Міністерство освіти і науки України
Український державний університет залізничного транспорту

МАТЕРІАЛИ

двадцять другої науково-практичної міжнародної конференції

«Міжнародна транспортна інфраструктура, індустріальні центри та корпоративна логістика»

(4-5 червня 2026 р. м. Харків, Україна)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІНІСТЕРСТВО РОЗВИТКУ ГРОМАД ТА ТЕРИТОРІЙ УКРАЇНИ
ТРАНСПОРТНА АКАДЕМІЯ УКРАЇНИ
АТ «УКРАЇНСЬКА ЗАЛІЗНИЦЯ»
CONSERVATOIRE NATIONAL DES ARTS ET MÉTIERS (FRANCE)
INSTITUTE OF AUTOMATIC CONTROL TELEMATICS OF TRANSPORT (POLAND)
УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ЗАЛІЗНИЧНОГО ТРАНСПОРТУ
ІНСТИТУТ ЕКОНОМІКИ ПРОМИСЛОВОСТІ НАН УКРАЇНИ

Матеріали

Двадцять другої науково-практичної

міжнародної конференції

«МІЖНАРОДНА ТРАНСПОРТНА ІНФРАСТРУКТУРА, ІНДУСТРІАЛЬНІ ЦЕНТРИ ТА КОРПОРАТИВНА ЛОГІСТИКА»

(4 – 5 червня 2026 р., м. Харків)

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова: ***Панченко С. В.***, д.т.н., проф., ректор Українського державного університету залізничного транспорту (Харків).

Заступники голови: ***Каграманян А. О.,*** к.т.н., доц., проректор з науково-педагогічної роботи Українського державного університету залізничного транспорту (Харків);
Дикань В. Л., д.е.н., проф., завідувач кафедри економіки та управління виробничим і комерційним бізнесом Українського державного університету залізничного транспорту (Харків).

Секретаріат:

Толстова А. В. к.е.н., доц., доцент кафедри економіки та управління виробничим і комерційним бізнесом Українського державного університету залізничного транспорту (Харків);

Шаповал Г. В. к.т.н., доц., заступник декана з денної форми навчання факультету управління процесами перевезень Українського державного університету залізничного транспорту (Харків);

Примаченко Г. О. к.т.н., доц., доцент кафедри транспортних систем та логістики Українського державного університету залізничного транспорту (Харків).

якості алгоритмів [2]. Тому розвиток АСУР потребує постійного вдосконалення аналітичних механізмів та гармонізації з міжнародними стандартами Всесвітньої митної організації. Отже, АСУР трансформує митний контроль від суб'єктивного до автоматизованого, забезпечуючи баланс між спрощенням торгівлі та безпекою держави.

[1] Накорнєєв В. О. Аналіз впливу АСУР на зменшення людського фактора в митних органах України у 2021–2023 рр. : дис. … канд. екон. наук. Тернопіль, 2024. 215 с.
[2] Микуляк О. В. Система управління ризиками у митній справі України : [монографія]. Львів : ЛНУ імені Івана Франка, 2024. 70 с.
[3] Осіпчук Д. С. Управління ризиками у митній справі в умовах воєнного стану. *Економіка та управління*. 2024. № 4 (102). С. 34–41.
[4] Про затвердження Порядку здійснення аналізу та оцінки ризиків, розроблення і реалізації заходів з управління ризиками в Державній митній службі України : наказ Міністерства фінансів України від 31 лип. 2020 р. № 468. URL: https://zakon.rada.gov.ua/laws/show/z0877-20 (дата звернення: 29.05.2026).
[5] Щодо застосування в автоматизованій системі управління ризиками Держмитслужби суб'єктоорієнтованих критеріїв. *Державна митна служба України*. URL: https://customs.gov.ua/documents/shchodo-zastosuvannia-v-avtomatizovanii-sistemi-upravlinnia-rizikami-derzhmitsluzhbi-subiektooriientovanikh-kriteriyiv-505 (дата звернення: 29.05.2026).
[6] Суб'єктоорієнтовані критерії в дії. *Державна митна служба України*. URL: https://customs.gov.ua/news/zagalne-20/post/subiektooriientovani-kriteriyi-v-diyi-584 (дата звернення: 29.05.2026).
[7] IT трансформація Митниці: Розпочато випробування оновленої системи управління ризиками — АСУР 2.0. *Державна митна служба України*. URL: https://customs.gov.ua/en/news/novini-20/post/it-transformatsiia-mitnitsi-rozpochato-viprobuvannia-onovlenoyi-sistemi-upravlinnia-rizikami-asur-2-0-439 (дата звернення: 29.05.2026).
[8] Держмитслужба інтегрувала ШІ та BI в АСУР для підвищення ефективності управління ризиками. *Державна митна служба України*. 2025. URL: https://customs.gov.ua/news/it-transformatsiia-62/post/derzhmitsluzhba-integruvala-shi-ta-bi-v-asaur-dlia-pidvishchennia-efektivnosti-upravlinnia-rizikami-2016 (дата звернення: 29.05.2026).

