УДК 004.056.5 doi: 10.20998/2413-4295.2026.02.05

ОРГАНІЗАЦІЯ ФІЗИЧНОГО ЗАХИСТУ КОМП'ЮТЕРНИХ СИСТЕМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ СТАНДАРТІВ ТА РЕКОМЕНДАЦІЙ МАГАТЕ

С.С. ЛИС*, А.Я. ІСОПЕНКО, В.В. ЗАГАРОВСЬКИЙ

Інститут комп'ютерних технологій, автоматики та метрології, Національний університет «Львівська політехніка», Львів, УКРАЇНА
**e-mail: Lysss@ukr.net*

АНОТАЦІЯ *Розглянуто теоретичні та практичні аспекти фізичного захисту комп'ютерних систем як невід'ємного елементу комплексної інформаційної безпеки підприємств критичної інфраструктури. Проаналізовано сучасні підходи до організації фізичного захисту відповідно до міжнародних стандартів і рекомендацій МАГАТЕ, зокрема принципи багаторівневого захисту та зональної архітектури безпеки. Визначено основні категорії заходів безпеки (технічні, адміністративні та фізичні) та обґрунтовано їх взаємодоповнюючий характер. Особливу увагу приділено ідентифікації чутливих цифрових активів, класифікації загроз фізичній безпеці комп'ютерних систем, включаючи внутрішні загрози, атаки на ланцюг постачання та ризики відмови фізичних систем захисту. Розглянуто сучасні засоби контролю фізичного доступу, захисту обладнання на рівні пристроїв, а також механізми управління конфігураціями та безпеки знімних носіїв. Запропоновано модель зональної архітектури фізичного захисту комп'ютерних систем для об'єктів критичної інфраструктури. Наведено приклад її практичного впровадження на умовному підприємстві водопостачання, що демонструє ефективність застосування запропонованого підходу. Отримані результати підтверджують, що інтеграція фізичного захисту в загальну програму комп'ютерної безпеки суттєво підвищує рівень захищеності інформаційних систем.*
Ключові слова: *фізичний захист, комп'ютерні системи, інформаційна безпека, критична інфраструктура, зональна модель, багаторівневий захист, контроль доступу.*

ORGANIZATION OF PHYSICAL PROTECTION OF COMPUTER SYSTEMS OF CRITICAL INFRASTRUCTURE BASED ON IAEA STANDARDS AND RECOMMENDATIONS

S. LYS*, A. ISOPENKO, V. ZAHAROVSKYI

Institute of Computer Technologies, Automation and Metrology, Lviv Polytechnic National University, Lviv, Ukraine

ABSTRACT *The paper examines theoretical and practical aspects of physical protection of computer systems as an integral component of comprehensive information security for critical infrastructure enterprises. Modern approaches to organizing physical protection in accordance with international standards and IAEA recommendations are analyzed, in particular the principles of layered (defense-in-depth) protection and zonal security architecture. The main categories of security measures (technical, administrative, and physical) are identified, and their complementary nature is substantiated. Special attention is paid to the identification of sensitive digital assets, classification of threats to the physical security of computer systems, including insider threats, supply chain attacks, and risks associated with failures of physical protection systems. Modern means of physical access control, device-level equipment protection, as well as configuration management mechanisms and removable media security are considered. A model of zonal architecture for physical protection of computer systems for critical infrastructure facilities is proposed. An example of its practical implementation at a hypothetical water supply enterprise is provided, demonstrating the effectiveness of the proposed approach. The obtained results confirm that the integration of physical protection into the overall computer security program significantly enhances the level of protection of information systems.*
Keywords: *physical protection, computer systems, information security, critical infrastructure, zonal model, layered protection, access control.*

Вступ

Сучасні комп'ютерні системи є основою функціонування критичної інфраструктури від атомних електростанцій і підприємств оборонно-промислового комплексу до банківського сектору та органів державної влади. Динамічне зростання кількості кіберзагроз і постійне вдосконалення методів атак змусили фахівців з інформаційної безпеки переосмислити традиційні підходи до захисту. Сьогодні стало очевидним, що суто програмні або мережеві засоби захисту є недостатніми без відповідного фізичного рівня безпеки, тобто рівня, який нерідко залишається поза увагою при проєктуванні систем захисту.

Фізичний захист комп'ютерних систем охоплює сукупність заходів, спрямованих на запобігання несанкціонованому фізичному доступу до обладнання, його пошкодженню, знищенню або несанкціонованій модифікації. Такі заходи утворюють

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

перший і найбільш матеріальний рівень захисту в моделях інформаційної безпеки, оскільки будь-яка цифрова система фізично існує у вигляді апаратного забезпечення, що може бути знищене, вкрадене або модифіковане.

Міжнародне агентство з атомної енергії (МАГАТЕ) у своїй публікації «Методи комп'ютерної безпеки для ядерних об'єктів» [1], одному з найбільш деталізованих міжнародних стандартів у сфері захисту комп'ютеризованих систем, окремо виділяє фізичний контроль як самостійний та рівноправний рівень заходів безпеки. Хоча ця публікація розроблена для потреб ядерної галузі, закладені в ній методологічні підходи мають універсальний характер і можуть застосовуватися в будь-яких організаціях, що управляють критично важливими інформаційними системами.

Традиційно основна увага у сфері інформаційної безпеки приділяється програмним і мережевим засобам захисту. Проте практика останніх років демонструє, що ігнорування фізичного рівня безпеки призводить до виникнення критичних вразливостей. Отримавши фізичний доступ до обладнання, зловмисник може обійти більшість логічних механізмів захисту, що робить фізичний захист невід'ємною складовою комплексної системи безпеки.

Особливої актуальності ця проблема набуває в умовах зростання кількості комбінованих атак, які поєднують кібернетичні та фізичні вектори впливу, а також загроз, пов'язаних із внутрішніми порушниками та компрометацією ланцюгів постачання обладнання. У таких умовах виникає необхідність формування інтегрованого підходу до захисту комп'ютерних систем, що враховує взаємозалежність фізичних і логічних механізмів безпеки.

Аналіз літературних джерел та постановка проблеми дослідження

Методологічною основою цього дослідження слугує публікація Міжнародного агентства з атомної енергії "Методи комп'ютерної безпеки для ядерних об'єктів" (Серія МАГАТЕ з ядерної захищеності, Технічні настанови № 17-Т, 2021) [1], як один із найбільш систематизованих міжнародних документів у галузі захисту комп'ютеризованих систем критичної інфраструктури. Документ формалізує концепції чутливих цифрових активів, зонального підходу та трирівневої моделі заходів безпеки (технічні, адміністративні, фізичні). Суміжну проблематику організаційного впровадження програм комп'ютерної безпеки розглядає Керівництво з впровадження МАГАТЕ № 42-G "Комп'ютерна безпека для ядерної захищеності" [2], а захист ядерної інформації як складову фізичного захисту носіїв і каналів передачі даних – публікація NSS 23-G [3]. Разом ці три документи утворюють ієрархічну систему вимог МАГАТЕ, що охоплює стратегічний, операційний і технічний рівні захисту та є точкою відліку для порівняльного аналізу будь-яких галузевих підходів.

