АКТУАЛЬНІ ПРОБЛЕМИ У СФЕРІ ПУБЛІЧНОГО УПРАВЛІННЯ

УДК 351:37:004.02
DOI https://doi.org/10.32782/TNU-2663-6468/2025.2/21

Дей Г.А.
ДЗВО «Університет менеджменту освіти»

РОЗРОБКА ТИПОВОГО РЕГЛАМЕНТУ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ В ОСВІТНЬОМУ СЕРЕДОВИЩІ

Зростання кількості кіберінцидентів в освітньому секторі України у 2024–2025 роках актуалізувало потребу у впровадженні уніфікованих регламентів реагування на цифрові загрози. У статті обґрунтовано необхідність створення типового регламенту як управлінського інструменту забезпечення кіберстійкості освітніх установ. Мета дослідження полягає у формуванні моделі типового регламенту реагування на кіберінциденти в освітньому середовищі, з урахуванням міжнародного досвіду, особливостей функціонування українських закладів освіти і зростаючих загроз цифровій безпеці. У дослідженні застосовано аналіз офіційних документів, описовий аналіз практик українських і зарубіжних закладів освіти, а також структурно-функціональне моделювання для побудови регламенту реагування. У процесі дослідження проаналізовано чинні нормативні та локальні документи в Україні, встановлено відсутність єдиної законодавчої вимоги щодо впровадження регламентів у сфері освіти, а також виявлено фрагментарність ініціатив на рівні окремих закладів. Ідентифіковано ключових суб'єктів у межах функціональної структури реагування на інциденти: керівництво, CISO, адміністратори цифрових сервісів, юридична служба, організатори навчального процесу, що дозволило сформувати повноцінну матрицю відповідальності. Проведено узагальнення структур міжнародних політик реагування (University of Glasgow, SUNY Empire, Vanderbilt University), виокремлено релевантні елементи – класифікацію загроз, міжфункціональну взаємодію, регулярне навчання персоналу та постінцидентну аналітику. На основі інтеграції отриманих результатів сформовано типовий регламент, адаптований до потреб українських освітніх закладів: він містить процедури виявлення, класифікації, технічного реагування, документації, навчання і щорічного перегляду. Наукова новизна полягає у створенні функціонально-інституційної моделі регламенту кіберреагування, яка враховує управлінські, технічні та правові аспекти в межах освітнього процесу і може бути застосована як основа для внутрішніх політик безпеки ЗВО. Розроблений типовий регламент забезпечує можливість системного реагування на кіберінциденти у сфері освіти, формалізує ролі й повноваження учасників процесу, підвищує організаційну готовність до цифрових загроз і створює передумови для інтеграції політик кібербезпеки у стратегії розвитку освітніх закладів.

Ключові слова: *кіберінцедент, кіберреагування, політика реагування, робоча група з цифрової безпеки, ІТ-відділ, заклади освіти.*

Постановка проблеми. Упродовж 2024–2025 років цифрові ризики, що проникають у сферу освіти, почали демонструвати тенденцію не лише до кількісного зростання, але й до якісного ускладнення. У 2024 році Україна зазнала рекордного зростання кіберзагроз, що суттєво вплинуло на освітній сектор. За даними CERT-UA, кількість кіберінцидентів зросла на 70% порівняно з попереднім роком, досягнувши 4 315 випадків. Основними цілями атак стали органи місцевого самоврядування, державні установи, енергетичний сектор та телекомунікаці [1]. У 2025 році ситуація набрала обертів – лише за перший квартал 2025 року команда реагування на комп'ютерні надзвичайні ситуації CERT-UA при Держспецзв'язку та захисту інформації України зафіксувала понад 1500 кіберінцидентів (це вже більше третини з 4315 інцидентів, зареєстрованих за весь 2024 рік – рік, у якому відбувся рекордний стрибок на 70%) [2]. Європейська агенція ENISA у своєму звіті за 2024 рік виокремила освітній сектор як вразливий до багаторівневих атак, зокрема

з боку APT-груп, зазначаючи, що ransomware залишається ключовою кіберзагрозою для організацій, включаючи освітні та медичні заклади [3].

