O'ZBEKISTONDA SUG'URTA BOZORINING O'SISHI VA PASAYISHI: 1991-2026 YILLAR DINAMIKASINING TAHLILI	225
Ismailov Shaxobiddin	

DEVELOPMENT OF AN INTEGRATED SYSTEM FOR THREE-DIMENSIONAL GARMENT DESIGN AND AUTOMATED TECHNOLOGICAL PREPARATION OF APPAREL PRODUCTION.....	231
Karimberdiyeva Mokhinur Sherzod qizi	
ИНДЕКС ИНСТИТУЦИОНАЛЬНОЙ СРЕДЫ ФОРМИРОВАНИЯ И ЭФФЕКТИВНОГО ФУНКЦИОНИРОВАНИЯ ЧЕЛОВЕЧЕСКОГО КАПИТАЛА.....	238
Холбаева Сабина Рустамовна	
IMPROVING METHODS FOR DETECTING AND PREVENTING CYBERATTACKS IN COMPUTER NETWORKS.....	246
Babakulov Bekzod Mamatkulov	

IMPROVING METHODS FOR DETECTING AND PREVENTING CYBERATTACKS IN COMPUTER NETWORKS

Babakulov Bekzod Mamatkulov

Department of Information Systems and Technologies,
Jizzakh Branch of the National University of Uzbekistan named after Mirzo Ulugbek
E-mail: babakulov.bekzod23@gmail.com

Abstract. This study develops an adaptive hybrid framework for detecting and preventing cyberattacks in computer networks. The framework combines signature matching, supervised classification, unsupervised anomaly detection, behavioral correlation, asset context, and a safeguarded response policy. Its purpose is to preserve reliable detection when legitimate traffic changes and when previously unseen attacks do not match existing rules. A design-science methodology was used together with a controlled streaming emulation containing 120,000 training flows and 120,000 test flows distributed across baseline, benign-drift, and mixed zero-day-like windows. In the emulation, the proposed method achieved 98.94% accuracy, 98.31% precision, 97.39% recall, a 97.85% F1-score, and a 0.55% false-positive rate. The strongest advantage appeared in the mixed/zero-day window, where its F1-score reached 94.83%, compared with 73.90% for a static Random Forest and 57.26% for signature-only detection. The results support a practical conclusion: prevention should be separated from detection and activated gradually through logging, alerting, rate limiting, session interruption, and isolation, with higher-impact actions requiring corroboration and rollback.

Keywords: network intrusion detection; intrusion prevention; concept drift; Random Forest; Isolation Forest; behavioral analytics; zero-day attack; adaptive threshold; cyber resilience.

Annotatsiya. Ushbu tadqiqot kompyuter tarmoqlarida kiberhujumlarni aniqlash va oldini olish uchun adaptiv gibrid yondashuvni taklif etadi. Usul signaturali tekshiruv, nazoratli tasniflash, nazoratsiz anomaliya tahlili, xulqiy korrelyatsiya va aktivning muhimligini yagona xavf bahosida birlashtiradi. Tizim qonuniy trafik o'zgarganida hamda yangi hujumlar mavjud qoidalarga mos kelmaganida aniqlash barqarorligini saqlashga qaratilgan. Nazorat qilinadigan oqim emulyatsiyasida 120 000 ta o'quv va 120 000 ta sinov yozuvi ishlatildi. Taklif etilgan usul 98,94% aniqlik, 98,31% aniqlik darajasi, 97,39% to'liqlik, 97,85% F1 ko'rsatkichi va 0,55% yolg'on ijobiy natijaga erishdi. Aralash va nol-kun tipidagi oynada F1 94,83% bo'lib, statik Random Forest natijasidan sezilarli darajada yuqori bo'ldi. Natijalar bloklashni avtomatik tarzda keskin qo'llash emas, balki dalillarni tasdiqlash, bosqichli choralar va qaytarish mexanizmi bilan boshqarish zarurligini ko'rsatadi.

Kalit so'zlar: tarmoq hujumlarini aniqlash; hujumlarning oldini olish; konsept drift; Random Forest; Isolation Forest; xulqiy tahlil; nol-kun hujumi; adaptiv chegara; kiberbarqarorlik.

Аннотация. В исследовании предложен адаптивный гибридный подход к обнаружению и предотвращению кибератак в компьютерных сетях. Метод объединяет сигнатурный анализ, контролируемую классификацию, неконтролируемое выявление аномалий, поведенческую корреляцию и контекст критичности актива. Цель подхода состоит в сохранении устойчивости обнаружения при изменении легитимного трафика и появлении ранее неизвестных атак. В контролируемой потоковой эмуляции использовано 120 000 обучающих и 120 000 тестовых записей. Предложенный метод обеспечил точность 98,94%, precision — 98,31%, полноту — 97,39%, F1 — 97,85% и уровень ложных срабатываний — 0,55%. В смешанном окне с атаками типа zero-day значение F1 достигло 94,83%, превысив результат статического Random Forest. Полученные результаты показывают, что активное противодействие следует реализовывать поэтапно, с подтверждением несколькими источниками, возможностью отката и контролем аналитика.

Ключевые слова: обнаружение сетевых вторжений; предотвращение атак; дрейф концепции; Random Forest; Isolation Forest; поведенческий анализ; атака нулевого дня; адаптивный порог; киберустойчивость.