УДК 004.056:005.934

ПОПЕРЕДЖЕННЯ КІБЕРЗАГРОЗ В СУЧАСНИХ ОРГАНІЗАЦІЯХ ЯК ФУНКЦІЯ УПРАВЛІННЯ: АНАЛІЗ ТА КРИТИЧНІ СКЛАДОВІ

CYBER THREAT PREVENTION IN CONTEMPORARY ORGANIZATIONS AS A MANAGEMENT FUNCTION: ANALYSIS AND KEY CRITICAL ELEMENTS

К. С. Сердюков
Східноукраїнський національний університет ім. В. Даля (м. Київ)

K. Serdiukov
Volodymyr Dahl East Ukrainian National University (Kyiv)

Сьогодні в умовах розвитку інформаційного суспільства, що є надзвичайно динамічним і швидкісним, для діяльності організації, зокрема і в логістичній сфері, наряду з питаннями економічної безпеки все більше

актуальними стають питання інформаційного захисту функціонування її систем, належного його організації та контролю. Ефективність сучасних інформаційних систем, що є високопродуктивними, швидкодіючими та зручними в експлуатації, зводиться нанівець, якщо вони є не захищеними перед потенційними загрозами.

Разом з розвитком сучасних форм, методів та інструментів захисту інформації хакерська індустрія розвивається не менш стрімкими темпами, і будь-яка організація рано чи пізно стикається з питаннями інформаційного захисту. Економія коштів на інформаційній безпеці організації в процесі її діяльності в кінцевому випадку призводить до колосального збільшення витрат в умовах кіберінцидентів та ліквідації їх наслідків, що є економічно недоцільним і тягне за собою вже не тільки фінансові витрати на безпосередню ліквідацію наслідків, а ще й витрати людських та часових ресурсів разом з фінансовими витратами, збільшеними в геометричній прогресії. Логістичні компанії сьогодні володіють та обробляють величезні масиви даних, що визначають їх діяльність та забезпечують надання транспортних послуг та обслуговують всі сфери життєдіяльності.

Цифровізація без належної кібербезпеки веде до витоку даних, збільшення фінансових витрат, управлінського хаосу та паралічу діяльності організацій, особливо критичні наслідки цей факт має для публічної сфери.

В 2025 році Україна опинилась на другому місці в світі по кількості кібератак на її інформаційні ресурси [1]. Нажаль, вона стає майданчиком, де відпрацьовуються новітні методи та інструменти сучасних кібератак, до яких не готові звичайні компанії. Враховуючи те, що країна знаходиться в умовах воєнного стану, збільшення інфляційних процесів, збідніліть населення, погіршення фінансового стану юридичних осіб незалежно від їх організаційно-правових форм, що представляють різні сектори господарювання, тотальну нестачу кваліфікованих кадрів, ситуація із такою кількістю кіберінцидентів є дуже тривожною для країни та може призвести до непередбачуваних наслідків. Тому для держави цей факт повинен стати сигналом щодо необхідності втручання в процеси регулювання сфери інформаційного захисту та встановлення загальних правил, форм та стандартів в цій сфері та їх уніфікації та обов'язковості для всіх учасників, що користуються інформаційно-комунікативними системами.