Серед фундаментальних праць у галузі інженерії безпеки ключове місце посідає монографія Р. Андерсона "Інженерія безпеки" [4], яка системно розкриває принципи проектування надійних розподілених систем, зокрема питання фізичного захисту та моделювання загроз. Андерсон обґрунтовує необхідність розгляду фізичного рівня як інтегральної складової загальної архітектури безпеки, а не як ізольованого технічного завдання.

Нормативну базу досліджень формують два провідних стандарти. Міжнародний стандарт ISO/IEC 27001:2022 [5] встановлює вимоги до систем управління інформаційною безпекою, включаючи заходи фізичного та екологічного захисту, і задає системний підхід до управління ризиками на основі ідентифікації активів, оцінки загроз і вибору пропорційних засобів контролю. Американський стандарт NIST SP 800-53 Rev. 5 [6] деталізує конкретні заходи фізичного захисту для федеральних інформаційних систем і широко застосовується операторами критичної інфраструктури як практичний орієнтир незалежно від галузевої приналежності.

Значний внесок у розуміння практичних наслідків ігнорування фізичного рівня захисту зробили дослідження резонансних кіберінцидентів. Аналіз кібератаки на українську електромережу 2015 року [7] документально підтвердив, що комбіновані атаки, які поєднують цифрові та фізичні вектори, є найбільш руйнівними за своїми наслідками. Р. Лангнер у своєму аналізі Stuxnet [8] показав, що цей шкідливий код поширювався виключно через фізичні носії (USB-накопичувачі), долаючи мережі з "повітряним проміжком", тобто прецедент, що документально підтвердив критичну роль фізичного контролю над пристроями введення/виведення.

Практичні аспекти управління паролями та автентифікацією як складової фізичного доступу висвітлено у настанові K. Scarfone та M. Souppaya (NIST SP 800-118) [9]. Вітчизняна наукова школа представлена навчальним посібником Г. М. Гулака та П. М. Складанного "Основи інформаційної безпеки" [10], який систематизує теоретичні засади захисту інформації стосовно українських реалій правового регулювання.

IAEA-NSS-46-T [11] окреслює значення оцінювання ефективності систем фізичного захисту (PPS) і має практичну спрямованість як технічне керівництво. Водночас вона носить переважно описовий характер і не містить елементів наукової новизни чи методологічної деталізації. Відсутність конкретних підходів, метрик або результатів знижує її аналітичну цінність у науковому контексті.

Праця [12] висвітлює актуальну проблему кіберзахисту ядерних об’єктів і пропонує структурований підхід до оцінювання реагування на інциденти, що є її сильною стороною. Водночас методологія та результати описані узагальнено, без конкретних метрик ефективності чи порівняння з існуючими підходами. Стаття [13] демонструє чітко окреслену технічну новизну – ризик-орієнтовану модель із використанням транспортного графа для оцінки безпеки перевезення радіоактивних матеріалів.

Робота [14] охоплює актуальну проблему інтегрованого управління безпекою (IMSS) у ядерній галузі та спирається на різноманітні джерела, що підсилює її практичну значущість. Водночас методологія подана узагальнено, без чіткої конкретизації обсягу даних і критеріїв аналізу, а результати частково мають описовий характер без достатньої аналітичної глибини. В статті [15] висвітлено актуальну проблему підготовки з кібербезпеки, методологія систематичного огляду описана занадто загально, а результати мають декларативний характер без кількісного підтвердження чи конкретних KPI.

Разом із тим аналіз наявних джерел виявляє певну фрагментованість, тобто питання фізичного захисту комп’ютерних систем нерідко розглядаються відокремлено від логічних засобів, без належного акценту на їхній взаємозалежності.

Мета роботи

Метою роботи є аналіз концептуальних засад фізичного захисту комп’ютерних систем, дослідження сучасних методів і засобів забезпечення фізичної безпеки, а також розробка практичної моделі зональної архітектури захисту для об’єктів критичної інфраструктури.

Концептуальні основи фізичного захисту комп'ютерних систем

Трирівнева модель заходів безпеки. Сучасна теорія інформаційної безпеки розглядає захист комп'ютерних систем як багатовимірне завдання, що вимагає одночасного застосування заходів трьох категорій (рис. 1). Згідно з підходом МАГАТЕ [1], до цих категорій належать технічні, адміністративні та фізичні заходи контролю. Кожна категорія виконує власну функцію і компенсує природні обмеження інших.

Технічні заходи включають апаратне та програмне забезпечення, що використовується для запобігання, виявлення та пом'якшення наслідків несанкціонованих дій: міжмережеві екрани, системи виявлення вторгнень, засоби шифрування, механізми автентифікації [4]. Адміністративні заходи охоплюють організаційні процедури, нормативні документи, програми навчання персоналу та перевірку благонадійності співробітників.

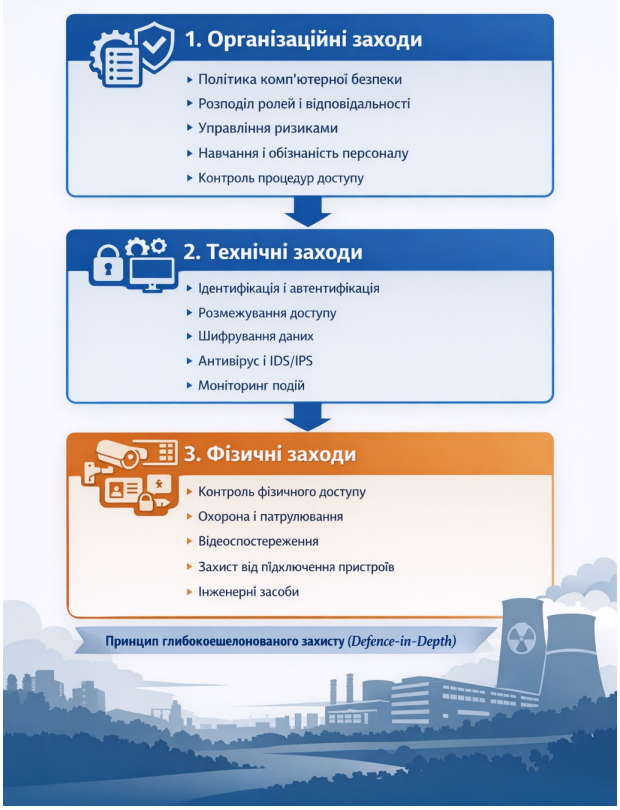

Рис. 1 – Трирівнева модель заходів комп'ютерної безпеки за класифікацією МАГАТЕ.

Фізичні заходи контролю утворюють базовий рівень, без якого ефективність двох інших категорій є суттєво обмеженою. Публікація МАГАТЕ дає таке визначення: «Заходи фізичного контролю – це фізичні бар'єри, що захищають прилади, комп'ютеризовані системи та допоміжні активи від фізичного пошкодження та запобігають несанкціонованому фізичному доступу» [1]. Це визначення підкреслює подвійну функцію фізичного захисту: превентивну – недопущення несанкціонованого доступу, та захисну – запобігання фізичному пошкодженню обладнання .

Заходи трьох категорій (рис. 1) не є взаємозамінними, а лише взаємодоповнюючими. Наприклад, навіть найдосконаліший міжмережевий екран не захистить систему від зловмисника, який отримав фізичний доступ до сервера і підключив до нього знімний носій із шкідливим програмним забезпеченням.