INTRODUCTION

Computer networks have become the operating fabric of public administration, banking, education, healthcare, industry, and everyday communication. That dependence has changed the impact of a successful cyberattack: the result is no longer limited to the loss of a few files but may include service interruption, fraudulent transfers, leakage of personal data, manipulation of industrial processes, and loss of public trust. The 2026 Verizon Data Breach Investigations Report (DBIR) states that 31% of breaches begin with software vulnerabilities and 48% involve

ransomware [1]. The FBI's 2025 Internet Crime Report recorded 1,008,597 complaints and USD 20.877 billion in reported losses, representing 26% more losses than in 2024 [2]. These sources measure different populations and must not be combined into a single prevalence estimate, but together they show that both technical exploitation and financially motivated abuse remain serious.

Traditional network defense usually relies on a firewall, a signature-based intrusion detection or prevention system, and manual incident response. This arrangement remains valuable because well-written rules are fast and explainable. Its weakness is equally clear: a rule cannot recognize a pattern that has not yet been described, while an excessively broad rule can interrupt legitimate services. Machine-learning methods address part of this gap, but a model trained on yesterday's traffic may deteriorate when applications, user behavior, encryption, cloud routing, or adversary tactics change. This non-stationarity is commonly described as concept drift [13–15].

The research object is network traffic and security telemetry generated in enterprise and institutional computer networks. The research subject is the set of methods used to identify malicious behavior, estimate its risk, and select a proportionate preventive action. The purpose of the work is to improve detection robustness without turning the prevention mechanism into an uncontrolled source of service denial. Accordingly, the paper treats detection and prevention as related but distinct decisions: an event may deserve investigation without yet justifying automatic blocking.

The central hypothesis is that no single detector is sufficient across known attacks, unknown attacks, and legitimate traffic drift. A more stable result can be obtained when signature evidence, a supervised classifier, an unsupervised anomaly score, and behavior and asset context are calibrated and fused, while the enforcement layer uses staged actions and explicit safeguards. Three research questions guide the study: (RQ1) Which combination of evidence provides the best balance between recall and false alarms? (RQ2) Can adaptive thresholds reduce deterioration during benign traffic drift? and (RQ3) How should a risk score be translated into prevention actions without creating an unsafe self-blocking system?

The contribution of this paper is an Adaptive Hybrid Detection and Prevention Framework (AHDPPF). The novelty lies not in the isolated use of Random Forest, Isolation Forest, or signatures, as each is well established [10–12]. Rather, the contribution lies in their operational integration with a label-free behavior score, per-window calibration, an explanation record, a policy gate, corroboration requirements for high-impact actions, and a feedback path for drift management. A controlled streaming emulation is used to test the behavior of the design. The emulation is intentionally described as synthetic and does not replace validation using production traffic.

Table 1. Current threat indicators and their defensive implications

Indicator	Latest reported value	Interpretation for network defense
Breaches beginning with software vulnerabilities	31%	Prioritize exposed-service inventory, patching, virtual patching, and exploit telemetry.
Breaches involving ransomware	48%	Detection must be connected to containment, backup protection, and lateral-movement controls.
Attack techniques assisted by generative AI	15%	Faster adversary iteration increases the value of behavior-based detection and model monitoring.
Higher click rate for mobile threats	40%	Network monitoring should incorporate identity, mobile, DNS, and cloud signals rather than perimeter traffic alone.
IC3 complaints in 2025	1,008,597	Reported cyber-enabled harm is high in volume; triage and automation are operational necessities.
IC3 reported losses in 2025	\$20.877 billion	Prevention decisions should be risk-weighted toward high-value assets and fraud pathways.

Source: Compiled from Verizon 2026 DBIR [1] and FBI 2025 IC3 Annual Report [2]. Indicators have different denominators and are not additive.

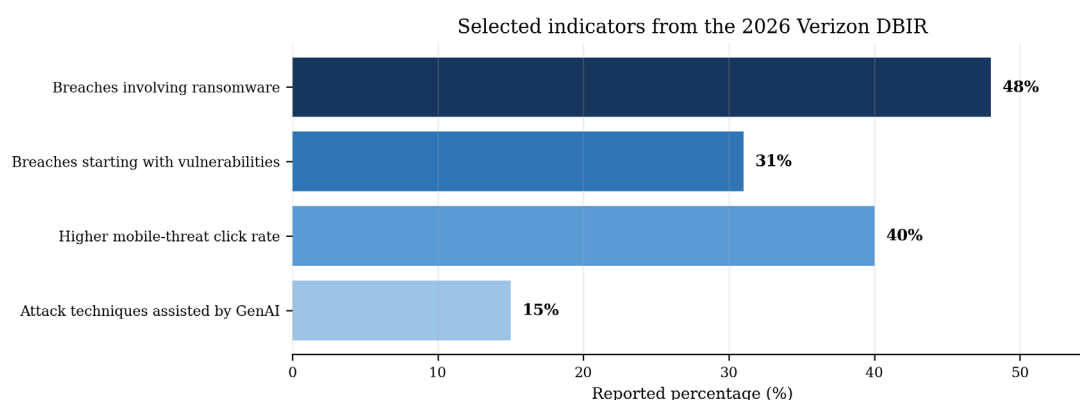


Figure 1. Selected indicators from the 2026 Verizon DBIR

Source: Prepared by the author from Verizon 2026 DBIR [1]. The bars are separate indicators, not parts of one total.

