ПЕДАГОГІЧНА АКАДЕМІЯ:
НАУКОВІ ЗАПИСКИ

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ

УДК 004.056:37.018.43:519.8

DOI https://doi.org/10.5281/zenodo.21875358

Математичне моделювання та гібридне управління кіберінцидентами в освітньому середовищі на основі wshedsec

Кашина Ганна Сергіївна,
доктор педагогічних наук, завідувач кафедри інтелектуальних систем та цифрових технологій, Академія праці, соціальних відносин і туризму, вул. Кільцева дорога, 3-А, Київ, 03188, Україна, e-mail: gannakashina@gmail.com, https://orcid.org/0000-0002-2829-9847

Краснік Андрій Анатолійович,
кандидат технічних наук, доцент кафедри інтелектуальних систем та цифрових технологій, Академія праці, соціальних відносин і туризму, Київ, 03188, Україна, https://orcid.org/0009-0004-8737-5389

Бацуровська Ілона Вікторівна,
доктор педагогічних наук, професор кафедри інтелектуальних систем та цифрових технологій, Академія праці, соціальних відносин і туризму, вул. Кільцева дорога, 3-А, Київ, 03188, Україна, e-mail: batsurovska_ilona@outlook.com, https://orcid.org/0000-0002-8407-4984

Прийнято: 14.05.2026 | Опубліковано: 30.05.2026

Анотація. *Мета дослідження полягає у теоретичному обґрунтуванні та формалізації моделі WSHEdSec для гібридного управління кіберінцидентами в*

освітньому середовищі, де поєднуються автоматизовані механізми виявлення, математичне оцінювання ризику та експертне прийняття рішень. Методи. Використано системний аналіз, теорію множин, марковські процеси, нечітке оцінювання, багатокритеріальну оптимізацію, сценарне моделювання та методи експертного узгодження. Освітню цифрову інфраструктуру подано як динамічний граф активів, користувачів, сервісів і залежностей. Стан кіберінциденту описано вектором ознак, що включає критичність активу, достовірність сигналу, масштаб поширення, вплив на безперервність навчання, чутливість даних та очікувані втрати. Результати. Запропоновано авторську модель WSHEdSec, у якій індекс пріоритету інциденту формується як зважена нелінійна композиція нормованих показників, а вибір реакції здійснюється гібридним контуром «аналітичний модуль – правила безпеки – відповідальна особа». Введено функцію сукупних втрат, що враховує прямий збиток, тривалість простою, педагогічні наслідки, репутаційний ризик і вартість контрзаходів. Сформовано матрицю переходів між станами «нормальне функціонування», «підозріла подія», «підтверджений інцидент», «локалізація», «відновлення» та «післяінцидентне вдосконалення». Визначено умови автоматичного реагування, ескалації та обов'язкового людського контролю. Проведене сценарне моделювання демонструє, що гібридна схема зменшує очікуваний час локалізації і ризик помилкових блокувань порівняно з виключно ручною або виключно автоматизованою моделлю. Висновки. WSHEdSec може використовуватися як методична основа для побудови ситуаційних центрів закладів освіти, планування кібернавчань, пріоритизації повідомлень систем моніторингу та узгодження технічних дій із вимогами безперервності освітнього процесу. Практична цінність моделі полягає в адаптивності до різних рівнів цифрової зрілості, можливості калібрування ваг за експертними та емпіричними даними й підтримці доказового післяінцидентного аналізу.

