КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1289
УДК 004.056:620.9

Добринчук Олександр Анатолійович
молодший науковий співробітник
Національний університет «Київський авіаційний інститут», Київ, Україна
ORCID: 0009-0002-2877-844X
oleksandr.dobrynchuk@npp.kai.edu.ua

Лукашенко Вікторія Вікторівна
д.т.н., професор, директор управління з навчально-наукової діяльності
Національний університет «Київський авіаційний інститут», Київ, Україна
ORCID: 0009-0009-0458-2590
viktoriia.lukashenko@kai.edu.ua

Гричук Сергій Анатолійович
старший викладач
Українська військово-медична академія, Київ, Україна
ORCID: 0009-0008-4799-597X
sg03111975dok@gmail.com

НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ЕНЕРГЕТИЧНОМУ СЕКТОРІ

Анотація. У статті проведено комплексне дослідження сучасних нормативно-правових та технічних підходів до забезпечення кібербезпеки в енергетичному секторі в умовах масштабної цифровізації та зростання гібридних загроз. Актуальність роботи зумовлена активною конвергенцією інформаційних (IT) та операційних технологій (OT), що відкриває нові вектори атак на системи промислової автоматизації та управління (IACS), такі як SCADA, DCS та ПЛК. Особливу увагу приділено специфіці захисту критичної інфраструктури України, чиї енергомережі вже ставали об’єктами цілеспрямованих атак, зокрема CrashOverride/Industroyer, що вимагає негайного зміцнення систем відповідно до міжнародних стандартів. Дослідження містить детальний огляд ключових міжнародних стандартів, серед яких серія ISA/IEC 62443, що впроваджує концепцію зон, каналів та рівнів безпеки (SL 1–4) для мінімізації ризиків саботажу та втручання в роботу енергетичних об'єктів. Проаналізовано вплив Директиви NIS2, яка встановлює обов'язкові вимоги до управління ризиками, безпеки ланцюгів постачання та відповідальності керівництва для суб’єктів життєво важливого значення. Окремо розглянуто роль стандартів NERC CIP для забезпечення надійності магістральних електромереж та гнучкий підхід NIST CSF 2.0 у поєднанні з моделлю зрілості C2M2. Значну увагу приділено захисту ядерної енергетики на основі стандартів IAEA NSS-17-T та IEC 62645, де пріоритет цілісності та доступності над конфіденційністю є критичним для запобігання радіаційним інцидентам. Стаття аналізує ступеневий підхід до захисту чутливих цифрових активів (SDA) та детерміновану ізоляцію критичних систем (модель NEI 08-09). Результати дослідження висвітлюють виклики майбутнього, зокрема «квантову загрозу» та стратегію зловмисників «збирай зараз, розшифровуй пізніше» (HNDL), що вимагає переходу на постквантову криптографію (PQC). Висвітлено потенціал штучного інтелекту (інструменти типу SecureAI) для автоматизованого виявлення аномалій у промислових протоколах Modbus/TCP та OPC UA, а також необхідність інтеграції управління ризиками ШІ через NIST AI RMF. У висновках наголошується, що для України гармонізація національних стандартів ДСТУ з європейськими нормами є необхідною умовою для транскордонної синхронізації енергомереж та забезпечення національної стійкості.

Ключові слова: кібербезпека; енергетичний сектор; критична інфраструктура; Директива NIS2; ISA/IEC 62443; операційні технології; ядерна безпека; управління ризиками; квантова стійкість; штучний інтелект.

ВСТУП

У сучасному цифровому середовищі захист критичної інфраструктури став одним із ключових пріоритетів національної безпеки, особливо в енергетичному секторі. Масштабна цифровізація галузі призвела до конвергенції інформаційних (IT) та операційних технологій (OT), що, хоч і підвищує ефективність, водночас створює нові складні виклики для безпеки. Енергетичні системи, включаючи електромережі, газопровідні мережі та об'єкти відновлюваної енергетики, дедалі більше залежать від складних систем промислової автоматизації та управління (IACS), таких як SCADA, DCS та ПЛК. Енергетичні системи дедалі частіше стають мішенями цілеспрямованих кіберзагроз, здатних дестабілізувати діяльність держави. Особливу гостроту ця проблема має для України, чиї енергомережі вже ставали об'єктами масштабних атак, таких як CrashOverride/Industroyer у 2015 та 2016 роках, що вимагає негайного зміцнення критичних систем відповідно до міжнародних стандартів для забезпечення транскордонної синхронізації та стійкості.

Важливим фактором актуальності є необхідність нормативно-правової відповідності міжнародним та європейським вимогам, зокрема Директиві NIS2, яка суттєво посилює відповідальність керівництва за управління ризиками та безпеку ланцюгів постачання в енергетичному секторі. Впровадження таких стандартів, як ISA/IEC 62443 та ISO/IEC 27001, дозволяє організаціям створити багаторівневу архітектуру захисту, де пріоритет надається доступності та цілісності процесів у режимі реального часу, що є критичним для запобігання відключенням електроенергії. Для ядерної енергетики актуальність підсилюється вимогами IAEA NSS-17-T та стандарту IEC 62645, які спрямовані на захист чутливих цифрових активів від радіаційного саботажу та несанкціонованого доступу в умовах сучасних гібридних загроз.

Додатковим викликом, що підкреслює своєчасність дослідження, є поява квантових комп'ютерів, здатних зламати наявні криптографічні засоби захисту, що створює довгострокові ризики для систем із тривалим життєвим циклом. Водночас активне впровадження штучного інтелекту відкриває як нові можливості для автоматизованого виявлення загроз у реальному часі, так і нові вразливості, пов'язані з цілісністю даних та прозорістю алгоритмів. Таким чином, інтеграція сучасних рамок управління ризиками та передових технологій є необхідною умовою для формування адаптивної системи кіберзахисту, здатної протидіяти складним постійним загрозам (APT) та забезпечувати безперервність функціонування життєво важливої інфраструктури.

Метою дослідження є огляд сучасних стандартів та рекомендацій щодо забезпечення кібербезпеки в енергетичному секторі.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Огляд міжнародних стандартів і рекомендацій

Нижче наведено короткий список стандартів так рекомендованих практик:

- ISA/IEC 62443 – міжнародна серія стандартів для кібербезпеки промислових автоматизованих систем управління (IACS). Визначає вимоги до безпечного життєвого циклу розробки, навчання, архітектури мереж, сегментації та захисту промислової автоматизації.
- Директива NIS2 – встановлює обов'язкові вимоги до кібербезпеки критичної інфраструктури (включно з енергетикою) у країнах-членах, розширює охоплення секторів та посилює санкції за порушення.
- NERC CIP – обов'язковий набір стандартів кібербезпеки North American Electric Reliability Corporation для захисту критичної інфраструктури електроенергії в Північній Америці.
- NIST CSF 2.0 – оновлена рамка кібербезпеки NIST (2024), що включає 6 функцій: Govern (управління), Identify, Protect, Detect, Respond, Recover.
- ISO/IEC 27001:2022 – міжнародний стандарт системи управління інформаційною безпекою (ISMS). Визначає вимоги до впровадження, моніторингу та підтримки ISMS для захисту інформаційних активів.
- ISO/IEC 27019:2024 – спеціалізована розширення ISO 27001 для енергетичного сектору (електричні комунальні підприємства). Визначає контрольні заходи безпеки для процесів енергетичних компаній.
- IAEA NSS-17-T – стандарт з технічних вимог кібербезпеки для ядерних установок. Визначає вимоги до захисту систем керування та захисту ядерних об'єктів від кіберзагроз.
- IEC 62645:2019 – стандарт для кібербезпеки систем захисту ядерних установок. Визначає вимоги до безпеки систем, що відповідають за безпеку ядерних реакторів.

- NEI 08-09 – галузевий посібник Nuclear Energy Institute для виконання вимог NRC з кібербезпеки ядерних об'єктів США. Визначає процес категоризації систем та впровадження контрольних заходів.
- IAEA NST-070 – надає практичні вказівки щодо впровадження кібербезпеки в ядерному секторі.
- NISR 2003 – стандарт Nucleare Energy Industry з кібербезпеки. Визначає вимоги до кібербезпеки для ядерної промисловості.

Далі наведено більш детальний огляд стандартів:

Стандарт ISA/IEC 62443 передбачає спеціалізовану систему кібербезпеки для енергетичного сектору, спрямовану на усунення вразливостей у системах промислової автоматизації та управління (IACS), таких як SCADA, DCS та ПЛК, що використовуються у виробництві, передачі та розподілі електроенергії. Він наголошує на принципі багаторівневого захисту за допомогою зон, каналів та рівнів безпеки (SL 1–4) для мінімізації ризиків, таких як атаки програм-вимагачів або атаки з боку держав на критичну інфраструктуру. Ці стандарти визначені як «горизонтальні», що робить їх безпосередньо застосовними до енергетичних операцій, а Міністерство енергетики США (DOE) схвалило їх через Виконавчу робочу групу з безпеки енергетичної інфраструктури (SEI ETF). ISA/IEC 62443 пропонує спеціалізовану структуру кібербезпеки для енергетичного сектору, зосереджуючись на захисті операційних технологій (OT), таких як SCADA, DCS, ПЛК та RTU у виробництві, передачі, розподілі та відновлюваних джерелах енергії. Вона адаптує принципи глибокого захисту до загроз, специфічних для енергетики, таких як атаки CrashOverride/Industroyer на енергомережі, надаючи пріоритет доступності, цілісності та безпеці над конфіденційністю. Енергетичні системи призначають рівні безпеки (SL 0–4) для кожної зони/каналу на основі суб’єктів загрози та наслідків (наприклад, ризики для здоров’я, безпеки та навколишнього середовища від відключень електроенергії). Рівні безпеки орієнтовані на можливості (навички/ресурси зловмисника) та ефективність (захисні заходи системи): SL1 – випадкові загрози або помилки – наприклад, польові датчики; SL2 – кіберзлочини та хакери – наприклад, периферійні IT-системи підприємства; SL3 – хактивісти та терористи – наприклад, SCADA підстанцій; SL4 – державна загроза – наприклад, датчики управління енергомережею. SEI ETF Міністерства енергетики США (DOE) використовує профілі 62443-5-x для електричних OT, визначаючи цілі SL для підстанцій (наприклад, безпечний зв'язок за стандартом IEC 61850) та інтеграції розподілених енергоресурсів (DER). Schneider Electric сертифікує управління енергоспоживанням на рівні SL2 (профіль компонента 62443-4-2). Українські енергомережі після атак 2015/2016 років використовують його для зміцнення SCADA «Укренерго», узгоджуючи з ДСТУ та EU NIS2 для транскордонної синхронізації.

