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.

СЕКЦІЯ 3. БЕЗПЕКА ХМАРНИХ ТЕХНОЛОГІЙ, ВІРТУАЛІЗАЦІЇ ТА ІОТ 125

Бабенко Віталіна Олексіївна НАСКРІЗНА МОДЕЛЬ БЕЗПЕКИ CLOUD-EDGE-IOT СИСТЕМ НА ОСНОВІ ПОВЕДІНКОВОГО МОНІТОРИНГУ ТЕЛЕМЕТРІЇ ЗАСОБАМИ EBPF..... 125

Яворський Дмитро Костянтинович, Крайнюк Олена Володимирівна КОНЦЕПТУАЛЬНА АРХІТЕКТУРА КІБЕРБЕЗПЕКИ РОЗПОДІЛЕНИХ ПЛАТФОРМ НАВЧАННЯ ОПЕРАТОРІВ БПЛА..... 129

Репринцева Руслана Романівна, Крайнюк Олена Володимирівна КІБЕРЗАХИЩЕНА СИСТЕМА АВТОНОМНОГО МОНІТОРИНГУ НЕБЕЗПЕЧНИХ ВИРОБНИЧИХ ЗОН ІЗ ВИКОРИСТАННЯМ БПЛА..... 136

Стрілець Дар'я Андріївна, Крайнюк Олена Володимирівна РОЗРОБКА АЛГОРИТМУ АВТОНОМНОГО ФУНКЦІОНУВАННЯ ІІОТ-ТЕРМІНАЛІВ ВИДАЧІ ЗАСОБІВ ІНДИВІДУАЛЬНОГО ЗАХИСТУ В УМОВАХ МЕРЕЖЕВИХ ОБМЕЖЕНЬ 141

Лисицький К. Є., Лисицька І. В. НЕЙРОМЕРЕЖЕВИЙ КРИПТОАНАЛІЗ ТА ЗАХИСТ ВІД АТАК ПО ПОБІЧНИХ КАНАЛАХ У КРИПТОСИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ 146

Лисицька І. В., Лисицький К. Є. ЕВОЛЮЦІЯ АРХІТЕКТУР БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ 148

СЕКЦІЯ 4. КІБЕРБЕЗПЕКА ТА ЦИФРОВІ ТЕХНОЛОГІЇ У СИСТЕМІ ЦИВІЛЬНОГО ЗАХИСТУ 152

Рисований Олександ Миколайович, Литовська Олена Олександрівна МЕХАНІЗМИ ХУКІНГУ В СИСТЕМІ КІБЕРБЕЗПЕКИ: КОНТРОЛЬ ТА ЗАХИСТ ПРОГРАМ БЕЗ БЕЗПОСЕРЕДНЬОЇ МОДИФІКАЦІЇ МАШИННОГО КОДУ 152

Рисований Олександр Миколайович, Литовська Олена Олександрівна ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ВЕКТОРИЗАЦІЇ НЕКРИПТОГРАФІЧНИХ ХЕШ-АЛГОРИТМІВ ІЗ ВИКОРИСТАННЯМ ІНСТРУКЦІЙ AVX-512 158

Усачов Дмитро Володимирович, Лялін Сергій Володимирович ІНФОРМАЦІЙНО-ТЕХНОЛОГІЧНЕ ЗАБЕЗПЕЧЕННЯ ЗАСТОСУВАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ПІД ЧАС ЛІКВІДАЦІЇ НАДЗВИЧАЙНИХ СИТУАЦІЙ..... 167

Трунцев Г.В., Борисова А.С., Ніжник В.В. ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ФІЗИЧНОГО ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ В УМОВАХ ПОВНОМАСШТАБНОЇ ВІЙНИ..... 173

СЕКЦІЯ 5. МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, УПРАВЛІННЯ КІБЕРРИЗИКАМИ ТА СОЦІАЛЬНА ІНЖЕНЕРІЯ 181

Балацька Валерія Сергіївна, Ящук Валентина Ігорівна, Юрків Анастасія Володимирівна УЗГОДЖЕНЕ ЗАСТОСУВАННЯ ПОЛІТИК ДОСТУПУ ДО ПЕРСОНАЛЬНИХ ДАНИХ У РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ 181