Проблематика кіберінцидентів уже давно не обмежується втратами доступу до електронних журналів чи витоками електронної пошти викладачів. Йдеться про системні загрози, які здатні паралізувати освітні платформи, модифікувати або знищити персональні дані про здобувачів освіти, а також викривити управлінські процеси в межах інституцій. Водночас, більшість закладів освіти України досі функціонують у режимі ситуативної реакції: без уніфікованого протоколу дій, без нормативно узгоджених сценаріїв реагування, без чітко визначеного понятійного апарату.

Не зовсім зрозуміло, чому за понад десять років активної цифровізації так і не сформувалася практика типового регламентування кіберзагроз в освітньому середовищі. Можливо, це наслідок надмірної фрагментації ІТ-політик між закладами різних рівнів акредитації, або відлуння більш глибокої інституційної проблеми, пов'язаної з недостатнім включенням кібербезпеки до пріоритетів освітнього менеджменту. У будь-якому разі, відсутність єдиного алгоритму дій у відповідь на кіберінциденти створює перманентну зону ризику, де випадковість часто замінює системність, а внутрішні ресурси використовуються без стратегічної оптимізації.

Аналіз останніх досліджень і публікацій. З огляду на загострення проблеми кіберінцидентів в освітньому секторі та відсутність уніфікованого механізму реагування, постає необхідність звернення до наукового дискурсу, який окреслює як концептуальні підходи, так і прикладні рішення у сфері кібербезпеки. Так, зокрема, в роботі авторів Б. В. Павлюка, Б. М. Розпутні та В. В. Кисліцина [4] аналізуються сучасні технологічні рішення у сфері захисту інформації в освітніх установах. Автори підкреслили важливість впровадження комплексних систем безпеки, що включають як технічні, так і організаційні заходи. У статті О. К. Юдіна [5] розглядається підхід до формування професійних компетентностей у сфері ІТ та кібербезпеки. Автор пропонує концепцію, яка передбачає інтеграцію теоретичних знань і практичних навичок, необхідних для ефективного реагування на кіберзагрози. У дослідженні інших авторів О. Шапрана, С. Сторожука та К. Войтеха [6] аналізуються існуючі підходи до формування компетентностей у сфері кібербезпеки серед наукових і науково-педагогічних працівників. Вони підкреслили важливість системного підходу до підготовки кадрів, що включає як теоретичну, так і практичну підготовку, а також розробку методичних рекомендацій і регламентів, які можуть бути використані в освітніх установах для підвищення рівня кібербезпеки. Науковець І. Діордіца [7] звертає увагу на невідповідність між актуальними кіберзагрозами і змістом освітніх програм з підготовки фахівців. Автор підкреслює потребу в інтеграції практичних навичок реагування на інциденти в освітні стандарти. Інший автор І. Татомир [8] досліджує поширення фішингових атак у вищій освіті та роль кінцевого користувача у послабленні захисту. Автор наголошує на необхідності підвищення обізнаності персоналу й студентів як частини системного підходу до кіберзахисту.

З-поміж зарубіжних джерел варто виокремити А. Алексей (A. Alexei) [9], яка формує фреймворк стратегічної кібербезпеки для освітніх установ. Її модель передбачає міжфункціональні комітети, сценарне планування інцидентів та їх документування – все це є потенційно адаптивним у межах українського контексту.

Нарешті, Й.Б. Ульвен та Г. Ванген (J.B. Ulven та G. Wangen) [10] здійснили типологію ризиків у закладах вищої освіти. Найбільш вагомим у цьому дослідженні є підхід до розмежування рівнів відповідальності за реагування на інциденти – від керівництва університету до ІТ-відділів і звичайних користувачів. Автори наголосили – без уніфікованого регламенту з чіткою градацією ризиків і процедур реагування, система кіберзахисту в освітніх закладах залишатиметься вразливою. Ця теза безпосередньо перегукується з українським контекстом, де відсутність типового регламенту призводить до імпровізованих реакцій і знижує ефективність управління інцидентами.