Чутливі цифрові активив. Ключовим об'єктом фізичного захисту є чутливі цифрові активи (ЧЦА) - будь-яке обладнання або компоненти, що використовуються для зберігання, обробки, контролю або передачі чутливої інформації: системи управління, мережі, інформаційні системи [1]. До ЧЦА відносяться комп'ютерні робочі станції, сервери баз даних, мережеве комутаційне обладнання,

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

програмовані логічні контролери (ПЛК), портативні пристрої та знімні носії інформації.

Чутлива інформація в контексті ЧЦА охоплює не лише дані як такі, а й програмне забезпечення виконання, вбудоване мікропрограмне забезпечення (firmware), інструменти розроблення, засоби технічного обслуговування та операційні системи [1]. Таке розширене розуміння є принципово важливим для побудови системи фізичного захисту, оскільки фізичний доступ до апаратного забезпечення потенційно надає зловмиснику можливість модифікації будь-якого з цих компонентів без залишення очевидних цифрових слідів.

Ідентифікація та інвентаризація всіх ЧЦА є першим практичним кроком у побудові системи фізичного захисту. Без чіткого розуміння того, яке саме обладнання потребує захисту, де воно розташоване і яку роль відіграє в загальній інфраструктурі, неможливо ефективно спланувати та впровадити заходи безпеки [1, 5, 6].

Зони комп'ютерної безпеки. Зональна модель є основоположним архітектурним рішенням для структурованого захисту комп'ютерних систем. Згідно з МАГАТЕ, «зона комп'ютерної безпеки – це група систем, що мають спільні фізичні та/або логічні межі і яким призначено однаковий рівень безпеки» [1]. Рівень комп'ютерної безпеки зони визначається найвищим ступенем захисту, необхідним будь-якій функції, що виконується системами в межах цієї зони.

Фізична зона і логічна зона безпеки можуть збігатися або відрізнятися. У зоні найвищого рівня (зона 1А) як фізичні, так і логічні межі визначаються строго, тобто потрібні і фізичні бар'єри, і логічне розмежування. На нижчих рівнях фізичні вимоги можуть бути менш жорсткими, однак повністю не знімаються [1]. Зональна модель дозволяє застосовувати диференційований підхід до захисту: найбільш критичні активи зосереджуються у найбільш захищених зонах з мінімальним числом уповноважених осіб.

Зональна модель та принцип багаторівневого захисту

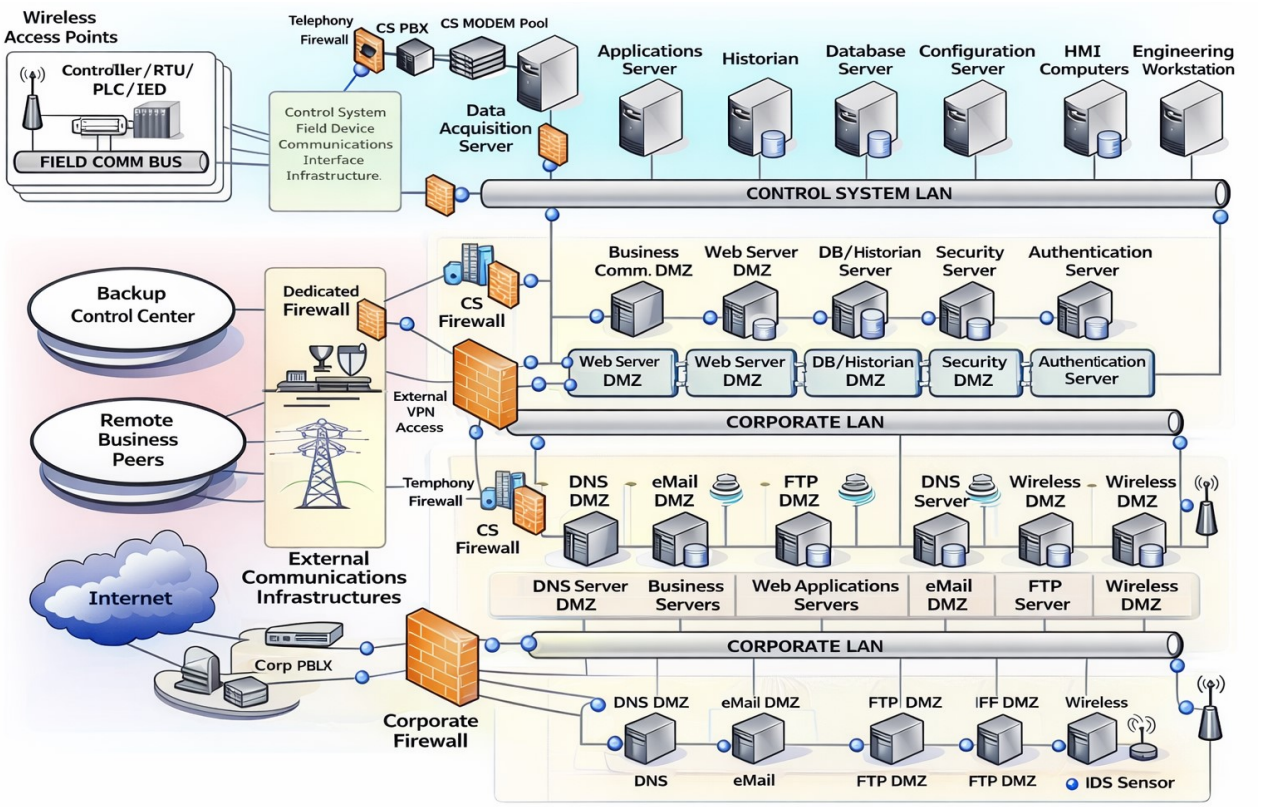

Рис. 2 – Архітектура концентричних зон безпеки за принципом багаторівневого захисту.

Межі зон (рис. 2) зазвичай обладнуються засобами фізичного контролю доступу - замкненими шафами, бар'єрами, блокаторами портів - та механізмами роз'єднання потоків даних - фільтрами пакетів, міжмережевими екранами, діодами даних [1]. Поєднання фізичних та логічних бар'єрів унеможливлює несанкціонований доступ навіть у разі часткового подолання одного з рівнів захисту.

Принцип багаторівневого захисту. Концепція багаторівневого захисту (від англ. defence in depth) передбачає, що жоден окремий засіб захисту не є абсолютно надійним, тому необхідно застосовувати кілька незалежних і гетерогенних шарів безпеки [4]. Відповідно до МАГАТЕ, будь-який зловмисник має подолати або обійти кілька шарів заходів комп'ютерної безпеки, перш ніж отримає можливість скомпрометувати критичну систему [1].

У контексті фізичного захисту це означає послідовне застосування: зовнішнього периметрового огородження; систем контролю доступу до будівлі; відеоспостереження та охорони; контролю доступу до серверних приміщень та апаратних залів; захищених серверних стійок із замками; блокаторів портів на окремих пристроях. Кожний шар компенсує можливі слабкості попереднього. Якщо зловмисник подолав зовнішній периметр, внутрішні бар'єри все одно перешкоджають йому дістатися до критичного обладнання.