 ISSN: 2786-9458

Ключові слова: *стохастична оцінка ризику, адаптивна реакція, цифрова стійкість, освітня інфраструктура, кіберризик, нечітка логіка, безперервність навчання, ситуаційний центр.*

Mathematical modelling and hybrid cyber-incident management in the educational environment based on WSHEdSec

Hanna Kashyna,
Doctor of Pedagogical Sciences, Head of the Department of Intelligent Systems and Digital Technologies, Academy of Labour, Social Relations and Tourism, 3-A Kiltseva Doroha St., Kyiv, 03188, Ukraine, e-mail: gannakashina@gmail.com, https://orcid.org/0000-0002-2829-9847

Andrii Krasnik,
Candidate of Technical Sciences, Associate Professor of the Department of Intelligent Systems and Digital Technologies, Academy of Labour, Social Relations and Tourism, Kyiv, 03188, Ukraine, https://orcid.org/0009-0004-8737-5389

Ilona Batsurovska,
Doctor of Pedagogical Sciences, Professor of the Department of Intelligent Systems and Digital Technologies, Academy of Labour, Social Relations and Tourism, 3-A Kiltseva Doroha St., Kyiv, 03188, Ukraine, e-mail: batsurovska_ilona@outlook.com, https://orcid.org/0000-0002-8407-4984

Abstract. *Objective. The study aims to substantiate and formalise the WSHEdSec model for hybrid cyber-incident management in an educational environment by combining automated detection, mathematical risk assessment and accountable human decision-making. Methods. The research employs systems*

analysis, set theory, Markov processes, fuzzy evaluation, multi-criteria optimisation, scenario modelling and expert weighting. Educational digital infrastructure is represented as a dynamic graph of assets, users, services and dependencies. Each incident is described by a feature vector including asset criticality, signal confidence, propagation scale, impact on learning continuity, data sensitivity and expected loss. Results. The proposed WSHEdSec model calculates an incident-priority index as a weighted nonlinear composition of normalised indicators and selects a response through a hybrid loop integrating an analytical module, security rules and a responsible decision maker. A total-loss function combines direct damage, downtime, pedagogical consequences, reputational risk and countermeasure costs. A transition matrix is formulated for the states of normal operation, suspicious event, confirmed incident, containment, recovery and post-incident improvement. Thresholds are defined for automatic response, escalation and mandatory human supervision. Scenario experiments indicate that the hybrid scheme can reduce expected containment time and the probability of disruptive false-positive actions compared with purely manual or purely automated approaches. Conclusions. WSHEdSec provides a methodological basis for educational security operations centres, cyber-exercise design, alert prioritisation and alignment of technical response with continuity-of-learning requirements. Its practical value lies in calibration for different levels of digital maturity, incorporation of expert and empirical data, and support for evidence-based post-incident learning.

Keywords: *stochastic risk assessment, adaptive response, digital resilience, learning infrastructure, fuzzy logic, continuity of education, security operations, decision support.*

Постановка проблеми. Цифрова трансформація освіти розширила функціональні можливості закладів освіти, але водночас створила складне середовище взаємозалежних інформаційних систем. Електронні журнали, системи управління навчанням, хмарні сховища, сервіси відеозв’язку, наукові

репозитарії, платформи дистанційного оцінювання та корпоративні облікові записи формують єдиний цифровий контур. Порушення роботи навіть одного критичного сервісу може спричинити каскадні наслідки: втрату доступу до навчальних матеріалів, зупинення комунікації, компрометацію персональних даних, спотворення результатів оцінювання або припинення роботи адміністративних процесів.

Сучасні стандарти кібербезпеки розглядають реагування на інциденти не як ізольовану технічну процедуру, а як складову загального управління ризиками. NIST Cybersecurity Framework 2.0 структурує діяльність організації навколо функцій Govern, Identify, Protect, Detect, Respond і Recover, наголошуючи на безперервному вдосконаленні [1]. Оновлені рекомендації NIST SP 800-61 Rev. 3 інтегрують реагування у всі стадії управління кіберризиком і передбачають постійне використання отриманих уроків [2]. Для освітніх установ ця логіка особливо важлива через необхідність одночасно захищати дані, забезпечувати доступність сервісів і не переривати навчальний процес.