Попри те, що у проаналізованих джерелах і простежується поступ до осмислення кіберзагроз в освіті, помітним залишається дефіцит робіт, які б формували цілісну, адаптивну ієрархічну модель типового регламенту реагування. Відсутній деталізований опис сценаріїв координації між адміністрацією, технічним персоналом і зовнішніми структурами в умовах реального інциденту, особливо у випадках, коли мова йде про малобюджетні або децентралізовані освітні інституції – таких ситуацій джерела здебільшого уникають або розглядають фрагментарно.

Постановка завдання. Гіпотеза цього дослідження полягає в тому, що відсутність типового регламенту є не лише результатом браку інфраструктурних можливостей, але й відображенням

розриву між державними нормотворчими процесами та фактичною динамікою кіберзагроз. Регламент, розроблений на основі емпіричних даних, правових норм і практик кіберрозвідки, може стати не інструкцією для формального виконання, а інструментом гнучкого адаптивного реагування – з урахуванням різного масштабу інцидентів і ресурсних можливостей установ.

Дослідження спрямоване на розробку типової моделі регламенту реагування на кіберінциденти для закладів освіти України з урахуванням міжнародного досвіду та сучасних кіберзагроз, з метою підвищення рівня інституційної кіберстійкості. Завдання дослідження наведено нижче по тексту:

1. Проаналізувати стан нормативного регулювання та практики реагування на кіберінциденти в українських закладах освіти з урахуванням національного законодавства, локальних ініціатив та державних рекомендацій.

2. Ідентифікувати ключові суб'єкти відповідальності у процесі розробки та реалізації регламенту в межах функціональної структури ЗВО.

3. Узагальнити міжнародний досвід розробки регламентів реагування на кіберінциденти в освітньому середовищі, зокрема моделі університетів США, Великобританії та Японії.

4. Розробити власну типову модель регламенту реагування на кіберінциденти для закладів вищої освіти України.

Виклад основного матеріалу. На сьогодні в Україні відсутній єдиний типовий регламент реагування на кіберінциденти, обов'язковий для всіх закладів освіти. Однак деякі освітні установи та органи влади впроваджують власні документи та практики, спрямовані на підвищення кібербезпеки.

Локальні ініціативи в закладах освіти. Деякі заклади освіти розробляють внутрішні плани реагування на кіберінциденти. Наприклад, Уманська районна військова адміністрація оприлюднила план дій у разі виявлення кібератаки або кіберінциденту. Цей план передбачає негайне повідомлення відповідальних осіб, інформування урядової команди реагування на кіберінциденти CERT-UA, Національного координаційного центру кібербезпеки та інших відповідних органів. Також визначено терміни подання технічної інформації та індикаторів компрометації [11].

Методичні рекомендації та навчальні програми. Державна служба спеціального зв'язку та захисту інформації України затвердила методичні рекомендації щодо реагування на різні види подій у кіберпросторі. Ці рекомендації спрямовані на суб'єктів забезпечення кібербезпеки, включаючи освітні установи, і містять загальні принципи реагування на кіберінциденти [12].

Крім того, в рамках підвищення обізнаності з кібербезпеки, Білоцерківський інститут неперервної професійної освіти розробив електронний навчальний курс для педагогічних працівників закладів професійної освіти. Курс охоплює основи кібербезпеки в цифровому освітньому середовищі та сприяє формуванню практичних навичок реагування на кіберзагрози [13].

Національні ініціативи та заходи. Національний координаційний центр кібербезпеки (далі – НКЦК) проводить регулярні кібернавчання й змагання, такі як HackWave та INCIDENT RESPONSE DAYS 2.0, спрямовані на підвищення готовності до реагування на кіберінциденти. Також організовано секторальні кібернавчання для різних галузей, включаючи освітній сектор, з метою підвищення кіберстійкості регіонів [14].