Проте, не зважаючи на всі ризики, через незадовільний фінансовий стан та нерозуміння менеджменту важливості функціонування системи кіберзахисту, в переважній більшості організацій заходи інформаційного захисту фінансуються за принципом спрямування на них коштів, які залишились вільними (зазвичай це 2-5 % загального бюджету організації). Тільки в минулому році, завдяки закріпленим на державному рівні

вимогам, щодо встановлення двохфакторної ідентифікації для інформаційних систем, цей спосіб захисту став обов'язковим для юридичних осіб публічного сектору, фінансових установ та інших юридичних осіб, при здійсненні операцій у визначених сферах [2; 3; 4]. Для всіх інших встановлені стандарти носять рекомендаційних характер.

Проте аналізуючи наслідки вторгнень, можна зробити висновок, що успішність значної їх кількості зумовлюється завдяки недостатності навичок персоналу в сфері інформаційного захисту, зокрема розпізнаванні інструментів кібератак, наприклад, фішингових інструментів, та відсутності елементарних знань щодо кібербезпеки та запобігання кіберінцидентам.

Нестача кіберфахівців через низьку заробітну плату в переважній більшості організацій та брак кадрів через об'єктивні причини, пов'язані з воєнними діями, вимагає від менеджменту організацій вирішувати проблеми фінансового забезпечення заходів із кіберзахисту, навчання персоналу організації базовим знанням та нивичкам в цій сфері, а також залучення сторонніх компаній, що спеціалізуються в даній сфері, що, в свою чергу, вимагає додаткових фінансових вкладень, проте інвестування сфери інформаційного захисту організації з метою профілактики та попередження майбутніх кіберзагроз дозволяє компанії в подальшому уникнути небажаних кіберінцидентів та витоку інформації в результаті несанкціонованого доступу.

Таким чином, кіберзахист сьогодні стає не стільки основним напрямом діяльності IT-підрозділу, а основною задачею менеджменту підприємства, вирішення якої повинно закладатися на первісному етапі формування стратегії діяльності компанії, формування загального бачення її результатів та корпоративної культури, а не як антикризовий захід у разі виникнення надзвичайної ситуації та ліквідації наслідків зовнішніх втручань.

Lifelong learning в сфері інформаційного захисту як безперервне навчання команди повинно стати ключовим месенджем в формуванні soft skills працівників в будь-якій організації, оскільки профілактика загроз на основі дотримання правил кібергігієни є більш дієвим і дешевим інструментом, ніж подолання наслідків кібератак.

[1] Огляд ринку кібербезпеки в Україні. Асоціація IT Ukraine. 2025. URL: https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf

[2] Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05 жовтня 2017 року № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text

[3] Про затвердження Вимог до засобів криптографічного захисту інформації, призначених для захисту таємної інформації, яка не становить державної таємниці, та конфіденційної інформації в державних органах, органах місцевого самоврядування, на підприємствах, в установах та організаціях, які належать до сфери їх управління, військових формуваннях які створені відповідно до закону: наказ Держспецзв'язку від 07 травня 2021 року № 278. URL: https://zakon.rada.gov.ua/laws/show/z0696-21#Text

[4] Про платіжні послуги: Закон України від 30 червня 2021 року № 1591-IX. URL: https://zakon.rada.gov.ua/laws/show/1591-20#Text

Зміст

Секція «Розвиток індустріальних центрів в умовах глобалізації»

МАТЕРІАЛИ
ДВАДЦЯТЬ ДРУГОЇ НАУКОВО-ПРАКТИЧНОЇ
МІЖНАРОДНОЇ КОНФЕРЕНЦІЇ
«МІЖНАРОДНА ТРАНСПОРТНА ІНФРАСТРУКТУРА,
ІНДУСТРІАЛЬНІ ЦЕНТРИ ТА КОРПОРАТИВНА ЛОГІСТИКА»

(4 – 5 ЧЕРВНЯ 2026 РОКУ)

Відповідальний за випуск А. В. Толстова

Підписано до друку 12 червня 2026 р.
Формат паперу 60х84 1/16. папір писальний.
Умовн.-друк. арк. **36,2**. Обл.– вид. арк. **36,8.**
Замовлення № Тираж 300. Ціна договірна

Видавництво УкрДУЗТу, свідоцтво ДК № 6100 від 21.03.2018 р.