Ландшафт загроз залишається динамічним: ENISA виокремлює атаки на доступність, програми-вимагачі та загрози даним серед провідних категорій інцидентів [3], а наступний огляд підтверджує зростання складності багатовекторних атак і потребу в контекстному аналізі [4]. Освітній сектор має специфічну поверхню атаки: велику кількість користувачів із різним рівнем цифрової компетентності, високу змінність облікових записів, поєднання застарілих і хмарних систем, відкритість академічної комунікації та обмежені ресурси для цілодобового моніторингу. Рекомендації CISA для освітніх організацій підкреслюють необхідність системного управління ризиками, планування реагування та пріоритизації базових захисних заходів [5].

У практиці закладів освіти часто співіснують дві крайні моделі. Перша ґрунтується на ручному аналізі, який забезпечує контекстне розуміння, але є повільним і залежним від доступності фахівців. Друга покладається на

автоматичні правила, які швидко блокують підозрілу активність, проте можуть спричиняти хибні спрацювання та порушувати навчання. Це зумовлює потребу в гібридній моделі, яка розподіляє функції між алгоритмами й відповідальними особами залежно від критичності, достовірності сигналу та допустимого часу реакції.

Аналіз останніх досліджень і публікацій. Проблематика управління кіберінцидентами розвивається у трьох взаємопов'язаних напрямах: стандартизація процесів реагування, математичне оцінювання пріоритету та моделювання практичної підготовки команд. У вищій освіті практичні рекомендації EDUCAUSE орієнтують установи на повний цикл підготовки, реагування, відновлення й безперервного поліпшення [6]. Окремо наголошується на потребі розглядати кібербезпеку як базову компетентність усіх учасників освітнього процесу, а не лише спеціалізованих підрозділів [7].

Моделі кібернавчань дають змогу перевіряти не тільки технічні навички, а й командну координацію. B. Alothman запропонував модель навчань із розподілом ролей між командами, що відтворює реальні сценарії реагування [8]. Дослідження адаптивних кіберполігонів демонструють ефективність збирання телеметрії навчальної діяльності й динамічного добору складності завдань [9]. Адаптивний формат практичної підготовки знижує перевантаження здобувачів і створює диференційовані траєкторії виконання сценарію [10]. Для освітнього середовища ці результати важливі, оскільки модель управління інцидентами має бути одночасно операційною та придатною для навчання персоналу.

Окремий блок досліджень присвячений математичній формалізації кіберризику. F. Sufi запропонував математичну та кластеризаційну основу для аналізу розподілу кіберзагроз між галузями [11]. A. Peralta та співавтори поєднали нечітку логіку й оброблення природної мови для динамічної пріоритизації інцидентів [12]. Перспективним є використання марковських процесів, теорії корисності та оптимального керування, що дає змогу

 ISSN: 2786-9458

представляти інцидент як послідовність станів і вибирати дію з урахуванням майбутнього ризику.

Організаційною основою для побудови процедур є стандарти ISO/IEC 27035-1:2023 щодо принципів управління інцидентами [13] та ISO/IEC 27001:2022 щодо систем управління інформаційною безпекою [14]. Європейська директива NIS2 посилює вимоги до управління ризиками, звітування та відповідальності керівництва [15]. Водночас наявні підходи переважно описують загальні процеси або окремі алгоритми пріоритизації та недостатньо враховують педагогічну ціну помилкової реакції, наприклад блокування платформи під час іспиту чи втрату доступу до матеріалів під час синхронного заняття.

Виділення невирішених раніше частин загальної проблеми. Недостатньо формалізованим залишається поєднання технічної критичності інциденту з безперервністю навчання, конфіденційністю освітніх даних і допустимим рівнем автоматизації. Не визначено універсального механізму, який одночасно враховує невизначеність сигналів, взаємозалежність сервісів, часову вартість затримки, ризик хибного блокування та потребу в людській відповідальності. Потребує розвитку також механізм перетворення післяінцидентних даних у навчальні сценарії та коригування політик.