Таким чином, хоча в Україні ще не існує уніфікованого типового регламенту реагування на кіберінциденти для закладів освіти, окремі установи та органи влади впроваджують власні документи та практики, спрямовані на підвищення кібербезпеки в освітньому середовищі. В таблиці 1 наведено функціональну структуру відповідальних осіб за розробку регламенту реагування на кіберінциденти в закладі освіти (див. таблицю 1).

На сьогоднішній день українське законодавство не містить прямої вимоги для освітніх закладів щодо обов'язкової розробки і впровадження регламенту реагування на кіберінциденти. Закон України «Про основні засади забезпечення кібербезпеки України» [15] та нещодавній Закон України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів…» 27.03.2025 року [16] встановлюють обов'язки в цій сфері переважно для органів державної влади, об'єктів критичної інформаційної інфраструктури і власників державних інформаційних ресурсів. Проте в умовах цифровізації освітнього процесу, гібридних форм навчання й зростання кіберзагроз, наявність такого документа перетворюється з формальної ініціативи на практичну необхідність для збереження безперервності освітнього процесу, захисту персональних даних та цифрових активів закладу.

Головне, що важливо відмітити по таблиці 1 – юристи часто залучаються на останньому етапі, проте саме від їх участі залежить легітимність регламенту, особливо при обробці персональних

Таблиця 1

Функціональна структура відповідальних осіб за розробку регламенту реагування на кіберінциденти в закладі освіти

№	Категорія відповідальних осіб	Посади	Повноваження та функції
1	Керівництво освітнього закладу	Ректор, директор	- Ініціює створення регламенту. - Видає розпорядчі документи. - Затверджує регламент як ЛНД.
2	Відповідальні за кібербезпеку	CISO, IT-директор, завідувач IT-відділу	- Розробляє регламент. - Координує взаємодію підрозділів. - Контролює аудит та захист IT-систем.
3	Юридичне забезпечення	Юрист, юрисконсульт	- Перевіряє відповідність законодавству. - Адаптує до вимог ЗУ «Про захист персональних даних».
4	Організатори навчального процесу	Проректори, декани, методисти	- Інтегрують правила до освітнього процесу. - Регламентують поведінку в LMS, e-mail тощо.
5	Адміністратори цифрової інфраструктури	Системні адміністратори, адміністратори LMS, email-сервісів	- Реагують на технічні інциденти. - Забезпечують ведення логів та безперервність сервісу.
6	Робоча група з цифрової безпеки (за потреби)	Міжкафедральна або міжструктурна група	- Проводить аналіз загроз - Розробляє сценарії реагування. - Проводить симуляції та навчання.

Джерело: сформовано автором

Примітка: ЛНД – локальний нормативний документ; CISO – Chief Information Security Officer (керівник з інформаційної безпеки); IT – інформаційні технології; LMS – Learning Management System (система управління навчанням).

даних згідно із ЗУ «Про захист персональних даних», GDPR та вимогами державних аудиторів. Адміністратори LMS та email-систем – це фактичні «перші респонденти», які помічають аномалії (злом акаунтів, масові розсилки, DDoS) раніше, ніж IT-відділ – отже, їх роль у регламенті має бути формалізована, хоча в більшості установ вона офіційно не закріплена. Робочі групи – хоч і рідко створюються в освітньому середовищі, саме вони можуть забезпечити стратегічну гнучкість і регулярну актуалізацію регламенту, з урахуванням змін технологій, ризиків і інфраструктури. Важливо також розуміти, що керівництво часто делегує відповідальність за кібербезпеку IT-відділам, не інтегруючи питання безпеки у загальну систему управління ризиками, що в разі серйозного інциденту ускладнює відповідальність та реагування.