Важливою вимогою до ефективного багаторівневого захисту є гетерогенність шарів - використання різних технологій і підходів знижує ймовірність того, що один вектор атаки дозволить подолати всі рівні одночасно [1, 10]. Наприклад, поєднання електронних замків, механічних бар'єрів та відеоспостереження робить обхід системи значно складнішим, ніж використання лише одного типу засобів.

Засоби та методи фізичного захисту

Контроль фізичного доступу до приміщень. Контроль фізичного доступу до приміщень, де розташоване комп'ютерне обладнання, є першочерговим завданням фізичного захисту. МАГАТЕ виділяє такі основні засоби: приміщення із контрольованим доступом, захищені двері з електронними або механічними замками, системи ідентифікації на основі ключ-карток або біометричних даних, датчики руху, системи відеоспостереження, а також індикатори несанкціонованого втручання [1, 6]. При використанні PIN-кодів та парольної автентифікації як складової систем контролю фізичного доступу (рис. 3) слід дотримуватися вимог щодо складності та регулярної зміни облікових даних, визначених у відповідних настановах [9].

Застосування цих засобів є диференційованим залежно від рівня безпеки зони. Серверні приміщення та апаратні зали, в яких розміщене найбільш критичне обладнання, потребують найвищого рівня контролю: доступ до них повинен надаватися лише мінімально необхідному числу осіб, кожен факт входу та виходу фіксується, а всі дії в приміщенні документуються [5, 6]. Це суттєво обмежує можливості як зовнішніх зловмисників, так і внутрішніх порушників.

Рис. 3 – Електронний замок із PIN-клавіатурою як засіб двофакторного контролю фізичного доступу до захищеного приміщення.

Окрему увагу слід приділяти так званим «сірим зонам» – місцям, де кабелі та обладнання виходять за межі захищених приміщень, наприклад: кабельні траси, технічні шахти, підвальні приміщення. МАГАТЕ вказує на необхідність захисту польових пристроїв, розташованих поза периметром фізичного захисту [1, 6], оскільки вони нерідко стають точкою проникнення в інфраструктуру.

Захист обладнання на рівні пристроїв. Поряд із захистом приміщень необхідно застосовувати засоби захисту на рівні окремих пристроїв. До таких засобів належать: замкнені серверні стійки та шафи, що запобігають фізичному доступу до серверів навіть у разі проникнення в серверне приміщення; блокатори USB-портів та інших інтерфейсів введення/виведення, що унеможливлюють підключення несанкціонованих зовнішніх пристроїв; замки Кенсінгтона та аналогічні кріпильні рішення для стаціонарного обладнання [1, 6].

Особливу роль відіграють індикатори втручання (tamper indicators) - пломби, спеціальні наклейки або механічні елементи, що фіксують сам факт несанкціонованого відкриття корпусу пристрою. МАГАТЕ наголошує, що обладнання повинно бути перевірено на відсутність слідів втручання при прийманні і надалі [1] (рис. 4).

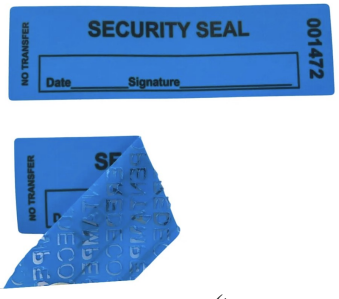

Рис. 4 – Індикатор втручання (tamper seal) на корпусі обладнання (засіб виявлення несанкціонованого фізичного доступу).

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

Такі індикатори є простим, але ефективним засобом раннього виявлення спроб фізичної атаки на апаратне забезпечення.

Управління конфігураціями як елемент фізичного захисту. Управління конфігураціями є важливим адміністративно-технічним інструментом, безпосередньо пов'язаним із фізичним захистом. Згідно з МАГАТЕ, воно передбачає ведення детальних актуальних записів про всі встановлені апаратні та програмні компоненти, їх розташування, з'єднання та параметри налаштування [1, 5]. Регулярна верифікація відповідності реального стану обладнання задокументованій конфігурації дозволяє своєчасно виявити будь-які несанкціоновані зміни.

Перед виконанням будь-яких процедур, що можуть обійти або знизити ефективність чинних заходів безпеки - наприклад, технічного обслуговування, яке вимагає тимчасового вимкнення засобів захисту, - необхідно проводити і документувати відповідні перевірки [1, 5]. У таких ситуаціях мають застосовуватися компенсуючі заходи, що забезпечують еквівалентний рівень захисту на час відключення основних засобів безпеки.

Фізична безпека знімних носіїв та мобільних пристроїв. Знімні носії інформації (USB-накопичувачі, компакт-диски, зовнішні жорсткі диски) та мобільні пристрої становлять особливий вектор фізичних загроз. МАГАТЕ наголошує, що персонал повинен забезпечити використання в межах об'єкту виключно дозволених знімних носіїв та мобільних пристроїв [1]. Для цього необхідний жорсткий реєстраційний контроль: будь-який носій, що вноситься в захищену зону або виноситься з неї, повинен бути задокументований.

Особливу небезпеку становить те, що навіть повністю ізольовані від мережі системи («повітряний проміжок», air gap) залишаються вразливими через переривчасте використання знімних носіїв для оновлень або передачі даних [1]. Саме через цей вектор було реалізовано кібератаку Stuxnet, що вразила промислові центрифуги для збагачення урану - і це є показовим прикладом того, як ігнорування фізичного контролю над носіями може мати катастрофічні наслідки [7, 8].

Загрози фізичній безпеці комп'ютерних систем

Внутрішні загрози. Внутрішні загрози є одними з найнебезпечніших у контексті фізичного захисту, оскільки внутрішній порушник - на відміну від зовнішнього зловмисника - вже має законний фізичний доступ до об'єкту і обладнання. МАГАТЕ класифікує внутрішніх порушників за рівнем авторизації та ступенем зловмисності намірів [1, 3]. До цієї категорії належать як навмисні порушники, що діють в інтересах третіх сторін або з особистих мотивів, так і ненавмисні - співробітники, що припускаються помилок через недбалість або незнання вимог безпеки. Порівняльний рівень усіх ідентифікованих загроз наведено на рис. 5.