Формулювання цілей статті (постановка завдання). Метою статті є розроблення математично формалізованої моделі WSHEdSec для гібридного управління кіберінцидентами в освітньому середовищі. Для досягнення мети поставлено завдання: визначити структуру станів і параметрів моделі; сформувати інтегральний індекс пріоритету; обґрунтувати функцію втрат та правило вибору реакції; визначити межі автоматизації й людського контролю; провести сценарне порівняння ручної, автоматизованої та гібридної стратегій; окреслити умови практичного впровадження.

Методи дослідження. Методологічну основу становлять системний і ризик-орієнтований підходи. Для формалізації інфраструктури використано теорію графів; для опису переходів між станами — дискретний марковський процес; для нормування нечітких експертних оцінок — функції належності; для вибору реакції — багатокритеріальну функцію втрат; для перевірки поведінки моделі — сценарне імітаційне моделювання. Значення ваг можуть визначатися методом аналізу ієрархій, експертним узгодженням або калібруванням за історичними даними SOC.

Виклад основного матеріалу дослідження. У межах статті WSHEdSec використовується як назва авторської зваженої стохастично-гібридної моделі безпеки освітнього середовища. Її призначення полягає не у заміні наявних стандартів, а в математичній конкретизації процесів оцінювання, ескалації та вибору дій відповідно до логіки NIST та ISO.

Освітню цифрову інфраструктуру подамо орієнтованим графом G=(V,E), де V — множина активів і суб’єктів, а E — множина функціональних, інформаційних та автентифікаційних залежностей. До вузлів належать LMS, електронний журнал, система управління контингентом, корпоративна пошта, файлові сховища, сервіси відеозв’язку, мережеві пристрої, робочі станції, облікові записи та зовнішні постачальники. Вага ребра відображає силу залежності: імовірність того, що порушення одного вузла вплине на інший.

Для кожного активу v_i задається вектор критичності c_i=(a_i,d_i,p_i,r_i), де a_i характеризує вимогу доступності, d_i — чутливість даних, p_i — педагогічну значущість, r_i — складність відновлення. Інцидент k описується вектором x_k=(q_k,s_k,g_k,t_k,u_k), де q_k — достовірність детектора, s_k — тяжкість технічного впливу, g_k — потенціал поширення, t_k — терміновість, u_k — невизначеність.

$$P\_k = \sigma(\Sigma_i w_i z_i + \Sigma_{i<j} \gamma_{ij} z_i z_j),$$

ISSN: 2786-9458

де P_k — інтегральний пріоритет інциденту; z_i — нормовані компоненти критичності й ознак; w_i — вагові коефіцієнти; γ_ij — коефіцієнти взаємодії; σ — логістична функція, що обмежує результат інтервалом [0;1]. Нелінійний член потрібний для врахування синергетичного ефекту: подія середньої технічної тяжкості може стати критичною, якщо відбувається на сервісі з високою педагогічною значущістю під час підсумкового оцінювання.

Таблиця 1

Параметри індексу пріоритету WSHEdSec

Параметр	Зміст	Джерело даних	Шкала
C_a	Критичність доступності сервісу	каталог активів, SLA	0–1
C_d	Чутливість і регуляторна значущість даних	класифікація інформації	0–1
C_p	Вплив на освітній процес	календар занять, тип активності	0–1
Q	Достовірність сигналу	SIEM/EDR, кореляція подій	0–1
G	Потенціал поширення	граф залежностей, мережевий контекст	0–1
T	Часова терміновість	динаміка інциденту, допустимий простій	0–1
U	Невизначеність	розбіжність детекторів, нестача даних	0–1

Джерело: розроблено авторами.

Функція втрат для дії a у стані s визначається як $L(s,a)=\lambda_1 D+\lambda_2 H+\lambda_3 P+\lambda_4 R+\lambda_5 C$, де D — очікувані прямі втрати даних та активів; H — втрати від простою; P — педагогічні наслідки; R — репутаційні та правові наслідки; C — вартість і побічний вплив контрзаходу. Оптимальна дія мінімізує очікувану суму поточних і майбутніх втрат:

$$a^* = arg\ min_a \{ L(s,a) + \beta \Sigma_{s'} Pr(s'|s,a)V(s') \}.$$

Коефіцієнт β визначає горизонт планування. За низького β система переважно мінімізує негайні втрати; за високого — враховує довгострокові наслідки, зокрема ризик повторного інциденту та необхідність відновлення довіри. Це дозволяє уникнути локально швидких, але стратегічно небезпечних рішень.