Таким чином, відсутність законодавчого зобов'язання не скасовує управлінської відповідальності. Навпаки, наявність проактивної регламентної політики з кіберреагування може стати фактором стійкості, довіри з боку здобувачів освіти та партнерів, а також критерієм акредитаційної зрілості. Формування такого документа має розглядатися як прояв цифрової автономії та стратегічної передбачливості. Цікаво також звернутися до міжнародного досвіду стосовно наявності та розробок регламентів щодо кіберреагування в закладах освіти.

У міжнародній практиці заклади вищої освіти активно впроваджують політики реагування на кіберінциденти, навіть якщо це не завжди є прямою законодавчою вимогою. Впровадження таких політик розглядається як невід'ємна частина комплексної системи кіберзахисту, особливо в умовах цифровізації навчального процесу. Прикладом такої передової практики є політика Університету Вандербільта (США), де чітко окреслено повний життєвий цикл кіберінциденту: від виявлення, класифікації та реагування до постінцидентного аналізу. У документі встановлено розподіл обов'язків між CISO, IT-допомогою та спеціальною групою Incident Response Team. Політика зобов'язує всіх працівників університету повідомляти про будь-яку підозрілу активність протягом 24 годин. Окремою перевагою є класифікація інцидентів за рівнями критичності, що дозволяє оперативно оцінювати ступінь загрози та визначати відповідні протоколи дій [17].

Державний університет Нью-Йорка (SUNY Empire State College) теж має розгорнуту політику, що базується на класифікації інцидентів за типом (інформаційні, операційні, критичні) і включає процедури взаємодії з держорганами у разі витоку персональних даних. Університет також

використовує «фішинг-карту» – візуалізацію частоти й характеру фішингових атак, що допомагає вчасно реагувати та коригувати політики безпеки [18].

Університет Західної Вірджинії (WVU) приділяє особливу увагу ризикам, що стосуються платформ дистанційного навчання. Політика базується на моделі CIA (Confidentiality – Integrity – Availability) і передбачає як технічне реагування, так і подальше навчання персоналу, який допустив інцидент. Журнали інцидентів обов'язкові для ведення, а повторне навчання – є умовою для доступу до критичних систем [19].

Університет Глазго (Велика Британія) має політику обробки інцидентів інформаційної безпеки, яка визначає загальні кроки для ефективного управління та вирішення інцидентів безпеки у структурований та послідовний спосіб. Спеціальна команда реагування на інциденти (UGCirt) несе загальну відповідальність та повноваження щодо управління всіма зареєстрованими інцидентами безпеки. Конкретні обов'язки щодо обробки певних інцидентів або їх аспектів покладаються на інші групи, такі як системні менеджери, IT-підтримка, адміністратори мереж та систем [20].

Аналіз наведених кейсів показує, що університети не лише мають регламенти, а й активно їх інтегрують у свої освітні платформи та щоденну адміністративну діяльність. Усі вивчені інституції мають спеціалізовані команди реагування, систему онлайн-звітування, класифікацію інцидентів за рівнем ризику та передбачають участь працівників і студентів у тренінгах. Ці елементи дозволяють університетам не лише ефективно реагувати на інциденти, але й запобігати їх повторенню.

Враховуючи вищезазначене, стає очевидним: хоча в українському законодавстві відсутня обов'язкова вимога щодо наявності регламенту реагування на кіберінциденти в освітніх закладах, міжнародна практика свідчить про ефективність та необхідність такої політики. Вона є не лише інструментом безпеки, а й засобом підвищення довіри до інституції, забезпечення безперервності освітнього процесу та готовності до нових викликів кіберпростору. Українським університетам варто орієнтуватися на ці стандарти та адаптувати їх відповідно до власного контексту, не чекаючи змін у нормативно-правовій базі.

