UDC 004.056.5 **doi:** https://doi.org/10.20998/3083-6298.2025.03.12

Dmytro Svitlychnyi[1], Andrii Tkachov[1]

[1] National Technical University “Kharkiv Polytechnic Institute”, Kharkiv, Ukraine

RESEARCH OF MODERN METHODS OF CLASSIFICATION OF ATTACKS ON CRITICAL INFRASTRUCTURE

Abstract. Topicality. Nowadays, Critical Infrastructure (CI) increasingly depends on interconnected digital and physical systems, making it a priority target for sophisticated cyber threats. In parallel, the field has produced a large and diverse body of research: taxonomies of attacks, methods for identification and detection, and protection and control techniques; yet practitioners still face the challenge of comparing these approaches in a consistent way. The NIST Cybersecurity Framework (CSF) 2.0 offers an outcome-based structure for such comparison. **The subject of study** in the article is to review modern methods for classifying cyber-attacks on CI and the associated approaches for Identify, Detect, Protect, control, and defense. **The purpose of the** article is twofold: to assess the strengths and limitations of the reviewed approaches through the lens of NIST CSF 2.0, and to reveal concrete opportunities to upgrade these approaches for real-world deployment in CI environments. **The following results** were obtained. The analysis delivers a detailed CSF 2.0 mapping for every reviewed approach, a concise summary of strengths and limitations per work, recommended profile elements and tier uplift actions, and cross-cutting improvement themes. **Conclusion.** Most reviewed approaches align well with Govern, Identify, Protect, and Detect, while Respond and Recover are addressed only minimally or not at all. This pattern suggests a clear upgrade path: complement technical controls with incident management, continuity, and validated recovery mechanics to raise organizational maturity. The proposed mappings, profiles, tiers, and comparison tables offer a reusable toolkit for CI organizations planning to adapt and operationalize the reviewed solutions under NIST CSF 2.0.

Keywords: cybersecurity; Cybersecurity Framework (CSF); critical infrastructure (CI); classification of cyber-attacks; NIST CSF 2.0.

Introduction

Problem relevance. Nowadays, the field of cybersecurity and especially security of Critical Infrastructure (CI) has become very important. CI is now inseparably cyber-physical, so attacks can traverse enterprise Information Technology (IT), control networks, and the physical process-creating cascade effects that traditional IT-only models miss [1, 2]. Network-borne techniques such as false-data injection, replay and Man-in-the-Middle (MITM), and DoS can degrade estimation, destabilize control loops, and precipitate unsafe states without modifying controller firmware [3]. Modern taxonomies therefore extend beyond Confidentiality-Integrity-Availability (CIA) to include process integrity and safety consequences (e.g., outages, equipment damage), reframing CI incidents as public-risk events rather than purely IT disruptions [4, 5]. Sector-specific mappings, for example, in power systems across Advanced Metering Infrastructure (AMI), meters, substations, and control centers, show that prioritization of threats and controls depends on domain-unique assets and protocols [6]. At the same time, legacy components and heterogeneous stacks remain widely deployed, compounding exposure when paired with modern connectivity [7, 8].

The rapid expansion of Industrial Internet of Things (IIoT) and cloud-integrated Supervisory Control and Data Acquisition (SCADA) further enlarges the attack surface and introduces new trust boundaries at device, edge, and cloud layers [9, 10, 11].

There a risk-management Cybersecurity Framework (CSF) exists known as NIST Cybersecurity framework 2.0 [12]. And it is interesting to check other solutions over this framework.

Literature review. Let's consider several scientific works addressing this topic from a cybersecurity perspective. The reviewed works [1–11] converges on viewing CI as a cross-domain system where threats traverse IT, Operational Technologies (OT), and the physical process.

Foundational work [1] proposes a six-platform classifier for cybersecurity metrics and the stochastic model of the formal description and analysis of security metrics for assessing the current state of the Cyber-Physical Security System (CPSS). CPSS allows for the objectivity and efficiency of obtaining information. It allows us to determine the level of provision of security services to various information assets using provided security services (confidentiality, integrity, authenticity, availability, involvement), secrecy level, and cost constraints.

Paper [2] formalizes cross-domain attack paths and motivates taxonomies that explicitly span cyber, control, and physical effects. Network-centric surveys deepen this by classifying control-network threats such as False-Data Injection (FDI), replay and MITM, routing attacks, and DoS, and linking them to estimation and control impacts, which is essential for mapping “vector - technique - process consequence” in Cyber-Physical System (CPS) and Industrial Control System (ICS) contexts [3].

A second strand extends classification beyond CIA to safety and process integrity. Broad CPS surveys organize attacks simultaneously by vector, control-loop role (sensor, actuator, controller, comm, etc), and consequence classes, arguing for safety-aware labels to capture real-world hazards (e.g., outages, equipment damage) [4]. To make such labels interoperable across disciplines, a harmonized taxonomy connects “assets – threats – risks – outcomes”, supporting consistent reporting between engineering, Security Operation Center (SOC), and governance functions [5].

Sector-specific work demonstrates the payoff of domain-tailored taxonomies. In the electric grid, threats are mapped to distinct domains (AMI, smart meters, substations, control centers) with protocol and asset peculiarities that drive prioritization and defense selection [6]. Complementary ICS syntheses catalog component-level attack surfaces and countermeasures (segmentation, access control, patching, ML-aided detection), helping practitioners tie classification directly to controls and validation plans [7].

Operationalization through Tactics, Techniques, Procedures (TTP)-based frameworks is another major theme. Mapping scenarios to MITRE ATT&CK for ICS exposes technique-level blind spots, e.g., Impair Process Control or Inhibit Response Function, and structures purple-team exercises around tactic and technique coverage across Purdue levels [8]. Parallel lines address the fast-growing IIoT perimeter: surveys classify attacks by device, edge, and cloud layers, protocols, and supply-chain vectors, emphasizing how IIoT expands paths between enterprise, plant, and cloud analytics workloads [9, 10]. Finally, cloud-based SCADA work reframes trust boundaries (identity, multitenancy, APIs) and proposes cloud-aware taxonomies aligned with service and deployment models, underscoring the need to re-think zones and conduits in hybrid architectures [11].

Across these studies, authors repeatedly note:

- limited empirical datasets and benchmarks for OT attacks and safety outcomes [3, 4];
- uneven coverage of consequence classes, especially standardized mappings from technique to engineered safety impacts [4, 5];
- scarce validation in live and hardware-in-the-loop settings for ATT&CK-mapped defenses [8];
- and emerging blind spots around cloud identity, shared-responsibility models, and IIoT supply chains [9–11].

