Куклінова Тетяна Вікторівна
к.е.н., доцент, доцент кафедри кібербезпеки,
Національний університет «Одеська юридична академія»

ІНТЕЛЕКТУАЛІЗАЦІЯ КІБЕРЗАХИСТУ ЕНЕРГЕТИЧНИХ ПІДПРИЄМСТВ: УПРАВЛІНСЬКИЙ ПІДХІД

DOI https://doi.org/10.36059/978-966-397-537-5-3

Сучасний етап цифрової трансформації суспільства супроводжується стрімким зростанням кіберзагроз, що особливо актуально для об'єктів критичної інфраструктури, зокрема енергетичного сектора. Енергетичні системи стають дедалі складнішими й водночас більш вразливими через активне впровадження цифрових технологій, систем автоматизації та дистанційного управління. Зловмисники дедалі частіше обирають енергетичні об'єкти як мішень для кібернападів, що може мати катастрофічні наслідки для економіки, національної безпеки та добробуту громадян. У зв'язку з цим зростає потреба у впровадженні інноваційних підходів до управління кіберзахистом енергетичних систем. Одним із найбільш перспективних рішень є використання технологій штучного інтелекту (ШІ), здатних забезпечити адаптивний, гнучкий та ефективний захист від динамічних кіберзагроз. Так, ШІ дає змогу в режимі реального часу аналізувати великі обсяги даних, виявляти аномалії, прогнозувати атаки та оперативно реагувати на кіберінциденти тощо.

У попередніх дослідженнях нами досліджувалися процеси системного впровадження ШІ в енергетичних компаніях, було надано визначення дефініції «системи ШІ», [1]. Також ми розглядали ключові переваги та інструменти ШІ в кібербезпеці енергогалузі, [2]. Незважаючи на зростаючу кількість досліджень у сфері кіберменеджменту таких вчених як Бойка В., Горбаченко С., Денисенко Г., Колодінського І., Федик В., Фроловой Я. та інших, існує потреба в системному науковому підході до інтеграції управління кібербезпекою в енергетиці з урахуванням можливостей ШІ.

Надійне енергопостачання є критично важливим для забезпечення національної безпеки. Вразливість енергетичної

інфраструктури призвела до серйозних соціально-економічних наслідків для України. Руйнування енергетичних об'єктів та фінансова нестабільність енергетичних компаній значно ускладнили ситуацію в енергетичному секторі України. Проблеми з енергетичними ресурсами спричиняють перебої в енергопостачанні, що, у свою чергу, негативно впливає на інші сектори економіки та населення. Розумні мережі дозволяють ефективно керувати енергетичними ресурсами, зменшують вплив на навколишнє середовище та підвищують енергетичну безпеку. Подальший розвиток у цій галузі вимагає синергії між урядом, бізнесом та академічними колами. Успішна цифровізація енергетичного сектору сприятиме створенню більш сталої, екологічно чистої та ефективної енергетичної системи у повоєнний період. Об'єктом дослідження є процеси управління кібербезпекою в енергетичному секторі.

Предметом дослідження виступають методи та моделі використання технологій ШІ для підвищення ефективності управління кіберзахистом енергетичних систем.

Метою дослідження є обґрунтування та розробка науково-методичних засад управління кіберзахистом енергетичного сектору з використанням технологій ШІ для підвищення ефективності виявлення, реагування та протидії сучасним кіберзагрозам.

Завдання дослідження:

1. Проаналізувати сучасний стан енергетичного сектора України.
2. Дослідити стан впровадження ШІ в енергомережі України.
3. Визначити основні вимоги до ефективної системи управління кібербезпекою в енергетиці.
4. Розробити шляхи управління кіберзахистом із застосуванням ШІ.

Енергетичні підприємства відіграють ключову роль в економічному розвитку будь-якої країни. Вони забезпечують безперебійне постачання електроенергії, тепла та палива, що є основою функціонування всіх галузей економіки. Без ефективної енергетичної системи неможливе стабільне виробництво, функціонування транспорт, зв'язку, сфери охорони здоров'я та інші сфери. Саме енергетика формує базу для індустріального, аграрного та цифрового секторів. Рівень розвитку енергетичних підприємств прямо впливає на конкурентоспроможність країни на світовому ринку.

Енергетичні підприємства належать до критичної інфраструктури держави. Їх стабільна робота є необхідною умовою життєдіяльності населення та функціонування державних інституцій. Порушення в роботі електростанцій, підстанцій чи газових магістралей можуть призвести до масштабних соціальних і економічних наслідків. Саме тому захист енергетичної інфраструктури є пріоритетом національної політики. Кібербезпека енергетичних підприємств – це не лише технологічне, а й стратегічне завдання. Використання цифрових технологій у енергетиці підвищує ефективність, але одночасно створює нові ризики. Тому енергетичний сектор потребує надійної системи кіберзахисту. Інвестиції в безпеку енергетичних підприємств – це інвестиції в стабільність України.

Крім того, енергетика забезпечує енергетичну незалежність та зміцнює національну безпеку. На тлі війни та гібридних загроз енергетичні об'єкти стали однією з головних мішеней для атак.

Таблиця 1 – Найпотужніші кібератаки на енергооб'єкти за період 2011–2024 р. [2]

Рік	Назва атаки	Ціль	Мета атаки
2011–2014	Dragonfly / Energetic Bear	Енергетичні компанії по всьому світу	Серія кібератак, зосереджених на тактиках, мотивах і наслідках для інтелектуальних мереж.
2017	NotPetya Ransomware	Енергетичні компанії по всьому світу	Порушення роботи систем енергоменеджменту, зв'язку та білінгу.
2016–2018	Industroyer / CrashOverride	Israel Electric Corporation	Серія атак на інфраструктуру електромереж, що спричинила масштабні збої.
2022–2024	Sandworm / Industroyer2	ДТЕК, енергетичні системи України	Багатоепізодні кібератаки з використанням нових методів впливу на системи керування й ОТ.

Кібератаки часто здійснюються злочинними угрупованнями, хактивістами або акторами, пов'язаними з державами, які мають конкретні цілі, такі як викрадення інтелектуальної власності, порушення роботи критичної інфраструктури або ведення шпигунської діяльності. Ці атаки можуть бути особливо руйнівними, оскільки вони спеціально адаптовані до конкретної цілі та часто залишаються непоміченими протягом тривалого часу. Починаючи з 2011 року, 84 % жертв, які постраждали від атак Dragonfly, належали до енергетичного та електроенергетичного сектору. Це свідчить про те, що більшість зусиль цієї групи були спрямовані на компрометацію критично важливої енергетичної інфраструктури, створюючи серйозні загрози для безпеки та стабільності енергосистем [3].

Так, Dragonfly (Energetic Bear) є однією з наймасштабніших і найтриваліших кібершпигунських операцій, спрямованих проти енергетичного сектору. Вперше активність цієї хакерської групи була зафіксована у 2011 році, з піковою інтенсивністю у період 2011–2014 рр. Основною метою атак були енергетичні компанії у США, Канаді та країнах Європи, з особливим акцентом на постачальників енергетичних технологій та операторів критичної інфраструктури. Так, група Dragonfly використовувала широкий спектр кіберзасобів, зокрема фішингові листи, шкідливі вебсайти, компрометацію оновлень програмного забезпечення та бекдори, вбудовані в легітимні програми. Однією з ключових особливостей було використання легальних інструментів адміністрування, що дозволяло хакерам залишатися непоміченими протягом тривалого часу.

Промисловість та ЖКГ споживають близько 80 % всіх енергоресурсів в країні і мають одні з найнижчих показників енергоефективності, а відповідно і найвищий потенціал її підвищення. Що також має ряд природоохоронних (екологічних) та соціальних ефектів. До екологічних можна віднести: зменшення спожитої енергії; зменшення викиду шкідливих речовин в навколишнє середовище; покращення загальної екологічної ситуації в регіоні. Серед соціальних впливів: можливість збільшення заробітних плат працівникам; збереження старих і створення нових робочих місць; покращення здоров'я та безпеки працівників; покращення корпоративної культури й зміцнення корпоративних цінностей.

Забезпечення стійкості енергетичної системи є необхідною умовою для швидкого повоєнного відновлення. Саме через енергетичну інфраструктуру реалізуються реформи зеленої трансформації та переходу до відновлюваних джерел енергії. Енергетичні підприємства – це також значне джерело бюджетних надходжень та зайнятості. Збереження та модернізація енергетичного комплексу – це фундамент для довгострокового економічного зростання.

