ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
АВТОМОБІЛЬНО-ДОРОЖНІЙ УНІВЕРСИТЕТ

КІБЕРСТІЙКІСТЬ У СУЧАСНОМУ СВІТІ: ВИКЛИКИ, ІННОВАЦІЇ, РІШЕННЯ



І ВСЕУКРАЇНСЬКА
НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ
ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ І МОЛОДИХ УЧЕНИХ

ХАРКІВ • 2026

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний автомобільно-дорожній університет

Кафедра кібербезпеки

Всеукраїнської науково-практичної конференції
здобувачів вищої освіти і молодих учених

«Кіберстійкість у сучасному світі: виклики, інновації, рішення»

Випуск І

Збірник статей і тез доповідей

6 листопада 2026
Харків 2026 р.

УДК 004.056:656.13:625.7/.8
К38

Друкується за рішенням Ради механічного факультету Харківського національного автомобільно-дорожнього університету
(протокол №3 від 13 листопада 2026 р.)

Електронне видання

Редакційна колегія:

Голова:

Холодов Антон Павлович, к.т.н, доцент, ректор ХНАДУ, Україна, Харків (Голова)

Члени оргкомітету:

Дмитрієв Ілля Андрійович, д.е.н., проф., проректор з наукової роботи ХНАДУ, Україна, Харків (Заступник Голови)

Єфименко Олександр Володимирович, к.т.н., проф., декан механічного факультету, ХНАДУ, Україна, Харків

Пономаренко Роман Володимирович, д.т.н., проф., начальник ІНДЦЗ НУЦЗ України, Україна, Київ

Каргін Анатолій Олексійович, д.т.н., проф., завідувач кафедри «Інформаційні технології», УкрДУЗТ, Україна, Харків

Крайнюк Олена Володимирівна, к.т.н., завідувачка кафедри кібербезпеки, Україна, Харлдків

Кіберстійкість у сучасному світі: виклики, інновації, рішення : матеріали І Всеукраїнської науково-практичної конференції. – Харків: ХНАДУ, 2026. – 357 с.

У збірнику представлено матеріали Всеукраїнської науково-практичної конференції здобувачів вищої освіти і молодих учених «Кіберстійкість у сучасному світі: виклики, інновації, рішення» в авторській редакції. Автори наукових публікацій несуть відповідальність за достовірність фактів, цитат, власних назв та гарантують відсутність академічного плагіату. Матеріали Всеукраїнської науково-практичної конференції призначено для застосування науковцями, викладачами закладів вищої освіти, фахівцями з кібербезпеки, інформаційних технологій та транспортної галузі, працівниками органів державної влади, підприємцями, здобувачами освіти різних рівнів.

Федін Вадим Віталійович, Сєвєрінов Олександр Васильович АНАЛІЗ ПОВЕДІНКОВИХ АНОМАЛІЙ ПРАЦІВНИКІВ ДЛЯ РАННЬОГО ВИЯВЛЕННЯ ІНСАЙДЕРСЬКИХ ЗАГРОЗ .. 65

Черкаський Олександр Валерійович, Буслов Павло Володимирович БАГАТОРІВНЕВА МОДЕЛЬ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ З ХМАРНИХ СЕРЕДОВИЩ 67

Машура Андрій Павлович, Олейніков Анатолій Миколайович ПОРІВНЯЛЬНИЙ АНАЛІЗ ЕФЕКТИВНОСТІ АКУСТИЧНИХ ТА УЛЬТРАЗВУКОВИХ МЕТОДІВ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ 70

Мордовцев М.В., Федюшин О.І., Морозов О.Ю. ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ПРИХОВУВАННЯ ІНФОРМАЦІЇ У PE-ФАЙЛАХ 75

Богданова Вероніка Валеріївна, Олешко Інна Вікторівна ПОРІВНЯЛЬНИЙ АНАЛІЗ ВРАЗЛИВОСТЕЙ ВЕБЗАСТОСУНКІВ НА ОСНОВІ ДОКУМЕНТІВ OWASP 82

Луценко Владислав Ігорович, Олешко Інна Вікторівна ПОРІВНЯЛЬНА ОЦІНКА ОПТИМІЗОВАНОГО ПІДХОДУ ГОМОМОРФНОГО ШИФРУВАННЯ ДЛЯ КОНФІДЕНЦІЙНОГО АНАЛІЗУ ТЕЛЕМЕТРІЇ МЕТОДАМИ МАШИННОГО НАВЧАННЯ . 87

Diana Ovcharenko, Volodymyr Zabolotnyi COMPARATIVE ANALYSIS OF INTERFEROMETRIC AND DOPPLER LASER-BASED ACOUSTIC RECONNAISSANCE SYSTEMS AND THE IMPACT OF CORNER REFLECTORS ON THEIR OPERATION 92