Together, these findings motivate classification-driven research and practice as a prerequisite for credible risk assessment, incident reporting, security modeling, design, and standards alignment in critical infrastructure. Future work should prioritize shared evaluation datasets, consequence-focused metrics, and cloud and IIoT-inclusive testbeds to strengthen classification-driven detection and risk governance.

NIST CSF 2.0 is a risk-management framework that organizes cybersecurity outcomes into six top-level functions: Govern, Identify, Protect, Detect, Respond, Recover; 22 categories, and a set of subcategories designed to be applied across sectors and technologies. Version 2.0 elevates governance (the new Govern function), expands guidance on profiles (organizational and community), and introduces tiers for characterizing the rigor of risk governance and management. For operational technology and critical infrastructure, CSF 2.0 aligns with NIST SP 800-82 Rev.3 and related NIST guidance, enabling consistent evaluation of OT and ICS defenses and incident response [12].

The purpose of the research is to assess the examined classification methods and approaches with the NIST CSF 2.0 and identify the strengths and limitations of each work in case of CI. To achieve this goal, the following tasks are addressed: review the list of works [1-11] by mapping the NIST CSF 2.0 core functions. For each work, make profiles and tier upgrade suggestions, produce a list of strengths and limitations relative to the framework. Synthesize the results in a comparative table that summarizes the framework function coverage across reviewed solutions in context of CI cybersecurity.

1. NIST CSF 2.0 description

In order to map the NIST CSF 2.0 to the reviewed works [1–11] the following core functions will be used:

Govern (GV) is used to set strategy, policy, and oversight. Has categories: Organizational Context (GV.OC), Risk Management Strategy (GV.RM), Roles, Responsibilities, and Authorities (GV.RR), Policy (GV.PO), Oversight (GV.OV), and Cybersecurity Supply Chain Risk Management (GV.SC).

Identify (ID) focuses on understanding assets, risks, and improvements. Has categories: Asset Management (ID.AM), Risk Assessment (ID.RA), and Improvement (ID.IM).

Protect (PR) includes authentication and access control, data and platform security outcomes. Has categories: Identity Management, Authentication and Access Control (PR.AA), Awareness and Training (PR.AT), Data Security (PR.DS), Platform Security (PR.PS), Technology Infrastructure Resilience (PR.IR).

Detect (DE) covers monitoring and analysis of potential attacks. Has categories: Continuous Monitoring (DE.CM), Adverse Event Analysis (DE.AE).

Respond (RS) is about incident handling. Has categories: Incident Management (RS.MA), Incident Analysis (RS.AN), Incident Response Reporting and Communication (RS.CO), Incident Mitigation (RS.MI).

Recover (RC) is based on restoration execution and communications. Has categories: Incident Recovery Plan Execution (RC.RP), Incident Recovery Communication (RC.CO).

Construction of CSF profiles and tiers will be based on CSF categories and subcategory outcomes. Organizational profile is a list of recommendations to increase cybersecurity strength of CI. There are 4 CSF tiers: Tier 1 (Partial), Tier 2 (Risk-Informed), Tier 3 (Repeatable), and Tier 4 (Adaptive). CSF tiers characterize the rigor of cybersecurity risk governance and management. Then strengths and limitations of which approach will be overviewed based on the overall information.

1.1. CSF 2.0 functions mapping on work [1]. The article [1] develops a solid solution using a stochastic model to quantify a CPSS and critical infrastructure asset's "Security" and "Insecurity".

Outcome coverage against CSF 2.0 functions:

- **Govern**. Strong coverage. Supports risk governance and performance oversight by defining a consistent measurement regime and prioritization of metrics tied to business-process continuity and secrecy levels; this directly informs policy and strategy setting and monitoring of outcomes.

- **Identify**. Moderate coverage. Requires cataloging information assets and their secrecy levels, plus understanding threat implementation probabilities and synergistic impacts; this improves risk understanding and prioritization.
- **Protect**. Moderate coverage. The framework selects and evaluates security service provision (confidentiality, integrity, authenticity, availability, involvement) and can form "security profiles" to safeguard prioritized assets.
- **Detect**. Moderate coverage. Includes explicit E_{attdet} (attack-detection effectiveness) among evaluation metrics, enabling anomaly, indicator tracking and timeliness assessments.
- **Respond** and **Recover**. Partial coverage. Indirectly supported: the quantified "Insecurity" and cost and impact metrics help prioritize incident response and recovery planning, but the paper does not provide playbooks, communication workflows, or recovery strategy design.

Profile and Tier implications:

- **Organizational Profile.** The classifier and scoring can be mapped to CSF outcomes to produce a measurable Current Profile and track movement toward a Target Profile.
- **CSF Tiers**. By institutionalizing measurement and governance of metrics, the approach can help move an organization from Tier 2 (Risk-Informed) toward Tier 3 (Repeatable) in governance and risk management rigor; however, Tier 4 (Adaptive) typically requires continuous, threat-informed adaptation and lessons-learned processes not specified here.

Noted strengths and limitations vs CSF:

- **Strengths**. Formalizes metric selection and aggregation; incorporates secrecy level, hybrid and synergistic threats, and economic and energy costs; supports governance and risk-prioritization decisions.
- **Limitations**. Limited explicit guidance for incident response communications and recovery planning, supply-chain risk, and continuous and adaptive feedback loops - areas to complement with CSF Implementation Examples and sector profiles.

1.2. CSF 2.0 functions mapping on work [2]. The work [2] introduces a cross-domain taxonomy that explicitly traces how attacks traverse IT to OT and control to physical layers in cyber-manufacturing systems. It classifies paths, assets, and effects across these domains and illustrates typical vectors (e.g., enterprise compromise to pivot into control to manipulation of the physical process).

Outcome coverage against CSF 2.0 functions:

- **Govern**. Strong coverage, conceptual support. The taxonomy helps leadership frame strategy, roles, and risk appetite across IT, OT, and physical domains (e.g., policy for cross-domain segmentation, accountability for handoffs).
- **Identify**. Strong coverage. Encourages complete asset and dependency mapping and business-impact analysis across enterprise apps, control systems, and physical processes; clarifies third-party and supply-chain touchpoints.
- **Protect**. Moderate coverage. Implicitly motivates controls at domain boundaries (identity, network segmentation, least privilege, engineering change control) but does not prescribe control baselines.
- **Detect**. Moderate coverage. Identifies where telemetry is needed (enterprise, control network, process sensors) and suggests cross-domain correlation; does not supply analytics or detection content.
- **Respond**. Partial coverage. Informs playbook scoping (who does what at which domain boundary) but lacks concrete response procedures, communications, or evidence handling guidance.
- **Recover**. Partial coverage. Highlights that physical recovery may be decoupled from IT restoration; offers no detailed recovery strategies or Recovery Time Objective (RTO) and recovery point objective (RPO) targets.