Представлений нижче регламент, розроблений з урахуванням досвіду університетів Великої Британії, Японії, США та країн ЄС (University of Glasgow, Keio University, University of Tokyo, SUNY Empire State College, рекомендації NIS2), і покликаний забезпечити системність і послідовність дій ЗВО у випадку виникнення кіберінциденту (див. таблицю 2). Його структура

Таблиця 2

Типовий регламент реагування на кіберінциденти в закладах вищої освіти України (на основі міжнародного досвіду)

1. Загальні положення 1.1. Цей регламент визначає порядок виявлення, класифікації, реагування та документування кіберінцидентів, що можуть впливати на інформаційні системи, сервіси, мережеву інфраструктуру та дані закладу вищої освіти (ЗВО). 1.2. Метою регламенту є забезпечення захисту конфіденційності, цілісності та доступності інформаційних ресурсів ЗВО, мінімізація шкоди від кіберінцидентів, своєчасне реагування та запобігання повторним випадкам. 1.3. Регламент базується на міжнародних практиках, зокрема політиках: − University of Glasgow, UK [20] − University of Tokyo, Japan [21] − SUNY Empire State College, USA [18]
2. Визначення термінів 2.1. *Кіберінцидент* – будь-яка подія, що негативно впливає або може вплинути на інформаційну безпеку ЗВО. 2.2. *Інформаційна система (ІС)* – сукупність апаратного та програмного забезпечення для обробки даних. 2.3. *Команда реагування на кіберінциденти (CSIRT)* – визначена група фахівців ЗВО, відповідальна за обробку інцидентів.
3. Класифікація кіберінцидентів 3.1. Кіберінциденти класифікуються за критичністю: • *Критичний рівень*: злом основних систем, витік персональних даних, зупинка освітнього процесу. • *Високий рівень*: масові фішингові атаки, шкідливе ПЗ, компрометація облікових записів працівників або студентів. • *Середній рівень:* виявлення вразливостей, спроби несанкціонованого доступу. • *Низький рівень*: випадкові технічні помилки або порушення політик безпеки без серйозних наслідків.

Продовження таблиці 2

4. Ролі та відповідальність 4.1. Керівник ЗВО – забезпечує загальну політику кібербезпеки, затверджує регламент. 4.2. CISO / IT-директор – координує дії CSIRT, звітує перед керівництвом про інциденти. 4.3. CSIRT – проводить аналіз, реагування, усунення наслідків, розробляє рекомендації для запобігання повтору. 4.4. Уповноважені викладачі / працівники – негайно повідомляють CSIRT про підозрілі дії або кіберінциденти.
5. Процедура реагування 5.1. *Виявлення*: інцидент може бути виявлений автоматизованими засобами (IDS, SIEM) або повідомлений персоналом. 5.2. *Повідомлення*: інцидент повідомляється до CSIRT протягом 1 години після виявлення (електронною поштою або через внутрішню форму). 5.3. *Оцінка*: CSIRT здійснює попередню оцінку масштабу та критичності. 5.4. *Ізоляція*: у разі потреби система або обліковий запис ізолюється для запобігання подальшому поширенню. 5.5. *Усунення та відновлення*: здійснюється очищення систем, оновлення ПЗ, зміна паролів, перевірка логів. 5.6. *Документування*: складається звіт про інцидент із зазначенням часу, джерел, наслідків та вжитих заходів.
6. Навчання та тестування 6.1. Усі працівники та студенти проходять базові онлайн-курси з кібергігієни щороку (практика SUNY Empire). 6.2. CSIRT проводить тренінги для персоналу з реагування на фішинг, шкідливе ПЗ тощо (практика UTokyo). 6.3. Один раз на рік проводиться симуляція кіберінциденту (penetration test або tabletop exercise).
7. Перегляд та оновлення регламенту 7.1. Регламент переглядається CSIRT щороку або після масштабного інциденту. 7.2. Пропозиції щодо змін подаються керівнику ЗВО та затверджуються наказом.
8. Контактна інформація CSIRT ЗВО (тут вказуються електронна адреса, телефон, відповідальна особа)

Джерело: сформовано автором

передбачає чітке визначення термінів, ролей і відповідальностей, класифікацію загроз, процедури виявлення та реагування, а також аспекти навчання персоналу й регулярного перегляду політики. Документ рекомендовано для використання як типовий шаблон при формуванні власного внутрішнього регламенту ЗВО.