Рой Євген Олександрович, Доленко Олексій Дмитрович, Петренко Ольга Євгенівна ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ АЛГОРИТМУ NTRU ДЛЯ КРИПТОГРАФІЧНОГО ЗАХИСТУ МОБІЛЬНИХ МЕСЕНДЖЕРІВ 96

СЕКЦІЯ 2. ПОБУДОВА ТА УПРАВЛІННЯ SOC, СУЧАСНІ АРХІТЕКТУРИ МОНІТОРИНГУ 101

Фещенко Р. Д., Калякін С. В. МІНІМАЛЬНО ЖИТТЄЗДАТНА АРХІТЕКТУРА SOC ДЛЯ РОЗПОДІЛЕНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ЗАКЛАДУ ВИЩОЇ ОСВІТИ 101

Бабенко Сергій Федорович ЗАБЕЗПЕЧЕННЯ КОНСЕНСУСУ ТА СТІЙКОСТІ ДО КОМПРОМЕТАЦІЇ ВУЗЛІВ У РОЗПОДІЛЕНИХ СИСТЕМАХ УПРАВЛІННЯ ПОДІЯМИ КІБЕРБЕЗПЕКИ (SIEM) 104

Балацька Валерія Сергіївна, Яремко Іванна-Вікторія Романівна РИЗИК-ОРІЄНТОВАНИЙ ПІДХІД ДО ПРІОРИТИЗАЦІЇ КІБЕРІНЦИДЕНТІВ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ 108

Нехороших Дмитро Михайлович, Туз Михайло Олександрович РИЗИК-ОРІЄНТОВАНА МОДЕЛЬ ПОБУДОВИ ТА УПРАВЛІННЯ SOC НА ОСНОВІ ІНТЕГРОВАНОЇ АРХІТЕКТУРИ МОНІТОРИНГУ 113

Власюк І. Д. УРАХУВАННЯ ЗАПІЗНІЛИХ ПОДІЙ ПІД ЧАС ОНОВЛЕННЯ ВИСНОВКІВ СИСТЕМ МОНІТОРИНГУ КІБЕРІНЦИДЕНТІВ 120

УДК 004.056.53:378.4

Балацька Валерія Сергіївна,

доктор філософії, доцент,
старший викладач кафедри управління інформаційною безпекою
Львівського державного університету безпеки життєдіяльності

Яремко Іванна-Вікторія Романівна,

студентка IV курсу Львівського державного
університету безпеки життєдіяльності

РИЗИК-ОРІЄНТОВАНИЙ ПІДХІД ДО ПРІОРИТИЗАЦІЇ КІБЕРІНЦИДЕНТІВ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ

Анотація. Розглянуто проблему визначення черговості реагування на події кібербезпеки в закладах вищої освіти за обмежених ресурсів моніторингу. Запропоновано спрощену ризик-орієнтовану модель первинного сортування повідомлень, яка поєднує оцінку можливих наслідків для освітнього процесу та ступінь підтвердження загрози. Для подій із ознаками активної компрометації передбачено правило позачергової ескалації. На навчальних прикладах показано порядок класифікації повідомлень і вибору першочергових дій. Визначено мінімальний набір відомостей картки інциденту, придатний для подальшого аудиту рішень. Запропонований підхід узгоджено із сучасними настановами NIST щодо управління кіберризиками та реагування на інциденти; його ефективність потребує окремої перевірки на знеособлених або синтетичних наборах подій.

Ключові слова: кіберінцидент, управління кіберризиками, моніторинг, SOC, пріоритизація, освітня інформаційна система.

Заклади вищої освіти використовують різнорідні цифрові сервіси: навчальні платформи, системи обліку результатів навчання, електронну пошту, кадрові ресурси, бібліотечні каталоги, файлові сховища та мережеву інфраструктуру. Кожен із них може генерувати численні повідомлення про підозрілі входи, помилки авторизації, зміну прав, запуск невідомого програмного забезпечення або недоступність сервісу. За невеликої команди адміністраторів обробляти всі повідомлення в порядку надходження нераціонально: низькозначущий сигнал може випередити ознаку захоплення облікового запису з широкими повноваженнями. Проблема особливо важлива для організацій, у яких кібербезпека забезпечується поєднанням централізованого контролю та локального адміністрування

факультетських або навчальних сервісів. Потрібне прозоре правило, яке допоможе визначити черговість розгляду повідомлень, не підмінюючи рішення фахівця автоматичним числом. NIST Cybersecurity Framework 2.0 розглядає виявлення й реагування як складові ширшої системи управління ризиками [1], а ISO/IEC 27005:2022 рекомендує організаціям системно ідентифікувати, оцінювати та обробляти інформаційні ризики [2].