Директива NIS2 (Директива (ЄС) 2022/2555) суттєво посилює вимоги до кібербезпеки в енергетичному секторі як «критично важливому» секторі, передбачаючи обов’язкове впровадження надійної системи управління ризиками для захисту критичної інфраструктури, такої як електромережі, газопровідні мережі та об’єкти відновлюваної енергетики, від зривів у роботі внаслідок кібератак. Вона виходить за межі NIS1, охоплюючи ланцюги постачання, системи операційної техніки (наприклад, SCADA на електростанціях) та відповідальність керівництва. До об’єктів життєво важливого значення належать виробники електроенергії, оператори передачі/розподілу, постачальники/сховища газу, оператори водневих мереж і навіть оператори зарядних станцій — це охоплює МСП (50+ співробітників або оборот 10 млн євро) без винятків для незначної діяльності. Україна, приєднуючись до асоціації з ЄС, застосовує подібні правила через національне законодавство з кібербезпеки для таких операторів, як «Укренерго», інтегруючи NIS2 із захистом критичної інфраструктури після атак на енергомережі у 2015/2016 роках. Енергетичні компанії повинні впроваджувати всі 10 базових заходів пропорційно до ризиків: постійні оцінки ризиків для OT/IT (наприклад, систем управління енергомережею); реагування на інциденти, забезпечення безперервності бізнесу, безпека ланцюга постачання (перевірка постачальників для підстанцій); MFA, шифрування, управління вразливостями та навчання з кібербезпеки; політики резервного копіювання та кризове управління на випадок відключень електроенергії. NIS2 доповнює 62443, вимагаючи впровадження програм на зразок CSMS (у відповідності до 62443-2-1 для комунальних підприємств), моделей зон/каналів для сегментації енергомереж (62443-3-2) та цільових рівнів безпеки (SL) для активів високого ризику, таких як SCADA систем передачі (SL3+). Енергетичні оператори використовують стандарт 62443 для технічної реалізації з метою дотримання «відповідних заходів» NIS2, як це передбачено в рекомендаціях ЄС щодо стійкості операційних технологій. У Польщі та Україні національні органи (PKN/DSTU) сприяють спільній адаптації стандартів для інтелектуальних мереж.

Стандарти NERC CIP (Critical Infrastructure Protection) – це обов’язкові вимоги до кібербезпеки, встановлені Північноамериканською корпорацією з надійності електропостачання (NERC) для магістральної електромережі (BES) у Північній Америці. Вони спрямовані на власників/операторів об’єктів високовольтної передачі електроенергії (>100–200 кВ) та великих об’єктів генерації (>1500 МВт) з метою запобігання кіберінцидентам, що можуть спричинити масштабні відключення електроенергії. Застосовуються до кіберресурсів BES (з високим/середнім/низьким рівнем впливу), таких як сервери

EMS/SCADA, захисні реле, системи управління генерацією та електронні периметри безпеки (ESP). Не поширюються на розподільчі мережі низької напруги (<100 кВ), інтелектуальні лічильники та приміщення споживачів; забезпечуються регіональними органами з накладенням штрафів до 1 млн доларів на день за кожне порушення. Основні стандарти: CIP-002 – Класифікація кіберсистем BES; CIP-005 – Електронний периметр безпеки; CIP-007 – Управління безпекою системи; CIP-008 – Реагування на інциденти та відновлення; CIP-010 – Управління змінами конфігурації; CIP-013 – Ланцюг постачання. NERC CIP узгоджується з управлінням ризиками NIS2 (наприклад, ланцюг постачання, реагування на інциденти) для північноамериканських операцій, інтегрованих з ЄС, та відповідає зонам 62443 (CIP-005 ESP), цілям SL (CIP-007) та CSMS (CIP-003). Українські енергетичні компанії, що мають зв'язки з Північною Америкою (наприклад, партнерства DTEK), посилаються на нього разом із NIS2/DSTU для забезпечення гібридної безпеки OT. Відповідність вимогам перевіряється щорічно шляхом самосертифікації/аудитів на місці.

«Рамка кібербезпеки NIST (CSF) 2.0» – це добровільний стандарт NIST, заснований на оцінці ризиків, який допомагає організаціям енергетичного сектору визначати пріоритетність та управляти ризиками кібербезпеки в системах операційних технологій (OT) та інформаційних технологій (IT), таких як SCADA, EMS та системи управління енергомережами. Оновлена у 2024 році, вона акцентує увагу на шести основних функціях – управління, ідентифікація, захист, виявлення, реагування, відновлення – для підвищення стійкості до таких загроз, як програми-вимагачі, спрямовані проти комунальних підприємств. Широко прийнята завдяки Керівництву з впровадження Рамки кібербезпеки енергетичного сектору від DOE, CSF інтегрується з C2M2 (варіант для підсектору електроенергетики) для оцінки зрілості у сферах виробництва, передачі та відновлюваних джерел електроенергії. Вона підтримує відповідність вимогам NERC CIP, NIS2 та ISA/IEC 62443, зосереджуючись на ризиках ланцюга постачання для пристроїв на периферії мережі (наприклад, інверторів, розподілених джерел енергії). Для «Енергоатому»/«Укренерго» профілі CSF надають пріоритет ідентифікації/захисту для систем безпеки ЗАЕС (загрози після 2022 року), використовуючи цілі C2M2 MIL2+: управління активами (домени AM) для інтерфейсів RPS, виявлення через SIEM на операційних технологіях, що не стосуються безпеки. Доповнює кіберправила SNRIU та транспозицію NIS2, з відповідністю DOE для західних програм допомоги. Швидкий старт за допомогою інструменту NIST CSF 2.0 Excel для багаторівневих профілів (Частковий→Адаптивний).

Стандарти інформаційної безпеки для енергетичного сектору ґрунтуються на концепціях кібербезпеки та спрямовані на захист конфіденційних даних, IT- та OT-систем, а також на забезпечення цілісності операційних процесів у таких об’єктах інфраструктури, як електромережі та об’єкти відновлюваної енергетики.

Стандарт ISO/IEC 27001:2022 забезпечує сертифіковану основу для створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (ISMS) в енергетичному секторі, зосереджуючись на захисті активів операційних технологій (OT) та інформаційних технологій (IT), таких як SCADA, EMS, ПЛК та потоки даних енергомережі, з урахуванням ризиків, щоб забезпечити їхню доступність та цілісність в умовах загроз, таких як APT або програми-вимагачі. Цикл PDCA (Plan-Do-Check-Act) стандарту адаптований до OT з високою доступністю: пункт 4 (Context) поширює дію ISMS на операції енергомережі (наприклад, підстанції, диспетчерські центри); пункт 5 (Leadership) покладає на вищий керівний склад відповідальність за політику, що забезпечує надійність у режимі 24/7; Пункт 6 (Planning) визначає плани реагування на ризики на основі стандарту 27005, надаючи пріоритет загрозам для систем типу BES. Пункт 7 (Support) наголошує на компетентності, специфічній для OT (наприклад, навчання операторів щодо аномалій протоколів); Пункт 8 (Operation) забезпечує безпечне управління змінами для оновлень прошивки; Пункти 9-10 стосуються аудитів та вдосконалень, із сертифікацією раз на три роки. «Укренерго»/«Енергоатом» застосовують стандарт 27001 для транспозиції NIS2, обмежуючи контроль зміцненням SCADA після 2015 року (наприклад, A.8.29 Синхронізація годинника для часових міток у WAMS). Синергія з 62443-2-1 (A.5.1 відображення CSMS) та політиками NERC CIP-003; сертифікація через UA DSTU покращує взаємодію з ЄС. SoA зазвичай обирає 70–80 заходів контролю для комунальних підприємств, які перевіряються щорічно.