Profile and Tier implications:

- **Organizational Profile.** Use the taxonomy to express Current versus Target outcomes across GV, ID, PR, DE, RS, and RC, emphasizing cross-domain dependencies (e.g., required segmentation outcomes, cross-domain monitoring outcomes, joint Incident Response (IR) outcomes).
- **CSF Tiers**. Adopting a formal cross-domain taxonomy, with documented ownership and periodic review, typically moves organizations from Tier 2 (Risk-Informed) toward Tier 3 (Repeatable). Achieving Tier 4 (Adaptive) would require continuous improvement loops (lessons learned, threat-informed updates) beyond the paper's scope.

Noted strengths and limitations vs CSF:

- **Strengths**. Makes cross-domain risk explicit, improving GV and ID outcomes and clarifying where PR and DE controls must sit. Natural scaffold for Profiles, gap analysis, and cross-team accountability (IT, OT, safety). Encourages evidence-based validation (segmentation, identity, telemetry coverage) at domain boundaries.
- **Limitations.** No concrete control catalogs or implementation examples; PR coverage is conceptual. Detection content (analytics, use-cases) not specified; relies on implementers. Response and Recovery playbooks, communications, and exercises are out of scope; needs augmentation with CSF IR and Business Continuity Planning (BCP) outcomes. Limited treatment of metrics and continuous-improvement mechanisms needed for Tier 4 Adaptive posture.

1.3. CSF 2.0 functions mapping on work [3]. In paper [3] authors provide a network-centric taxonomy for CPS and ICS attacks like DoS, deception and FDI, replay and MITM, routing and forwarding attacks with representative defenses and detection approaches. The main focus is on how network-layer threats propagate to control performance and safety.

Outcome coverage against CSF 2.0 functions:

- **Govern**. Moderate coverage. Frames network risks; limited guidance on roles, policies, supplier governance.
- **Identify**. Moderate coverage. Clarifies network assets and dependencies and exposure; not a full asset-to-mission mapping.
- **Protect**. Strong coverage (network layer). Emphasizes segmentation, access control, protocol hardening, protective tech.
- **Detect**. Strong coverage. Highlights anomaly and model-based detection for FDI, replay, and MITM; continuous monitoring.
- **Respond**. Partial coverage. Mentions mitigations; lacks playbooks, communications, and escalation mechanics.
- **Recover**. Partial coverage. Little on restoration beyond reconfiguration; no RTO and RPO or process-safe recovery detail.

Profile and Tier implications:

- **Organizational Profile.** Map current capabilities for PR and DE outcomes and set Target Profile thresholds per attack class (FDI, replay, DoS).
- **CSF Tiers**. Formalizing network-threat coverage and testing can lift maturity from Tier 2 (Risk-Informed) toward Tier 3 (Repeatable). Achieving Tier 4 (Adaptive) requires continuous improvement loops and lessons-learned processes not specified by the paper.

Noted strengths and limitations vs CSF:

- **Strengths**. Strong, practical alignment with PR and DE for network-layer threats. Clear linkage from network events to control-system impact is useful for Profile building and gap analysis.
- **Limitations**. Limited governance detail (policies, roles, risk strategy, supplier controls). Sparse Respond and Recover specifics (playbooks, communications, safe-state restoration). No built-in continuous-improvement or metrics framework needed for Tier 4 (Adaptive).

1.4. CSF 2.0 functions mapping on work [4]. A broad CPS taxonomy organized by attack vector, control-loop role (sensors, actuators, controllers, communications), and consequence (CIA plus safety and process integrity). It synthesizes technique families and defenses, stressing physics-aware analysis of impacts on real processes.

Outcome coverage against CSF 2.0 functions:

- **Govern**. Moderate–strong coverage. Elevates safety and mission outcomes into risk strategy and prioritization; good for policy setting and oversight across IT, OT, and physical domains.
- **Identify**. Strong coverage. Drives full asset and dependency mapping along the control loop and consequence-focused risk assessment.
- **Protect**. Moderate coverage. Describes safeguard families (segmentation, access control, integrity checks, engineering controls) but not a detailed control catalog.
- **Detect**. Moderate coverage. Surveys anomaly, state-estimation, and physics-based methods and continuous monitoring needs; analytics specifics and tuning left to implementers.
- **Respond**. Partial coverage. Implies cross-discipline IR (IT, OT, safety) but lacks procedures, comms paths, and evidence handling.
- **Recover**. Partial coverage. Recognizes safe-state and physical restoration concerns; does not prescribe RTO and RPO or recovery runbooks.

Profile and Tier implications:

- **Organizational Profile.** Use the paper’s axes to express Current versus Target outcomes: governance (risk strategy, roles), identification (asset, risk, consequence mapping), protection and detection at each control-loop point, and joint response and recovery expectations for process safety.
- **CSF Tiers**. Adopting this taxonomy with documented ownership and periodic review typically lifts maturity from Tier 2 (Risk-Informed) toward Tier 3 (Repeatable). Achieving Tier 4 (Adaptive) requires continuous improvement loops, metrics, and exercised playbooks beyond the paper’s scope.

Noted strengths and limitations vs CSF:

- **Strengths**. Strong alignment with Govern and Identify through explicit safety and process consequences. Provides a multi-axis lens that maps naturally into Profiles and helps place Protect and Detect controls at the right control-loop points.
- **Limitations**. Not prescriptive on concrete controls or detection content (Protect and Detect require implementation detail). Limited guidance for Respond and Recover playbooks, communications, and tested recovery strategies. No built-in metrics and continuous-improvement loop needed for Tier 4 (Adaptive).

1.5. CSF 2.0 functions mapping on work [5]. A harmonized taxonomy that links assets, threats, risks, outcomes, designed to standardize terminology across engineering, security operations, and governance. It’s a meta-classification meant to improve consistency, traceability, and measurement rather than a concrete control set.