Зазначимо, що виробниками електроенергії в Україні є 4 атомні електростанції, 15 теплових електростанцій (2 залишилися на неконтрольованій території), 43 теплові електростанції (10 розташовані на неконтрольованій території). Основою гідроенергетики України є каскад із 6 великих гідроелектростанцій на Дніпрі, а також Ташлицька гідроакумулююча електростанція на річці Південний Буг. Загалом працює 8 гідроелектростанцій та 3 гідроакумулюючі електростанції. Найбільшими приватними енергетичними компаніями в Україні є:

– ДТЕК (80 % теплової генерації країни) та інфраструктура збуту енергії та енергосервісна компанія.

– VS Energy – друга за величиною приватна енергетична компанія в Україні, яка контролює близько 1/3 ринку передачі енергії через локальні мережі в країні. Вона контролює «Київобленерго», «Рівнеобленерго», «Херсонобленерго», «Кіровоградобленерго», «Житомирobленерго», «Одесаобленерго», «Чернівціобленерго», «Севастопольенерго», група також має частку в «Ніколаєвобленерго» та «Хмельницькобленерго».

– «Укренергоконсалтинг» – холдингова компанія, яка контролює енергопостачальні компанії «Львівобленерго» та «Прикарпаттяобленерго».

Внаслідок російського вторгнення енергетичний сектор зазнав прямих збитків та непрямих фінансових збитків у розмірі 56,5 млрд доларів. Потреби у відновленні, що включають повну реконструкцію зруйнованих об’єктів за принципом «Відбудувати краще, ніж було», становлять 50,5 млрд доларів. Прямі збитки енергетичного сектору України станом на травень 2024 року становлять понад 16,1 млрд доларів. Найбільші збитки завдано руйнуванням об’єктів виробництва електроенергії (8,5 млрд доларів),

магістральних ліній електропередачі (2,1 млрд доларів), а також нафтогазової інфраструктури (3,3 млрд доларів) [4]. Мохор В. підкреслює, що з початком активних бойових дій енергетичний сектор України став об'єктом безперервних ракетних та артилерійських атак з боку російського агресора та станом на 30 квітня 2023 р. в секторі електроенергетики України загальна генеруюча потужність електростанцій зменшилася з 36 до 18,3 ГВт (на 51 %) [5, с. 75]. Під час нещодавніх обстрілів Україна втратила приблизно 25 % від загального споживання електроенергії. Основна маневрена генерація, включаючи гідро- та теплоелектростанції, втратила близько 80 % своєї потужності, тоді як атомна енергетика не в змозі оперативно задовольнити збільшений попит на електроенергію [6].

Загальновідомо, що процес перетворення енергії на електроенергію неминуче супроводжується викидами CO^2, особливо коли використовуються традиційні викопні джерела. Надмірна концентрація вуглекислого газу в атмосфері порушує природний баланс і сприяє глобальним кліматичним змінам. У той час як попит на електроенергію у світі постійно зростає, зростає і потреба в екологічно чистих, сталих джерелах її виробництва. Саме тому розвиток «зеленої» енергетики – на основі сонця, вітру, води та біомаси – стає критично важливим. Впровадження відновлюваних джерел енергії дозволяє не лише зменшити викиди CO^2, а й забезпечити довгострокову енергетичну безпеку, економічну ефективність і збереження довкілля для майбутніх поколінь.

За останні роки кількість промислових сонячних та вітрових електростанцій значно зросла. Більшість із них розташовані в південних регіонах України. Активний розвиток відновлюваної енергетики в Україні розпочався після прийняття «зеленого тарифу» у 2008 році, згідно з яким електроенергія, вироблена з енергії сонця, вітру тощо, закуповується в системі за ціною, що значно вища за ринкову. Чинна програма стимулювання розвитку відновлюваної енергетики розрахована до 2030 року. Водночас передбачається поступове зниження вартості «зеленої» електроенергії. Виробництво електроенергії з альтернативних джерел має зрости з 10 у 2023 році до 25–30 % до 2030 року [7].

В енергетичному секторі існують бар'єри, які уповільнюють впровадження змін. Один із головних – консервативне ставлення до нових

технологій, що часто зумовлене побоюваннями щодо їхньої ефективності та впливу на чинні бізнес-процеси. Багато енергокомпаній усе ще не завершили цифрову трансформацію, що потребує додаткових фінансових ресурсів та оновлення управлінських структур. Також значною проблемою залишається нестача кваліфікованих кадрів і залежність від застарілого обладнання, що ускладнює інтеграцію інновацій.

Кібербезпека і цифрова сталість енергогалузі взаємопов'язані, адже захист цифрових систем є основою їхньої стійкості. Проте на шляху впровадження технологій виникають труднощі, зокрема висока вартість, потреба у навчанні персоналу, стандартизації даних і забезпеченні конфіденційності.

Подолати цифрову інертність можна шляхом посилення внутрішньої комунікації, інвестування в підвищення кваліфікації працівників та активної підтримки з боку управлінців. Формування цифрової стійкості є необхідною умовою для модернізації енергетики та досягнення цілей сталого розвитку. Технології Smart Grid відкривають нові можливості для ефективного управління енергоресурсами, зменшення шкідливого впливу на довкілля та підвищення надійності енергосистем. Успішна цифровізація енергетичної галузі можлива лише за умов тісної взаємодії між державою, бізнесом та науковою спільнотою, що дозволить створити інноваційну, стійку та безпечну енергосистему. Атаки на Smart Grid можуть мати катастрофічні наслідки – від локальних збоїв до масштабних блекаутів.

Значна частина енергетичної інфраструктури України була збудована ще в радянський період і сьогодні перебуває у критичному стані, вимагаючи термінової модернізації. Застаріле обладнання функціонує з низькою ефективністю, спричиняючи суттєві втрати енергії та знижуючи надійність постачання. Фокусування на розвитку енергоефективного потенціалу сприятиме раціоналізації використання енергетичних ресурсів в Україні, зміцненню енергетичної безпеки, динамізації економічного зростання та формуванню передумов для сталого екологічного розвитку держави. В умовах постійного зростання вартості енергоносіїв і нестабільності їх постачання, раціональне та ефективне використання енергії стає визначальним чинником забезпечення довгострокової економічної

стабільності, стійкості та динамічного розвитку бізнес-структур. Низька продуктивність виробництва часто обумовлена неефективністю виробничих процесів, що значною мірою зумовлено нераціональним використанням енергетичних ресурсів. Оптимізація енергоспоживання, зокрема через впровадження сучасних технологічних рішень, зокрема ШІ, сприяє зростанню продуктивності праці та відповідному збільшенню доходів підприємства. Скорочення енергоспоживання позитивно впливає не лише на економічні показники, а й на екологічний стан довкілля, водночас покращуючи репутаційний капітал підприємства. У зв'язку з цим, впровадження енергоефективних технологій із використанням ШІ на підприємствах, в установах та організаціях є актуальним і стратегічно важливим кроком для сталого розвитку.

В умовах сучасних викликів головним завданням для України є зміцнення енергетичної безпеки та підвищення стійкості енергосистеми. Оскільки Україна інтегрована в загальноєвропейську енергетичну мережу, модернізація її енергетичного сектору має здійснюватися з урахуванням європейських стандартів і вимог.

Один із ключових напрямів трансформації української – цифровізація енергетичних мереж на базі децентралізації. Вона відкриває нові можливості для підвищення ефективності управління системами, зменшення втрат, швидкого реагування на аварійні ситуації та інтеграції відновлюваних джерел енергії. Цифрова модернізація є основою для створення гнучкої, розумної та екологічно орієнтованої енергетичної інфраструктури майбутнього.

На відміну від застарілих систем, Smart Grid інтегрує інформаційно-комунікаційні технології, а також рішення для збору й аналізу даних про виробництво, передачу та споживання електроенергії. Це дозволяє ефективно контролювати та управляти всіма рівнями енергетичної системи в режимі реального часу. Сучасне розумне місто неможливе без Smart Grid. Ця інфраструктура не лише підвищує енергоефективність та надійність постачання, а й створює умови для інноваційного розвитку, зменшення шкідливих викидів та підвищення безпеки. Її ключовим компонентом є інтелектуальні лічильники, які передають точні дані про споживання електроенергії майже в реальному часі. Завдяки цьому споживачі можуть:

– планувати використання енергії в залежності від тарифів (наприклад, уночі, коли електроенергія дешевша);

– оптимізувати витрати, використовуючи великі прилади – як-от пральні або посудомийні машини – у позапікові години;

– керувати зарядкою електромобіля, щоб зменшити навантаження на мережу та зекономити.