Таблиця 2

Стани життєвого циклу інциденту у моделі WSHEdSec

Позначення	Стан	Критерій переходу	Типові дії
S0	Нормальне функціонування	немає підтверджених аномалій	моніторинг, профілактика
S1	Підозріла подія	аномалія перевищує поріг спостереження	збагачення даних, повторна перевірка
S2	Підтверджений інцидент	сукупність доказів перевищує поріг підтвердження	класифікація, призначення відповідального
S3	Локалізація	обрано й активовано контрзахід	ізоляція, блокування, обмеження доступу
S4	Відновлення	поширення зупинено, ризик контрольований	відновлення сервісів, перевірка цілісності
S5	Післяінцидентне вдосконалення	операційна стабільність відновлена	аналіз причин, оновлення правил і навчань

Джерело: розроблено авторами.

Перехід між станами задається матрицею P=[p_ij], елементи якої оцінюються за журналами подій або експертно. Матриця є контекстною: у період вступної кампанії чи сесії ймовірність ескалації та ціна простою змінюються. Тому WSHEdSec використовує часовий контекст h(t), який коригує критичність сервісів. Наприклад, недоступність LMS уночі в міжсеместровий період і під час синхронного іспиту має різні наслідки.

Гібридність управління реалізується трьома контурами. Автоматичний контур виконує оборотні та низькоризикові дії: збагачення події, ізоляцію сесії,

примусову повторну автентифікацію, тимчасове обмеження підозрілого токена. Напівавтоматичний контур формує рекомендований план і вимагає підтвердження відповідальної особи. Експертний контур застосовується, коли дія може суттєво порушити навчання, вплинути на великі групи користувачів, спричинити юридичні наслідки або коли рівень невизначеності перевищує допустимий поріг.

Таблиця 3

Правила вибору режиму реагування

Умова	Автоматичний режим	Напівавтоматичний режим	Обов'язковий експертний контроль
$P\_k < 0{,}35$	реєстрація, збагачення, спостереження	необов'язково	ні
$0{,}35 \le P\_k < 0{,}65$	оборотні локальні дії	рекомендовано	за високого U
$0{,}65 \le P\_k < 0{,}85$	лише за затвердженим playbook	так	для критичних активів
$P\_k \ge 0{,}85$	аварійне стримування за правилами	негайна ескалація	так
$U \ge 0{,}60$	мінімально необхідні оборотні дії	обов'язково	так, якщо дія впливає на навчання

Джерело: розроблено авторами.

Для оцінювання ефективності визначено такі показники: середній час підтвердження інциденту MTTC, середній час локалізації MTTCn, середній час відновлення MTTR, частка хибнопозитивних реакцій FPR, частка інцидентів із порушенням безперервності навчання EDI та залишковий ризик RR. Інтегральний показник результативності може бути поданий як $E=\alpha_1(1-MTTCn\_norm)+\alpha_2(1-FPR)+\alpha_3(1-EDI)+\alpha_4(1-RR)$, де всі складові нормовано.

Сценарне моделювання здійснено для трьох типових ситуацій: компрометація облікового запису викладача; поширення шкідливого програмного забезпечення в комп'ютерній лабораторії; DDoS-атака на

платформу дистанційного навчання. Порівнювалися ручна стратегія, автоматизована стратегія з фіксованими правилами та WSHEdSec. Для кожного сценарію виконано 1000 імітацій із варіацією достовірності детекторів, часу доступності фахівця, швидкості поширення та педагогічної критичності моменту.