Outcome coverage against CSF 2.0 functions:

- **Govern**. Strong coverage. Directly supports policy and standard alignment, risk strategy, roles & responsibilities, performance oversight, and change control through common vocabulary.
- **Identify**. Strong coverage. Promotes systematic asset inventories, dependency and business-context mapping, and risk assessment with clear traceability to outcomes.
- **Protect**. Moderate coverage. Helps select and organize families of safeguards but is not a prescriptive control baseline.
- **Detect**. Moderate coverage. Aids outcome-oriented monitoring design and labeling; analytics and use-case content must be provided by the implementer.
- **Respond**. Partial–moderate coverage. Improves incident communications and coordination via shared labels; does not supply playbooks or escalation mechanics.
- **Recover**. Partial coverage. Facilitates post-incident taxonomy updates and lessons-learned alignment; lacks detailed recovery and BCP procedures.

Profile and Tier implications:

- **Organizational Profile.** Use the taxonomy to express Current compared to Target CSF outcomes with end-to-end traceability (from assets and threats to desired outcomes and evidence). This works well for Organization or Community Profile templates.
- **CSF Tiers**. Formal adoption (governance ownership, versioning, training, periodic review) typically advances maturity from Tier 2 (Risk-Informed) to Tier 3 (Repeatable). Reaching Tier 4 (Adaptive) requires metrics, continuous-improvement triggers, and exercised playbooks, and these are not covered by work [6].

Noted strengths and limitations vs CSF:

- **Strengths**. Excellent for Govern and Identify: shared vocabulary, end-to-end traceability, auditability, and faster Profile construction. Natural backbone for evidence management and cross-team alignment (engineering, SOC, risk, compliance).
- **Limitations**. Lacks prescriptive control catalogs (Protect) and concrete detection content (Detect), thus must be added via references (SP 800-53/82, IEC 62443, ATT&CK for ICS). Does not provide detailed Respond and Recover playbooks or tested BCP and Disaster Recovery (DR) mechanics, so needs organization-specific procedures and exercises. To reach Tier 4 (Adaptive), organizations must add metrics, continuous-improvement triggers, and regular joint exercises.

1.6. CSF 2.0 functions mapping on work [6]. A smart-grid–specific taxonomy that maps threats and mitigations across grid domains. AMI and smart meters, Distributed Energy Resource (DER) and Electric Vehicle (EV) charging, substations (IEC-61850), control centers and SCADA, communications backbones. It surveys common attack classes (e.g., FDI on state estimation, load-altering attacks, meter tampering and remote disconnect abuse, protocol spoofing and replay, DoS and jamming, privacy leakage) and pairs them with families of countermeasures (segmentation, authn, authz, crypto-management, key-management, protocol security, anomaly detection, privacy controls).

Outcome coverage against CSF 2.0 functions:

- **Govern**. Moderate coverage. Sector lens helps articulate risk appetite and roles (utility ops, OT engineering, market ops), but governance mechanics (policy versioning, metrics, supplier oversight) are not prescriptive.
- **Identify**. Strong coverage. Encourages domain-wise asset, dependency, and impact mapping (AMI, head-end; substation Intelligent Electronic Devices (IEDs); Phasor Measurement Units (PMUs); DER aggregators), including cyber-physical consequences.
- **Protect**. Moderate–strong coverage. Recommends segmentation (zones and conduits), access control, protocol hardening (e.g., IEC-61850/IEC-62351 concepts), crypto-management, key-management, firmware and secure boot, tamper-resistance, privacy safeguards, but not a full control catalog.
- **Detect**. Strong coverage (grid-specific). Highlights state-estimation residuals, PMU-based analytics, Intrusion Detection System (IDS) at substation and AMI layers, cross-domain telemetry for FDI, replay, load-altering, and DoS.
- **Respond**. Partial coverage. Implies operational responses (e.g., bad-data isolation, protective relaying set-changes, demand curtailment), yet lacks runbooks, communications, escalation playbooks.
- **Recover**. Partial coverage. Notes needed for service restoration (AMI reprovisioning, DER and EV re-sync, substation config baselines) but does not define RTO and RPO, black-start and islanding procedures.

Profile and Tier implications:

- **Organizational Profile.** Use the paper's grid domains as Profile dimensions: document Current versus Target outcomes for AMI, substation, control center, DER and EV, and backbone communications across PR and DE (with governance and IR touchpoints).
- **CSF Tiers**. Formalizing domain-specific controls and analytics and reviewing them cyclically can move posture from Tier 2 (Risk-Informed) toward Tier 3 (Repeatable). Tier 4 (Adaptive) will require metrics, exercised playbooks (islanding, black-start), supplier governance, and continuous improvement loops not specified by the paper.

Noted strengths and limitations vs CSF:

- **Strengths**. Excellent sector specificity for ID and DE, and good coverage of PR families at grid choke points. Natural scaffold for Profiles and gap analysis per grid domain; helps prioritize analytics and boundary controls.
- **Limitations**. Governance mechanics (policies, metrics, supplier oversight, training) only implicitly need CSF-style formalization. Limited Respond and Recover playbook detail (communications, escalation, black-start, islanding drills). No built-in metrics or continuous-improvement loop needed for Tier 4 (Adaptive), must be added by the utility.

1.7. CSF 2.0 functions mapping on work [7]. A survey that: decomposes ICS components and architectures (Programmable Logic Controller (PLC), Remote Terminal Unit (RTU), Human-Machine Interface (HMI), historian, engineering workstation, networks, protocols); catalogs threat and attack vectors; reviews machine-learning–based defenses (anomaly, IDS, classification, forecasting, intrusion detection at network and process layers), including datasets and performance metrics. It is a bridge between ICS architecture and ML-driven detection and defense design.

Outcome coverage against CSF 2.0 functions:

- **Govern**. Moderate coverage. Motivates risk strategy around ML use (model governance, evaluation, retraining), but does not prescribe policy, role-clarity matrix for Responsible, Accountable, Consulted, and Informed (RACI), metrics or supplier oversight.
- **Identify**. Strong coverage. Clear mapping of assets, data flows, and dependencies across Purdue levels; good basis for risk assessments tied to components and processes.
- **Protect**. Moderate coverage. Recommends families of safeguards (segmentation, access control,

hardening) as architectural context for ML deployments; not a control baseline.

- **Detect**. Strong coverage. Core contribution: ML-based detection for network and process anomalies, with datasets, features, and performance measures; guidance on telemetry placement.
- **Respond**. Partial coverage. ML alerts imply response actions but playbooks, communications, and escalation are not detailed.
- **Recover**. Partial coverage. No concrete recovery and BCP mechanics; RC implications are indirect (e.g., model rollback, restoring baselines).