Для енергетичних компаній, операторів розподільчих мереж (колишніх обленерго) та на рівні держави впровадження Smart Grid відкриває нові можливості: зокрема, підвищується надійність енергопостачання завдяки своєчасному виявленню або попередженню аварій, покращується балансування навантажень, що дозволяє уникати відключень та втрат, забезпечується цифрове управління мережею зі зниженими експлуатаційними витратами, а також зростає загальна енергоефективність та екологічність енергосистеми.

В Україні робота з впровадження нових технологій в національну енергосистему розпочалася відносно недавно. Так, з 2014 року бельгійська компанія Tractebel розробляє та впроваджує низку пілотних технологій та проєктів Smart Grid на рівні системного оператора – НЕК «Укренерго». Оператори систем розподілу також поступово намагаються впроваджувати елементи розумних електричних мереж.

Товариство з впровадження технологій найбільш активно впроваджує ТОВ «ДТЕК Енерго». Компанія активно встановлює розумні лічильники та автоматизує систему електропостачання за допомогою сучасного програмного забезпечення. Це допоможе їй швидше «бачити» аварії та, як наслідок, набагато швидше їх усувати.

У 2019 році ТОВ «ДТЕК Енерго» почало цифровізацію своїх електростанцій, збільшуючи впровадження ШІ в управління тепловими електростанціями. SCADA-системи (Supervisory Control and Data Acquisition – диспетчерське управління та збір даних) використовуються ДТЕК для моніторингу та управління складними інфраструктурними або промисловими об'єктами в режимі реального часу. Вона допомагає диспетчерам бачити всю енергетичну систему області в режимі онлайн, контролювати режим її роботи та краще оцінювати критичну або аварійну ситуації. В разі аварії саме SCADA автоматично надсилатиме у чат-бот та на сайт повідомлення про відключення та повернення світла, то ж ви дізнаватиметесь про це за лічені

секунди. Ця система є частиною розвитку «розумних» електромереж, які мають забезпечити безперебійне електропостачання.

Але однією з головних вразливостей Smart Grid є SCADA-системи, які забезпечують управління та моніторинг об'єктів енергетичної інфраструктури. Хакери можуть отримати доступ до цих систем через несанкціонований віддалений доступ, фішинг або шкідливе програмне забезпечення.

MODUS X – це дочірня IT-сервісна компанія, виділена з IT-департаменту групи ДТЕК у 2022 році, для масштабного впровадження цифрових та AI-рішень как усередині холдингу, так і на ринку загалом. Вона має понад 500 інженерів, архітекторів, фахівців з кібербезпеки та дата-сайєнтистів, працює за принципом data-driven управління.

MODUS X реалізувала широкий спектр рішень:

– цифровий двійник шахт і енергоблоків;
– автоматизація сервісів (документообіг, HR, мобільні додатки);
– оптимізація логістики й прогнозування технічного стану з AI-алгоритмами;
– системи цифрової безпеки для енергетичної інфраструктури.

Також використовуючи моделі машинного навчання, MODUS дозволяє:

– виявляти складні та приховані атаки на IT- та OT-інфраструктуру;
– аналізувати поведінкові патерни користувачів і пристроїв;
– попереджати інциденти за допомогою предиктивної аналітики.

Так, у межах цифрової трансформації енергетичного сектору компанія MODUS X спільно з групою ДТЕК реалізує комплексні рішення на основі ШІ, машинного навчання та інструментів Microsoft Copilot Studio. Основна мета співпраці – забезпечення сталого розвитку та підвищення ефективності бізнес-процесів завдяки глибокій аналітиці, автоматизації та створенню інноваційного середовища. Microsoft Copilot – інструмент, що допомагає автоматизувати типові дії

Центральним елементом трансформації є перехід до data-driven моделі управління, де дані стають основою прийняття рішень. Такий підхід дозволяє не лише підвищити оперативність і точність

управлінських рішень, але й забезпечити гнучкість та адаптивність енергетичної компанії до викликів ринку.

Серед стратегічних цілей проєкту:

– Оптимізація процесів: використання алгоритмів машинного навчання для прогнозування, підтримки прийняття рішень, автоматизації рутинних задач і зниження операційних витрат.

– Масштабування експертизи: створення умов, за яких як технічні, так і бізнес-підрозділи можуть ефективно використовувати ШІ-інструменти у своїй діяльності.

– Формування культури data-driven: впровадження практик, коли аналітика та цифрові інструменти є обов'язковим елементом кожного етапу життєвого циклу бізнесу.

– Інституціалізація інноваційної спільноти: створення внутрішніх екосистем для обміну знаннями, менторства та підвищення цифрової зрілості персоналу.

Реалізація таких ініціатив потребує системного підходу: інтеграції гнучких цифрових технологій, розбудови внутрішньої експертизи та наявності стратегічного бачення розвитку. Таким чином ШІ розглядається не лише як технологічний інструмент, а як стратегічний ресурс, що здатен підвищити конкурентоспроможність, стійкість і інноваційність компанії [8].

Компанія «Українські розподільні мережі» здійснює корпоративне управління державними частками у семи обласних енергетичних компаніях, зокрема таких як Хмельницькобленерго, Миколаївобленерго, Запоріжжяобленерго та Тернопільобленерго. Ця компанія працює над 12 пілотними проєктами з іноземними інвестиціями для розвитку концепції Smart Grid серед компаній групи. Група телемеханізувала 65 % усіх високовольтних підстанцій та встановила 12 % розумних медичних пристроїв.

У жовтні 2022 року Кабінет Міністрів України затвердив Концепцію впровадження Smart Grid до 2035 року та ухвалив відповідний план заходів для її реалізації.

Ключова мета цього документа – зменшити втрати електроенергії в національних електромережах з 11,6 % до 7,5 %, що відповідає економії близько 6 млрд кВт·год електроенергії на рік. Такий обсяг еквівалентний спаленню приблизно 3 мільйонів тонн вугілля

на теплових електростанціях, що матиме значний екологічний та економічний ефект [9]. Впровадження Smart Grid розглядається як невід'ємна частина процесу відновлення та модернізації енергетичної інфраструктури України, яка зазнала масштабних руйнувань унаслідок російської військової агресії.

Повільне впровадження «розумних мереж» в Україні пов'язане, перш за все, з недостатнім фінансуванням. Регіональні компанії, що відповідають за експлуатацію, обслуговування та розвиток розподільчих мереж, мають обмежені бюджети. В середньому їхні інвестиційні програми становлять лише 300 мільйонів гривень. На державному та експертному рівнях обговорюються різні варіанти інвестування. Це включає міжнародне донорське фінансування конкретних проєктів, кредити європейських та світових банків, а також системи тарифів на основі стимулювання [10].

На нашу думку, повоєнна Україна повинна модернізувати свою енергетичну інфраструктуру на основі передових технологій, включаючи системи розумних мереж (Smart Grid), щоб досягти енергетичної незалежності та інтегрувати відновлювані джерела енергії. Інтеграція технологій ШІ, Інтернету речей та великих даних покращує прогнозування попиту, підвищує ефективність використання відновлюваної енергії та зменшує втрати в енергомережах. Крім того, цифрова стійкість енергетичного сектору є основоположною для зміцнення енергетичної безпеки та сприяння розвитку розумних міст.

Сьогодні основним джерелом інвестицій для будівництва Smart Grid є інвестиційні програми компаній, чого недостатньо для побудови Smart Grid. Процес впровадження ШІ в енергетичних компаніях часто супроводжується проблемою вибору розробника та інтегратора цифрових рішень і продуктів, а іноді, навпаки, ускладнюється відсутністю необхідних пропозицій на ринку.

На нашу думку, впровадження Smart Grid в Україні зіткнеться з перешкодами:

1. Будівництво та модернізація інфраструктури вимагають значних інвестицій.

2. Поєднання нових технологій із застарілими енергетичними системами може бути складним завданням.

3. Сонячна та вітрова енергетика залежать від погодних умов, що вимагає рішень для балансування навантаження та накопичення енергії.