Бількевич Артем Віталійович, Піксасов Михайло Михайлович Менеджмент інформаційної безпеки, управління кіберризиками та соціальна інженерія..... 186

Колодяжна Т. В. КІБЕРСТІЙКІСТЬ ЯК СКЛАДОВА СОЦІАЛЬНО-ЕКОНОМІЧНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СУСПІЛЬСТВА 190

Муха А., Крайнюк Олена Володимирівна ВПЛИВ ЛЮДСЬКОГО ФАКТОРА НА БЕЗПЕКУ РОБОТОТЕХНІЧНИХ СИСТЕМ: РИЗИКИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ ТА РЕКОМЕНДАЦІЇ З ЦИФРОВОЇ ГІГІЄНИ ДЛЯ ІНЖЕНЕРНОГО ПЕРСОНАЛУ 197

СЕКЦІЯ 5. МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, УПРАВЛІННЯ КІБЕРРИЗИКАМИ ТА СОЦІАЛЬНА ІНЖЕНЕРІЯ

УДК 004.056.5:378.4

Балацька Валерія Сергіївна,

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

Ящук Валентина Ігорівна,

к.е.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності

Юрків Анастасія Володимирівна,

студентка IV курсу Львівського державного університету безпеки життєдіяльності

УЗГОДЖЕНЕ ЗАСТОСУВАННЯ ПОЛІТИК ДОСТУПУ ДО ПЕРСОНАЛЬНИХ ДАНИХ У РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ

Анотація. Розглянуто проблему несинхронного оновлення правил доступу до персональних даних у взаємопов'язаних інформаційних системах закладів вищої освіти. Запропоновано організаційно-технічну послідовність переходу до нової редакції політики, що передбачає попереднє розгортання правил, перевірку готовності критичних сервісів, узгоджений момент активації та контроль чинності локальної версії. Обґрунтовано можливість використання дозволеного блокчейну для фіксації погоджень і доказів переходу, не розміщуючи в реєстрі персональні дані. На умовному сценарії зміни посадових повноважень показано порядок ухвалення рішення про активацію. Виокремлено обмеження підходу для термінового відкликання доступу та визначено критерії подальшої перевірки працездатності.

Ключові слова: політика інформаційної безпеки, контроль доступу, персональні дані, версіонування політик, дозволений блокчейн, заклад вищої освіти.

Інформаційна інфраструктура сучасного закладу вищої освіти охоплює електронні кабінети здобувачів, систему управління навчанням, електронний документообіг, облік кадрових даних та інші сервіси. При цьому один користувач може мати різні повноваження в кількох системах. Коли змінюється його службова роль або припиняється тимчасове доручення, усі пов'язані рішення про доступ мають спиратися на актуальні правила. На практиці адміністрування сервісів часто здійснюють різні

підрозділи, тому нові правила можуть набувати чинності неодночасно. Контрольованість редакцій і документування рішень відповідають підходу до системи управління інформаційною безпекою, який покладено в основу ISO/IEC 27001:2022 [1].

Небезпека полягає не лише в помилковому формулюванні політики, а й у часовому проміжку між її затвердженням і фактичним застосуванням. Наприклад, відомості про завершення адміністративного доручення вже оновлено в кадровій системі, проте електронний документообіг досі дозволяє підписання документів за попередньою роллю. Такий стан створює ризик неправомірного доступу й ускладнює аудит. Закон України «Про захист персональних даних» установлює загальну правову основу обробки відповідних відомостей [2], а настанови NIST щодо атрибутного контролю доступу пропонують оцінювати не лише роль користувача, а й атрибути ресурсу, операції та середовища [3].

Метою дослідження є обґрунтування послідовності узгодженого застосування нової версії політики доступу в кількох інформаційних системах закладу освіти. На відміну від звичайного надсилання оновленої інструкції адміністраторам, запропонований підхід пов’язує управлінське рішення з перевірюваним технічним станом кожного сервісу. Дослідження має концептуально-прикладний характер: наведені нижче значення і сценарії є умовними та не становлять результатів виробничого експерименту.