Profile and Tier implications:

- **Organizational Profile.** Use the paper's component model to express Current against Target outcomes for DE (coverage, quality thresholds) and PR (controls that host ML safely). Add GV items for ML model governance (approval, monitoring, retraining).
- **CSF Tiers**. Standing up documented ML detection with monitoring and periodic evaluations can move you from Tier 2 (Risk-Informed) to Tier 3 (Repeatable). Tier 4 (Adaptive) needs continuous improvement loops (drift detection, post-incident model updates, KPI-driven thresholds).

Noted strengths and limitations vs CSF:

- **Strengths**. Strong Identify (clear ICS component and risk context) and Detect (ML methods, datasets, metrics). Provides a practical scaffold for Profiles with measurable DE outcomes and evidence requirements.
- **Limitations**. Governance specifics (policy, RACI, metrics for ML, supplier oversight) are implicit, and must be formalized for GV and higher Tiers. Lacks prescriptive Protect control catalogs and Respond and Recover playbooks; organizations must integrate with IR, BCP, and OT safety procedures. To reach Tier 4 (Adaptive), add robust drift monitoring, post-incident learning, and automated Profile updates.

1.8. CSF 2.0 functions mapping on work [8]. A TTP-centric validation approach that maps MITRE ATT&CK for ICS tactics and techniques to concrete test scenarios for OT environments. It uses ATT&CK as the backbone to evaluate whether controls and detections actually work against technique classes (e.g., Impair Process Control, Inhibit Response Function, Modify Alarm and Trip Parameters, Program Download).

Outcome coverage against CSF 2.0 functions:

- **Govern**. Moderate coverage. Enables policy-level expectations for periodic validation and reporting, but governance mechanics (roles, metrics, supplier oversight) are not prescriptive.
- **Identify**. Moderate coverage. Requires enumerating assets and paths to select relevant techniques (engineering workstations, PLCs, RTUs, HMIs, historians), yet full business-impact mapping is outside scope.
- **Protect**. Strong coverage (control efficiency). Directly tests whether preventive controls (segmentation, Role-Based Access Control (RBAC), allow-listing, change control) withstand specific TTPs.
- **Detect**. Strong coverage. Centers on validating anomaly and rule detections with log and telemetry coverage for ATT&CK techniques across Purdue levels.
- **Respond**. Partial coverage. Triggers and alerts from tests can exercise IR, but the paper does not provide playbooks, communications paths, or evidence-handling procedures.
- **Recover**. Partial coverage. Does not prescribe recovery and BCP mechanics (safe-state, config restore, RTO and RPO), though test outcomes can inform them.

Profile and Tier implications:

- **Organizational Profile.** Build a Current Profile by mapping implemented ATT&CK-covered detections and controls to CSF subcategories (especially PR.AC, PR.PT, PR.DS, DE.AE, DE.CM). Define a Target Profile by adding missing techniques and required evidence.
- **CSF Tiers**. Instituting scheduled, documented ATT&CK-based validations typically moves posture from Tier 2 (Risk-Informed) to Tier 3 (Repeatable). To reach Tier 4 (Adaptive), add continuous improvement loops (threat-intel driven updates, lessons-learned remediations, Key Performance Indicators (KPI) thresholds that auto-adjust the Profile).

Noted strengths and limitations vs CSF:

- **Strengths**. Operationally powerful for Protect and Detect: directly verifies that controls and detections work against real technique classes. Natural scaffold for Profiles, KPI dashboards, and purple-team roadmaps; improves transparency to leadership (Govern).
- **Limitations**. Governance specifics (RACI, cadence, audit metrics) and supplier oversight are implicit. Respond and Recover playbooks, BCP and DR mechanics are not provided, they must be integrated with organizational IR and BCP. Does not itself deliver asset to mission consequence mapping (ID) or safety-engineering constraints; pair with OT guidance (e.g., NIST SP 800-82, sector profiles).

1.9. CSF 2.0 functions mapping on work [9]. A layered IIoT survey that classifies threats and countermeasures across device to edge, fog-to-cloud-to-application. It highlights vectors such as weak device identity, insecure firmware and Over-the-Air (OTA), protocol abuse, API and identity misuse, data leakage, and supply-chain risk, and reviews defenses: strong IAM, secure boot and firmware signing, encryption management, key management, segmentation, IDS and anomaly detection, privacy controls, and ML and BC technologies.

Outcome coverage against CSF 2.0 functions:

- **Govern**. Moderate coverage. Motivates governance for device identity and OTA and third-party risk, but does not prescribe RACI, metrics, and audit cadence.
- **Identify**. Strong coverage. Encourages complete inventories and data-flow mapping across device, edge, and cloud, including dependencies and exposure points.
- **Protect**. Moderate–strong coverage. Emphasizes IAM and least privilege, crypto and Key Management Service (KMS), secure boot and firmware

signing, segmentation, API security, secrets management; not a full control baseline.

- **Detect**. Moderate–strong coverage. Promotes IDS and anomaly detection across layers and telemetry correlation; analytic content and tuning left to implementers.
- **Respond**. Partial coverage. Implies quarantine, revocation, and rotation actions but lacks detailed playbooks or communications.
- **Recover**. Partial coverage. Notes OTA and reprovisioning and service restoration; no tested RTO and RPO or structured recovery runbooks.

Profile and Tier implications:

- **Organizational Profile.** Express Current compared to Target outcomes per layer (device, edge, cloud, application) for PR and DE; add GV items for supplier and OTA governance and ID items for inventories and data-flows.
- **CSF Tiers**. Documented controls, telemetry, and periodic validation can lift from Tier 2 (Risk-Informed) to Tier 3 (Repeatable). Reaching Tier 4 (Adaptive) requires metrics, drift and lessons-learned loops, and automated cert, OTA pipelines beyond the paper's scope.

Noted strengths and limitations vs CSF:

- **Strengths**. Strong Identify and solid Protect and Detect alignment for IIoT-specific risks; practical scaffold for layered Profiles and choke-point controls and telemetry.
- **Limitations**. Governance mechanics (policy, RACI, metrics, supplier oversight cadence) are implicit. Respond and Recover detail (playbooks, communications, tested RTO and RPO) not prescribed. Limited coverage of process-safety where IIoT interfaces with OT, paired with NIST SP 800-82 and plant procedures.

1.10. CSF 2.0 functions mapping on work [10]. A layered IIoT survey that classifies threats and defenses across device, edge, cloud, and application tiers. It catalogs common vectors (weak device identity, insecure firmware and OTA, protocol abuse, API and identity misuse, supply-chain risks) and countermeasures (strong IAM, lightweight crypto, secure boot and firmware signing, network segmentation, IDS and anomaly detection, privacy controls).