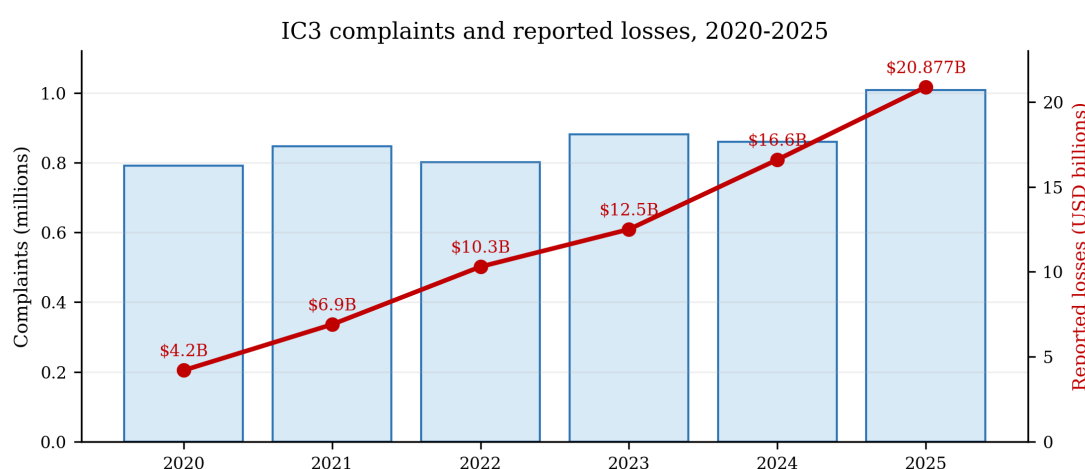


Figure 2. IC3 complaints and reported losses, 2020-2025

Source: Prepared by the author from FBI IC3 annual data summarized in the 2025 report [2]. Complaints are reports received, not an estimate of all cybercrime.

LITERATURE REVIEW

Signature-based detection compares packets, flows, protocol fields, or log events with known indicators and rules. Its principal advantages are speed, direct explainability, and a clear connection between evidence and action. Suricata, for example, can operate inline and apply drop or reject rules to unwanted traffic [16]. However, exact signatures are fragile when attackers change encodings, timing, infrastructure, or payload structure. They also provide limited coverage for slow, low-volume, or previously unseen behavior.

Anomaly-based detection models normality and marks observations that deviate from it. Isolation Forest is attractive because it isolates unusual observations without requiring attack labels [11]. This can increase sensitivity to zero-day-like behavior, but a change in legitimate usage may appear equally unusual. For a security operations center, a detector that identifies almost every attack but produces thousands of false alarms can be less useful than a slightly less sensitive method with stable precision.

Supervised classifiers learn a decision boundary from labeled examples. Random Forest remains a practical baseline because it handles nonlinear interactions, mixed feature importance, noise, and class weighting at a moderate computational cost [10]. Nevertheless, the closed-world assumption is problematic in network security. Sommer and Paxson warned that laboratory accuracy may fail to transfer when training and operational environments differ [5]. The same concern appears in later dataset surveys, which emphasize the recording environment, attack diversity, labels, and realism [6].

Recent research has therefore focused on adaptation. Seth, Chahal, and Singh combined an adaptive Random Forest with statistical drift tests and reported strong performance on CSE-CIC-IDS2018 [13]. García-Huitztl, Bustio-Martínez, and Cumplido combined K-Means, an adaptive Random Forest, and drift analysis, reporting 98.66% accuracy and a 1.14% false-alarm rate on NSL-KDD [14]. Shyaa et al. reviewed concept- and feature-drift-aware

intrusion detection and identified the need to integrate adaptation more directly into operational IDS design [15]. These studies show that adaptation is no longer an optional model enhancement; it is part of maintaining detection validity.

Explainability is another operational requirement. An analyst needs to know whether a high score was driven by a burst of SYN packets, unusual destination diversity, failed authentication, high outbound volume, or an unknown encrypted destination. Feature-attribution methods such as SHAP can provide local explanations for complex predictions [12]. In the proposed framework, a lightweight explanation record is generated for every high-risk event, while more computationally expensive attribution can be reserved for cases escalated to an analyst.

The prevention problem has received less attention than detection accuracy. NIST CSF 2.0 treats Govern, Identify, Protect, Detect, Respond, and Recover as concurrent and interconnected functions [3], while NIST SP 800-61r3 emphasizes continuous improvement and the integration of incident response across organizational operations [4]. This supports a policy architecture in which automated actions are proportionate, observable, reversible, and connected to learning. MITRE ATT&CK can provide a common vocabulary for relating observed behavior to adversary objectives and mitigations [17].

Table 2. Benchmark datasets relevant to the proposed evaluation

Dataset	Traffic scope	Features / scale	Attack coverage	Key caution
CICIDS2017	Five-day enterprise-like traffic with labeled flows and PCAP	More than 80 flow features; about 2.8 million flows	Brute force, DoS/DDoS, web attacks, botnet, infiltration, Heartbleed	Strong class imbalance and capture-specific artifacts
CSE-CIC-IDS2018	Larger emulated organization: 420 machines, 30 servers, 50 attack hosts	80 CICFlowMeter-V3 features plus logs and PCAP	Seven attack scenarios	Large scale, but still an emulated environment
UNSW-NB15	100 GB hybrid normal and synthetic malicious traffic	49 attributes; 2,540,044 records reported in the literature	Nine attack categories	Generated traffic and older protocol behavior may not represent every modern network

Source: Compiled from the official CICIDS2017 [7], CSE-CIC-IDS2018 [8], and UNSW-NB15 [9] dataset descriptions and the dataset survey [6].

The review leads to two methodological choices. First, reported benchmark accuracy is not treated as proof of effectiveness in production environments because data leakage, repeated flows, class imbalance, and capture-specific artifacts may inflate the results. Second, the proposed method is evaluated across sequential windows rather than solely through a random train-test split. This approach makes legitimate traffic drift and previously unknown attack behavior visible instead of averaging them out.