Стандарт ISO/IEC 27019:2024 доповнює стандарт ISO/IEC 27002:2022 галузевими рекомендаціями для підприємств енергетики, що не пов’язані з атомною енергетикою, та передбачає спеціалізовані заходи інформаційної безпеки для систем управління технологічними процесами (PCS), таких як SCADA, DCS, ПЛК, RTU, а також пов’язаних з ними мереж у сферах виробництва, передачі, розподілу та зберігання електроенергії, газу, нафти та тепла. Він враховує обмеження, характерні для операційних технологій (OT) – операції в режимі реального часу, застарілі пристрої, які неможливо оновлювати, критичність з точки зору безпеки та навколишнього середовища, а також пріоритет доступності над конфіденційністю – допомагаючи підприємствам ефективно впроваджувати ISMS ISO 27001 в умовах таких загроз, як Industroyer або програми-вимагачі. Не охоплює ядерну енергетику (на яку поширюється дія стандарту IEC

(наприклад, IEC 61850), телеуправління та дистанційне обслуговування. Додає ~12 рекомендацій «ENR», що інтерпретують пункти стандарту 27002 з урахуванням реалій ОТ, таких як вікна сканування без переривання роботи та ризики, пов'язані з конкретними протоколами (DNP3, Modbus). Відповідає вимогам 62443 FR (наприклад, ENR-6 до сегментації FR 3), NERC CIP-007 (конфігурації), NIST CSF Protect/Detect, заходам NIS2. Українські енергетичні підприємства (Енергоатом для неядерних частин) застосовують після 2015 року: ENR-8 для безпечних дистанційних операцій на інтерфейсах ЗАЕС, покращуючи відповідність DSTU/NIS2. Сертифікація свідчить про готовність до тендерів ЄС.

Документ IAEA NSS-17-T (Rev. 1) під назвою «Методи комп'ютерної безпеки для ядерних об'єктів» є технічним посібником із серії «Ядерна безпека» IAEA, що містить детальні практичні рекомендації, засновані на оцінці ризиків, щодо захисту комп'ютерних систем на ядерних об'єктах від кіберзагроз, таких як саботаж, несанкціонований доступ або викрадення ядерних матеріалів. Вона спрямована на цифрові активи — включаючи чутливі цифрові активи (SDA), такі як SCADA, системи I&C для управління реакторами, системи фізичного захисту (PPS), облік ядерних матеріалів (NMAC) та допоміжні IT – протягом усього життєвого циклу (від планування до виведення з експлуатації). У ній наголошується на ступеневому підході через рівні комп'ютерної безпеки (1–5, де 1 – найсуворіший) та зони для захисту функцій, критично важливих для інтерфейсів безпеки/захисту, запобігаючи кібератакам (наприклад, маніпуляціям із RPS або PPS). Рівні безпеки: Рівень 1 (найвищий) – мінімальні взаємодії (наприклад, система захисту реактора PLS); Рівень 2 – контрольовані взаємодії (наприклад, керовані PPS); Рівень 3 – моніторовані взаємодії (наприклад, бази даних NMAC); Рівень 4 – фільтровані взаємодії (наприклад, інженерні робочі станції); Рівень 5 (найнижчий) – загальні взаємодії (наприклад, корпоративні IT). «Енергоатом»/Держатомрегулювання вимагає виконання NSS-17-T відповідно до місій IAEA (наприклад, огляди ЗАЕС у 2022 році), що застосовується до не пов'язаних з безпекою систем операційного обладнання (SCADA рівня 3) щодо загроз після 2022 року: роз'єднання зон для інтерфейсів РСЗ, заходи щодо запобігання зловживанням з боку інсайдерів (перевірка). Доповнює NPBU-1.016-98, NRC 73.54, 62443 FR; перевірено експертними оцінками МАГАТЕ SALTO. Безкоштовний PDF-файл містить сценарії Додатку I для моделювання загроз.

Стандарт IEC 62645:2019 (2-е вид.) встановлює вимоги до кібербезпеки систем вимірювально-контрольної апаратури та електропостачання (I&C) атомних електростанцій, зосереджуючись на програмованих цифрових системах, таких як PLC, DCS, SCADA та системи I&C безпеки, з метою запобігання, виявлення та реагування на кібератаки, які можуть спричинити небезпечні умови, пошкодження обладнання або погіршення його експлуатаційних характеристик. Застосовується до цифрових систем I&C протягом усього життєвого циклу АЕС, використовуючи ступеневий підхід на основі впливу на безпеку/доступність (наприклад, категорія А: функції безпеки, такі як RPS; категорія С: допоміжні системи). Не охоплює фізичну безпеку, конфіденційність (основна увага приділяється цілісності/доступності), нешкідливі відмови (охоплюються стандартами IEC 61508/61226) та людські помилки, за винятком тих, що сприяють атакам. Базується на принципах IAEA NSS-17, але адаптований до вимог ядерного регулювання (наприклад, 10 CFR 50 App. B, WENRA). Відповідає концепціям ISO 27001, але адаптований до ядерної галузі:

Пункт 5: Система управління – політика, ролі (наприклад, керівник служби безпеки, незалежний від оперативного персоналу), цілі (наприклад, відсутність незахищених вразливостей у PLC безпеки).

Пункт 6: Оцінка ризиків – моделювання загроз (у відповідності до DBT), категоризація активів, прийняття залишкового ризику регуляторним органом.

Пункт 7: Заходи контролю – запобігання (захист), виявлення (моніторинг), реагування (ізоляція).
«Енергоатом» (ЗАЕС, Рівне) інтегрує IEC 62645 із SNRIU NPBU-1.016-98 та IAEA NSS-17 для кіберзахисту після 2022 року: ізоляція категорії А для системи реагування на аварійні ситуації (RPS) ВВЕР-1000, сегментація категорії В для SCADA, що не стосується безпеки. Доповнює NRC 73.54 для західних технологій; місії SALTO перевіряють ступінчасті заходи контролю, узгоджуючи їх з NIS2 для інтерфейсів енергомереж. Придбати можна через інтернет-магазин IEC; попередній перегляд підтверджує фокус на ядерній ОТ.

Директива NIS2 (EU 2022/2555) класифікує операторів ядерної енергетики як об'єкти життєво важливого значення відповідно до Додатка I, що накладає на великі та середні АЕС, об'єкти паливного циклу та системи поводження з відходами суворі зобов'язання щодо кібербезпеки через пов'язані з ними системні ризики (наприклад, радіаційний витік, відключення електромереж внаслідок кіберсаботажу). Вона вимагає дотримання всіх 10 базових заходів з управління ризиками (ст. 21) пропорційно до загроз, причому відповідальність керівництва та безпека ланцюга поставок поширюються на постачальників систем управління та контролю. Застосовується до операторів, пов'язаних з ЄС/Україною (наприклад, «Енергоатом» через угоду з ЄС), щодо мереж/інформаційних систем, що підтримують операції, включаючи не пов'язані з безпекою операційні та інформаційні технології, такі як SCADA, адміністративні мережі та

інтерфейси енергомереж, але питання ІК класу безпеки відкладає на розгляд ядерних регуляторів (наприклад, ДНЯР, NRC). Порогові значення: >50 співробітників або оборот 10 млн євро; винятків для МСП немає. Охоплює інтеграцію водню/відновлюваних джерел енергії на майданчиках АЕС. Заходи NIS2 безпосередньо відповідають IEC 62645 CSP (ст. 21→пункт 5), зонам IAEA NSS-17 (сегментація), цілям 62443 SL та NIST CSF Govern/Protect. Для Запоріжжя/Рівного NIS2 сприяє зміцненню не пов'язаної з безпекою операційної техніки (наприклад, ланцюга постачання для систем російського походження), доповнюючи правила безпеки SNRIU NPBU-1.016-98. Транспозиція України (очікується у 2026 році) через ДСТУ вимагає подвійної сертифікації. Термін дотримання вимог: зазвичай 12 місяців, з пріоритетом ланцюга постачання (найбільший розрив).

NEI 08-09 – це галузевий шаблон «Плану кібербезпеки для ядерних енергетичних реакторів», розроблений Інститутом ядерної енергетики з метою виконання вимог 10 CFR 73.54, що забезпечує захист критичних цифрових активів (CDA) від кібератак аж до рівня DBT із «високим ступенем надійності», гарантуючи безпеку, охорону, готовність до надзвичайних ситуацій, та допоміжних функцій від радіаційного саботажу. Поширюється на АЕС США (Частина 50/52): CDA включають системи безпеки I&C (RPS/ECCS), PPS (IDS/CCTV), EP (позамайданчикові ERDS), допоміжні системи (BOP SCADA, якщо це впливає на безпеку, згідно з роз'ясненням 2017 року). Виключає нецифрові/виключно фізичні активи; тест на зв'язок BOP: компрометація призводить до радіаційного ризику/ризику для здоров'я населення. 4-рівнева модель з пасивним зонуванням (відсутність довіри між рівнями): Рівень 0: Зовнішній/Інтернет – заблоковано, Рівень 1: CDA безпеки/захисту/EP – з повітряним проміжком, детерміновані, Рівень 2: Допоміжні CDA (наприклад, шлюзи MCR) – контрольований доступ, Рівень 3/4: LAN/WAN – фільтровані. «Енергоатом» посилається на архітектуру NEI 08-09 для модернізацій Westinghouse/BBEP (наприклад, повітряні проміжки рівня 1 у Рівному), узгоджуючи її із зонами SNRIU/IEC 62645, NSS-17 IAEA, ланцюгом постачання NIS2. ЗАЕС після 2022 року використовує подібні рамки CDA/IR для OT, що не стосується безпеки; місії IAEA схвалюють це як найкращу практику для парку BBEP.