Outcome coverage against CSF 2.0 functions:

- **Govern**. Moderate coverage. Highlights policy needs (device identity and OTA governance, supplier risks) but does not prescribe RACI, metrics, or audit cadence.
- **Identify**. Strong coverage. Encourages asset and dependency mapping across device-to-edge-to-cloud, including data flows and third-party components.
- **Protect**. Moderate–strong coverage. Emphasizes IAM, key management, secure boot and firmware signing, encrypted comms, segmentation, and API security; not a full control baseline.
- **Detect**. Strong coverage. Promotes IDS and anomaly detection at device, edge, cloud and telemetry correlation.
- **Respond**. Partial coverage. Implies actions (isolate and quarantine devices, revoke credentials) but lacks playbooks and communications.
- **Recover**. Partial coverage. Notes needed for secure OTA and reprovisioning and service restoration; no RTO and RPO or tested recovery runbooks.

Profile and Tier implications:

- **Organizational Profile.** Structure Current compared to Target outcomes by layer (device, edge, cloud) and function (PR and DE); add GV items for supplier and OTA governance and ID items for comprehensive IIoT inventories and data-flow maps.
- **CSF Tiers**. Documented controls and periodic validation can elevate from Tier 2 (Risk-Informed) to Tier 3 (Repeatable). Tier 4 (Adaptive) requires continuous improvement (metrics, post-incident learning, automated certificate and OTA pipelines) beyond the paper's scope.

Noted strengths and limitations vs CSF:

- **Strengths**. Strong Identify (complete layer and dependency view), Protect, and Detect alignment for IIoT-specific risks. Practical scaffold to build layered Profiles and prioritize controls and telemetry by choke point.
- **Limitations**. Governance specifics (policy, RACI, metrics, supplier oversight cadence) are implicit, and must be formalized to advance Tiers. Respond and Recover details (playbooks, communications, RTO and RPO) are not prescribed. Limited treatment of process-safety outcomes compared to OT-centric works, paired with OT guidance (e.g., NIST SP 800-82) if IIoT interfaces with ICS processes.

1.11. CSF 2.0 functions mapping on work [11]. A survey and taxonomy of cloud-based SCADA architectures and risks across service models (IaaS, PaaS, SaaS) and deployment models (public, private, hybrid). It highlights cloud-specific threats, identity and API abuse, misconfiguration, multitenancy and virtualization risks, data residency and exfiltration, supply-chain dependencies; and families of safeguards (strong IAM, private connectivity, network segmentation, encryption and KMS, logging and monitoring, posture management).

Outcome coverage against CSF 2.0 functions:

- **Govern**. Moderate–strong coverage. Emphasizes shared-responsibility with providers, contractual controls and Service Level Agreement (SLA), and risk ownership; not a full governance playbook (RACI, metrics, cadence).
- **Identify**. Strong coverage. Drives asset and data-flow mapping across on-premises OT to cloud (control plane and data plane), third-party services, and trust boundaries; includes data classification and residency concerns.
- **Protect**. Moderate–strong coverage. Advocates least-privilege Identity and Access Management (IAM), Single Sign-On (SSO), Multi-Factor Authentication (MFA), private links (Virtual Private Network (VPN), direct connect), network segmentation, Virtual Private Clouds (VPCs), encryption with Customer Master Keys (CMKs) and Key Management System (KMS), secure

configuration baselines and secrets management; not a prescriptive control catalog.

- **Detect**. Moderate–strong coverage. Calls for cloud audit logging, workload and network telemetry, Security Information and Event Management (SIEM) integration, Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP); analytic content and tuning left to implementers.
- **Respond**. Partial coverage. Notes needed for provider-integrated IR (isolation, key rotation, API-driven containment), but lacks detailed runbooks, communications, evidence handling.
- **Recover**. Partial coverage. Mentions backup and DR, multi-region failover, but not tested RTO and RPO, black-start and islanding, or offline-operations playbooks.

Profile and Tier implications:

- **Organizational Profile.** Build a Cloud-SCADA Profile with outcomes per layer: control plane, data plane, tenant network, identity, keys and secrets, logging, posture management, and the on-premises OT boundary. Document Current compared to Target outcomes across PR, DE, GV, RS, and RC touchpoints.
- **CSF Tiers**. Formal shared-responsibility matrices, baselined configs as code, posture monitoring, and periodic tests can lift from Tier 2 (Risk-Informed) to Tier 3 (Repeatable). Achieving Tier 4 (Adaptive) requires metrics-driven continuous improvement, provider change intelligence, and exercised cross-region DR beyond the paper's scope.

Noted strengths and limitations vs CSF:

- **Strengths**. Strong ID across cloud and on-premises boundaries and practical PR and DE families for cloud risks. Natural structure for a Cloud-SCADA CSF Profile (control plane, identity, keys, network, logging, posture, DR) and for provider and customer responsibility mapping.
- **Limitations**. Lacks prescriptive Respond and Recover runbooks, tested DR, and governance mechanics (RACI, metrics, audit cadence). Limited treatment of OT process-safety and offline operations if cloud is degraded, must be paired with OT guidance (e.g., NIST SP 800-82) and plant procedures. To reach Tier 4 (Adaptive), organizations need continuous posture analytics, threat-informed updates, and regular cross-region DR exercises.

2. Approaches comparison

To compare the approaches proposed in the reviewed literature [1–11], Table 1 reports the extent to which each approach maps to the NIST CSF 2.0 core functions. Coverage is rated on an ordinal scale: partial (minimal or no coverage), moderate (mapped but incomplete), and strong (comprehensive or near-complete).

Table 1 – **Mapping reviewed papers solutions to NIST CSF 2.0 core functions summary**

Paper #	GV	ID	PR	DE	RS	RC
1	Strong	Moderate	Moderate	Moderate	Partial	Partial
2	Strong	Strong	Moderate	Moderate	Partial	Partial
3	Moderate	Moderate	Strong	Strong	Partial	Partial
4	Strong	Strong	Moderate	Moderate	Partial	Partial
5	Strong	Strong	Moderate	Moderate	Partial	Partial
6	Moderate	Strong	Strong	Strong	Partial	Partial
7	Moderate	Strong	Moderate	Strong	Partial	Partial
8	Moderate	Moderate	Strong	Strong	Partial	Partial
9	Moderate	Strong	Strong	Strong	Partial	Partial
10	Moderate	Strong	Strong	Strong	Partial	Partial
11	Strong	Strong	Strong	Strong	Partial	Partial

The results in Table 1 indicate each solution's compatibility with NIST CSF 2.0. Greater compatibility generally implies a faster, less complex path to adoption for critical infrastructure organizations.