До складу моделі включено власника політики, уповноважених погоджувачів, сховище контрольованих редакцій, координатор переходу, систему керування ідентичностями та локальні точки застосування правил доступу. Для кожної редакції v формується ідентифікатор і криптографічний відбиток $H(v)$, який дозволяє перевірити, що сервер отримав саме погоджений текст правил. Важливо відокремити стан «затверджено» від стану «активовано»: наявність документа у сховищі ще

не означає, що сервіс уже застосовує його до запитів.

Пропонується така послідовність переходу: спочатку власник політики формулює зміну, зазначає підставу, відповідальні підрозділи, перелік задіяних ресурсів та дату запланованого набуття чинності. Після погодження редакція поширюється в неактивному стані. Кожен сервіс перевіряє цілісність документа, відповідність локального механізму контролю доступу новим умовам та контрольні сценарії «дозволити/заборонити». Позитивний результат фіксується як підтвердження готовності, прив'язане до версії, відбитка, сервісу й часу перевірки. Для переходу до активації недостатньо простої більшості сервісів. Системи, від яких безпосередньо залежить коректність прав доступу, доцільно визначити як критичні та вимагати їх обов'язкової готовності. Для решти застосовується зважена частка готових компонентів. Якщо $r_i \in \{0; 1\}$ позначає готовність системи i, w_i – її вагу, C – множину критичних систем, а θ – установлену частку готовності, то рішення про активацію $A(v)$ можна визначити так:

$$A(v) = 1 \Leftrightarrow (\forall i \in C : r_i = 1) \wedge (\Sigma w_i r_i / \Sigma w_i \geq \theta).$$

Умови цієї формули розглядаються разом: досягнення порога не компенсує неготовності критичного компонента. Зазначена формалізація є спрощеною управлінською моделлю; конкретні ваги й поріг повинні встановлюватися після аналізу залежностей і ризиків, а не обиратися однаково для всіх закладів.

Розглянемо навчальний приклад із чотирма сервісами: керування ідентичностями (вага 0,40), система обліку здобувачів (0,30), платформа навчання (0,20) та електронний документообіг (0,10). Перші два сервіси визначено критичними. Якщо вони і платформа навчання готові до нової редакції, а документообіг ще ні, сумарна готовність становить 0,90. За умовного порога $\theta = 0{,}85$ рішення про планову активацію допускається, але неготовий сервіс після завершення дозволеного терміну чинності

попередньої редакції має припиняти видачу позитивних рішень за застарілими правилами. Цей приклад ілюструє логіку вибору, а не доводить безпечність конкретної конфігурації.

Після фіксації готовності визначається спільний момент переходу $t*$. До його настання сервіси обробляють запити за чинною редакцією; після $t*$ локальний механізм має перевіряти збіг активної версії та контрольного відбитка з авторитетним станом. Якщо перевірку виконати неможливо або строк дії локального підтвердження минув, доцільно застосовувати обмежувальну поведінку за принципом fail closed. Таке рішення зменшує ризик прихованого використання застарілих дозволів, однак може тимчасово знизити доступність окремих навчальних процесів.

Для фіксації станів погодження та підтверджень готовності може застосовуватися дозволений блокчейн. NIST розглядає блокчейн як один із засобів забезпечення перевірюваності й узгодження записів у системах контролю доступу [4]. У Hyperledger Fabric політики підтвердження транзакцій дають змогу визначити, які організації мають підтримати відповідну зміну [5]. Водночас розгортання правил, узгоджена активація та локальна перевірка версій можливі й без блокчейну: його потенційна перевага пов’язана насамперед із незалежно перевірюваною історією між адміністративними доменами, а не з автоматичним скороченням затримки. Раніше блокчейн застосовували для забезпечення достовірності персональних даних у державних реєстрах [6]; тут предметом контролю є життєвий цикл самої політики доступу.