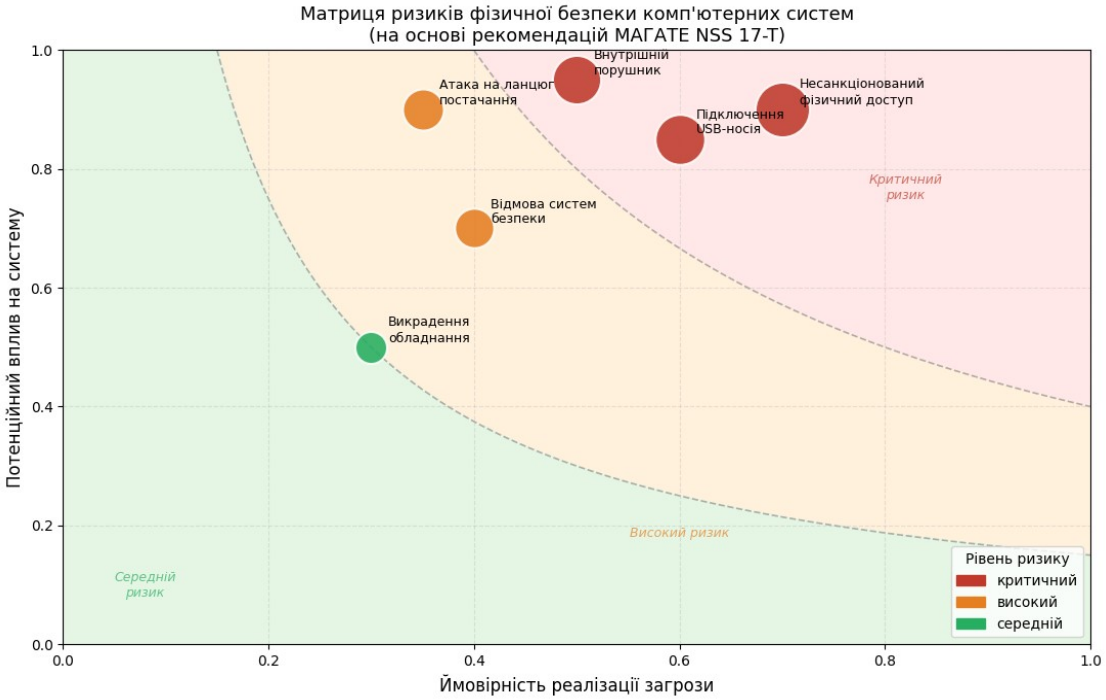

Рис. 5 – Матриця ризиків фізичної безпеки комп'ютерних систем.

Для протидії внутрішнім загрозам застосовується комплекс взаємодоповнюючих заходів. Принцип мінімальних привілеїв передбачає обмеження фізичного доступу персоналу лише тими зонами та пристроями, які безпосередньо необхідні для виконання їхніх службових функцій. Принцип двох осіб (two-person rule) вимагає присутності двох незалежних уповноважених осіб для виконання

певних критичних операцій з обладнанням, що унеможливлює одноосібні несанкціоновані дії. Розподіл службових обов'язків між різними особами та підрозділами не дає одній людині отримати повний контроль над критичними активами.

МАГАТЕ також указує, що процедури, які містять інструкції щодо вимкнення або обходу заходів безпеки, повинні гарантувати фіксацію таких дій у журналах [1]. Обов'язкове протоколювання всіх привілейованих дій з обладнанням є водночас стримуючим фактором для потенційних порушників і засобом ретроспективного розслідування інцидентів.

Модель зональної архітектури фізичного захисту

Для практичної ілюстрації концептуальних засад, викладених у попередніх розділах, розроблено модель зональної архітектури фізичного захисту комп'ютерних систем організації, що управляє критично важливою інформаційною інфраструктурою (таб. 1). Модель базується на градуйованому підході МАГАТЕ [1] і відображає триярусну ієрархію зон безпеки із відповідними засобами фізичного та логічного контролю на кожному рівні.

Таблиця 1 – Модель зональної архітектури фізичного захисту комп'ютерних систем

Зона / Рівень	Об'єкти захисту (ЧЦА)	Засоби фізичного контролю	Засоби логічного контролю на межі
ЗОНА А (Найвищий рівень)	Сервери БД, системи резервного копіювання, мережеве ядро, ПЛК, криптографічні модулі	Біометрика + смарт-картка + PIN; замкнені стійки; блокатори портів; CCTV 24/7; правило двох осіб; індикатори втручання	Діод даних; міжмережевий екран класу L4; суворе білісписання; ізоляція мережного сегмента
ЗОНА Б (Середній рівень)	Робочі станції персоналу, адміністративні термінали, мережеве комутаційне обладнання, знімні носії	Смарт-картка + PIN; електронні замки; CCTV; блокатори USB; реєстр відвідувань; принцип мінімальних привілеїв	Фільтр пакетів; VLAN-ізоляція; IDS/IPS; контроль цілісності конфігурацій
ЗОНА В (Базовий рівень)	Загальнодоступні термінали, мережева інфраструктура загального використання, польові пристрої на периметрі	Механічні замки; CCTV; індикатори втручання на обладнанні; контроль доступу до приміщень	Зовнішній периметровий ME; DMZ; базова автентифікація; загальний моніторинг мережі
Зовнішній периметр: огородження об'єкту, охорона, системи виявлення вторгнення на периметрі			

Запропонована модель реалізує принцип концентричних зон захисту, де кожна внутрішня зона є більш захищеною, ніж зовнішня. Межі між зонами є точками застосування засобів одночасно фізичного та логічного контролю, що унеможливлює несанкціонований доступ навіть у разі часткового подолання одного рівня. Важливою особливістю моделі є її масштабованість. Вона може бути адаптована до будь-якого типу організації, від невеликого підприємства (де зони А та Б можуть бути суміщені в одному приміщенні) до розгалуженої критичної інфраструктури з множинними майданчиками. Розподіл обов'язків та принцип мінімальних привілеїв застосовуються як на рівні фізичного доступу до кожної зони, так і на рівні логічних прав у відповідних мережних сегментах, що відповідає рекомендаціям МАГАТЕ щодо інтеграції фізичного та логічного захисту в єдину програму комп'ютерної безпеки [1].

Таблиця 2 – Матриця відповідності загроз фізичної безпеки та контрзаходів

Загроза	Рівень ризику	Превентивні контрзаходи	Детективні / реактивні заходи
Несанкціонований фізичний доступ до приміщення	Критичний	Багатофакторна автентифікація; зонування доступу; правило двох осіб; замки з fail-secure	CCTV; журнали доступу; сигналізація; негайне сповіщення адміністратора безпеки
Підключення несанкціонованого знімного носія (USB)	Критичний	Фізичні блокатори портів; реєстр дозволених носіїв; заборона особистих пристроїв у зонах А, Б	Endpoint DLP; аудит підключень; сканування носіїв перед використанням
Внутрішній порушник (навмисний)	Критичний	Принцип мінімальних привілеїв; розподіл обов'язків; перевірка благонадійності персоналу	Аудит дій персоналу; протоколювання привілейованих операцій; UEBA-системи
Атака на ланцюг постачання (апаратні закладки)	Високий	Вимоги безпеки у специфікаціях закупівель; перевірені постачальники; контроль цілісності при прийманні	Перевірка індикаторів втручання; верифікація прошивки; апаратний аудит після встановлення
Відмова фізичних систем безпеки внаслідок кібератаки	Високий	Резервне живлення (ДБЖ); механічне резервування замків; ізоляція мереж управління СКУД	Моніторинг стану систем СКУД; автоматичне сповіщення при відмові; регулярне тестування
Фізичне знищення або викрадення обладнання	Середній	Замки Кенсінгтона; стійки з замками; шифрування дисків; геолокаційний моніторинг активів	CCTV із записом; інвентаризаційний облік; процедура дистанційного знищення даних

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

Наведена матриця відображає комплексний підхід до управління фізичними ризиками, де для кожної загрози передбачено як превентивні (що знижують імовірність реалізації загрози), так і детективні та реактивні заходи (що забезпечують виявлення та реагування у разі її реалізації) таблиця 2. Такий підхід узгоджується з принципом багаторівневого захисту, оскільки відмова превентивного шару не означає повного успіху атаки, детективний шар забезпечує своєчасне виявлення та мінімізацію наслідків [1].