Документ IAEA NST-070 під назвою «Інформаційна безпека в контексті ядерної безпеки» – це проект/розроблюваний посібник із впровадження в рамках Серії публікацій IAEA з ядерної безпеки (NSS), що містить практичні рекомендації щодо захисту конфіденційної інформації, пов'язаної з ядерними та іншими радіоактивними матеріалами, об'єктами та діяльністю, від несанкціонованого розголошення, зміни або знищення, що може спричинити зловмисні дії, такі як саботаж або крадіжка. Призначений для операторів ядерних об'єктів, регуляторних органів та постачальників, які працюють з інформацією про ядерну безпеку (NSI) – наприклад, проектними кресленнями RPS/PPS, даними NMAC, графіками транспортування, оцінками загроз – протягом усього життєвого циклу (проектування, експлуатація, виведення з експлуатації). Доповнює NSS-17-T (комп'ютерна безпека) та NSS-13 (системи ядерної безпеки), зосереджуючись на конфіденційності (на відміну від цілісності/доступності, орієнтованих на безпеку), використовуючи класифікацію з урахуванням ризиків (наприклад, рівні IAEA: L1 (Життєво важливий – вихідний код прошивки РПС); L2 (Важливий – конфігурації ППС); L3 (рутинний – навчальні матеріали) та ступеневі заходи контролю для зменшення загроз зсередини/APT. «Енергоатом»/ Держатомрегулювання застосовує проект принципів NST-070 для ЗАЕС/Рівне після 2022 року: класифікація L1 для російських документів з управління та контролю, DLP для мереж OT, що взаємодіють із системами безпеки. Відповідає NPBU-1.016-98, IEC 62645 (пункти щодо інформаційної безпеки), ланцюгу постачання NIS2 та місіям IAEA SALTO; підтримує вступ до ЄС шляхом гармонізації з WENRA. Як проект, використовувати для найкращих практик до остаточного затвердження. Безкоштовні проекти через IAEA Nucleus.

Правила безпеки ядерної промисловості 2003 року, з поправками) – це законодавство Великої Британії, виконання якого забезпечує Управління з ядерного регулювання (ONR) у сфері цивільної ядерної безпеки (CNS). Воно встановлює обов'язкові заходи безпеки для об'єктів цивільної ядерної енергетики, перевізників та осіб, що працюють з ядерними матеріалами/інформацією, з метою захисту від саботажу, крадіжки або несанкціонованого доступу з боку супротивників відповідно до рівня загрози, що лежить в основі проектування (DBT) у Великій Британії. У секторі ядерної енергетики ці правила регулюють діяльність ліцензованих об'єктів (АЕС, підприємства з виробництва палива, сховища відходів), вимагаючи від відповідальних осіб (ліцензіатів/операторів) дотримання затверджених планів безпеки ядерних об'єктів (NSSP) та заяв про безпеку перевезень (TSS). Застосовується до всіх цивільних ядерних об'єктів Великої Британії (наприклад, Селлафілд, Хінклі-Пойнт С), визначених розщеплюваних матеріалів (категорії I–III) та конфіденційної ядерної інформації (SNI) – усіх даних із захисним грифом (від «ОФІЦІЙНО-КОНФІДЕНЦІЙНО» до «ЦІЛКОМ ТАЄМНО»), що генеруються/зберігаються галуззю або отримуються від уряду Великої Британії. Охоплює кадрову, фізичну та інформаційну безпеку; виключає військові об'єкти (Міністерство оборони). ONR затверджує плани, проводить інспекції та видає дозволи. Вимоги:

Плани безпеки (Регламент 6–9): Специфічні для об'єкта NSSP детально описують реагування на загрози, збройне реагування (через Цивільну ядерну поліцію – CNC), виявлення вторгнення на периметр, контроль доступу (наприклад, правило двох осіб для матеріалів категорії I).

Безпека персоналу (Регламент 15–20): Перевірки за базовим стандартом безпеки персоналу (BPSS); перевірка на відповідність вимогам національної безпеки (NSV) для ключових посад (наприклад, операторів диспетчерських, які працюють з даними RPS).

Захист SNI (Регламент 23-27): Маркування, зберігання (сховища/SCIF), передача (захищені кур'єри/шифрування), очищення; повідомлення про втрати до ONR протягом 24 годин.

Хоча принципи NISR 2003 стосуються конкретно Великої Британії, вони впливають на глобальну ядерну безпеку через NSS-13/17 IAEA (наприклад, збройне реагування, поводження з SNI) та еталони WENRA. «Енергоатом»/ Держатомрегулювання посилається на подібні режими для ЗАЕС (після 2022 року): захист об'єктів ВВЕР на зразок CNC, класифікація SNI відповідно до проектів NST-070, зони IEC 62645. Підтримує транспозицію NIS2 в Україні через перевірку ланцюгів постачання західних постачальників (наприклад, Westinghouse).

Огляд сучасних наукових публікацій

У сучасному цифровому середовищі захист критичної інфраструктури від кібератак став одним із головних пріоритетів національної безпеки, особливо в енергетичному секторі. У міру поширення цифровізації та розвитку гібридної війни енергетична інфраструктура дедалі частіше стає мішенню кіберзагроз, здатних порушити функціонування життєво важливих служб та дестабілізувати діяльність держави. Отже, забезпечення безпеки та стійкості енергетичних систем вимагає ефективних стратегій кібербезпеки та чіткого розуміння обмежень існуючих механізмів захисту. У цій статті представлено комплексний огляд літератури щодо підходів до кібербезпеки, що використовуються для захисту критичної енергетичної інфраструктури та систем «розумних» енергомереж від кібератак (рис. 1). У дослідженні [1] розглядаються загальноприйняті стратегії захисту, інтеграція технологій кібербезпеки в енергетичні системи та операційні виклики, пов'язані з їх впровадженням. Також аналізуються слабкі сторони та обмеження сучасних підходів до захисту, приділяючи особливу увагу таким питанням, як складність систем, еволюція методів атак та обмеження існуючих механізмів захисту. Загалом у статті підкреслюється, що розуміння недоліків сучасних засобів захисту кібербезпеки є необхідним для вдосконалення стратегій захисту, зміцнення стійкості енергетичної інфраструктури та підвищення національної безпеки в контексті сучасних цифрових та гібридних загроз.

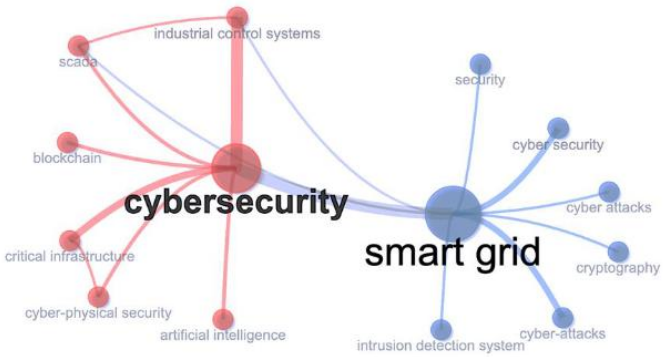

Рис. 1. Карта співвипадковості тем у проаналізованій літературі

Поява квантових комп'ютерів, здатних розшифровувати шифри (CRQC), становить серйозну загрозу для безпеки та криміналістичної цілісності систем промислового управління (ICS) та операційних технологій (OT) у критичній інфраструктурі, зокрема на атомних електростанціях. Квантові атаки, включаючи кампанії «Збирай зараз, розшифровуй пізніше» (HNDL) з використанням таких алгоритмів, як алгоритм Шора, можуть порушити існуючі криптографічні засоби захисту, підірвати цифрові докази та сприяти складним саботажам. У статті [2] представлено криміналістично-орієнтовану структуру для досягнення квантової стійкості в середовищах з високими наслідками. У ній аналізуються квантові загрози в архітектурі Purdue та демонструється, як зловмисники можуть використовувати тривалі життєві цикли OT та криптографічні монокультури для атак на системи безпеки та створення криміналістичних викликів (рис. 2). Для зменшення цих ризиків у дослідженні пропонується поетапна стратегія переходу до

постквантової криптографії (PQC), що включає гібридний обмін ключами, криптографічну різноманітність, безпечну синхронізацію часу та реалізації, стійкі до бокових каналів, що відповідають стандартам ISA/IEC 62443 та NIST. Загалом, у статті наголошується на нагальній потребі у засобах кібербезпеки, стійких до квантових загроз, для захисту операцій критичної інфраструктури та збереження цілісності цифрових криміналістичних доказів у майбутніх сценаріях квантових загроз.

Crypto Type	Algorithms	Variants	Key Length (bits)	Strengths (bits)		Vulnerabilities	Quantum Threats (STRIDE)	Possible QC-resistant Solutions
				Classic	Quantum			
Asymmetric	ECC [42], [43]	ECC 256	256	128	0	Broken by Shor's Algorithm [6].	For digital signatures: • **Spoofing:** Complete signature forgery capability. • **Tampering:** Integrity checks can be bypassed. • **Repudiation:** Valid signatures can be forged. For KEM/ENC: • **Info. Disclosure:** All encrypted data can be decrypted.	PQC migration (CRYSTALS-Dilithium, Kyber, SPHINCS+), hybrid implementations, crypto-agility frameworks.
		ECC 384	384	192	0			
		ECC 521	521	260	0			
	FFDHE [44]	DHE2048	2048	112	0			
		DHE3072	3072	128	0			
	RSA [45]	RSA 1024	1024	80	0			
		RSA 2048	2048	112	0			
		RSA 3072	3072	128	0			
Symmetric	AES [46]	AES 128	128	128	64	Weakened by Grover's Algorithm [7].	• **Info. Disclosure:** Effective key strength halved, enabling faster brute-force attacks.	Upgrade to Advanced Encryption Standard (AES)-256; strengthen key management.
		AES 192	192	192	96			
		AES 256	256	256	128			
	SHA2 [47]	SHA 256	-	128	85†	Weakened by Brassard et al.'s Algorithm [48].	• **Spoofing:** Fake hash values can be created. • **Tampering:** Data integrity compromised by finding collisions.	Upgrade to SHA-384/512; enhanced integrity verification.
		SHA 384	-	192	128†			
		SHA 512	-	256	170†			
	SHA3 [47]	SHA3 256	-	128	85†			
		SHA3 384	-	192	128†			
		SHA3 512	-	256	170†			