RESEARCH METHODOLOGY

The study follows a design-science sequence: defining the operational problem, synthesizing requirements from relevant standards and literature, constructing an artifact, and evaluating its behavior in a controlled setting. Evidence was drawn from current threat reports [1, 2], NIST guidance [3, 4], benchmark dataset documentation [7–9], and peer-reviewed studies on machine learning, anomaly detection, explainability, and concept drift [10–15]. The evaluation does not claim to reproduce a specific enterprise network. Instead, it examines whether the proposed control logic responds coherently to three conditions that commonly undermine static systems: ordinary baseline traffic, legitimate distribution shifts, and zero-day-like attacks. Artificial intelligence tools were used in a limited supporting capacity during the preparation and linguistic refinement of the manuscript, accounting for no more than 10% of the overall work, while all methodological decisions, analyses, interpretations, and conclusions remained the responsibility of the authors.

Proposed framework

AHDPF processes flow records and related telemetry through four evidence channels. The signature engine represents deterministic IDS/IPS rules. The supervised engine estimates the probability that a flow belongs to a known malicious class. The anomaly engine estimates how isolated an observation is from the learned benign baseline. The behavior-context channel evaluates combinations such as unusual destinations with regular beaconing intervals or high-entropy outbound transfers accompanied by abnormal traffic volumes. Asset criticality, identity

risk, vulnerability exposure, and time-of-day context can then modify the operational priority without altering the raw detector output.

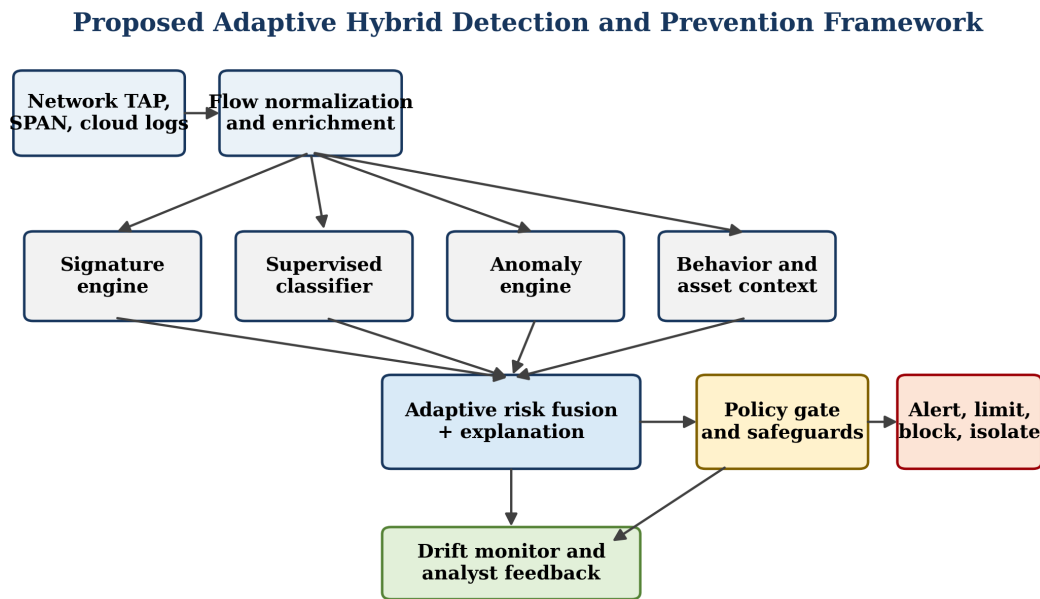


Figure 3. Architecture of the proposed adaptive hybrid detection and prevention framework

Source: Developed by the author.

Feature Representation

Twelve normalized flow features were used in the emulation: flow duration, packet rate, bytes per packet, SYN, ACK, and RST ratios, destination-port diversity, new-destination score, failed-authentication rate, payload entropy, outbound ratio, and interarrival-time variability. No payload content was required; payload entropy was used solely as an aggregate numerical indicator. In production environments, encrypted-traffic analysis should focus primarily on metadata and behavioral characteristics rather than on decryption by default.

Risk Fusion and Adaptive Threshold

Let (S_t) , (C_t) , (A_t) , and (B_t) denote the signature, classifier, anomaly, and behavior scores, respectively, for observation (t) , with each score lying within the interval $[0,1]$. The emulation used a maximum-fusion structure so that an exact, high-confidence signature would not be diluted by the outputs of other engines, while corroborated statistical evidence could still elevate the risk score of an unknown attack. The implemented risk score was defined as follows:

$$[R_t = \max \left\{ S_t; 0.50C_t + 0.32A_t + 0.18 \max(S_t, C_t, A_t); 0.68B_t + 0.32A_t \right\}]$$

The coefficients represent initial engineering values rather than universal constants. They assign the supervised model the principal role in identifying known attacks, preserve a meaningful contribution from anomaly evidence, and require behavioral coherence for the escalation of zero-day-like activity. In production environments, these coefficients should be calibrated using time-separated validation data and periodically reviewed by the responsible security authority.

For each window (w) , the decision threshold (T_w) was estimated from low-risk candidate traffic and constrained to the interval $[0.47, 0.61]$. The candidate set excluded observations with strong signature matches or high classifier scores. The threshold was defined as the 99.2nd percentile of candidate risk scores plus a safety margin of 0.07 and was then clipped to the approved interval. This mechanism increased the threshold when legitimate cloud-like traffic became more novel, thereby limiting alert flooding, while preventing indefinite threshold inflation.