Таблиця 3 демонструє, що розглянуті заходи фізичного захисту мають чітку нормативну основу в усіх трьох провідних стандартах, що підтверджує їхню обґрунтованість і міжнародне визнання.

Таблиця 3 – Відповідність заходів фізичного захисту вимогам стандартів МАГАТЕ, ISO/IEC 27001 та NIST SP 800-53

Захід фізичного захисту	МАГАТЕ NSS 17-T [1]	ISO/IEC 27001:2022 [5]	NIST SP 800-53 Rev.5 [6]
Контроль фізичного доступу до приміщень	Розділ 5 (Фізичні заходи контролю), Зони КБ	Annex A 7.2 — Фізичний вхід; A 7.3 — Захист офісів	PE-2 Авторизація фіз. доступу; PE-3 Контроль доступу
Зональна модель (defence in depth)	Розділ 4 (Зони КБ); Градуйований підхід	A 5.29 — ІБ при перебоях; A 8.22 — Сегрегація мереж	SC-7 Захист меж; PE-19 Витік інформації
Захист знімних носіїв та блокування портів	Розділ 5.7 (Знімні носії та мобільні пристрої)	A 7.10 — Носії інформації; A 8.11 — Маскування даних	MP-7 Використання носіїв; SC-41 Відключення портів
Управління конфігураціями та індикатори втручання	Розділ 5.8 (Управління конфігураціями)	A 8.9 — Управління конфігурацією; A 7.4 — Моніторинг фіз. безпеки	CM-2 Базова конфігурація; PE-6 Моніторинг фіз. доступу
Принцип мінімальних привілеїв та розподіл обов'язків	Розділ 6.3 (Внутрішні загрози); Правило двох осіб	A 5.3 — Розподіл обов'язків; A 5.15 — Контроль доступу	AC-5 Розподіл обов'язків; AC-6 Найменші привілеї
Відеоспостереження та моніторинг	Розділ 5.2 (Виявлення та реагування); Моніторинг ефективності	A 7.4 — Моніторинг фізичної безпеки	PE-6 Моніторинг фіз. доступу; IR-5 Відстеження інцидентів

Наявність відповідних вимог одночасно у рекомендаціях МАГАТЕ [1], ISO/IEC 27001:2022 [5] та NIST SP 800-53 [6] свідчить про консенсус міжнародної спільноти фахівців з безпеки щодо необхідності та пріоритетності цих заходів. Для організацій, що прагнуть досягти відповідності кільком стандартам одночасно, реалізація заходів, представлених у таблиці, забезпечить виконання вимог усіх трьох нормативних документів у частині фізичного захисту.

Практичний сценарій впровадження зональної моделі на регіональному підприємстві водопостачання

Для ілюстрації практичного застосування розглянутих концепцій розглянемо умовний сценарій на основі типового регіонального підприємства водопостачання, що управляє автоматизованими системами диспетчерського управління (SCADA) та відповідає за постачання питної води населенню чисельністю близько 300 тисяч осіб. Вибір саме такого об'єкта зумовлений тим, що підприємства водопостачання є типовими операторами критичної інфраструктури, які поєднують промислові системи управління (ПЛК, SCADA) із загальноофісними інформаційними системами, а отже, демонструють типову для таких об'єктів неоднорідність вимог до фізичного захисту [1, 5].

Стан до впровадження заходів. До проведення аудиту безпеки підприємство мало такий стан фізичного захисту: серверна кімната, в якій розміщено SCADA-сервер та бази даних технологічних параметрів, закривалася на один механічний замок без журналювання доступу; всі USB-порти на робочих станціях диспетчерів були відкриті; персонал мав звичку підключати особисті флеш-накопичувачі для перенесення документів; ПЛК на насосних станціях, розташованих за периметром будівлі, фізично не були захищені від стороннього доступу; відеоспостереження було відсутнє в серверному приміщенні і вкрай обмеженим на виробничому майданчику. Водночас підприємство мало непогано налаштований мережевий периметр (міжмережевий екран, антивірус), що створювало хибне відчуття захищеності [4, 10].

Інвентаризація чутливих цифрових активів. Першим кроком стала повна інвентаризація всіх ЧЦА відповідно до методології МАГАТЕ [1]. Було ідентифіковано: SCADA-сервер та інженерну робочу станцію в серверній кімнаті головного офісу; три ПЛК Siemens S7-300 на насосних станціях № 1, 2, 3 за периметром будівлі; чотири диспетчерські робочі станції в операційному залі; мережеве комутаційне обладнання (два керованих комутатори та маршрутизатор); архівний сервер з базою даних технологічних параметрів за останні 5 років. Для кожного активу було визначено його місцезнаходження, рівень критичності та перелік осіб, що мають доступ до нього.

Визначення зон безпеки та їх меж. На основі інвентаризації було визначено три зони відповідно до градуйованого підходу МАГАТЕ [1]: Зона А (найвищий рівень) – серверна кімната з SCADA-сервером та архівним сервером, доступ лише для системного адміністратора та начальника відділу АСУ (2 особи); Зона Б (середній рівень) – операційний зал з диспетчерськими станціями, доступ для 12 диспетчерів і 3 інженерів у межах робочих змін; Зона В (базовий рівень) – решта

офісних та виробничих приміщень, включно з насосними станціями, де встановлено ПЛК. Польові пристрої (ПЛК) були виокремлені як окремий підтип Зони В з підвищеними вимогами через їх розташування поза будівлею [1, 6].

Впровадження засобів фізичного контролю по зонах. Для Зони А: механічний замок замінено на електронний замок зі зчитувачем смарт-карток та PIN-кодом (двофакторна автентифікація); встановлено IP-камеру всередині приміщення з безперервним записом; на серверних стійках встановлено окремі замки; усі USB-порти на серверах фізично заблоковано; введено правило двох осіб для будь-яких технічних робіт усередині Зони А. Для Зони Б: встановлено електронні замки зі зчитувачами карток на дверях операційного залу; USB-порти на диспетчерських станціях заблоковано фізичними блокаторами та заборонено на рівні групових політик; запроваджено реєстр дозволених знімних носіїв. Для ПЛК на насосних станціях: шафи з ПЛК закрито на замки та обладнано індикаторами втручання (tamper seals); встановлено датчики відкриття дверей шафи з сигналом до диспетчерського центру [1, 5, 6] (рис. 6).