Рис. 2. Класична криптографія та квантова криптографія: аналіз судових та операційних ризиків у контексті OT/ICS

Промислові системи управління (ICS), що забезпечують функціонування критичної інфраструктури, потребують структурованої оцінки ризиків у сфері кібербезпеки для встановлення надійних та обґрунтованих вимог безпеки для середовищ промислової автоматизації. З огляду на останні досягнення у сфері великих мовних моделей (LLM) зростає інтерес до того, чи можуть ці системи сприяти процесам оцінки ризиків на ранніх етапах відповідно до стандарту IEC 62443-3-2, а також до того, як результати їхньої роботи відрізняються залежно від моделі. У цій статті [3] представлено якісне порівняння «ШІ проти ШІ» артефактів оцінки ризиків за стандартом IEC 62443, згенерованих у контрольованих умовах однопрохідного проходження з використанням спільної моделі системи та стандартизованої структури завдань на основі стандарту IEC 62443-3-2 (рис. 3). У дослідженні порівнюються результати моделей у трьох вимірах: еволюція моделей у межах одного сімейства LLM, порівняння передових моделей різних постачальників та порівняння моделей преміум-рівня з базовими передовими моделями. Оцінка зосереджується на структурі оцінки, архітектурній узгодженості та внутрішній узгодженості з принципами стандарту IEC 62443, а не на порівнянні із зовнішніми еталонними даними. Результати показують значні відмінності в тому, як моделі структурують сценарії загроз, визначають деталізацію зонування, призначають цільовірівні безпеки (SL-T) та враховують операційні припущення. Ці висновки висвітлюють як можливості, так і обмеження використання великих мовних моделей (LLM) як інструментів підтримки прийняття рішень на початкових етапах оцінки ризиків кібербезпеки об'єктів критичної інфраструктури. Дослідження свідчить про те, що, хоча великі мовні моделі можуть сприяти структурованому аналізу та прискорювати процес документації, специфічні особливості моделей можуть впливати на якість та послідовність оцінки, що підкреслює незмінну важливість експертного нагляду у процесі планування безпеки об'єктів критичної інфраструктури.

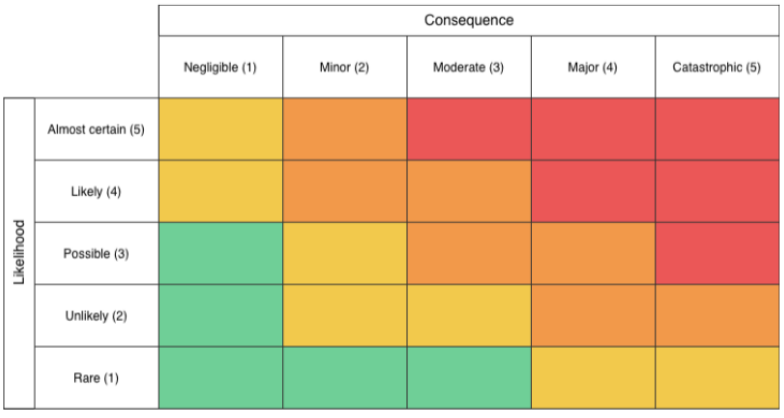

Рис. 3. Матриця ризиків, що відображає ймовірність (1–5) та наслідки (1–5) за чотирма рівнями ризику

У міру все більшої цифровізації промислових систем конвергенція інформаційних технологій (IT) та операційних технологій (OT) породила нові виклики у сфері кібербезпеки. Хоча IT-системи користуються перевагами відпрацьованих методів забезпечення безпеки, середовища OT, що керують критичною інфраструктурою, такою як енергетичні, виробничі та транспортні системи, часто залишаються вразливими до кіберзагроз. Оскільки порушення роботи OT можуть спричинити операційні ризики та ризики для безпеки, забезпечення захисту цих систем стало головним пріоритетом. У цій статті [4] представлено стратегічний план дій для організацій, які розпочинають свою діяльність у сфері кібербезпеки OT. Починаючи з мінімального рівня безпеки, у ній окреслено впровадження стандарту ISO/IEC 27001 як основи для управління інформаційною безпекою (рис. 4). Далі у статті описано перехід до стандарту ISA/IEC 62443 – системи стандартів, спеціально розробленої для систем промислової автоматизації та управління. Цей перехід передбачає впровадження заходів захисту, специфічних для OT, таких як управління ризиками, сегментація мережі, зони безпеки та стратегії глибокого захисту. Крім того, у статті підкреслюється важливість постійного моніторингу, виявлення загроз, реагування на інциденти та навчання персоналу для забезпечення як безперебійності роботи, так і стійкості кібербезпеки. Загалом, дослідження надає практичні рекомендації та найкращі практики для організацій, які прагнуть забезпечити безпеку середовищ OT та захистити критичну інфраструктуру від постійно мінливих кіберзагроз.

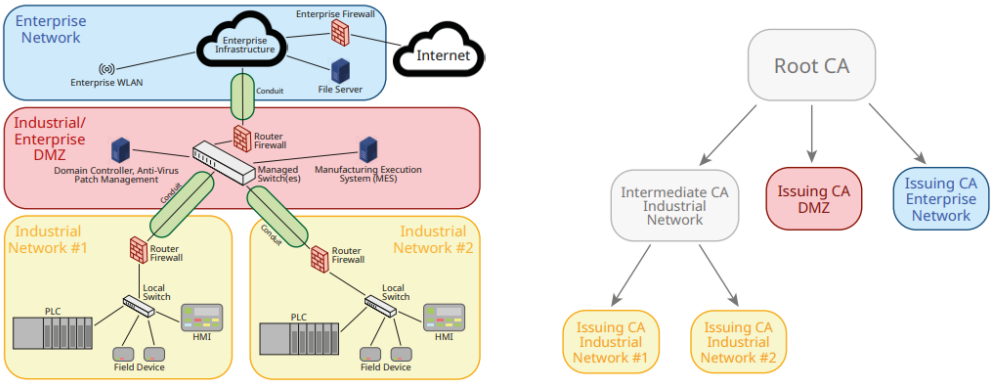

Рис. 4. Спрощена ієрархія CA, відображена у зоновій моделі на основі стандарту ISA/IEC 62443

Директива NIS2 встановлює більш суворі вимоги щодо кібербезпеки та повідомлення про інциденти для критично важливих суб'єктів, зокрема операторів енергетичного сектору. Однак багато організацій стикаються з труднощами у перетворенні цих юридичних зобов'язань на ефективні щоденні заходи безпеки, особливо в середовищах операційних технологій (OT), де можливості візуалізації та скоординованого реагування часто є обмеженими. У цій статті [5] розглядається, як SecureAI – інструмент виявлення та збагачення аномалій на основі штучного інтелекту в екосистемі розвідки кіберзагроз (CTI) – може сприяти дотриманню ключових вимог NIS2. Дослідження поєднує якісний кабінетний аналіз, порівняльне зіставлення функцій SecureAI зі статтями 20–26 NIS2 та сценарій, орієнтований на OT, на основі останніх моделей вторгнень. Аналіз показує, що SecureAI може виявляти аномальну активність у телеметрії мережі та хостів, збагачувати сповіщення контекстуальною інформацією про активи та події, а також генерувати структуровані результати для підтримки прийняття рішень операторами. Інтегровані з інфраструктурою CTI, ці сповіщення можуть бути перетворені на об'єкти STIX/TAXII для звітності, документації та обміну інформацією. Модельований сценарій вторгнення, що включає несанкціонований віддалений доступ та підозрілу активність HMI-PLC, демонструє, як система підтримує виявлення аномалій, аналіз інцидентів та робочі процеси звітності. Загалом, це дослідження підкреслює потенціал інструментів CTI на основі штучного інтелекту для посилення заходів з кібербезпеки в сфері операційних технологій, а також сприяння практичній реалізації вимог щодо відповідності NIS2.

У цій статті [6] представлено порівняльний аналіз стандартів «Захисту критичної інфраструктури» Північноамериканської корпорації з надійності електропостачання (NERC-CIP) та концепції кібербезпеки Національного інституту стандартів і технологій (NIST). У дослідженні розглядаються їхні сильні та слабкі сторони, а також проблеми, пов'язані з впровадженням цих стандартів у сфері захисту систем критичної інфраструктури. Хоча NERC-CIP встановлює обов'язкові вимоги до кібербезпеки для магістральних електромереж, система NIST пропонує гнучкий та добровільний підхід до більш широкого управління ризиками кібербезпеки (рис. 5). У статті підкреслюється, як ці дві системи можуть доповнювати одна одну

для підтримки розвитку стійкої та безпечної інфраструктури. У ній пропонується комплексна стратегія кібербезпеки, що поєднує визначення пріоритетів на основі ризиків, принципи глибокої оборони, постійний моніторинг та міжорганізаційну співпрацю. Крім того, у дослідженні наголошується, що лише дотримання нормативних вимог є недостатнім для протидії мінливим кіберзагрозам. Тому рекомендується впроваджувати передові методи виявлення загроз, архітектури «нульової довіри» та навчання з питань кібербезпеки для подальшого зміцнення рівня безпеки організацій, що відповідають за критичну інфраструктуру. Загалом у статті показано, що поєднання структурованого підходу до дотримання вимог NERC-CIP з гнучким підходом до управління ризиками NIST може забезпечити більш ефективну та комплексну систему кібербезпеки для захисту критичної інфраструктури.