Risk-based prevention workflow with staged controls and rollback

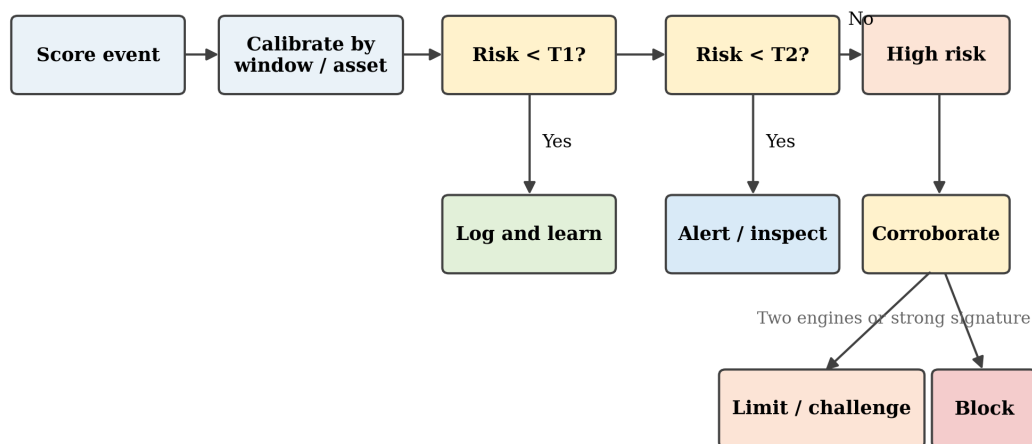


Figure 4. Risk-based prevention workflow with staged controls and rollback

Source: Developed by the author. T1 and T2 are locally approved adaptive thresholds.

Controlled Streaming Emulation

The training stream contained 120,000 observations, comprising 72% benign traffic and 28% known attacks, including DDoS, port-scanning, brute-force, and web-exploitation attacks. The test stream contained 120,000 observations divided into three consecutive windows of 40,000 observations each. Window W1 followed the initial baseline; W2 introduced a legitimate shift toward higher-volume, encrypted, cloud-oriented traffic; and W3 combined this shift with command-and-control beaconing and data-exfiltration patterns that were absent from the supervised training data. Feature values were sampled from bounded distributions with attack-specific dependencies. A fixed random seed of 20260724 was used to ensure reproducibility.

Table 3. Emulation design and model settings

Parameter	Value	Reason
Training size	120,000 flows	Provides a stable baseline while remaining reproducible on a standard workstation
Test size	120,000 flows	Supports narrow confidence intervals and separate sequential windows
Known attacks	DDoS, port scan, brute force, web exploit	Represents common volume, reconnaissance, identity, and application attacks
Unseen test attacks	C2 beacon, data exfiltration	Tests label-free anomaly and behavior channels
Supervised model	Random Forest, 140 trees, max depth 18	Nonlinear baseline with class balancing
Anomaly model	Isolation Forest, 120 trees, 2.5% contamination	Label-free detection on a benign subset
Sequential windows	Baseline, benign drift, mixed/zero-day	Separates nominal performance from drift robustness
Random seed	20260724	Reproducibility

Source: Author's controlled experiment. This is a synthetic evaluation and not a measurement of a specific production network.

Evaluation Metrics

The confusion matrix is based on true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN). Precision measures the proportion of generated alerts that correspond to genuinely malicious events, recall measures the proportion of malicious events successfully detected, the F1-score balances precision and recall, and the false-positive rate (FPR) measures the disruption imposed on benign traffic.

$$[\text{Precision}] = \frac{\text{TP}}{\text{TP} + \text{FP}}; \quad \text{and}$$

$$[\text{Recall}] = \frac{\text{TP}}{\text{TP} + \text{FN}}.]$$

$$[\text{F1} = \frac{2(\text{Precision} \times \text{Recall})}{\text{Precision} + \text{Recall}}]$$

$$[\text{Precision}] + [\text{Recall}]; \quad \text{and}$$

$$\text{FPR} = \frac{\text{FP}}{\text{FP} + \text{TN}}.]$$

Wilson 95% confidence intervals were calculated for the precision, recall, and FPR of the proposed method. Because all methods were evaluated using the same synthetic data stream, the emphasis is placed on their comparative behavior across sequential windows rather than on claims of universally applicable accuracy.

ANALYSIS AND RESULTS

Overall Performance

Across the complete test stream, the proposed adaptive hybrid method produced 28,826 true positives, 89,905 true negatives, 495 false positives, and 774 false negatives. It achieved an accuracy of 98.94%, a precision of 98.31%, a recall of 97.39%, and an F1-score of 97.85%, with an FPR of 0.55%. The Wilson 95% confidence intervals were 98.16%–98.45% for precision, 97.20%–97.56% for recall, and 0.50%–0.60% for the FPR.

The signature-only method achieved perfect precision in the emulation because its rules were deliberately narrow; however, its recall was only 66.75%. Conversely, anomaly-only detection achieved a recall of 99.82% but generated an FPR of 11.30%. These two extremes illustrate why neither component should control preventive actions independently.

Table 4. Overall detection performance

Method	Accuracy	Precision	Recall	F1	FPR
Signature-only	91.80%	100.00%	66.75%	80.06%	0.00%
Static Random Forest	96.30%	99.06%	85.80%	91.96%	0.27%
Anomaly-only	91.45%	74.31%	99.82%	85.20%	11.30%
Proposed adaptive hybrid	98.94%	98.31%	97.39%	97.85%	0.55%

Source: Author's controlled streaming emulation ($n = 120,000$ test flows).

Robustness Across Sequential Windows

The random-split-like baseline window favored the static Random Forest, which achieved an F1-score of nearly 100%. Although this result is useful, it may be misleading because it largely reflects the similarity between the training and testing distributions. Under benign drift, the static model remained strong in this emulation, whereas the F1-score of the anomaly-only method declined to 85.16% because many legitimate cloud-like observations became statistically unusual. The adaptive hybrid increased its decision threshold from 0.47 in W1 to 0.553 in W2, maintaining an F1-score of 98.97% and an FPR of 0.66%.