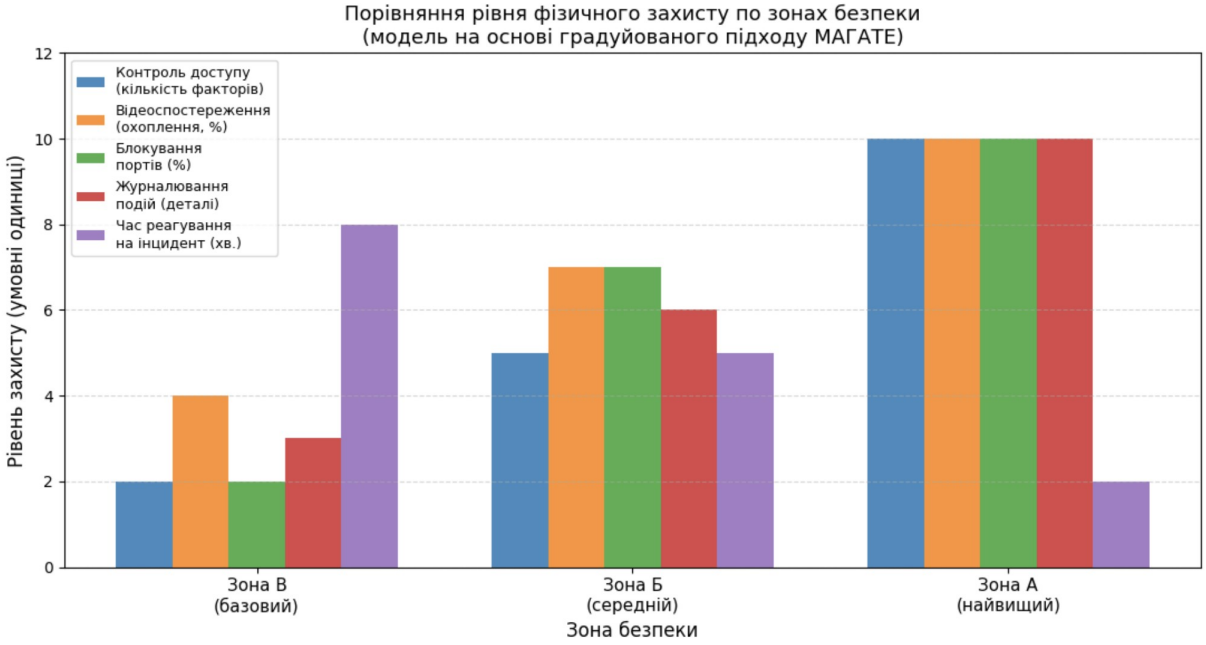

Рис. 6 – Порівняння рівня фізичного захисту по зонах безпеки умовного підприємства водопостачання після впровадження зональної моделі.

Крок 4. Організаційні заходи та управління конфігурацією. Паралельно з технічними заходами було впроваджено організаційні процедури: затверджено перелік уповноважених осіб для кожної зони з принципом мінімальних привілеїв; розроблено інструкцію щодо поводження зі знімними носіями; введено обов'язкове документування всіх технічних робіт у серверній кімнаті; складено та затверджено базову конфігурацію для кожного ЧЦА з регулярною верифікацією відповідності реального стану. Крім того, електронний замок Зони А налаштовано в режимі fail-secure (у разі відключення живлення двері залишаються замкненими), а для живлення замку передбачено резервний акумулятор [1, 5].

Результати впровадження. Через три місяці після впровадження під час планової перевірки один із підрядників, що мав доступ до Зони В для технічного обслуговування насосного обладнання, спробував підійти до шафи ПЛК насосної станції № 2 без відповідного дозволу. Датчик відкриття дверей зафіксував спробу і автоматично надіслав сповіщення диспетчеру, а інцидент було задокументовано та розслідувано. До впровадження такий підхід залишився б непоміченим. Аудит журналів доступу до Зони А також виявив кілька спроб входу за межами дозволених годин, що дозволило своєчасно переглянути рівні доступу персоналу. Жодного інциденту, пов'язаного з підключенням несанкціонованих USB-носіїв, зафіксовано не було, тоді як до блокування такі факти відбувалися, за оцінками, до двох разів на місяць [1, 7].

Наведений сценарій підтверджує, що навіть відносно нескладне і бюджетно доступне впровадження зональної моделі та базових засобів фізичного контролю дає вимірюваний практичний ефект: інциденти, які раніше залишалися непоміченими, стають видимими та відстежуваними. Ключовим є не вартість технічних засобів, а системність підходу – дотримання принципів МАГАТЕ щодо інвентаризації ЧЦА, визначення зон, застосування багаторівневого захисту та безперервного моніторингу [1, 2, 5].

ISSN 2079-5459 (print)
ISSN 2413-4295 (online)

Висновок

У роботі розглянуто принципи багаторівневого захисту, зонування безпеки, класифікацію загроз та підходи до їх нейтралізації відповідно до міжнародних стандартів і рекомендацій МАГАТЕ.

Показано, що фізичний захист комп'ютерних систем є самостійним і рівноправним рівнем інформаційної безпеки, що не може бути замінений технічними або адміністративними заходами. Ігнорування фізичного рівня безпеки створює критичні вразливості навіть у системах, що добре захищені з програмної точки зору. Зловмисник, що отримав фізичний доступ до обладнання, здатен обійти будь-які логічні засоби захисту.

Встановлено, що зональна модель та принцип багаторівневого захисту є найбільш ефективними архітектурними підходами до організації фізичного захисту. Вони дозволяють диференційовано застосовувати заходи залежно від критичності активів і забезпечують стійкість системи до атак завдяки відсутності єдиної точки відмови: подолання одного шару захисту не дає змоги скомпрометувати всю систему.

Доведено, що внутрішні загрози та атаки на ланцюг постачання є специфічними векторами, для протидії яким стандартних периметрових засобів захисту недостатньо. Необхідне системне застосування принципів мінімальних привілеїв, розподілу обов'язків, двох осіб, а також суворий контроль процесів закупівель і приймання обладнання.

Як бачимо, повноцінна ефективність фізичного захисту досягається лише за умови його інтеграції в загальну програму комп'ютерної безпеки організації, узгодженості з планом фізичного захисту об'єкту та безперервного моніторингу. Методологічний підхід МАГАТЕ, розроблений для захисту ядерних установок, є зразковим і може бути адаптований до будь-яких організацій, що управляють критично важливими інформаційними системами, тобто від промислових підприємств до установ державного управління.

Список літератури

1. International Atomic Energy Agency. Computer Security Techniques for Nuclear Facilities. IAEA Nuclear Security Series No. 17-T. Vienna: IAEA, 2021. 242 p.
2. International Atomic Energy Agency. Computer Security for Nuclear Security. IAEA Nuclear Security Series No. 42-G, Implementing Guide. Vienna: IAEA, 2021.
3. International Atomic Energy Agency. Security of Nuclear Information. IAEA Nuclear Security Series No. 23-G, Implementing Guide. Vienna: IAEA, 2015.
4. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Hoboken, NJ: John Wiley & Sons, 2020. 1232 p.
5. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: ISO, 2022.
6. NIST Special Publication 800-53, Revision 5. Security and Privacy Controls for Information Systems and Organizations. Gaithersburg, MD: National Institute of Standards and Technology, 2020.
7. Lee, R. M., Assante, M. J., Conway, T. Analysis of the Cyber Attack on the Ukrainian Power Grid. Washington, DC: SANS Industrial Control Systems, 2016. 28 p.
8. Langner, R. Stuxnet: Dissecting a Cyberwarfare Weapon. IEEE Security & Privacy. 2011. Vol. 9, No. 3. P. 49–51.
9. Scarfone K., Souppaya M. Guide to Enterprise Password Management. NIST Special Publication 800-118 (Draft). Gaithersburg: NIST, 2009.
10. Бурячок В. Л., Киричок Р. В., Складанний П. М. Основи інформаційної та кібернетичної безпеки : навчальний посібник. Київ : Київський університет імені Бориса Грінченка, 2019. 320 с.
11. IAEA-NSS-46-T, Evaluation of Physical Protection Systems at Nuclear Facilities, Technical Guidance, International Atomic Energy Agency (IAEA), 2025. https://doi.org/10.61092/iaea.pckz-it39
12. Aneka Choi, Cheonho Park, JuHyeon Lee, Seungho Jeon, Jung Taek Seo. Framework for evaluating cyber incident response capabilities of nuclear facility operators through operation-based exercises. Nuclear Engineering and Technology, Volume 57, Issue 11, 2025. https://doi.org/10.1016/j.net.2025.103772
13. Amal Touarsi, Amina Kharchaf, Chakir El Mahjoub. A novel methodology assessment to study the performance of the physical protection system for enhancing the security of nuclear and other radioactive materials during transport. Annals of Nuclear Energy, Volume 219, 2025. https://doi.org/10.1016/j.anucene.2025.111408
14. Marja Ylönen, Kim Björkman. Integrated management of safety and security (IMSS) in the nuclear industry — Organizational culture perspective. Safety Science, Volume 166, 2023. https://doi.org/10.1016/j.ssci.2023.106236
15. Nabin Chowdhury, Vasileios Gkioulos. Cyber security training for critical infrastructure protection: A literature review. Computer Science Review, Volume 40, 2021. https://doi.org/10.1016/j.cosrev.2021.100361