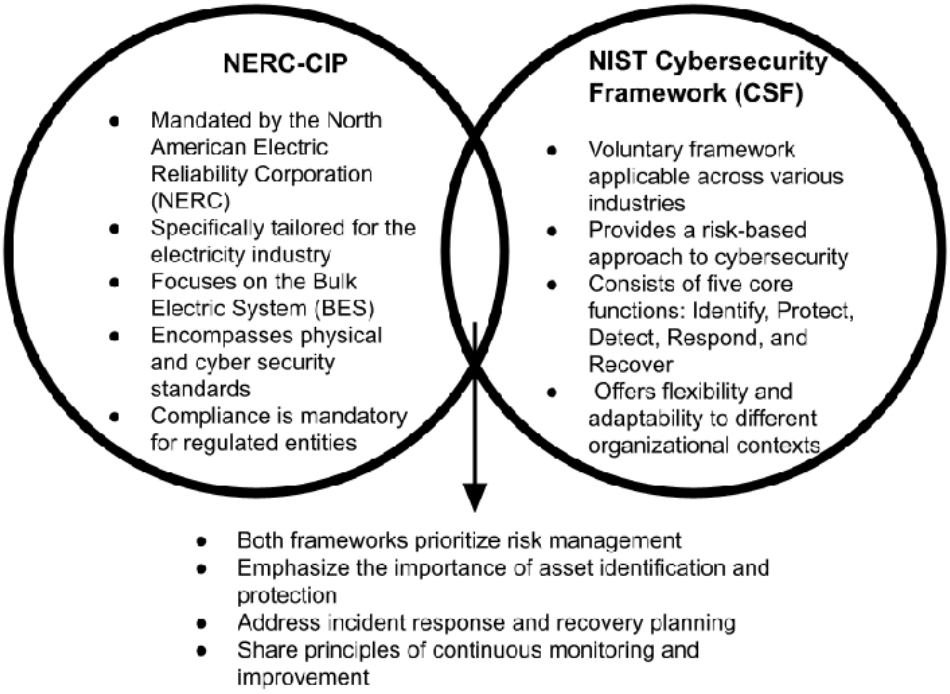

Рис. 5. Відмінності та подібності між NERC та NIST

У цьому дослідженні [7] розглядається дедалі актуальніша проблема забезпечення безпеки комунікацій SCADA, що передаються через оптоволоконні мережі з використанням оптичного заземлюючого проводу (OPGW) та повністю діелектричних самонесучих кабелів (ADSS) у рамках великих електроенергетичних систем США (рис. 6). Хоча оптоволоконні канали зв’язку забезпечують високу технічну ефективність, вони залишаються вразливими до кіберзагроз, фізичних та експлуатаційних загроз, які можуть вплинути на прозорість системи, цілісність команд та загальну стійкість. У дослідженні пропонується та емпірично оцінюється інженерна структура, що відповідає вимогам NERC CIP, призначена для підвищення безпеки та стійкості комунікацій SCADA. У дослідженні розглядається вплив інженерних засобів безпеки, захисту каналів зв'язку, заходів контролю доступу, можливостей моніторингу та виявлення, а також відповідності стандартам NERC CIP на захист середовищ SCADA. Використовуючи кількісний поперечний дизайн, було зібрано дані від 220 фахівців, які працюють у сферах експлуатації комунальних мереж, кібербезпеки, інженерії SCADA та забезпечення відповідності вимогам. Статистичний аналіз продемонстрував високу надійність та значущі позитивні взаємозв’язки між усіма дослідженими факторами безпеки та стійкістю комунікацій SCADA. Серед оцінених змінних здатність до моніторингу та виявлення виявилася найсильнішим предиктором ефективності безпеки. Результати також показали, що середовища ADSS сприймаються як більш вразливі, ніж середовища OPGW, що підкреслює необхідність стратегій захисту, специфічних для конкретних засобів комунікації. Загалом, у дослідженні наголошується на важливості поєднання технічних засобів контролю, постійного моніторингу, управління доступом та дотримання нормативних вимог для підвищення стійкості критично важливих систем зв’язку комунальних підприємств та покращення захисту кібербезпеки в сучасних інфраструктурах SCADA.

Рис. 6. Система управління дотриманням вимог CIP від NERC у системах магістральних електромереж

Системи критичної інфраструктури стають дедалі вразливішими до складних і розвинених кіберзагроз, що зумовлює зростаючу потребу в проактивних та інтелектуальних рішеннях у сфері кібербезпеки. У цьому дослідженні [8] представлено систему аналізу загроз на основі штучного інтелекту, що базується на Рамках кібербезпеки NIST (NIST CSF) і призначена для забезпечення захисту середовищ критичної інфраструктури в режимі реального часу. Запропонована система поєднує основні функції NIST CSF – ідентифікацію, захист, виявлення, реагування та відновлення – з передовими технологіями штучного інтелекту для забезпечення безперервного моніторингу, раннього виявлення загроз та адаптивного реагування на інциденти. Система використовує моделі машинного навчання та глибокого навчання для аналізу різноманітних джерел даних безпеки, включаючи мережевий трафік, системні журнали, активність кінцевих точок та канали інформації про загрози. Ці моделі на основі штучного інтелекту виявляють аномальну поведінку, корелюють події з різних джерел та прогнозують потенційні кібератаки в режимі реального часу. Централізований рівень аналітики загроз збагачує та контекстуалізує інформацію з безпеки, покращуючи ситуаційну обізнаність у взаємопов'язаних інфраструктурних системах. Крім того, платформа включає механізми автоматизованого реагування, які визначають пріоритетність та мінімізують загрози на основі ступеня ризику, дотримуючись при цьому вимог управління NIST CSF. Можливості адаптивного навчання дозволяють системі розвиватися разом із новими техніками атак, покращуючи стійкість та точність виявлення з часом. Експериментальні оцінки, проведені в модельованих середовищах критичної інфраструктури, свідчать про те, що запропонований підхід підвищує швидкість виявлення загроз, зменшує кількість помилкових спрацьовувань та підвищує ефективність реагування на інциденти порівняно з традиційними системами безпеки, що базуються на правилах. Загалом, дослідження підкреслює ефективність поєднання стандартизованого управління кібербезпекою з аналітикою загроз на основі штучного інтелекту для забезпечення масштабованого захисту сучасної критичної інфраструктури в режимі реального часу.

Штучний інтелект (ШІ) дедалі більше трансформує сектори критичної інфраструктури, такі як енергетика, водопостачання та транспорт, завдяки прогнозній аналітиці, автоматизації та прийняттю рішень у режимі реального часу. Однак впровадження ШІ в середовищах, де безпека має вирішальне значення, створює нові ризики, що виходять за межі традиційних проблем кібербезпеки, зокрема упередженість моделей, відсутність прозорості, проблеми з цілісністю даних та системні вразливості. Хоча Рамка кібербезпеки NIST (CSF) 2.0 надає рекомендації щодо управління ризиками кібербезпеки, Рамка управління ризиками ШІ NIST (AI RMF) зосереджується на надійному управлінні ШІ. У цій статті [9] представлено інтегрований підхід, який поєднує AI RMF NIST із CSF 2.0 для створення єдиної моделі управління та управління ризиками для критичної інфраструктури, що використовує ШІ. У дослідженні розроблено перехресну таблицю між двома рамками, узгоджено їхні основні функції та запропоновано стратегії впровадження, адаптовані до таких середовищ, як інтелектуальні енергомережі, системи SCADA, водопостачальні підприємства та транспортні мережі. У статті також розглядаються специфічні для

сектору ризики ШІ, зокрема суперечливі атаки, незахищені канали передачі даних та збої в системах автоматизованого прийняття рішень. Загалом, дослідження демонструє, що інтеграція управління ШІ з рамками кібербезпеки є необхідною для побудови стійких, адаптивних та надійних систем критичної інфраструктури.

Багаторівневий підхід, передбачений документом IAEA NSS 17-T, у поєднанні з жорстко обмеженим трафіком у промислових мережах підвищує значення методів приховування інформації (ІН) для кіберзлочинців (рис. 7). Приховані канали зв'язку можуть дозволити просунутим постійним загрозам (APT) залишатися невиявленими в середовищах критичної інфраструктури, що робить механізми виявлення та відновлюваності надзвичайно важливими. У цій статті [10] розглядаються приховані канали зв'язку, виявлені в промислових протоколах, таких як Modbus/TCP та OPC UA, а також у допоміжних протоколах, зокрема Syslog та NTP, у межах оновленої структури NSS 17-T. У дослідженні обговорюються потенційні вектори атак, включаючи внутрішні загрози, атаки на ланцюг постачання та несанкціонований доступ до чутливих цифрових активів. У статті також оцінюється ефективність заходів безпеки, таких як зони безпеки, контроль фізичного доступу та механізми роз'єднання потоків даних, у запобіганні кібератакам із використанням ІН. Загалом, дослідження підкреслює важливість інтеграції можливостей виявлення та стійких архітектур безпеки для посилення кібербезпеки в системах промислової та ядерної інфраструктури.