Розвиток технології Smart Grid дозволить оптимізувати виробництво, передачу та використання електроенергії, що стимулюється для зменшення споживання енергії. Оскільки впровадження енергоефективності зменшить втрати енергії, необхідно також стимулювати інших виробників електроенергії, включаючи іноземних, до підтримки монополій. Зокрема, впровадження технологій «мікромереж» зможе підвищити стійкість української системи до військових та стихійних лих.

Україні потрібні заходи щодо стимулювання створення малих енергетичних компаній з метою побудови цивілізованого європейського ринку електроенергії з привабливою нормою прибутку для компаній, забезпечення доступу до дешевих довгострокових банківських кредитів, збалансування та оптимізації структури вітчизняної генерації в напрямку відновлюваної електроенергії. Проблеми декарбонізації пов'язані з передачею електроенергії та необхідністю створення нових ліній, технології дозволяють розширити потужність існуючих мереж для сонячної та вітрової енергії.

Децентралізація енергосистеми є ключовим напрямом трансформації енергетичного сектору України в умовах післявоєнного відновлення та стійкого розвитку. Вона передбачає перехід від централізованої моделі генерації до гнучкої мережі малих і середніх виробників, інтегрованих у єдину цифрову інфраструктуру. Такий підхід дозволяє зменшити залежність від великих централізованих об'єктів, які є вразливими до кібератак та військових дій, а також посилити енергетичну стійкість громад і регіонів.

Особливої актуальності набуває впровадження Smart Grid як інтелектуальної енергосистеми нового покоління, яка забезпечує двосторонній обмін енергією між споживачами та генераторами, враховує динамічні потреби ринку й дозволяє в режимі реального часу здійснювати балансування навантаження, моніторинг споживання та виявлення відхилень.

Децентралізовані системи на базі ВДЕ (сонячної, вітрової енергії, біомаси) у поєднанні з накопичувачами енергії та енергетичними

кооперативами дають змогу не лише забезпечити енергетичну автономію громад, а й активізувати локальний бізнес, створити нові робочі місця та підвищити інвестиційну привабливість регіонів.

Крім того, інтеграція ШІ у в управління децентралізованими мережами дозволяє автоматизувати процеси оптимізації виробництва та споживання, прогнозування аварій, і тим самим – мінімізувати технічні втрати та забезпечити надійність системи.

Таким чином, децентралізація енергосистеми України, з опорою на Smart Grid, цифрові технології та інноваційне управління, не лише підвищить енергетичну безпеку держави, а й сприятиме її інтеграції до європейського енергетичного простору на засадах сталості, відкритості та інновацій.

Технології ШІ в Smart Grid ефективні у використанні, але їх поширення створює серйозні виклики для енергетичної галузі. Системи ШІ сьогодні виступають не лише технологічним рушієм, а й стратегічним партнером у досягненні цілей сталого розвитку. Їхнє впровадження в різні сфери суспільного життя сприяє створенню більш ефективних і екологічно безпечних рішень. Водночас автоматизація, що базується на ШІ, здатна змінити структуру ринку праці. Зростання технологічного безробіття стає однією з ключових проблем, з якими стикається індустрія інформаційних технологій та цифрових послуг.

Попри побоювання щодо конкуренції між ШІ та людською працею, основне призначення таких систем – не замінити людину, а підсилити її можливості. ШІ ефективно виконує повторювані, аналітичні завдання, тоді як людина зосереджується на креативних, стратегічних і емоційно забарвлених аспектах роботи. Співпраця з інтелектуальними системами дозволяє фахівцям розвивати унікальні навички, підвищуючи продуктивність і задоволення від професійної діяльності. Крім того, розвиток ШІ відкриває нові можливості працевлаштування в галузях, пов'язаних з його розробкою, впровадженням і управлінням.

Також інтеграція ШІ в робочі процеси сприяє переосмисленню ролі працівника у цифровій економіці. Людина стає не просто виконавцем, а куратором інтелектуальних систем, аналітиком даних, стратегом інновацій. Це зумовлює потребу в нових компетенціях, таких як цифрова грамотність, навички роботи з великими даними, етичне управління ШІ та кросдисциплінарне мислення.

В енергетичному секторі, впровадження ШІ дозволяє зменшити ризики, пов'язані з людським фактором, підвищити безпеку об'єктів критичної інфраструктури, а також скоротити витрати за рахунок автоматизації складних технічних процесів. Проте це не усуває потреби в людському контролі – навпаки, зростає роль фахівців, здатних забезпечити прозорість, надійність і соціальну відповідальність у взаємодії «людина – машина».

Більше того, розвиток етичних стандартів і нормативної бази у сфері ШІ є критично важливим для запобігання дискримінації, помилок систем і зловживань. Саме людина повинна задавати цінності, пріоритети та межі використання ШІ, щоб гарантувати, що технології працюють на благо суспільства.

Таким чином, ШІ не витісняє людину, а виводить її роль на якісно новий рівень, де креативність, гнучкість, моральний вибір і стратегічне мислення залишаються незамінними. Це відкриває перед суспільством унікальні можливості для трансформації ринку праці, освіти та моделей управління, спрямованих на сталий і людяний розвиток.

ШІ вже відіграє важливу роль у трансформації економічних, соціальних та екологічних процесів, наближаючи сталий розвиток. У післявоєнної відбудови Україна має унікальний шанс модернізувати енергетичну інфраструктуру, орієнтуючись на інноваційні технології, зокрема ті, що базуються на ШІ. Це робить інтелектуальні системи незамінним інструментом для підприємств, які прагнуть залишатися гнучкими, інноваційними й конкурентоспроможними у динамічному глобальному середовищі.

Крім того, значну загрозу становлять внутрішні загрози – як ненавмисні, так і навмисні дії співробітників. Нерідко колишні працівники зберігають доступ до критичних систем після звільнення, що створює додаткові ризики. Низький рівень обізнаності щодо інформаційної безпеки серед співробітників, відсутність регулярних тренінгів та навчання посилюють проблему. Часто працівники не усвідомлюють важливості кібербезпеки або сприймають вимоги безпеки як зайву формальність. В умовах перевантаження, стресу або рутини знижується уважність, імовірність допущення помилок зростає.

В енергетичному секторі, де системи управління мають пряме відношення до об'єктів критичної інфраструктури, наслідки людських помилок можуть бути особливо серйозними. Через недбалість або неуважність персоналу зловмисники можуть отримати контроль над процесами, які впливають на енергозабезпечення регіонів. Часто керівництво підприємств недооцінює важливість інвестування в розвиток культури кібербезпеки. Замість впровадження ефективних програм навчання, відповідальність перекладається виключно на ІТ-відділ, хоча кібербезпека – це спільна відповідальність усього колективу.

Надзвичайно важливо створити на підприємстві середовище, де кожен працівник усвідомлює свою роль у забезпеченні безпеки. Впровадження автоматизованих систем контролю дій користувачів, регулярне оновлення паролів, обмеження доступу, системи виявлення аномалій – усе це може зменшити ризики, пов'язані з людським фактором. Проте навіть найсучасніше програмне забезпечення не буде ефективним без належної поведінки з боку персоналу. Навчання, симуляції атак, регулярні інструктажі, інформаційні кампанії – усе це має стати частиною щоденної роботи.

Розвиток водневої енергетики посідає провідне місце в глобальній стратегії переходу до відновлюваних джерел енергії та формування низьковуглецевої економіки. Інтеграція ШІ у цю сферу відкриває нові перспективи для оптимізації процесів виробництва, зберігання та споживання водню. В умовах зростаючих викликів, пов'язаних з енергетичною безпекою, необхідністю зменшення викидів парникових газів і пошуком стійких енергетичних рішень, роль інновацій стає визначальною.

Зелений водень, що виробляється з використанням відновлюваних джерел енергії, є екологічно чистим видом палива – при його спалюванні утворюється лише вода. Це робить його важливим інструментом у процесі декарбонізації, особливо в секторах, де електрифікація є складною або економічно невигідною, таких як важка промисловість, авіація чи морські перевезення. ШІ відіграє ключову роль в оптимізації процесів у водневій енергетиці, зокрема під час електролізу, знижуючи енергоспоживання та підвищуючи загальну ефективність виробництва. Системи на основі машинного навчання

дозволяють динамічно налаштовувати параметри роботи обладнання в реальному часі відповідно до змін зовнішніх умов, що підвищує гнучкість і стабільність процесів.