Table 2 presents Profile and Tier recommendations to enhance the durability, sustainability, and security of CI. In general, higher Tiers correspond to more mature and comprehensive cybersecurity governance and operations.

Table 2 – **NIST CSF 2.0 profile and tier implications for the reviewed papers solutions**

Paper #	Profiles (summary)	Tier implications (summary)
1	Map metrics to CSF outcomes; use Security and Insecurity scores to express Current to Target profile; attach metric catalog and secrecy levels as evidence.	Enables Tier 2 to Tier 3 via measurement governance; Tier 4 requires adaptive loops, IR and BCP integration.
2	Cross-domain Profile (IT, OT, physical) stating Current to Target outcomes at boundaries; include joint incident-response outcomes.	Moves Tier 2 to Tier 3 with documented taxonomy and reviews; Tier 4 needs continuous improvement and exercised playbooks.
3	Attack-class matrix (DoS, FDI, replay, routing) mapped to PR and DE subcategories; set mean time to detect and recall targets and evidence.	Tier 2 to Tier 3 via formalized network controls and tests; Tier 4 needs metrics-driven CI and lessons learned.
4	Consequence-first mapping; place PR and DE at sensors, actuators, controllers, and communications; document safe-state expectations.	Tier 2 to Tier 3 with consequence-aware governance; Tier 4 requires metrics, feedback loops, and exercised IR and RC.
5	Harmonized taxonomy enables	Tier 2 to Tier 3 through standardized

Paper #	Profiles (summary)	Tier implications (summary)
	traceable Current to Target profile map (assets, threats, risks, outcomes) with evidence links.	governance; Tier 4 needs metrics and continuous-improvement triggers.
6	Grid-domain Profile (AMI, Substation, Control, DER, Backbone) with PR, DE outcomes and domain-specific evidence.	Tier 2 to Tier 3 via domain baselines and tests; Tier 4 requires drills (islanding, black-start), supplier governance, and KPIs.
7	Component model and ML detection; define DE coverage, quality and PR guardrails; add ML model-governance artifacts.	Tier 2 to Tier 3 with documented ML operations and evaluation; Tier 4 needs drift monitoring and post-incident model updates.
8	ATT&CK to NIST CSF crosswalk; inventory techniques covered; set Target gaps for missing detections, controls and evidence.	Tier 2 to Tier 3 through scheduled ATT&CK validations; Tier 4 requires threat-informed updates and KPI-driven improvements.
9	Layered IIoT Profile (device, edge, cloud, app); govern OTA and supplier risk; set PR and DE targets per layer.	Tier 2 to Tier 3 with documented controls and telemetry; Tier 4 needs automated OTA and certification workflows and continuous improvement.
10	Layered IIoT Profile (device, edge, cloud, app) emphasizing device identity and OTA lifecycle; map detections and recovery paths.	Tier 2 to Tier 3 via layered baselines and tests; Tier 4 requires metrics, lessons learned, and automated pipelines.
11	Cloud-SCADA Profile (control plane, identity, keys, network, logging, posture, DR) with a shared-responsibility matrix.	Tier 2 to Tier 3 via IaC baselines, CSPM, and DR tests; Tier 4 requires metrics-driven adaptation and cross-region DR exercises.

Discussion of results

Table 1 indicates that most reviewed approaches to CI cybersecurity concentrate on the first four NIST CSF 2.0 core functions: Govern, Identify, Protect, and Detect; while Respond and Recover are addressed only minimally or not at all. In particular, the approaches in papers [6, 9--11] exhibit the strongest alignment with CSF 2.0; the remaining works show partial alignment but still offer substantial value for organizing CI cybersecurity.

More specifically, work [1] is notably strong in Govern, establishing direction and oversight, while Identify, Protect, and Detect are only moderate and Respond, Recover are indirect or absent. The current solution has a good potential according to the NIST CSF 2.0 because the GV function has more priority over the other core functions.

Papers [2, 4, 5] show similar patterns, with a somewhat stronger Identify capability.

Works [3, 8] place less emphasis on Govern and Identify but provide deeper treatment of Protect and Detect, reflecting a defensive, control and monitoring-oriented focus.

Work [7] is strong in Identify and Detect but only moderate in Govern and Protect, indicating a monitoring and alerting tilt.

Articles [6, 9, 10] deliver robust Identify, Protect, and Detect coverage with moderate Govern, combining thorough monitoring and prevention.

Paper [11] comes closest to a well-rounded implementation of NIST CSF 2.0 core functions, demonstrating high coverage across GV, ID, PR, and DE and thus a strong basis for coordinated control, monitoring, and attack prevention for CI cybersecurity.

Ranking by closeness to comprehensive NIST CSF 2.0 core functions coverage:

- Strong coverage: [6], [9–11].
- Moderate-strong coverage: [1], [2], [4], [5].
- Moderate coverage: [3], [7], [8].

Table 2 provides paper-specific recommendations for building an Organizational Profile for each work [1–11]. Advancing from Tier 2 to Tier 3 or Tier 4 generally requires additional measures. Common cross-cutting actions include:

- Adaptive feedback loops, continuous improvement, and exercised playbooks: [1], [2], [4], [5], [9].
- Measurement governance and KPIs: [1], [3–6], [8–11].
- Network control hardening and validation testing: [3], [6–8], [10], [11].

These enhancements can be incorporated when integrating the reviewed solutions within CI cybersecurity programs.

Conclusions

This study evaluated papers [1–11] through the lens of the NIST CSF 2.0 core functions [12], mapping each proposed solution to the core functions and formulating corresponding organizational profiles and tier assessments. The findings indicate a substantial potential for most approaches: [1, 2, 4–6, 9–11], and a good potential for the remaining works: [3, 7, 8].

It was provided targeted recommendations to increase tier levels and strengthen overall CI cybersecurity when implementing each approach. Overall, the results suggest clear opportunities to enhance the reviewed solutions and to develop more integrated, robust CI cybersecurity frameworks.