W3 provided a more informative test because it combined legitimate traffic drift with command-and-control (C2) beaconing and data-exfiltration patterns that were absent from the supervised training data. The F1-score of the signature-only method declined to 57.26%, while that of the static Random Forest fell to 73.90%. The anomaly-only method detected almost every attack but misclassified 20.95% of benign flows in that window. By contrast, the adaptive hybrid achieved an F1-score of 94.83% with an FPR of 0.93%. These findings address RQ1 and RQ2: the integration of complementary evidence improved recall for previously unknown behavior, while the adaptive threshold and behavioral corroboration helped restrain false alarms.

Table 5. Performance by sequential evaluation window

Window	Method	Precision	Recall	F1	FPR
W1 baseline	Signature-only	100.00%	84.35%	91.51%	0.00%
W1 baseline	Static Random Forest	99.98%	100.00%	99.99%	0.01%
W1 baseline	Anomaly-only	93.29%	99.88%	96.47%	2.27%
W1 baseline	Proposed adaptive hybrid	99.79%	100.00%	99.90%	0.07%
W2 benign drift	Signature-only	100.00%	77.99%	87.63%	0.00%
W2 benign drift	Static Random Forest	99.36%	99.99%	99.67%	0.20%

Window	Method	Precision	Recall	F1	FPR
W2 benign drift	Anomaly-only	74.26%	99.82%	85.16%	10.93%
W2 benign drift	Proposed adaptive hybrid	97.96%	100.00%	98.97%	0.66%
W3 mixed/zero-day	Signature-only	100.00%	40.12%	57.26%	0.00%
W3 mixed/zero-day	Static Random Forest	97.24%	59.60%	73.90%	0.59%
W3 mixed/zero-day	Anomaly-only	62.60%	99.78%	76.93%	20.95%
W3 mixed/zero-day	Proposed adaptive hybrid	97.22%	92.56%	94.83%	0.93%

Source: Author's controlled streaming emulation. W3 includes attack profiles absent from supervised training.

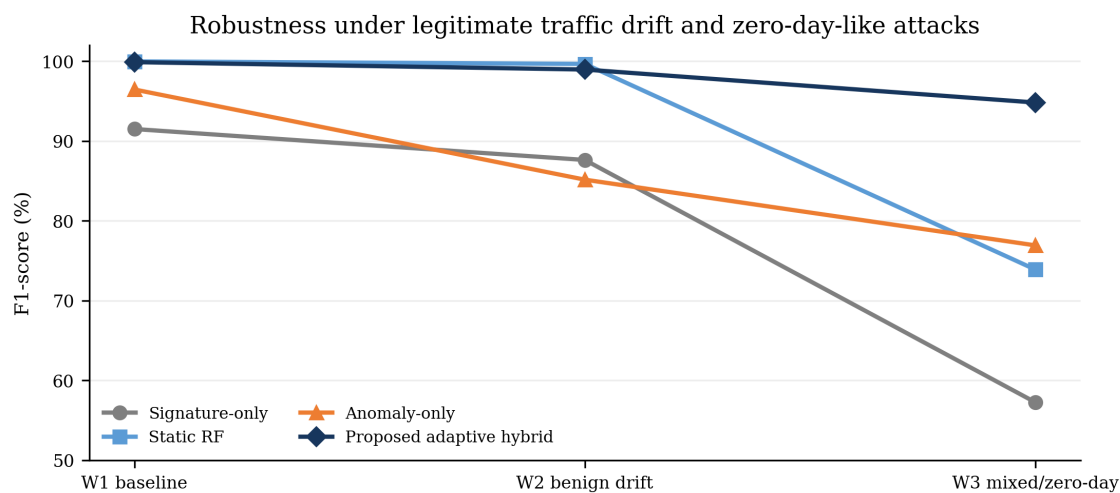


Figure 5. F1-score across baseline, benign-drift, and mixed zero-day-like windows

Source: Author's controlled streaming emulation.

Attack-Level Detection

All methods performed well in detecting high-volume or strongly expressed known attacks, although the signature-only rule for web exploits detected only 49.16% of such cases. The most significant difference emerged in the detection of previously unseen behavior. Signature-only detection identified none of the command-and-control (C2) beaconing or data-exfiltration patterns because no exact rule represented them. The static classifier detected 31.92% of beaconing cases and only 6.50% of data-exfiltration cases. By contrast, the proposed hybrid method detected 79.65% and 90.58%, respectively.

The remaining missed C2 cases indicate that low-and-slow communication remains the most difficult attack class to detect. Its detection should therefore be supplemented with longer temporal observation windows, endpoint telemetry, DNS reputation data, and identity context.

Table 6. Recall by attack profile

Attack profile	Signature-only	Static RF	Anomaly-only	Adaptive hybrid
DDoS	89.64%	100.00%	100.00%	100.00%
Port scan	88.15%	100.00%	100.00%	100.00%
Brute force	96.53%	100.00%	99.36%	100.00%
Web exploit	49.16%	99.97%	99.98%	100.00%
C2 beacon	0.00%	31.92%	99.54%	79.65%
Data exfiltration	0.00%	6.50%	100.00%	90.58%

Source: Author's controlled streaming emulation.