Крім того, ШІ використовується для аналізу ринкової ситуації та прогнозування попиту на водень, що дозволяє більш точно планувати обсяги виробництва, логістику та зберігання ресурсу. Завдяки інтелектуальній аналітиці можливе своєчасне виявлення технічних аномалій і запобігання поломкам, що знижує ризики аварій і продовжує термін служби обладнання.

Також алгоритми ШІ сприяють балансуванню енергетичних систем, забезпечуючи ефективну інтеграцію водневих технологій з відновлюваними джерелами енергії, такими як сонячна та вітрова. Це відкриває нові горизонти для розвитку сталої, гнучкої та безпечної енергетичної інфраструктури.

Для України розвиток водневої енергетики є надзвичайно актуальним і стратегічно важливим. Це нове джерело енергії може суттєво посилити енергетичну незалежність держави та сприяти декарбонізації економіки. Водночас для його впровадження необхідно вирішити низку інфраструктурних і фінансових питань. Передусім, потрібне забезпечення фінансування на модернізацію обладнання, будівництво електролізерів та розвиток супутньої інфраструктури.

Особливу увагу слід приділити адаптації української газотранспортної системи до транспортування водню. Оптимальним варіантом є переорієнтація наявної газової інфраструктури для створення повноцінного ланцюга – від виробництва до логістики та кінцевого споживання. Крім того, важливо розробити проєкти з переоснащення вугільних електростанцій для їх переходу на водневе паливо, а також ініціювати запуск муніципального транспорту, що працює на водневій енергії.

Інтеграція ШІ у водневу енергетику є не просто технологічною новацією, а критично важливим елементом стратегії переходу до низьковуглецевої економіки. ШІ забезпечує підвищення ефективності всіх етапів – від виробництва до транспортування та споживання водню, сприяючи оптимізації ресурсів, зниженню витрат та підвищенню надійності енергетичних систем. Такий підхід дозволить

Україні не лише модернізувати свою енергетичну інфраструктуру, а й зайняти гідне місце на глобальному енергетичному ринку майбутнього.

Але високий рівень цифровізації енергогалузі призводить до кіберзагроз, які спрямовані на безпеку електромереж і створюють серйозну проблему через численні атаки. Тому кібербезпека стає важливим елементом енергетичної безпеки. Повномасштабна збройна агресія Російської Федерації проти України спричинила безпрецедентну хвилю кібератак, скерованих передусім на енергетичну інфраструктуру та інші об'єкти критично важливого значення.

Так, до повномасштабного вторгнення Україну атакували окремі угруповання хакерів. Підкреслюється, що зараз хакерів координує один центр. Росія витрачає на кожну кібератаку мільйони доларів. У 2023 році було зафіксовано близько 55 кібератак на енергооб'єкти. Кібератаки комбінуються з ракетними ударами та атаками дронів по енергооб'єктах. З 24 лютого 2022 року кількість кіберинцидентів на держкомпанії «Укренерго» зросла втричі, порівняно з попереднім роком. До повномасштабної війни російських хакерів цікавила фінансова вигода: викуп за повернення систем у лад чи крадіжку даних із метою продажу. Зараз дестабілізація критичної інфраструктури, щоб припинити енергопостачання. Російські хакери використовують різні підходи: від сканування IT-периметра до DDoS-атак. Під час однієї з DDoS-атак на Укренерго кількість запитів могла перевищувати 5 млн за кілька годин [11].

Крім того, кібератаки можуть впливати не лише на енергетичну систему України, а й на енергосистеми сусідніх країн. Подібні кібератаки мають ризик повторення в інших державах. Це обумовлено тим, що структура українських мереж є типовою для багатьох країн. Типи обладнання, що використовуються в українській енергосистемі, також широко розповсюджені за її межами.

Враховуючи набутий практичний досвід, Україна здатна зробити суттєвий внесок у формування глобальної архітектури кібербезпеки, зокрема через обмін знаннями, розробку стандартів протидії гібридним загрозам та участь у міжнародних ініціативах з кіберзахисту критичної інфраструктури.

Українські енергетичні компанії впровадили багаторівневу систему кіберзахисту, яка охоплює постійний моніторинг, програму підготовки персоналу, міжнародну технічну підтримку та використання адаптивних технологій. Такий підхід забезпечив високий рівень стійкості до скоординованих гібридних атак з боку Росії. Продовження цих зусиль, розширення захисту на малих та середніх операторів, а також активніше впровадження ІТ-рішень на основі ШІ дозволить зміцнити кіберщит національної енергетичної інфраструктури.

Згідно з дослідженнями, ефективність російських атак залишається низькою саме завдяки високому рівню кіберстійкості України. Попри численні масштабні спроби втручання, жодна з атак за останні роки не призвела до порушення роботи автоматизованих систем управління підстанціями.

Українські енергокомпанії щороку витрачають понад 100 мільйонів гривень на ліцензійне програмне забезпечення для кіберзахисту, навіть за умов обмеженої ліквідності. Частина витрат компенсується завдяки донорській міжнародній підтримці. При цьому великі державні компанії – зокрема «Укренерго», «Енергоатом» та «Нафтогаз» – мають кращий рівень захищеності через доступ до значно більших фінансових ресурсів.

Поєднане використання кібератак, дронів та ракет стало визначальною ознакою тактики російських військ у зимовий період. Такий гібридний підхід спрямований на максимальне порушення роботи критичної інфраструктури, зокрема енергетичної системи, шляхом одночасного фізичного та цифрового впливу.

Система захисту енергетичної інфраструктури повинна охоплювати механізми виявлення, запобігання та реагування на дії зловмисників, з метою мінімізації впливу кібератак на мережу та пов'язані економічні наслідки. Вона також має забезпечувати автоматичне виявлення, усунення або зменшення наслідків технічних несправностей як на локальному, так і на загальносистемному рівні. У критичних ситуаціях система повинна мати змогу впроваджувати вимушені обмеження споживання електроенергії, а також стимулювати управління попитом, щоб збалансувати навантаження та зберегти стабільність енергопостачання.

Ця затяжна кібервійна стала справжнім випробуванням для національної системи кіберзахисту, водночас сформувавши унікальний масив практичного досвіду, що має стратегічну цінність у глобальному контексті. Посилення кіберзагроз унаслідок бойових дій суттєво актуалізувало необхідність впровадження інтелектуальних, адаптивних та автономних систем захисту, здатних забезпечувати стійку та безперебійну роботу критичної інфраструктури навіть в умовах кризових ситуацій. Україна, внаслідок прямого зіткнення з кібервійною, здобула безцінні знання щодо методів виявлення, нейтралізації та запобігання масштабним кіберінцидентам, зокрема у сферах енергетики, зв'язку та фінансів. Цей досвід набуває особливого значення у світлі зростаючої цифровізації економіки та суспільства, яка, у свою чергу, підвищує потребу в надійних засобах кіберзахисту як у державному, так і в приватному секторах. Системна загроза, що постала перед Україною, стимулювала не лише розвиток внутрішнього ринку послуг у сфері кібербезпеки, а й викликала зростаючий інтерес міжнародної спільноти до підтримки кіберстійкості країни шляхом надання технічної, експертної та матеріально-логістичної допомоги.

Найпопулярніші види кібератак: DDoS, Ransomware, Phishing 2020. Найбільша частка ринку припадає на США, Китай, Німеччину та Велику Британію. Країни, на які здійснюється найбільша кількість кібератак: США, Україна, Південна Корея, Китай. UAC-0010 (Gamaredon/ФСБ) залишається найбільш активним російським.

Кіберінциденти у Smart Grid можуть призводити до порушення балансу навантаження, пошкодження обладнання та зниження якості електропостачання. В умовах воєнного конфлікту кіберзагрози набувають гібридного характеру і можуть бути частиною стратегічних атак на державну інфраструктуру.

Аналіз наведених даних про кібератаки на різні сектори України у 2024 році показує загальне зростання кіберзагроз у другій половині року порівняно з першою половиною. Найбільш динамічне зростання спостерігається у військовому секторі (+82 %) та в структурах місцевої влади (+53 %). Водночас енергетичний сектор демонструє найменшу зміну – лише +2 %, що потребує окремого аналізу. Незначне зростання кількості атак на енергетичний сектор (+2 %) не означає зниження інтересу до нього з боку зловмисників.