Таким чином, запровадження системного підходу до реагування на кіберінциденти в освітньому середовищі є важливим елементом сучасного управління інформаційною безпекою. Типовий регламент, сформований на основі кращих європейських, американських та азійських практик, покликаний не лише врегулювати оперативні дії у разі кіберінциденту, а й підвищити загальну культуру кібергігієни в межах закладу.

Висновки. Таким чином, дослідження показало, що в українських закладах освіти переважає фрагментарний підхід до реагування на кіберінциденти, а законодавство не містить прямої вимоги щодо наявності відповідних регламентів на рівні закладів освіти. Проведений аналіз функціональної структури управління кіберінцидентами засвідчив необхідність чіткого розмежування ролей між керівництвом, IT-фахівцями, юристами, адміністраторами цифрової інфраструктури та організаторами навчального процесу, з урахуванням їх впливу на ефективність реагування. Міжнародна практика підтвердила доцільність запровадження спеціалізованих політик реагування з високим рівнем формалізації процедур, регулярним навчанням, класифікацією інцидентів та визначенням ступенів відповідальності, що є релевантним для імплементації в українському освітньому контексті.

Запропонований типовий регламент, побудований на міжнародних підходах, адаптований до української специфіки, здатен забезпечити не лише технічну відповідь на кіберінциденти, а й сформувати інституційний рівень цифрової зрілості освітньої установи.

Список літератури:

1. The Odessa Journal. The number of cyberattacks on Ukraine has increased by 70% over the past year: the main targets of hackers. 2025. URL:https://surl.lu/luerek (дата звернення: 29.03.2025).

2. Potii O. Inside Ukraine's new digital defense strategy to counter Russian cyber onslaught. *United24 Media.* 2025. URL: https://surl.li/cuehcd (дата звернення: 29.03.2025).

3. European Union Agency for Cybersecurity. ENISA Threat Landscape 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (дата звернення: 29.03.2025).

4. Павлюк Б. В., Розпутня Б. М., Кисліцин В. В. Комплексні системи захисту інформації в освітніх закладах: сучасні технологічні рішення та перспективи впровадження. *Педагогічна Академія: Наукові Записки*. 2024. № 7. С. 1-17. DOI: https://doi.org/10.57125/pedacademy.2024.06.29.10

5. Юдін О. К. Концепція формування професійних компетентностей фахівців з інформаційних технологій та кібербезпеки. *Наукоємні Технології*. 2019. № 3. С. 330-342. DOI: https://doi.org/10.18372/2310-5461.43.13984

6. Шапран О., Сторожук С., Войтех К. Аналіз підходів формування компетентності з кібербезпеки наукових та науково-педагогічних працівників. *Журнал «Перспективи та Інновації Науки».* 2025. Т. 1, №47. С. 1283-1296. DOI: https://doi.org/10.52058/2786-4952-2025-1(47)-1283-1296

7. Діордіца І. Освітні стандарти підготовки фахівців із кібербезпеки. Jurnalul Juridic Național: Teorie și Practică. 2017. Т. 1, №23. С. 46-49. URL: https://ibn.idsi.md/vizualizare_articol/50742 (дата звернення: 29.03.2025).

8. Татомир І. Кібербезпека університетів як спосіб протидії фішинговому шахрайству. *Економічний Дискурс*. 2020. Т. 1, №1. С. 59-67. DOI: https://doi.org/10.36742/2410-0919-2020-1-7

9. Alexei (Lachi) A. Cyber security strategies for higher education institutions. *Journal of Engineering Science.* 2021. Т. 28, №4. С. 74–92. DOI: https://doi.org/10.52326/jes.utm.2021.28(4).07

10. Ulven J. B., Wangen G. A systematic review of cybersecurity risks in higher education. *Future Internet.* 2021. Т. 13, №2. С. 39. DOI: https://doi.org/10.3390/fi13020039

11. Внутрішній план реагування на кібератаки та кіберінциденти. Уманська державна адміністрація. 2024. URL: https://uman-rda.gov.ua/news/1695715938/ (дата звернення: 29.03.2025).