Таблиця 4

Узагальнені результати сценарного моделювання

Стратегія	Нормований час локалізації	Хибні блокування	Порушення навчання	Залишковий ризик
Ручна	0,72	0,08	0,31	0,34
Автоматизована	0,29	0,24	0,27	0,22
WSHEdSec	0,34	0,11	0,14	0,16

Джерело: розроблено авторами.

Результати показують, що виключно автоматизована стратегія забезпечує найменший час локалізації, але має найвищу частку хибних блокувань. Ручна стратегія краще враховує контекст, проте поступається за швидкістю, що збільшує залишковий ризик. WSHEdSec зберігає близьку до автоматизованої швидкість і водночас істотно зменшує негативний вплив на навчальний процес. Числові значення мають демонстраційний характер і повинні калібруватися на фактичних даних конкретної установи.

Практичне впровадження моделі передбачає п’ять кроків. Спочатку формується каталог активів і залежностей. Далі встановлюються профілі критичності з урахуванням календаря освітніх подій. На третьому кроці налаштовуються джерела телеметрії, правила кореляції та початкові ваги. Четвертий крок охоплює розроблення playbook-сценаріїв із чітким визначенням оборотних і необоротних дій. П’ятий крок полягає у регулярному калібруванні моделі за результатами реальних інцидентів і кібернавчань.

ISSN: 2786-9458

WSHEdSec може виконувати й дидактичну функцію. Дані про переходи станів, рішення та наслідки перетворюються на анонімізовані кейси для підготовки студентів і працівників. У кіберполігоні параметри моделі можуть змінюватися, щоб демонструвати компроміс між швидкістю й безпечністю реакції. Такий підхід узгоджується з результатами досліджень адаптивних середовищ кібернавчання [8–10].

Важливою умовою є прозорість. Для кожної рекомендації система має зберігати пояснення: які показники вплинули на пріоритет, яке правило спрацювало, чому обрано конкретний режим і хто затвердив дію. Це забезпечує аудит, підтримує відповідальність і знижує ризик неконтрольованого використання автоматизації. Модель не повинна приймати незворотні рішення щодо персоналу або студентів; її призначення — підтримка операційного управління технічними й організаційними заходами.

Обмеження дослідження пов’язані з залежністю результатів від якості телеметрії та вагових коефіцієнтів. Установи з низькою цифровою зрілістю можуть не мати достатньої історії інцидентів для статистичного калібрування. У такому разі доцільно починати з експертних ваг, проводити tabletop-вправи та поступово уточнювати модель. Іншим обмеженням є можливість зміни поведінки атакувальника у відповідь на передбачувані автоматичні правила, тому playbook-сценарії мають регулярно переглядатися.

Висновки. Розроблено авторську модель WSHEdSec для математичного моделювання та гібридного управління кіберінцидентами в освітньому середовищі. Модель поєднує графове подання інфраструктури, зважений нелінійний індекс пріоритету, марковський опис життєвого циклу, функцію сукупних втрат і правила розподілу рішень між автоматичним, напівавтоматичним та експертним контурами. На відміну від універсальних схем реагування, запропонований підхід безпосередньо враховує педагогічну

критичність сервісів, календарний контекст і ризик порушення безперервності навчання.

Сценарне моделювання засвідчило потенційну перевагу гібридної стратегії: вона забезпечує швидке стримування загроз за меншої частки хибних блокувань і нижчого впливу на освітній процес. Практичне застосування потребує каталогу активів, якісної телеметрії, формалізованих playbook-сценаріїв, визначених меж автоматизації та регулярного післяінцидентного навчання. Перспективи подальших досліджень пов'язані з емпіричним калібруванням ваг на даних закладів освіти, розробленням програмного прототипу, дослідженням стійкості до навмисного спотворення сигналів та інтеграцією моделі з кіберполігонами.

Список використаних джерел

1. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg, 2024. DOI: 10.6028/NIST.CSWP.29.

2. Nelson A., Rekhi S., Souppaya M., Scarfone K. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. NIST SP 800-61 Rev. 3. Gaithersburg, 2025. DOI: 10.6028/NIST.SP.800-61r3.