Таблиця 2 – Динаміка кібератак на ключові сектори України у 2024 році

Сектор	І півріччя 2024 року	ІІ півріччя 2024 року	Темп приросту, %
Військовий сектор	276	502	+82 %
Державні організації	473	665	+41 %
Енергетичний сектор	124	127	+2 %
Телеком та ІТ-сектор	26 (19+7)	37 (33+4)	+42 %
Місцева влада	542	831	+53 %

Джерело: складено за даними [12]

Це, швидше за все, свідчить про вже високу базову активність та постійну присутність загроз. Енергетика залишається однією з головних цілей кібератак, особливо в умовах війни, оскільки атаки на енергосистему мають високий дестабілізуючий потенціал. Незначна динаміка може бути результатом покращення кіберзахисту в галузі після масових атак попередніх періодів. Водночас можлива і зміна тактики атак: менше шумних або масових атак, натомість точкові, приховані, націлені на порушення SCADA-систем або ланцюги постачання. Порівняно з державними органами (+41 %) чи телекомунікаційним та ІТ-сектором (+42 %), де спостерігається значне зростання атак, енергетика виглядає «стабільною». Водночас місцева влада (+53 %) та військові структури (+82 %) стали новими центрами загострення, що може відволікати ресурси уваги від енергетичної сфери. Незважаючи на невелике зростання, ризики залишаються високими, оскільки енергетика тісно інтегрована з іншими секторами – зокрема з місцевою владою, телекомом та держструктурами. Атаки на один із сегментів можуть мати ланцюговий ефект.

SWOT-аналіз показує, що попри наявність суттєвих слабких сторін та зовнішніх загроз, енергетичні підприємства України мають потужний потенціал для формування ефективної системи кіберзахисту. Реалізація можливостей, пов'язаних із впровадженням інтелектуальних технологій та підвищенням рівня цифрової грамотності персоналу, дозволить значно зміцнити кіберстійкість галузі. При цьому необхідно приділяти особливу увагу управлінським, освітнім та нормативно-правовим аспектам. Кіберстійкість енергосистеми має стати пріоритетом державної політики у сфері національної безпеки

Таблиця 3 – Свот-аналіз енергетичної галузі України

Сильні сторони	Слабкі сторони
• Високий рівень усвідомлення критичності кібербезпеки серед керівництва підприємств. • Початок впровадження систем моніторингу та реагування на інциденти. • Співпраця з міжнародними партнерами у сфері кіберзахисту. • Досвід реального протистояння кіберзагрозам в умовах війни.	• Застаріла ІТ-інфраструктура на багатьох енергетичних об'єктах. • Обмежене фінансування заходів із кібербезпеки. • Низький рівень кваліфікації персоналу у сфері ІТ-захисту. • Відсутність комплексної стратегії кіберменеджменту на рівні підприємств.
Можливості	**Загрози**
• Інтеграція ШІ, машинного навчання та big data для підвищення ефективності захисту. • Державні ініціативи щодо цифрової трансформації та захисту критичної інфраструктури. • Можливість отримання грантів та технічної підтримки від міжнародних донорів. • Стандартизація та сертифікація кібербезпеки.	• Зростання складності кібератак та використання кібервійни як інструменту гібридного впливу. • Зовнішні атаки на інфраструктуру з боку ворожих держав або організованих хакерських угруповань. • Поширення шкідливих програм, зокрема через уразливі IoT-пристрої. • Недостатній правовий захист у випадку кібератак на приватні енергетичні компанії.

Джерело: складено особисто автором

Сьогодні кібербезпека перестала бути виключно технічною категорією – вона трансформувалася в критичний елемент національної безпеки, стійкості бізнесу та довіри громадян до державних і корпоративних систем. Особливо гостро ця проблема постає для України, яка з початку повномасштабного вторгнення Росії стала мішенню для безпрецедентної хвилі кібератак, зокрема на критичну інфраструктуру та енергетичні підприємства. Кіберзахист повинен розглядатися не як реакція на інциденти, а як інтегрована складова стратегії стримування, аналогічна до традиційної оборонної політики.

Одним із нових викликів є децентралізація кіберзлочинності. Сучасні загрози стають дедалі більш автономними, мобільними та технологічно оснащеними, тоді як нормативно-правове регулювання, як правило, не встигає за темпами інновацій. Якщо країни не розроблятимуть гнучкі механізми кіберрегулювання, вони ризикують постійно відставати у протидії новим вразливостям.

Технології подвійного призначення, криптографічні рішення та ШІ одночасно слугують інструментами інновацій та джерелами загроз. Все залежить від того, хто контролює ці інструменти та в якій системі управління вони функціонують. ШІ може бути як щитом, так і зброєю – і саме ефективна модель кіберменеджменту визначає, якою стороною буде реалізований потенціал ШІ.

Цифрова трансформація енергетичної галузі виводить концепцію Smart Grid на передній план модернізаційних процесів. Інтелектуальні енергетичні мережі забезпечують оптимізацію споживання, підвищення надійності систем та інтеграцію відновлюваних джерел енергії. Однак, поряд з перевагами, зростає спектр кіберзагроз, які можуть мати катастрофічні економічні, технологічні та соціальні наслідки. Критична інфраструктура, до якої належать енергетичні мережі, вимагає пріоритетного захисту на всіх етапах життєвого циклу систем.

Одним із ключових принципів безпеки у Smart Grid має стати "Security by Design" – вбудована з початку розробки концепція безпеки, яка враховує моделювання загроз, визначення вимог до кожного компонента мережі, постійний аудит та дотримання стандартів безпеки впродовж усього життєвого циклу проєкту. Такий підхід дозволяє мінімізувати необхідність пізньої перебудови небезпечних елементів, яка може призводити до затримок у впровадженні інновацій.

Найбільш серйозні наслідки кібератак на Smart Grid включають: порушення енергопостачання, пошкодження обладнання, витік персональних даних користувачів, репутаційні втрати та вимушені надзвичайні інвестиції у енергетичні системи. Цільові атаки стають дедалі складнішими, зокрема на SCADA-системи, що керують об'єктами критичної інфраструктури.

Багаторівнева стратегія захисту Defense in Depth є фундаментом кібербезпеки Smart Grid. Вона передбачає логічну сегментацію мережі відповідно до критичності компонентів, створення

контрольованих точок доступу між сегментами, розгортання незалежних захисних механізмів на кожному рівні, а також регулярне тестування ізоляції сегментів для виявлення вразливостей. Важливим залишається баланс між безпекою і функціональністю: надмірна ізоляція може знижувати ефективність системи, а недостатній рівень сегментації створює ризики для масштабних кібератак.

Важливою складовою сучасної кібербезпеки є управління ризиками третіх сторін. Екосистема Smart Grid охоплює обладнання, програмне забезпечення та сервіси від численних постачальників. Аналітичні дані вказують, що понад 60 % кіберінцидентів у критичній інфраструктурі пов'язані з уразливостями сторонніх компонентів. Стратегія управління цими ризиками включає встановлення чітких вимог до постачальників, проведення незалежного аудиту, моніторинг вразливостей та наявність планів реагування на інциденти, пов'язані з ланцюгами постачання.

Таблиця 4 – Види ШІ для протидії кіберзагрозам

Категорія	**Застосування у сфері кібербезпеки енергетики**
1	2
Аналітичний ШІ	Надання експертних порад щодо захисту та виявлення аномалій у трафіку. Прогнозування атак та розробка превентивних стратегій.
Функціональний ШІ	Автоматичне виявлення та реагування на загрози через IoT-пристрої. Постійний моніторинг і захист інтернет-пристроїв.
Інтерактивний ШІ	Взаємодія з операторами в реальному часі під час інцидентів. Проведення симуляцій та тренінгів для персоналу.
Текстовий ШІ	Автоматичний аналіз логів і текстових даних для виявлення аномалій. Застосування NLP для аналізу зовнішніх повідомлень про загрози.
Візуальний ШІ	Біометричний контроль доступу до критичних зон.Аналіз відео з метою виявлення несанкціонованих дій.
Роботизована автоматизація процесів	Автоматичне оновлення ПЗ, патч-менеджмент, моніторинг мережі. Фізичний контроль інфраструктури за допомогою роботів.