References

1. International Atomic Energy Agency. Computer Security Techniques for Nuclear Facilities. IAEA Nuclear Security Series No. 17-T. Vienna: IAEA, 2021. 242 p.
2. International Atomic Energy Agency. Computer Security for Nuclear Security. IAEA Nuclear Security Series No. 42-G, Implementing Guide. Vienna: IAEA, 2021.
3. International Atomic Energy Agency. Security of Nuclear Information. IAEA Nuclear Security Series No. 23-G, Implementing Guide. Vienna: IAEA, 2015.
4. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Hoboken, NJ: John Wiley & Sons, 2020. 1232 p.
5. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: ISO, 2022.
6. NIST Special Publication 800-53, Revision 5. Security and Privacy Controls for Information Systems and Organizations. Gaithersburg, MD: National Institute of Standards and Technology, 2020.
7. Lee, R. M., Assante, M. J., Conway, T. Analysis of the Cyber Attack on the Ukrainian Power Grid. Washington, DC: SANS Industrial Control Systems, 2016. 28 p.
8. Langner, R. Stuxnet: Dissecting a Cyberwarfare Weapon. IEEE Security & Privacy. 2011. Vol. 9, No. 3. P. 49–51.
9. Scarfone K., Souppaya M. Guide to Enterprise Password Management. NIST Special Publication 800-118 (Draft). Gaithersburg: NIST, 2009.

10. Buryachok V. L., Kyrychok R. V., Skladanyy P. M. Osnovy informatsiynoyi ta kibernetychnoyi bezpeky : navchal′nyy posibnyk. Kyyiv : Kyyivs′kyy universytet imeni Borysa Hrinchenka, 2019. 320 s.
11. IAEA-NSS-46-T, Evaluation of Physical Protection Systems at Nuclear Facilities, Technical Guidance, International Atomic Energy Agency (IAEA), 2025. https://doi.org/10.61092/iaea.pckz-it39
12. Aneka Choi, Cheonho Park, JuHyeon Lee, Seungho Jeon, Jung Taek Seo. Framework for evaluating cyber incident response capabilities of nuclear facility operators through operation-based exercises. Nuclear Engineering and Technology, Volume 57, Issue 11, 2025. https://doi.org/10.1016/j.net.2025.103772
13. Amal Touarsi, Amina Kharchaf, Chakir El Mahjoub. A novel methodology assessment to study the performance of the physical protection system for enhancing the security of nuclear and other radioactive materials during transport. Annals of Nuclear Energy, Volume 219, 2025. https://doi.org/10.1016/j.anucene.2025.111408
14. Marja Ylönen, Kim Björkman. Integrated management of safety and security (IMSS) in the nuclear industry — Organizational culture perspective. Safety Science, Volume 166, 2023. https://doi.org/10.1016/j.ssci.2023.106236
15. Nabin Chowdhury, Vasileios Gkioulos. Cyber security training for critical infrastructure protection: A literature review. Computer Science Review, Volume 40, 2021. https://doi.org/10.1016/j.cosrev.2021.100361

Відомості про авторів / About the Authors

Лис Степан Степанович – кандидат технічних наук, доцент; Інститут комп'ютерних технологій, автоматики та метрології, Національний університет «Львівська політехніка», вул. С. Бандери, 12, м. Львів, Україна, 79013; e-mail: lysss@ukr.net, тел.: (032) 258-23-15; ORCID: 0000-0002-7359-1177.

Stepan Lys – Assoc. Prof., Ph.D., Institute of Computer Technologies, Automation and Metrology, Lviv Polytechnic National University, 12 S. Bandery St., Lviv, 79013, Ukraine, Tel. 0038 032 258 25 15; Email: lysss@ukr.net; ORCID: 0000-0002-7359-1177.

Ісопенко Андрій Ярославович – студент; Інститут комп'ютерних технологій, автоматики та метрології, Національний університет «Львівська політехніка», вул. С. Бандери, 12, м. Львів, Україна, 79013; e-mail: andrii.isopenko.kb.2024@lpnu.ua, тел.: (032) 258-23-15.

Andrii Isopenko – student, Institute of Computer Technologies, Automation and Metrology, Lviv Polytechnic National University, 12 S. Bandery St., Lviv, 79013, Ukraine, Tel. 0038 032 258 25 15; Email: andrii.isopenko.kb.2024@lpnu.ua.

Загаровський Віталій Васильович – студент; Інститут комп'ютерних технологій, автоматики та метрології, Національний університет «Львівська політехніка», вул. С. Бандери, 12, м. Львів, Україна, 79013; e-mail: vitalii.zaharovskyi.kb.2024@lpnu.ua, тел.: (032) 258-23-15.

Vitalii Zaharovskyi – student, Institute of Computer Technologies, Automation and Metrology, Lviv Polytechnic National University, 12 S. Bandery St., Lviv, 79013, Ukraine, Tel. 0038 032 258 25 15; Email: vitalii.zaharovskyi.kb.2024@lpnu.ua.

Будь ласка, посилайтесь на цю статтю наступним чином:

Лис С. С., Ісопенко А. Я., Загаровський В.В. Організація фізичного захисту комп’ютерних систем критичної інфраструктури на основі стандартів та рекомендацій МАГАТЕ. *Вісник Національного технічного університету «ХПІ». Серія: Нові рішення в сучасних технологіях*. – Харків: НТУ «ХПІ». 2026. № 2 (28). С. 35-45. doi:10.20998/2413-4295.2026.02.05.

Please cite this article as:

Lys S., Isopenko A., Zaharovskyi V. Organization of physical protection of computer systems of critical infrastructure based on IAEA standards and recommendations. *Bulletin of the National Technical University "KhPI". Series: New solutions in modern technology*. – Kharkiv: NTU "KhPI", 2026, no. 2(28), pp. 35–45, doi:10.20998/2413-4295.2026.02.05.

Надійшла (received) 07.04.2026
Прийнята (accepted) 28.04.2026
Опублікована (published) 05.06.2026