Метою роботи є запропонувати відтворювану процедуру первинної пріоритизації подій кібербезпеки для інформаційних систем закладу вищої освіти. Її застосування передбачено на етапі аналізу повідомлення черговим фахівцем або відповідальним адміністратором. Запропонована шкала є навчальною моделлю для подальшого калібрування на реальних процесах установи, а не нормативним методом оцінювання тяжкості кіберінцидентів.

На першому етапі формується перелік критичних сервісів і пов’язаних інформаційних активів. Для системи результатів навчання критичним наслідком може бути несанкціоноване редагування оцінок; для обліку здобувачів – розкриття персональних даних; для платформи дистанційного навчання – тривала відсутність доступу під час контрольних заходів; для системи керування обліковими записами – розширення повноважень порушника на інші ресурси. Наслідки слід оцінювати окремо за конфіденційністю, цілісністю та доступністю, після чого вибирати найбільший обґрунтований рівень впливу. Власник інформаційного активу та відповідальний за безпеку повинні узгоджувати такі критерії в межах системи управління інформаційною безпекою [3].

На другому етапі для кожного повідомлення визначається рівень потенційного впливу $I \in \{1, 2, 3\}$, де 1 означає локальні незначні наслідки, 2 – обмежене порушення роботи або доступу до даних, 3 – можливе істотне порушення критичного процесу чи компрометацію чутливих відомостей. Окремо визначається рівень підтвердження загрози $E \in \{1, 2, 3\}$: 1 – одинична неперевірена ознака; 2 – кілька взаємопов’язаних ознак; 3 –

технічно підтверджена підозріла дія, наприклад зміна прав без належного погодження. Вибір оцінок має спиратися на зафіксовані факти, а не на інтуїцію оператора. Поділ за впливом і ступенем обґрунтованості спирається на загальні підходи до оцінювання ризиків, викладені в NIST SP 800-30 [4], але запропоновані бали не є шкалою цього стандарту.

Для початкового сортування пропонується індикатор $S = I \times E$ з можливими значеннями від 1 до 9. Діапазони 1-3, 4-6 і 7-9 умовно відповідають низькому, середньому й високому пріоритету розгляду. S не є імовірністю інциденту й не характеризує фактичний фінансовий збиток. Його функція – задати послідовний порядок ручної перевірки однотипних звернень. Для випадків із ознаками активного поширення шкідливого коду, підтвердженої компрометації привілейованого облікового запису, витоку персональних даних або блокування критичного сервісу вводиться правило негайної ескалації, яке має перевагу над обчисленим балом.

Наприклад, для навчального набору подій розглянемо три повідомлення. Перше – успішний вхід до адміністративного облікового запису платформи навчання з незвичного пристрою із подальшою непогодженою зміною ролі: $I = 3, E = 3, S = 9$; повідомлення отримує високий пріоритет і передається на термінову перевірку. Друге – масове фішингове розсилання на студентські адреси без підтверджених переходів за посиланням: $I = 2, E = 2, S = 4$; спочатку необхідно перевірити доставку, наявність взаємодії користувачів і поширити попередження. Третє – низка відхилених спроб входу до некритичного публічного ресурсу без ознак подальшого доступу: $I = 2, E = 1, S = 2$; подію варто зафіксувати й відстежити в динаміці. Усі приклади є штучними й наведені лише для пояснення процедури.

Практичне значення підходу залежить від його включення в регламент реагування. Згідно з NIST SP 800-61 Rev. 3, реагування доцільно розглядати як безперервний елемент управління кіберризиками, пов’язаний

з підготовкою, виявленням, реагуванням і відновленням [5]. Тому картка повідомлення повинна фіксувати не лише оцінений пріоритет, а й власника ресурсу, дату і джерело сигналу, обґрунтування впливу, перевірені технічні ознаки, відповідального виконавця, рішення щодо ескалації, виконані дії та момент закриття. Така картка створює мінімальний доказовий ланцюг для внутрішнього контролю й аналізу повторюваних проблем. Під час формування ризик-орієнтованого підходу до пріоритизації кіберінцидентів доцільно враховувати узгодженість політик інформаційної безпеки з технічними механізмами захисту [6], а також вимоги до цілісності, простежуваності та перевірюваності журналів подій, що використовуються для аналізу інцидентів [7]. Показовим є розмежування події та інциденту. Аномалія входу або спрацювання мережевого правила не означає автоматично, що відбулося порушення безпеки. Первинна оцінка лише визначає терміновість перевірки; статус інциденту надається після встановлення відповідності внутрішнім критеріям організації. Для попередження хибних позитивних спрацювань корисно зіставляти журнали різних джерел: служби ідентифікації, поштового шлюзу, антивірусного захисту, мережевих компонентів і прикладної системи. При цьому некоректно збирати повний вміст навчальних або особистих повідомлень, якщо для аналізу достатньо технічних метаданих. Обсяг оброблюваної інформації слід визначати з урахуванням мети обробки й вимог законодавства про захист персональних даних [8].