Продовження таблиці 4

1	2
Розпізнавання мови та комп'ютерний зір	Ідентифікація голосових команд і контроль доступу. Аналіз відеопотоків для виявлення підозрілої активності.
Data Science	Обробка великих даних для аналізу трафіку та логів. Побудова моделей ML для прогнозування атак.
Reactive Machine та Limited Memory AI	Реакція в реальному часі на кіберзагрози. Виконання базових завдань моніторингу та виявлення аномалій.
Theory of Mind AI та Self-Awareness AI	Розуміння намірів кіберзлочинців для покращення захисту. Автономне прийняття рішень щодо кібербезпеки на основі самосвідомості.

Джерело: складено за даним [13]

Кібербезпека все частіше розглядається як інтегрована складова ESG-стратегії (екологічні, соціальні та управлінські фактори). Інвестиції в захист Smart Grid прямо корелюють із довгостроковою стійкістю компаній. Захист критичної інфраструктури сприяє уникненню екологічних інцидентів (Environmental), забезпечує стабільне енергопостачання для спільнот (Social) та демонструє відповідальне управління ризиками (Governance). Компанії з високим рівнем кіберзахисту мають вищу інвестиційну привабливість та стійкість у кризових ситуаціях.

Таким чином, безпека Smart Grid виходить за межі IT-дисципліни і постає як стратегічне завдання для енергетичних компаній, державних органів та глобальних партнерств. В умовах гібридної війни, технологічної еволюції та діджиталізації саме проактивний, архітектурно вбудований і багаторівневий підхід до кіберзахисту здатен забезпечити надійність, стійкість та довіру до енергетичної інфраструктури майбутнього.

Але ШІ підвищує економічну ефективність, зменшуючи ймовірність людської помилки – однієї з основних причин порушень кібербезпеки. Для забезпечення ефективного управління, моніторингу та захисту Smart Grid ми виокремлюємо наступні категорії ШІ.

Кіберменеджмент є ключовим елементом управління сучасною цифровою організацією. Він охоплює планування, координацію,

впровадження та контроль заходів з кібербезпеки. Ефективний кіберменеджмент забезпечує стійкість ІТ-інфраструктури до внутрішніх і зовнішніх загроз. Він передбачає формування політик інформаційної безпеки на рівні підприємства. До завдань кіберменеджера входить управління ризиками, інцидентами та реагуванням на атаки. Важливою складовою є постійний моніторинг систем і аналіз аномалій. Роль кіберменеджменту зростає в умовах гібридної війни та цифровізації. Він тісно пов'язаний з ІТ-менеджментом, кризовим управлінням та стратегічним плануванням [14]. Ефективні протоколи доступу та контроль ідентифікації є його невід'ємною частиною. Кіберменеджмент передбачає інтеграцію ШІ для виявлення та прогнозування загроз. Навчання персоналу є критично важливим для формування кіберстійкої культури. Кіберменеджмент має бути адаптивним до змін середовища загроз. До функцій також належить управління зовнішніми підрядниками та провайдерами. Важливе значення має аудит систем безпеки та проведення тестів на проникнення. Кіберменеджери повинні володіти навичками як у сфері технологій, так і управління. Кіберменеджмент охоплює захист конфіденційності, цілісності та доступності інформації. Він потребує належного фінансування та підтримки з боку топменеджменту. Ефективна комунікація під час кіберінцидентів – ще один критично важливий аспект. Успішний кіберменеджмент сприяє підвищенню довіри клієнтів і партнерів. З огляду на критичну важливість енергетичного сектору для національної безпеки, кіберменеджмент набуває стратегічного значення. Інтеграція кіберменеджменту з енергоменеджментом є критично важливою для формування енерго- та кіберстійкості. Успішна реалізація цієї інтеграції вимагає міжгалузевої співпраці, державної політики кіберзахисту критичної інфраструктури та інвестицій у новітні технології безпеки.

Людський фактор є одним із ключових елементів, що визначають рівень кібербезпеки енергетичних підприємств. Досвід показує, що більшість кібератак стаються не через технічні недоліки, а через помилки або необережні дії персоналу. Найчастіше зловмисники використовують методи соціальної інженерії, зокрема фішинг, коли працівник самостійно надає доступ до систем, вважаючи повідомлення або запит легітимним. Однією з головних проблем залишається

недотримання працівниками політик безпеки – використання слабких паролів, ігнорування багатофакторної автентифікації, відкритий доступ до конфіденційної інформації.

Критичний дефіцит кадрів, які здатні працювати на перетині цифрових та виробничих сфер, створює додаткові ризики. Однією з актуальних проблем у сфері кібербезпеки є гостра нестача кваліфікованих фахівців. Зі зростанням кількості та складності кіберзагроз зростає й потреба в професіоналах, здатних ефективно реагувати на атаки, забезпечувати безпеку інформаційних систем і впроваджувати сучасні технології захисту. Проте темпи підготовки спеціалістів не відповідають викликам часу: багато освітніх програм залишаються теоретичними, а молоді фахівці не завжди мають достатній практичний досвід для роботи в умовах реальних кіберінцидентів.

Таким чином, фахівці повинні мати можливість працювати з реальними кіберзагрозами в умовах, максимально наближених до реальності. Це суттєво зменшує ризики, пов'язані з навчанням, що базується виключно на теорії, та сприяє формуванню практичних навичок. Використання ШІ у симуляційних платформах дозволяє моделювати сценарії з реальними кіберінцидентами – від фішингових атак і DDoS-ударів до шкідливого програмного забезпечення. Завдяки цьому здобувачі освіти мають змогу взаємодіяти з цифровим середовищем, приймати управлінські рішення, випробовувати різні методи захисту та аналізувати їхню результативність. Такий підхід поєднує глибокі теоретичні знання з цінним практичним досвідом, необхідним для протидії кіберзагрозам у сфері енергетики. Тому особливої важливості набуває розвиток освітніх ініціатив, симуляційних платформ, дуальної освіти та тісної співпраці між навчальними закладами, бізнесом і державними структурами для оперативної підготовки нової генерації кіберфахівців.

Також віддалена робота, використання незахищених Wi-Fi-з'єднань, домашніх пристроїв у корпоративних середовищах створюють нові вектори для проникнення, які особливо активно експлуатуються фішинговими кампаніями. Ці атаки все частіше використовують елементи ШІ для створення персоналізованих повідомлень у реальному часі, що значно підвищує їхню ефективність і складність виявлення. Статистикою підтверджено, що 96 % кібератак і витоку

даних розпочинається з e mail. E-mail захищений так само, як поштова листівка, адже електронні листи «проходять» через вразливі та потенційно небезпечні поштові сервери. При цьому, SSL/TSL не гарантує безпеки. Сьогодні перехоплення даних та «взлом» можливі всього за $ 200, а мережеві імпланти для перехоплення трафіку коштують всього від $ 60. Не дивно, що браузери назвичайно вразливі до «взломів». E-mail інфраструктура не верифікує відправника. Засоби захисту периметру компанії не захищають e-mailпісля відправки листів [15].

Навчання персоналу та підвищення кіберграмотності є ключовими для зменшення ризиків людського чинника. Кібербезпека повинна бути інтегрована в проєктування смарт-мереж на всіх етапах життєвого циклу. Впровадження стандартів допомагає уніфікувати політики безпеки. Умови децентралізації енергогенерації, зокрема використання ВДЕ, створюють додаткові виклики для забезпечення захисту від кібератак. Співпраця між операторами енергосистем, IT-компаніями та урядом є необхідною для створення єдиного захисного середовища. Важливу роль відіграє створення систем раннього попередження та обміну інформацією про інциденти.

Втім, стрімкий розвиток ШІ породжує дотримання етичних норм під час їх використання. Також одним із ключових напрямів впровадження ШІ в Україні, на нашу думку, є аналіз мережевого трафіку та моніторинг поведінки енергетичних систем у режимі реального часу з використанням інтелектуальних алгоритмів. Такий підхід дозволяє не лише оперативно виявляти потенційні кіберзагрози, але й підвищувати загальну стійкість критичної енергетичної інфраструктури до зовнішніх впливів.