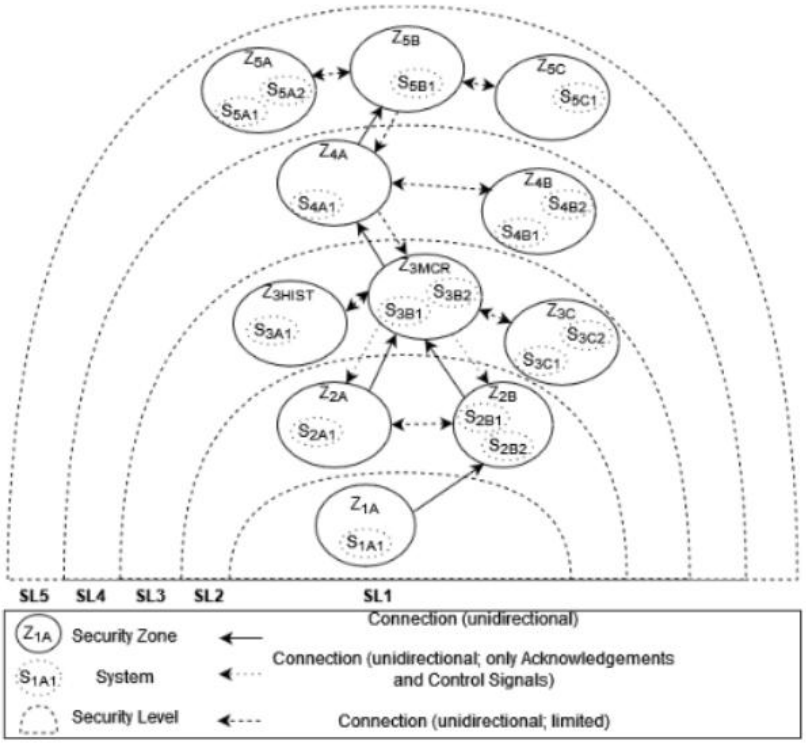

Рис. 7. Схема обміну інформацією в рамках DCSA. Приклад на основі документа IAEA NSS 17-T

Зростаюча складність кіберзагроз вимагає від організацій дотримання стандартів та рамок кібербезпеки для ефективного зниження та управління кіберризиками. Стандарт ISO/IEC 27001 пропонує структурований підхід до підвищення рівня кібербезпеки шляхом впровадження системи управління інформаційною безпекою (СУІБ). Водночас Європейська директива NIS2 вводить додаткові зобов’язання щодо кібербезпеки та звітності, які організації мають виконати, щоб досягти відповідності вимогам. У цьому дослідженні [11] пропонується чотириетапний підхід до зіставлення, розроблений для того, щоб допомогти організаціям узгодити наявні заходи контролю ISO/IEC 27001 з вимогами NIS2. Запропонована система підтримує гармонізовані практики кібербезпеки в усіх європейських державах-членах, одночасно покращуючи координацію та обмін інформацією щодо кіберзагроз. У статті також наведено детальний аналіз наявних практик ISMS та вимог, визначених Директивою NIS2. Крім того, у ній представлено порівняльне зіставлення статей, преамбули, пунктів та зобов’язань NIS2 з заходами контролю ISO/IEC

впровадження. Загалом, дослідження пропонує практичні рекомендації для організацій, які шукають ефективні та структуровані способи досягнення відповідності вимогам NIS2.

У міру все більшої цифровізації промислових систем злиття інформаційних технологій (IT) та операційних технологій (OT) породило серйозні виклики у сфері кібербезпеки. Хоча IT-системи розвивалися разом із досконалими практиками кібербезпеки, середовища OT, що керують критичною інфраструктурою, такою як енергетичні мережі, виробничі об'єкти та транспортні системи, часто залишаються вразливими до кіберзагроз. Оскільки порушення роботи середовищ OT можуть призвести до операційних збоїв та ризиків для безпеки, забезпечення захисту цих систем стало надзвичайно важливим пріоритетом. У цій статті [12] представлено стратегічний та технічний план дій для організацій, які розпочинають свій шлях до кібербезпеки OT з мінімального рівня безпеки. У ній окреслено впровадження стандарту ISO/IEC 27001 як основоположної рамки для управління інформаційною безпекою, а потім описано перехід до стандарту ISA/IEC 62443 – системи стандартів, спеціально розробленої для систем промислової автоматизації та управління. Цей перехід передбачає впровадження засобів контролю, орієнтованих на OT, таких як управління ризиками, сегментація мережі, зони безпеки та стратегії глибокої оборони. У статті також підкреслюється важливість постійного моніторингу, проактивного виявлення загроз, планування реагування на інциденти та навчання персоналу для забезпечення як безперебійної роботи, так і стійкості кібербезпеки. Загалом, це дослідження містить практичні рекомендації та передові практики для організацій, які прагнуть забезпечити безпеку операційних технологій (OT), дотримуватися нормативних вимог та посилити захист критичної інфраструктури від постійно еволюціонуючих кіберзагроз.

У цій статті [13] розглядаються стійкі засоби виявлення загроз у сфері кібербезпеки, передбачені проєктом стандарту IEC 63096 для ядерної галузі – який є подальшим розвитком стандарту IEC 62645 – з акцентом на захисті від складних постійних загроз (APT) у ядерних та промислових системах управління. Спираючись на такі атаки, як Stuxnet, дослідження підкреслює необхідність засобів виявлення, що працюють незалежно від програмного забезпечення управління процесами, щоб зловмисні маніпуляції можна було виявити навіть у разі компрометації систем управління. У статті розглядаються вибір та моніторинг критичних змінних процесу, методи збору та агрегації даних, логіка виявлення та інтеграція з системами управління інформацією та подіями безпеки (SIEM). Також досліджується, як існуючі аналізи впливу на ядерну безпеку можна адаптувати до кібербезпеки, замінивши сценарії випадкових відмов на сценарії цілеспрямованих атак. Запропонований підхід використовує концепції контролю безпеки додатків (ASC) з ISO/IEC 27034-х та відповідає вимогам ядерного стандарту IEC 62859 щодо координації безпеки та кібербезпеки. Загалом, дослідження підкреслює важливість незалежних та стійких архітектур виявлення загроз для покращення кібербезпеки в системах ядерної інфраструктури, мінімізуючи при цьому вплив на операції, критичні для безпеки.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У Проведений аналіз дозволяє стверджувати, що сучасна парадигма захисту критичної енергетичної інфраструктури остаточно змістилася від ізольованих IT-рішень до комплексних екосистем управління ризиками, де стандарти ISA/IEC 62443 та ISO/IEC 27001 виступають фундаментом для забезпечення безперервності процесів. Головним результатом трансформації галузі є визнання того, що конвергенція IT та OT вимагає не просто технічних засобів, а багаторівневої архітектури «глибокого захисту», здатної забезпечити стійкість навіть у разі компрометації окремих вузлів мережі. Впровадження Директиви NIS2 та стандартів NERC CIP перетворює кібербезпеку з рекомендаційної площини на жорстку юридичну вимогу, де відповідальність керівництва та контроль ланцюгів постачання стають обов'язковими елементами життєвого циклу будь-якої енергетичної системи.

Особливе значення має висновок щодо специфічності захисту ядерних об'єктів, де пріоритет цілісності та доступності над конфіденційністю є абсолютним, а використання ступеневого підходу згідно з IAEA NSS-17-T та IEC 62645 дозволяє ізолювати найважливіші функції безпеки від зовнішніх впливів. Проте дослідження висвітлює критичний розрив між поточними методами захисту та загрозами майбутнього, зокрема «квантовим викликом». Стратегія зловмисників «збирай зараз, розшифровуй пізніше» (HNDL) робить системи з тривалим життєвим циклом вразливими вже сьогодні, що вимагає негайного планування переходу на постквантову криптографію.

Інтеграція штучного інтелекту в системи моніторингу, як-от використання SecureAI для аналізу аномалій, демонструє високу ефективність у виявленні загроз у реальному часі, проте вона ж створює нові системні ризики, пов'язані з цілісністю даних та прозорістю алгоритмів. Ключовим вектором подальшого

розвитку має стати поєднання NIST CSF 2.0 із рамками управління ризиками ШІ (NIST AI RMF) для мінімізації суперечливих атак на моделі управління [14].