Окремим питанням є безперервність освітнього процесу. Якщо цифровий сервіс тимчасово недоступний через технічний збій або переривання електропостачання, це не завжди кіберінцидент. Проте одночасні відмови засобів захисту, нетипові мережеві з’єднання та зміни облікових записів можуть бути підставою для перевірки кіберскладової. У правилах пріоритизації доцільно відокремлювати інформацію про причину від наслідків для навчання: навіть за невизначеної причини відповідальний

підрозділ має забезпечити оперативний перехід до резервного процесу, якщо цього потребує критичність послуги. Щоб перевірити практичну придатність моделі, наступним кроком доцільно сформувати знеособлений набір навчальних журналів, визначити експертну еталонну черговість подій та порівняти її з порядком за індикатором S. Оцінюванню підлягають частка правильно підвищених у пріоритеті критичних випадків, кількість зайвих ескалацій, узгодженість оцінок між двома аналітиками та середній час від надходження повідомлення до початку перевірки. Важливо окремо оцінювати ризик пропуску критичної події: зменшення числа спрацювань саме по собі не є ознакою кращої безпеки.

Отже, ризик-орієнтована пріоритизація може допомогти впорядкувати роботу відповідальних за кіберзахист осіб у закладі вищої освіти. Запропонована процедура поєднує контекст активу, підтвердженість сигналу, правило позачергової ескалації та документування управлінського рішення. Її результатом є не автоматичне встановлення факту інциденту, а обґрунтований порядок первинного реагування. Для впровадження потрібні адаптація шкал до критичності ресурсів закладу, навчання виконавців, затвердження регламенту та емпірична перевірка на безпечному тестовому наборі даних.

Список використаних джерел

1. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg : NIST, 2024. DOI: https://doi.org/10.6028/NIST.CSWP.29.
2. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection – Guidance on managing information security risks. Geneva : ISO, 2022.
3. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva : ISO, 2022.
4. Joint Task Force Transformation Initiative. Guide for Conducting Risk

Assessments. NIST Special Publication 800-30, Revision 1. Gaithersburg : NIST, 2012. DOI: https://doi.org/10.6028/NIST.SP.800-30r1.
5. Nelson A., Rekhi S., Souppaya M., Scarfone K. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. NIST Special Publication 800-61, Revision 3. Gaithersburg : NIST, 2025. DOI: https://doi.org/10.6028/NIST.SP.800-61r3
6. Балацька В. С., Івануса А. І., Пановик У. М. Метод інтеграції політик інформаційної безпеки, стандартів та протоколів у процес побудови комплексної системи захисту інформації в організації. Кібербезпека: освіта, наука, техніка. 2025. Т. 3, № 31. С. 283-297. DOI: https://doi.org/10.28925/2663-4023.2025.31.1021.
7. Балацька В. С. Блокчейн-орієнтований підхід до забезпечення простежуваності та перевірюваності виконання політик КСЗІ. Кібербезпека: освіта, наука, техніка. 2026. Т. 4, № 32. С. 674-685. DOI: https://doi.org/10.28925/2663-4023.2026.32.1136
8. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17.

УДК 004.056:004.89:623.746.4-519

Нехороших Дмитро Михайлович

асистент кафедри Безпеки інформаційних технологій
Харківський національний університет радіоелектроніки

Туз Михайло Олександрович

студент VI курсу Харківського
національного університету радіоелектроніки

РИЗИК-ОРІЄНТОВАНА МОДЕЛЬ ПОБУДОВИ ТА УПРАВЛІННЯ SOC НА ОСНОВІ ІНТЕГРОВАНОЇ АРХІТЕКТУРИ МОНІТОРИНГУ

Анотація: У роботі запропоновано ризик-орієнтовану модель побудови та управління операційним центром безпеки (Security Operations Center, SOC), яка поєднує бізнес-контекст, критичні активи, сценарії кіберризику, вимоги до виявлення, багатоджерельну телеметрію, централізовану аналітику SIEM та спеціалізовані засоби EDR/XDR/NDR. Обґрунтовано перехід від технологічно орієнтованої моделі SOC до моделі, у якій склад джерел моніторингу і сценарії виявлення визначаються ризиками. Запропоновано замкнений цикл SOC: від виявлення й розслідування до реагування, метрик, засвоєння уроків та переоцінювання ризиків.

Ключові слова: SOC, SIEM, EDR, XDR, NDR, телеметрія безпеки, кіберризик, моніторинг, виявлення, реагування на інциденти, кіберстійкість.