Захист Smart Grid вимагає комплексного підходу, що включає як технічні, так і організаційні заходи. Необхідно впроваджувати багаторівневу автентифікацію, шифрування даних та безпечні протоколи комунікації. Кібербезпека повинна охоплювати як рівень генерації та передачі енергії, так і кінцевих споживачів. Особливо важливо забезпечити ізоляцію критичних компонентів від загальнодоступних мереж. Постійний моніторинг аномалій у мережевому трафіку дозволяє виявляти потенційні загрози на ранніх стадіях. Інтеграція систем ШІ у кіберзахист Smart Grid забезпечує вищий рівень

адаптивності до нових типів атак. Використання машинного навчання сприяє покращенню виявлення аномальної поведінки пристроїв. Необхідно проводити регулярні тести на проникнення для виявлення вразливих місць. Законодавча база повинна регулювати вимоги до кіберзахисту у Smart Grid та передбачати відповідальність за нехтування безпекою.

Постійне оновлення програмного забезпечення та патч-менеджмент повинні бути частиною щоденної практики управління кіберризиками. Розвиток цифрових двійників (digital twins) у Smart Grid дає нові можливості для моделювання атак і тестування захисту. Кібератаки на лічильники та пристрої користувачів можуть використовуватися для підриву довіри до всієї системи. Впровадження кіберменеджменту на підприємствах енергетичного сектору має здійснюватися в рамках загальної стратегії цифрової трансформації. Майбутнє смарт-енергетики тісно пов'язане з розвитком ефективної, гнучкої та прогнозованої системи кібербезпеки. Саме поєднання технологічних інновацій із проактивною безпековою політикою дозволить досягти високого рівня захищеності критичної енергетичної інфраструктури.

Таким чином, в сучасних умовах глобальної цифровізації та зростання кіберзагроз питання забезпечення кібербезпеки енергетичних підприємств набуває критичного значення. Особливо це актуально для України, де енергетична інфраструктура регулярно стає об'єктом цілеспрямованих атак з боку державних та приватних акторів. У відповідь на зростання складності та частоти кібератак виникає потреба у новій парадигмі управління кібербезпекою, що базується на застосуванні інтелектуальних технологій. Інтелектуалізація кіберзахисту передбачає інтеграцію ШІ, машинного навчання, аналітики великих даних та автоматизованих систем ухвалення рішень у процеси управління кіберризиками. Такий підхід дозволяє не лише виявляти загрози в режимі реального часу, а й прогнозувати їх розвиток, оцінювати вразливості та формувати проактивні стратегії захисту. Управлінський аспект інтелектуалізації кіберзахисту охоплює стратегічне планування, розподіл ресурсів, навчання персоналу, впровадження стандартів та забезпечення безперервності бізнес-процесів в умовах цифрових загроз. Ключовими бар'єрами

є низька обізнаність управлінців у сфері цифрової безпеки, недостатнє фінансування інновацій та обмежений доступ до висококваліфікованих фахівців. Разом із тим, міжнародний досвід демонструє, що впровадження ШІ в систему кібербезпеки суттєво знижує рівень втрат від інцидентів та підвищує надійність критичних інфраструктур.

В умовах зростаючої нестабільності в Чорноморському регіоні та посилення гібридних загроз, необхідним кроком є розширення міжнародної співпраці, зокрема з ЄС і НАТО. Спільне реагування на інциденти, обмін аналітикою та уніфікація стандартів захисту критичної інфраструктури повинні стати пріоритетами кіберстратегії України.

Основними шляхами мають бути:

Інтелектуальний моніторинг – використання алгоритмів машинного навчання для аналізу мережевого трафіку та виявлення аномальної активності.

Проактивне управління ризиками – прогнозування можливих сценаріїв атак із урахуванням історичних даних та поведінкових патернів.

Автоматизоване реагування – впровадження систем, здатних автономно виявляти та ізолювати шкідливі впливи до моменту ескалації.

Інтеграція кіберменеджменту в стратегічне управління енергетичною галузю – включення питань кіберзахисту до стратегій розвитку, інвестиційних планів.

Освітній компонент – формування культури кібербезпеки серед персоналу, включаючи регулярні тренінги, симуляції атак та сертифікацію фахівців.

Список використаних джерел

1. Дегтярьова О. О., Куклінова Т. В., Куклінова С. І. Системи ШІ в оптимізації енергетичних процесів:інноваційні підходи до ефективного управління сталим розвитком підприємства. *Вісник Хмельницького національного університету.* 2024. № 1. С. 359–362.

2. Degtiareva O., Shyriaieva N. Kuklinova T. Artificial Intelligence Solutions for Cybersecurity in Energy Systems. 2024 IEEE International Workshop on Technologies for Defense and Security (*TechDefense*). Naples, Italy. 2024. P. 177–182. DOI: 10.1109/TechDefense63521.2024.10863745.

3. Khan F., Mohsin S., Durad H. Dragonfly Cyber Threats: A Case Study of Malware Attacks Targeting Power Grids. *Journal of Computing & Biomedical Informatics*. 2023. Vol. 04. Is. 02. P. 172–185.

4. Збитки та втрати енергетичного сектору України внаслідок повномасштабного вторгнення Росії перевищили $56 млрд. Оцінка KSE Institute станом на травень 2024 року. Kyiv School of Economics. 2024. URL: https://kse.ua/ua/about-the-school/news/zbitki-ta-vtrati-energetichnogo-sektoru-ukrayini-vnaslidok-povnomasshtabnogo-vtorgnennya-rosiyi-perevishhili-56-mlrd-otsinka-kse-institute-stanom-na-traven-2024-roku/

5. Мохор В. В. Цифрова трансформація енергетики як запорука забезпечення її стійкості : Стенограма доповіді на засіданні Президії НАН України 4 жовтня 2023 року. *Вісник Національної академії наук України.* 2023. № 12. С. 74–79.

6. Омельченко В. Чому насправді відключають світло. *Центр Разумкова.* 2024. URL: https://razumkov.org.ua/napriamky/videokomentari/chomu-naspravdi-vidkliuchaiut-svitlo-ekspert

7. Особливості вітчізняного виробництва електроенергії. *Ukrainian Energy Exchange*. 2024. URL: https://www.ueex.com.ua/rus/presscenter/news/osobennosti-otechestvennogo-proizvodstva-elektroenergii/

8. Як Modus X розробляє та впроваджує рішення на ML та Copilot у DTEK. *Speka*. 2024. URL: https://speka.media/yak-modus-x-rozroblyaje-ta-vprovadzuje-risennya-na-ml-ta-copilot-u-dtek-936wmx

9. Держава почала створювати розумні електричні мережі – уже є 12 пілотних проєктів. Liga.net. 2024. URL: https://biz.liga.net/ua/all/all/novosti/derzhava-pochala-stvoriuvaty-rozumni-elektrychni-merezhi-uzhe-ie-12-pilotnykh-proiektiv

10. Голіздра О. Розбудова Розумна мережа – шлях до підвищення стійкості енергосистеми України. Укрінформ. 2024. URL: https://www.ukrinform.ua/rubric-economy/3863598-rozbudova-smart-grid-slah-do-pidvisenna-stijkosti-energosistemi-ukraini.html.

11. Чайка О. Російські хакери координують дії з військовими та посилюють атаки напередодні зими. Як Україна протистоїть кібератакам на енергосистему. November 15. 2023. *Forbes Ukraine.* URL: https://forbes.ua/company/rosiyski-khakeri-koordinuyut-dii-z-

viyskovimi-ta-posilyuyut-ataki-naperedodni-zimi-yak-ukraina-protistoit-kiberatakam-na-energosistemu-08112023-17242

12. Russian cyber operations: analytics for the H2 2024. State Service of Special Communications and Information Protection of Ukraine. Kyiv: State Service of Special Communications and Information Protection of Ukraine, 2024. 22 p.

13. Дегтярьова О. О. Соціально-економічні перспективи застосування ШІ в бізнес-середовищі: переваги та ризики. *Вісник соціально-економічних досліджень* : зб. наук. праць. Одеса : Одеський національний економічний університет. № 1–2. 2023. С. 118–130.

14. Горбаченко С. Місце менеджменту кібербезпеки у сучасній управлінській науці та практиці. *Сталий розвиток економіки*. 2024. № 1 (48). С. 144–149. URL: https://doi.org/10.32782/2308-1988/2024-48-19.

15. Краус К. М., Краус Н. М., Штепа О. В. Цифрова трансформація кібербезпеки на мікрорівні в умовах воєнного стану. URL: https://elibrary.kubg.edu.ua/id/eprint/42325/1/Kraus_Tsyfrova_transformatsiia_kiberbezpeky_2022.pdf