From Detection to Safe Prevention

RQ3 concerns enforcement. The results demonstrate why a binary “detected/not detected” output is

inadequate. If every alert automatically triggered blocking, an anomaly-only system would have denied more than one in five benign flows in W3. AHDPF therefore separates the detection score from the action policy. Low-risk events are retained for learning; medium-risk events generate an alert or challenge; high-risk events may be rate-limited or have their sessions interrupted; and network isolation is reserved for cases involving strong signatures, agreement between independent detection engines, or a critical asset with analyst authorization. Every automated action records the supporting evidence, expiration time, responsible owner, and rollback instructions.

Table 7. Risk-to-response policy for staged intrusion prevention

Risk band	Required evidence	Default action	Safeguard
$R < T1$	No strong rule; weak statistical evidence	Log, aggregate, and update baseline statistics	No user-visible action
$T1 \leq R < T2$	One engine or moderate multi-engine evidence	Create alert; enrich with identity, DNS, endpoint, and asset context	Deduplicate and rate-limit alerts
$T2 \leq R < 0.82$	Two engines agree or behavior is persistent	Rate limit, step-up authentication, or interrupt the suspicious session	Short time-to-live and automatic rollback
$R \geq 0.82$	Strong signature or corroborated high-confidence attack	Drop connection, quarantine host, or isolate network segment	Critical assets require approval unless a pre-authorized emergency rule applies
Post-action	Response outcome and analyst verdict	Update case, rule, model labels, and drift monitor	Audit trail; do not auto-train on unreviewed labels

Source: Developed by the author using the Detect-Respond-Recover logic of NIST CSF 2.0 [3] and incident-response guidance in NIST SP 800-61r3 [4].

Deployment Implications

The framework can be implemented incrementally without replacing an existing IDS/IPS. A practical deployment sequence includes visibility and asset mapping, baseline construction, shadow-mode evaluation, limited reversible prevention, and adaptive operation. Mature detection rules should be preserved, while their alerts and associated flow metadata are fused with model outputs. Automated prevention should initially rely on narrowly targeted actions, such as rate limiting or short-lived session interruption, and should be extended to host or network-segment isolation only after rollback procedures have been tested and operational thresholds have been formally approved.

Limitations

Several limitations should be acknowledged. First, the evaluation uses synthetic, normalized features; therefore, it demonstrates the logic of evidence fusion and adaptation but cannot provide an estimate of production-level accuracy. Second, the feature distributions were designed by the author and may favor the selected behavioral combinations. Third, the emulation did not model encrypted-payload inspection, endpoint process trees, user behavior, or adversarial evasion techniques. Fourth, the thresholds and weighting coefficients were not optimized using organization-specific cost functions.

Future validation should include time-separated experiments using the CICIDS2017, CSE-CIC-IDS2018, and UNSW-NB15 datasets, followed by a monitored pilot based on locally collected traffic and conducted with appropriate legal, ethical, and privacy approval. Adversarial testing should also address data poisoning, behavioral mimicry, feature manipulation, and denial-of-service attacks directed against the detection system itself.

CONCLUSIONS AND RECOMMENDATIONS

Improving cyberattack detection in computer networks is not simply a matter of selecting a more complex classifier. Signature rules, supervised learning, anomaly detection, and behavioral context address different failure modes and become more effective when they are calibrated, explained, and governed as components of an integrated system. In the controlled emulation, the proposed hybrid method achieved an overall F1-score of 97.85% and a false-positive rate of 0.55%. Under the mixed zero-day-like condition, its F1-score remained at 94.83%, compared with 73.90% for the static Random Forest and 57.26% for signature-only detection. Although these synthetic results do not establish accuracy in live-network environments, they support the value of complementary evidence and bounded adaptation.

Practical implementation should progress from network visibility and data quality assessment to the construction of time-separated baselines, shadow-mode validation, limited and reversible enforcement, and

broader automation. Organizations should measure signature coverage and false-alarm rates, combine supervised and unsupervised evidence, maintain separate thresholds for alerting and blocking, require corroboration before isolating critical systems, and assign every preventive action an owner, time-to-live period, rollback path, and verification step. Local chronological validation and adversarial testing for data poisoning, evasion, resource exhaustion, and telemetry loss should precede production deployment. This approach preserves human accountability and aligns the proposed method with the NIST Govern–Identify–Protect–Detect–Respond–Recover cycle [3, 4].