У реєстрі керування достатньо зберігати номер редакції, відбиток політики, ідентифікатори уповноважених ролей, позначки готовності та час переходу. Персональні дані здобувачів і працівників, зміст документів та детальні журнали читання мають залишатися в захищених прикладних системах. Окремої уваги потребують метадані: навіть ідентифікатори ролей чи структурних підрозділів можуть розкривати внутрішню організацію

доступу. Плановий перехід не слід ототожнювати з терміновим відкликанням небезпечного права. Якщо встановлено факт компрометації привілейованого облікового запису або підтверджено незаконне використання даних, обмеження доступу потрібно ініціювати без очікування готовності всіх систем. У такому випадку окремий терміновий механізм блокування повинен мати власний регламент, перевірку повноважень та журналювання дій. Також до впровадження необхідно перевірити роботу за втрати мережевого зв'язку, відмови координатора, неповної доставки подій і повернення системи після простою.

Отже, для закладів вищої освіти доцільно розмежовувати процедури погодження, технічної підготовки та активації політик доступу. Запропонована модель поєднує перевірку критичних залежностей із простим індикатором готовності та створює основу для аудиту переходу між редакціями. Подальше дослідження має передбачати прототип з окремими тестовими сервісами, порівняння централізованого і блокчейн-координованого журналів, а також вимірювання часових інтервалів застарілого доступу і втрат доступності. Без такої перевірки кількісні переваги підходу стверджувати передчасно.

Список використаних джерел

1. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva : ISO, 2022.
2. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17.
3. Hu V. C., Ferraiolo D., Kuhn R. та ін. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. NIST Special Publication 800-162. Gaithersburg : NIST, 2014 (оновлено 2019). DOI: https://doi.org/10.6028/NIST.SP.800-162.
4. Hu V. C. Blockchain for Access Control Systems. NIST Interagency Report 8403. Gaithersburg : NIST, 2022. DOI: https://doi.org/10.6028/NIST.IR.8403.

5. Hyperledger Fabric. Endorsement Policies : документація. URL: https://hyperledger-fabric.readthedocs.io/en/release-2.5/endorsement-policies.html.

6. Balatska V., Poberezhnyk V., Opirskyy I. Method for Ensuring the Reliability and Security of Personal Data in Blockchain Systems of State Registers. CEUR Workshop Proceedings. 2025. Vol. 3991. P. 293-310. URL: https://ceur-ws.org/Vol-3991/paper21.pdf.

УДК 004.056:005.334

Бількевич Артем Віталійович,

студент І курсу Харківського національного автомобільно-дорожнього університету

Піксасов Михайло Михайлович,

к.т.н., доцент, кафедри кібербезпеки Харківського національного автомобільно-дорожнього університету

МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, УПРАВЛІННЯ КІБЕРРИЗИКАМИ ТА СОЦІАЛЬНА ІНЖЕНЕРІЯ

Анотація. У роботі розглядаються теоретико-практичні аспекти управління інформаційною безпекою суб'єктів господарювання. Досліджено вплив людського фактора на загальну стійкість корпоративних інформаційних систем. Проаналізовано методи соціальної інженерії як ключовий вектор атак на конфіденційні дані підприємств. Обґрунтовано необхідність комплексного підходу до управління кіберризиками, що поєднує технічні засоби захисту з організаційно-управлінськими заходами. Доведено важливість впровадження спеціалізованих програм навчання та тестування персоналу для формування культури кібергігієни. Запропоновано організаційні рішення для мінімізації ймовірності успішних соціотехнічних атак на інфраструктуру компаній.

Ключові слова: інформаційна безпека, управління кіберризиками, соціальна інженерія, людський фактор, соціотехнічні атаки.

Сучасне ділове середовище вимагає від суб'єктів господарювання постійного вдосконалення систем управління інформаційною безпекою задля забезпечення безперебійності операційних процесів та захисту конфіденційних даних від зовнішніх і внутрішніх загроз. Технологічний розвиток супроводжується пропорційним збільшенням кількості вразливостей, які експлуатуються кіберзлочинцями для отримання