REFERENCES

1. Yevseiev, S., Milov, O., Opirskyy, I., Dunaievska, O., Huk, O., Pogorelov, V., Bondarenko, K., Zviertseva, N., Melenti, Y., & Tomashevsky, B. (2022), “Development of a concept for cybersecurity metrics classification”, *Eastern-European Journal of Enterprise Technologies,* vol. 4 (4 (118)), pp. 6–18, doi: https://doi.org/10.15587/1729-4061.2022.263416
2. Wu, M., & Moon, Y. B. (2017), “Taxonomy of cross-domain attacks on cyber-manufacturing system”, *Procedia Computer Science,* vol. 114, pp. 367–374, doi: https://doi.org/10.1016/j.procs.2017.09.050
3. Cao, L. W., Jiang, X. N., Zhao, Y. M., Wang, S. G., You, D., & Xu, X. L. (2020), “A survey of network attacks on cyber-physical systems”, *IEEE Access,* vol. 8, pp. 44219–44227, doi: https://doi.org/10.1109/ACCESS.2020.2977423
4. Duo, W. L., Zhou, M. C., & Abusorrah, A. (2022), “A survey of cyber attacks on cyber physical systems: Recent advances and challenges”, *IEEE/CAA Journal of Automatica Sinica*, vol. 9(5), pp. 784–800, doi: https://doi.org/10.1109/JAS.2022.105548
5. Pool, J. H., & Venter, H. (2022), “A harmonized information security taxonomy for cyber physical systems”, *Applied Sciences,* vol. 12(16), pp. 8080, doi: https://doi.org/10.3390/app12168080
6. Ding, J., Qammar, A., Zhang, Z., Karim, A., & Ning, H. (2022), “Cyber threats to smart grids: Review, taxonomy, potential solutions, and future direction”, *Energies,* vol. 15(18), pp. 6799, doi: https://doi.org/10.3390/en15186799
7. Nankya, M., Chataut, R., & Akl, R. (2023), “Securing industrial control systems: Components, cyber threats, and machine learning-driven defense strategies”, *Sensors,* vol. 23(21), pp. 8840, doi: https://doi.org/10.3390/s23218840
8. Afenu, D. S., Asiri, M., & Saxena, N. (2024), “Industrial control systems security validation based on MITRE Adversarial Tactics, Techniques, and Common Knowledge framework”, *Electronics,* vol. 13(5), 917, doi: https://doi.org/10.3390/electronics13050917
9. Alnajim, A., Habib, S., Islam, M., Thwin, S., & Alotaibi, F. (2023), “A comprehensive survey of cybersecurity threats, attacks, and effective countermeasures in Industrial Internet of Things”, *Technologies,* vol. 11(6), 161, doi: https://doi.org/10.3390/technologies11060161
10. Tsiknas, K., Taketzis, D., Demertzis, K., & Skianis, C. (2021), “Cyber threats to industrial IoT: A survey on attacks and countermeasures”, *IoT,* vol. 2(1), pp. 163–186, doi: https://doi.org/10.3390/iot2010009
11. Wali, A., & Alshehry, F. (2024), “A survey of security challenges in cloud-based SCADA systems”. *Computers,* vol. 13(4), pp. 97, doi: https://doi.org/10.3390/computers13040097
12. Pascoe, C., Quinn, S. & Scarfone, K. (2024). “*The NIST Cybersecurity Framework (CSF) 2.0”*, NIST Cybersecurity White Paper (CSWP 29). Gaithersburg, MD: National Institute of Standards and Technology, doi: https://doi.org/10.6028/NIST.CSWP.29

Received (Надійшла) 06.10.2025
Accepted for publication (Прийнята до друку) 20.10.2025

ВІДОМОСТІ ПРО АВТОРІВ/ ABOUT THE AUTHORS

Світличний Дмитро Олександрович – аспірант кафедри кібербезпеки, Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна;
Dmytro Svitlychnyi – PhD student of Cyber Security Department, National Technical University “Kharkiv polytechnic institute”, Kharkiv, Ukraine;
e-mail: Dmytro.O.Svitlychnyi@cs.khpi.edu.ua; ORCID Author ID: https://orcid.org/0009-0002-0945-8221.

Ткачов Андрій Михайлович – к.т.н., с.н.с., доцент кафедри кібербезпеки, Національний технічний університет “Харківський політехнічний інститут”, Харків, Україна;
Andrii Tkachov – candidate of technical sciences, senior researcher, associate professor of Cyber Security Department, National Technical University “Kharkiv polytechnic institute”, Kharkiv, Ukraine;
e-mail: Andrii.Tkachov@khpi.edu.ua; ORCID Author ID: https://orcid.org/0000-0003-1428-0173;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57416821200.

ДОСЛІДЖЕННЯ СУЧАСНИХ МЕТОДІВ КЛАСИФІКАЦІЇ АТАК НА КРИТИЧНУ ІНФРАСТРУКТУРУ

Д. О. Світличний, А. М. Ткачов

Анотація. Актуальність. На сьогоднішній день об’єкти критичної інфраструктури (КІ) дедалі більше залежать від взаємопов’язаних цифрових і фізичних систем, що робить їх пріоритетною ціллю для витончених кібератак. Паралельно в цій галузі сформовано великий і різноманітний масив досліджень. Водночас існують виклики яким чином порівнювати ці підходи узгоджено й на спільній основі. Фреймворк кібербезпеки (ФК) NIST 2.0 пропонує структуру для такого порівняння. **Предметом дослідження** у статті є огляд сучасних методів класифікації кібератак на ОКІ та пов’язаних із ними підходів. **Метою статті** є подвійний намір: оцінити сильні сторони та обмеження розглянутих підходів крізь призму NIST ФК 2.0 та окреслити конкретні можливості їхнього вдосконалення для практичного впровадження у середовищах КІ. **Були отримані наступні результати.** Проведено детальне мапування кожного підходу на шість основних функцій ФК 2.0 щоб показати, де покриття є сильним, а де лише частковим. На основі цього мапування сформовано організаційні профілі та запропоновано орієнтовні рівні ретельності. Узагальнення подано у порівняльних таблицях, що полегшують аналіз відмінностей. Додатково наведено стислий підсумок сильних сторін і обмежень для кожної розглянутої роботи, рекомендовані елементи профілю й дії для підвищення рівня, а також наскрізні напрями вдосконалення. **Висновок.** Більшість розглянутих підходів добре узгоджуються з функціями Управління, Ідентифікації, Захисту та Виявлення, тоді як Реагування та Відновлення висвітлено мінімально або взагалі не розглянуто. Така картина окреслює можливий шлях модернізації. Запропоновані мапування, профілі, рівні та порівняльні таблиці становлять багаторазовий інструментарій для об'єктів КІ, які планують адаптувати розглянуті рішення відповідно до NIST ФК 2.0.

Ключові слова: кібербезпека; фреймворк кібербезпеки (ФК); критична інфраструктура (КІ); класифікація кібератак; NIST CSF 2.0.