REFERENCES

- [1] Verizon. 2026 Data Breach Investigations Report [Электронный ресурс]. – 2026. – URL: <https://www.verizon.com/business/resources/reports/dbir/> – Дата обращения: 24.07.2026.
- [2] Federal Bureau of Investigation. 2025 Internet Crime Report [Электронный ресурс]. – Washington, DC: Internet Crime Complaint Center, 2026. – URL: https://www.fbi.gov/file-repository/2025_ic3report.pdf – Дата обращения: 24.07.2026.
- [3] National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. – Gaithersburg, MD: National Institute of Standards and Technology, 2024. – (NIST CSWP 29). – DOI: <https://doi.org/10.6028/NIST.CSWP.29>.
- [4] Nelson A., Rekhi S., Souppaya M., Scarfone K. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. – Gaithersburg, MD: National Institute of Standards and Technology, 2025. – (NIST SP 800-61r3). – DOI: <https://doi.org/10.6028/NIST.SP.800-61r3>.
- [5] Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection // 2010 IEEE Symposium on Security and Privacy. – 2010. – P. 305–316. – DOI: <https://doi.org/10.1109/SP.2010.25>.
- [6] A Survey of Network-Based Intrusion Detection Data Sets / M. Ring, S. Wunderlich, D. Scheuring [et al.] // Computers & Security. – 2019. – Vol. 86. – P. 147–167. – DOI: <https://doi.org/10.1016/j.cose.2019.06.005>.
- [7] Canadian Institute for Cybersecurity. Intrusion Detection Evaluation Dataset (CIC-IDS2017) [Электронный ресурс]. – Fredericton: University of New Brunswick, 2017. – URL: <https://www.unb.ca/cic/datasets/ids-2017.html> – Дата обращения: 24.07.2026.
- [8] Canadian Institute for Cybersecurity. CSE-CIC-IDS2018 on AWS [Электронный ресурс]. – Fredericton: University of New Brunswick, 2018. – URL: <https://www.unb.ca/cic/datasets/ids-2018.html> – Дата обращения: 24.07.2026.
- [9] Moustafa N., Slay J. UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems // 2015 Military Communications and Information Systems Conference (MilCIS). – 2015. – P. 1–6. – DOI: <https://doi.org/10.1109/MilCIS.2015.7348942>.
- [10] Breiman L. Random Forests // Machine Learning. – 2001. – Vol. 45, No. 1. – P. 5–32. – DOI: <https://doi.org/10.1023/A:1010933404324>.
- [11] Liu F. T., Ting K. M., Zhou Z.-H. Isolation Forest // 2008 Eighth IEEE International Conference on Data Mining. – 2008. – P. 413–422. – DOI: <https://doi.org/10.1109/ICDM.2008.17>.
- [12] Lundberg S. M., Lee S.-I. A Unified Approach to Interpreting Model Predictions // Advances in Neural Information Processing Systems. – 2017. – Vol. 30. – DOI: <https://doi.org/10.5555/3295222.3295230>.
- [13] Seth S., Chahal K. K., Singh G. Concept Drift-Based Intrusion Detection for Evolving Data Stream Classification in IDS: Approaches and Comparative Study // The Computer Journal. – 2024. – Vol. 67, No. 7. – P. 2529–2547. – DOI: <https://doi.org/10.1093/comjnl/bxae023>.
- [14] García-Huitzil E., Bustio-Martínez L., Cumplido R. Adaptive Intrusion Detection System: Hybrid K-Means and Random Forest Approach with Concept Drift Detection // Computación y Sistemas. – 2025. – Vol. 29, No. 1. – P. 29–42. – DOI: <https://doi.org/10.13053/cys-29-1-5528>.
- [15] Evolving Cybersecurity Frontiers: A Comprehensive Survey on Concept Drift and Feature Dynamics-Aware Machine and Deep Learning in Intrusion Detection Systems / M. A. Shyaa, N. F. Ibrahim, Z. Zainol [et al.] // Engineering Applications of Artificial Intelligence. – 2024. – Vol. 137. – Art. 109143. – DOI: <https://doi.org/10.1016/j.engappai.2024.109143>.
- [16] Open Information Security Foundation. Suricata IPS Concept Documentation [Электронный ресурс]. – 2026. – URL: <https://docs.suricata.io/en/latest/ips/ips-concept.html> – Дата обращения: 24.07.2026.
- [17] MITRE. MITRE ATT&CK Enterprise Matrix [Электронный ресурс]. – 2026. – URL: <https://attack.mitre.org/matrices/enterprise/> – Дата обращения: 24.07.2026.
- [18] Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. – Gaithersburg, MD: National Institute of Standards and Technology, 2020. – (NIST SP 800-207). – DOI: <https://doi.org/10.6028/NIST.SP.800-207>.

Proofreader: Zokir ALIBEKOV

Layout and Designer: Oloviddin Sobir ugli

2026. № 7

© When materials are reproduced, the INNOVATION SCIENCE AND TECHNOLOGY journal must be cited as the source. Authors are responsible for the accuracy of the information in materials and advertisements published in the journal. Editorial opinions may not always align with those of the authors. Submitted materials will not be returned to the editorial office.

To publish articles in this journal, you may submit articles, advertisements, stories, and other creative materials through the following links. Materials and advertisements are published on a paid basis.

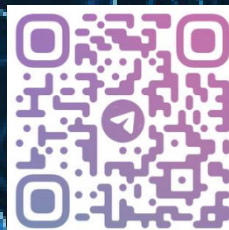
You may subscribe to the journal at any time using the following details. Once subscribed, please send a screenshot or photo of your payment confirmation to our Telegram page @iqtisodiyot_77. Based on this, we will send the latest issue of the journal to your address each month.

“The journal “INNOVATION SCIENCE AND TECHNOLOGY” has been registered by the Agency for Information and Mass Communications under the Administration of the President of the Republic of Uzbekistan from 09.10.2024 under the registration number №390637. License number: C-5669633. PNFL: 30407832680027

Our address: Tashkent city, Yunusobod district, 19th block,
House 17.



**TASHKENT STATE
UNIVERSITY OF ECONOMICS**



Google
Scholar

OPEN ACCESS

ULRICHSWEB™
GLOBAL SERIALS DIRECTORY

**Academic
Resource
Index**
ResearchGate

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INTERNATIONAL CENTRE

CYBERLENINKA

OpenAIRE

ROAD

LIBRARY.RU
НАУЧНАЯ ЭЛЕКТРОННАЯ
БИБЛИОТЕКА

BASE INDEX COPERNICUS
INTERNATIONAL

Crossref

doi Digital
Object
Identifier

CiteFactor
Academic Scientific Journals

zenodo



Acceptance of articles

Published every
monthly



Directions

Social, economic, political,
technological, scientific



Scopus || Scientific electronic journal specializing in Scopus

CERTIFICATE NUMBER: №390637

**ORDER NUMBER ACCORDING TO
THE LICENSE REGISTER: C-5669633**

CONTACT:



Contact us
+998 50 737 87 88



Telegram channel
t.me/scopus_IST2100



Journal official website
<https://ist-journal.uz/index.php/IST>