3. European Union Agency for Cybersecurity. ENISA Threat Landscape 2024. Athens : ENISA, 2024.

4. European Union Agency for Cybersecurity. ENISA Threat Landscape 2025. Athens : ENISA, 2025.

5. Cybersecurity and Infrastructure Security Agency. Protecting Our Future: Partnering to Safeguard K-12 Organizations from Cybersecurity Threats. Washington, 2023.

6. Grajek S., Brooks D. C. Cybersecurity Incident Management and Response Guide. EDUCAUSE Review. 2024.

7. EDUCAUSE. 2024 Horizon Report: Cybersecurity and Privacy Edition. Louisville : EDUCAUSE, 2024.

8. Alothman B. Developing a Cyber Incident Exercises Model to Educate Security Teams. Electronics. 2022. Vol. 11, No. 10. Article 1575. DOI: 10.3390/electronics11101575.

9. Vykopal J., Seda P., Švábenský V., Čeleda P. Smart Environment for Adaptive Learning of Cybersecurity Skills. 2023. arXiv:2307.05281.

10. Seda P., Vykopal J., Švábenský V., Čeleda P. Reinforcing Cybersecurity Hands-on Training with Adaptive Learning. 2022. arXiv:2201.01574.

11. Sufi F. Mathematical Modeling and Clustering Framework for the Distribution of Cyber Threats across Industries. Mathematics. 2025. Vol. 13, No. 4. Article 655. DOI: 10.3390/math13040655.

12. Peralta A. et al. A Hybrid Mathematical Framework for Dynamic Incident Prioritization in Enterprise Environments. Mathematics. 2025. Vol. 13, No. 12. Article 1941. DOI: 10.3390/math13121941.

13. ISO/IEC 27035-1:2023. Information technology — Information security incident management — Part 1: Principles and process. Geneva : ISO, 2023.

14. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva : ISO, 2022.

15. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union. Official Journal of the European Union. 2022. L 333. P. 80–152.

References

1. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

2. Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile (NIST SP 800-61 Rev. 3). https://doi.org/10.6028/NIST.SP.800-61r3

3. European Union Agency for Cybersecurity. (2024). ENISA Threat Landscape 2024.

4. European Union Agency for Cybersecurity. (2025). ENISA Threat Landscape 2025.

5. Cybersecurity and Infrastructure Security Agency. (2023). Protecting Our Future: Partnering to Safeguard K-12 Organizations from Cybersecurity Threats.

6. Grajek, S., & Brooks, D. C. (2024). Cybersecurity Incident Management and Response Guide. EDUCAUSE Review.

7. EDUCAUSE. (2024). 2024 Horizon Report: Cybersecurity and Privacy Edition.

8. Alothman, B. (2022). Developing a Cyber Incident Exercises Model to Educate Security Teams. Electronics, 11(10), 1575. https://doi.org/10.3390/electronics11101575

9. Vykopal, J., Seda, P., Švábenský, V., & Čeleda, P. (2023). Smart Environment for Adaptive Learning of Cybersecurity Skills. arXiv:2307.05281.

10. Seda, P., Vykopal, J., Švábenský, V., & Čeleda, P. (2022). Reinforcing Cybersecurity Hands-on Training with Adaptive Learning. arXiv:2201.01574.

11. Sufi, F. (2025). Mathematical Modeling and Clustering Framework for the Distribution of Cyber Threats across Industries. Mathematics, 13(4), 655. https://doi.org/10.3390/math13040655

12. Peralta, A., et al. (2025). A Hybrid Mathematical Framework for Dynamic Incident Prioritization in Enterprise Environments. Mathematics, 13(12), 1941. https://doi.org/10.3390/math13121941

13. International Organization for Standardization. (2023). ISO/IEC 27035-1:2023 Information security incident management — Part 1: Principles and process.

14. International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security management systems — Requirements.

15. European Parliament and Council. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union. Official Journal of the European Union, L 333, 80–152.

 ISSN: 2786-9458