Окремої уваги потребує проблема прихованих каналів зв'язку в промислових протоколах (Modbus/TCP, OPC UA), які дозволяють просунутим загрозам APT залишатися непоміченими. Вирішенням цієї проблеми вбачається розробка та впровадження незалежних архітектур детектування, передбачених проектом IEC 63096, які здатні виявляти маніпуляції незалежно від стану основного програмного забезпечення системи управління. Для України, враховуючи постійний тиск гібридних загроз, гармонізація національних стандартів ДСТУ з вимогами NIS2 та ISA/IEC 62443 є не лише технічним завданням, а необхідною умовою для транскордонної синхронізації енергомереж та забезпечення національної безпеки. Таким чином, фокус майбутніх розробок має зміститися з реактивного реагування на створення адаптивних, квантово-стійких систем із вбудованими механізмами автономного виявлення аномалій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kreso Phd, Inda. (2025). Cybersecurity in the energy sector: an overview of defense strategies and best practices. 130-148.
2. Baseri, Yaser & Waller, Edward. (2026). Quantum Attacks Targeting Nuclear Power Plants: Threat Analysis, Defense and Mitigation Strategies. 10.48550/arXiv.2602.21524.
3. Bernard, Andreas & Pfister, Mathias. (2026). AI-Driven Risk Assessment for Critical Infrastructure Based on IEC 62443 Using Large Language Models. 10.21203/rs.3.rs-9050939/v1.
4. Heinl, Michael & Pursche, Maximilian & Puch, Nikolai & Peters, Sebastian & Giehl, Alexander. (2023). From Standard to Practice: Towards ISA/IEC 62443-Conform Public Key Infrastructures. 10.1007/978-3-031-40923-3_15.
5. Siivola, Jani & Paronen, Rami & Tariq, Uzair & Pham, Quyet & Villegas, Warren & Tikanmäki, Ilkka & Rajamäki, Jyri. (2026). Exploring NIS2 Compliance in the Energy Sector Using AI-Driven Cyber Threat Intelligence. International Conference on Cyber Warfare and Security. 21. 714-717. 10.34190/iccws.21.1.4482.
6. Chatterjee, Suchismita. (2021). A Comparative Study between NERC-CIP and NIST Compliance-Defining the Critical Framework for Building Cyberrisk Free Infrastructure. ESP Journal of Engineering & Technology Advancements. 1. 273-281. 10.56472/25832646/JETA-V1I1P129.
7. Mosharraf, Abu. (2026). Securing SCADA Communications Over OPGW And ADSS Fiber In U.S. Bulk Electric Systems: A NERC CIP-Aligned Engineering Framework. American Journal of Advanced Technology and Engineering Solutions. 06. 416-459. 10.63125/hn42nw39.
8. Jean, Guillaume & Smith, Hussein. (2026). NIST Cybersecurity Framework-Driven AI Threat Intelligence System for Real-Time Critical Infrastructure Protection.
9. Kate, Austin. (2026). Integrating the NIST AI Risk Management Framework with Cybersecurity Framework Profiles for Sector-Specific Critical Infrastructure (Energy, Water, Transportation).
10. Lamshöft, Kevin & Hildebrandt, Mario & Altschaffel, Robert & Keil, Oliver & Hempel, Ivo & Dittmann, Jana & Neubert, Tom & Vielhauer, Claus. (2022). Resilience Against and Detection of Information Hiding in Nuclear Instrumentation and Control Systems within the Scope of NSS 17-T.
11. Khalid Bennouk, Dorra Mahouachi, Nawal Ait Aali, Youness El Bouzekri El Idrissi, Bechir Sebai, Abou Zakaria Faroukhi (2026). From Standards to Regulation Compliance: Leveraging ISO/IEC 27001 to Apply the NIS2 Directive. 10.4018/979-8-2600-0888-1.ch009.
12. Alenezi, Ali. (2024). Securing OT Devices: A Comprehensive Journey from Zero to Compliance with ISO/IEC 27001 and ISA/IEC 62443. 10.13140/RG.2.2.17672.02560
13. Gupta, Deeksha & Waedt, Karl & Gao, Yuan. (2018). Detective Application Security Controls for Nuclear Safety.
14. Dobrynchuk, O., & Lukashenko, V. (2025). Energy critical infrastructure under attack: incident analysis and implications for ICS/SCADA resilience . Ukrainian Scientific Journal of Information Security, 31(2), 112–129. https://doi.org/10.18372/2225-5036.31.20706

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Oleksandr O. Dobrynchuk
Junior Researcher
National University "Kyiv Aviation Institute", Kyiv, Ukraine
ORCID: 0009-0002-2877-844X
oleksandr.dobrynchuk@npp.kai.edu.ua

Viktoriia V. Lukashenko
Doctor of Technical Sciences, Professor, Director of the Management for Educational and Scientific Activities
National University "Kyiv Aviation Institute", Kyiv, Ukraine
ORCID: 0009-0009-0458-2590
viktoriia.lukashenko@kai.edu.ua

Serhii A. Hrychuk
Senior Lecturer
Ukrainian Military Medical Academy, Kyiv, Ukraine
ORCID: 0009-0008-4799-597X
sg03111975dok@gmail.com

LEGAL AND REGULATORY FRAMEWORK FOR ENSURING CYBERSECURITY IN THE ENERGY SECTOR

Abstract. The article conducts a comprehensive study of modern regulatory and technical approaches to ensuring cybersecurity in the energy sector amidst large-scale digitalization and the rise of hybrid threats. The relevance of the research is driven by the active convergence of information technology (IT) and operational technology (OT), which opens new attack vectors against industrial automation and control systems (IACS), such as SCADA, DCS, and PLCs. Special attention is paid to the specifics of protecting Ukraine's critical infrastructure, whose power grids have already been targets of sophisticated attacks, such as CrashOverride/Industroyer, necessitating immediate system hardening in line with international standards. The study provides a detailed overview of key international standards, including the ISA/IEC 62443 series, which implements the concept of zones, conduits, and security levels (SL 1–4) to minimize the risks of sabotage and interference in energy facility operations. The impact of the NIS2 Directive is analyzed, as it establishes mandatory requirements for risk management, supply chain security, and leadership accountability for entities of high criticality. The role of NERC CIP standards in ensuring the reliability of the bulk electric system and the flexible approach of NIST CSF 2.0 combined with the C2M2 maturity model are examined separately. Significant attention is devoted to the protection of nuclear energy based on IAEA NSS-17-T and IEC 62645 standards, where the priority of integrity and availability over confidentiality is critical to preventing radiation incidents. The article analyzes the graded approach to protecting sensitive digital assets (SDA) and the deterministic isolation of critical systems as per the NEI 08-09 model. The research results highlight future challenges, particularly the "quantum threat" and the "harvest now, decrypt later" (HNDL) adversary strategy, which requires a transition to post-quantum cryptography (PQC). The potential of artificial intelligence (tools like SecureAI) for automated anomaly detection in industrial protocols such as Modbus/TCP and OPC UA is highlighted, along with the need to integrate AI risk management through the NIST AI RMF. The conclusions emphasize that for Ukraine, the harmonization of national DSTU standards with European norms is a necessary condition for the cross-border synchronization of power grids and ensuring national resilience.

Keywords: cybersecurity; energy sector; critical infrastructure; NIS2 Directive; ISA/IEC 62443; operational technology; nuclear safety; risk management; quantum resilience; artificial intelligence.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Kreso Phd, Inda. (2025). Cybersecurity in the energy sector: an overview of defense strategies and best practices. 130-148.
2. Baseri, Yaser & Waller, Edward. (2026). Quantum Attacks Targeting Nuclear Power Plants: Threat Analysis, Defense and Mitigation Strategies. 10.48550/arXiv.2602.21524.
3. Bernard, Andreas & Pfister, Mathias. (2026). AI-Driven Risk Assessment for Critical Infrastructure Based on IEC 62443 Using Large Language Models. 10.21203/rs.3.rs-9050939/v1.
4. Heinl, Michael & Pursche, Maximilian & Puch, Nikolai & Peters, Sebastian & Giehl, Alexander. (2023). From Standard to Practice: Towards ISA/IEC 62443-Conform Public Key Infrastructures. 10.1007/978-3-031-40923-3_15.
5. Siivola, Jani & Paronen, Rami & Tariq, Uzair & Pham, Quyet & Villegas, Warren & Tikanmäki, Ilkka & Rajamäki, Jyri. (2026). Exploring NIS2 Compliance in the Energy Sector Using AI-Driven Cyber Threat Intelligence. International Conference on Cyber Warfare and Security. 21. 714-717. 10.34190/iccws.21.1.4482.
6. Chatterjee, Suchismita. (2021). A Comparative Study between NERC-CIP and NIST Compliance-Defining the Critical Framework for Building Cyberrisk Free Infrastructure. ESP Journal of Engineering & Technology Advancements. 1. 273-281. 10.56472/25832646/JETA-V1I1P129.
7. Mosharraf, Abu. (2026). Securing SCADA Communications Over OPGW And ADSS Fiber In U.S. Bulk Electric Systems: A NERC CIP-Aligned Engineering Framework. American Journal of Advanced Technology and Engineering Solutions. 06. 416-459. 10.63125/hn42nw39.
8. Jean, Guillaume & Smith, Hussein. (2026). NIST Cybersecurity Framework-Driven AI Threat Intelligence System for Real-Time Critical Infrastructure Protection.
9. Kate, Austin. (2026). Integrating the NIST AI Risk Management Framework with Cybersecurity Framework Profiles for Sector-Specific Critical Infrastructure (Energy, Water, Transportation).
10. Lamshöft, Kevin & Hildebrandt, Mario & Altschaffel, Robert & Keil, Oliver & Hempel, Ivo & Dittmann, Jana & Neubert, Tom & Vielhauer, Claus. (2022). Resilience Against and Detection of Information Hiding in Nuclear Instrumentation and Control Systems within the Scope of NSS 17-T.
11. Khalid Bennouk, Dorra Mahouachi, Nawal Ait Aali, Youness El Bouzekri El Idrissi, Bechir Sebai, Abou Zakaria Faroukhi (2026). From Standards to Regulation Compliance: Leveraging ISO/IEC 27001 to Apply the NIS2 Directive. 10.4018/979-8-2600-0888-1.ch009.
12. Alenezi, Ali. (2024). Securing OT Devices: A Comprehensive Journey from Zero to Compliance with ISO/IEC 27001 and ISA/IEC 62443. 10.13140/RG.2.2.17672.02560.
13. Gupta, Deeksha & Waedt, Karl & Gao, Yuan. (2018). Detective Application Security Controls for Nuclear Safety.
14. Dobrynchuk, O., & Lukashenko, V. (2025). Energy critical infrastructure under attack: incident analysis and implications for ICS/SCADA resilience. Ukrainian Scientific Journal of Information Security, 31(2), 112–129. https://doi.org/10.18372/2225-5036.31.20706

Отримано редакцією журналу / Received: 07.03.26
Прорецензовано / Revised: 20.03.26
Схвалено до друку / Accepted: 25.06.26