12. Держспецзв'язку затвердила Методичні рекомендації щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі. Державна служба спеціального зв'язку та захисту інформації України. 2023. URL: https://surl.li/wyxjqn (дата звернення: 29.03.2025).

13. Гончарова І.П. *Кібербезпека в цифровому освітньому середовищі закладів професійної освіти: електронний навчальний курс.* БІНПО ДЗВО «УМО» НАПН УКРАЇНИ, 2022. 80 с.

14. Річний аналітичний огляд: жовтень 2023 – вересень 2024. Національний координаційний центр кібербезпеки при РНБО України. 2024. URL: https://surli.cc/rgeyqh (дата звернення: 29.03.2025).

15. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 29.03.2025).

16. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/4336-IX#Text (дата звернення: 29.03.2025).

17. Incident response policy. Vanderbilt University. 2025. URL: https://www.vanderbilt.edu/cybersecurity/policies/incident-response-policy/ (дата звернення: 29.03.2025).

18. Information security incident response policy. Empire State College. 2021. URL: https://sunyempire.edu/policies/?search=cid%3D134541 (дата звернення: 29.03.2025).

19. Computer security incident policy. West Virginia University. 2025. URL: https://it.wvu.edu/policies-and-procedures/security/computer-security-incident (дата звернення: 29.03.2025).

20. Incident handling policy. University of Glasgow. 2025. URL: https://surl.li/tkbvoc (дата звернення: 29.03.2025).

21. Information security policies. University of Tokyo. URL: https://www.u-tokyo.ac.jp/en/about/information-security.html (дата звернення: 29.03.2025).

22. European Commission. Cybersecurity policies. 2025. URL: https://surli.cc/qyqaaa (дата звернення: 29.03.2025).

Dei H.A. DEVELOPMENT OF MODEL REGULATIONS FOR RESPONDING TO CYBER INCIDENTS IN THE EDUCATIONAL ENVIRONMENT

The increase in the number of cyber incidents in the education sector of Ukraine in 2024–2025 has highlighted the need to implement unified regulations for responding to digital threats. The article substantiates the need to create a standard regulation as a management tool for ensuring the cyber resilience of educational institutions. The purpose of the study is to form a model of a standard regulation for responding to cyber incidents in the educational environment, taking into account international experience, the peculiarities of the functioning of Ukrainian educational institutions and growing threats to digital security. The study used an analysis of official documents, a descriptive analysis of the practices of Ukrainian and foreign educational institutions, as well as structural and functional modeling to build a response regulation. In the process of the study, the current regulatory and local documents in Ukraine were analyzed, the absence of a single legislative requirement for the implementation of regulations in the field of education was established, and the fragmentation of

initiatives at the level of individual institutions was also revealed. Key actors within the functional structure of incident response were identified: management, CISO, digital service administrators, legal department, and educational process organizers, which allowed for the formation of a full-fledged matrix of responsibility. The structures of international response policies were summarized (University of Glasgow, SUNY Empire, Vanderbilt University), and relevant elements were identified: threat classification, cross-functional interaction, regular staff training, and post-incident analytics. Based on the integration of the results obtained, a standard regulation was formed, adapted to the needs of Ukrainian educational institutions: it contains procedures for detection, classification, technical response, documentation, training, and annual review. The scientific novelty lies in the creation of a functional and institutional model of cyber response regulations, which takes into account managerial, technical, and legal aspects within the educational process and can be used as the basis for internal security policies of higher education institutions. The developed standard regulations provide the possibility of a systematic response to cyber incidents in the field of education, formalize the roles and powers of the participants in the process, increase organizational readiness for digital threats, and create the prerequisites for integrating cybersecurity policies into the development strategy of educational institutions.

Key words: *cyber incident, cyber response, response policy, digital security working group, IT department, educational institutions.*