УДК 004.89:621.31
DOI https://doi.org/10.32689/maup.it.2025.3.3

Віктор БОЙКО
кандидат технічних наук, доцент, доцент кафедри кібербезпеки,
Національний університет «Одеська юридична академія»,
boyko-work@ukr.net
***ORCID:** 0000-0001-5929-657X*

Валерія СЛАТВІНСЬКА
доктор філософії в галузі «Право», асистент кафедри кібербезпеки,
Національний університет «Одеська юридична академія»,
slatvinskaya_valeriya@ukr.net
***ORCID:** 0000-0002-6082-981X*

Євгеній ПШЕНИЧНИЙ
здобувач вищої освіти,
Національний університет «Одеська юридична академія»,
psck@ukr.net
***ORCID:** 0009-0005-9534-9196*

ПРОБЛЕМА СТІЙКОСТІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ В УМОВАХ ЕНЕРГЕТИЧНИХ ЗБОЇВ

Анотація. *Метою статті є аналіз загроз для інформаційно-комунікаційних мереж (Information-Communication Networks – ICN) через перебої в живленні та розробка проактивної системи для підвищення їхньої стійкості.*

Методологія. *Дослідження базується на аналізі статистичних даних про зростання частоти блекаутів (на 64% більше збоїв у США за 2011–2021 роки порівняно з попереднім десятиліттям) та оцінці їхніх наслідків, таких як економічні збитки (понад 400 млн євро на Піренейському півострові) та втрата даних у енергозалежній оперативній пам'яті (RAM), що призводить до пошкодження системних файлів і каскадних збоїв у хмарних дата-центрах. Традиційні методи захисту (ДБЖ, генератори) оцінено як недостатні через високу вартість, експлуатаційні витрати, деградацію обладнання та залежність від людського фактора. Запропоновано проактивну систему прогнозування ризиків, яка використовує методи машинного навчання (ARIMA, LSTM) для аналізу історичних даних енергомереж (напруга, частота), метеорологічних факторів і даних операторів енергосистем. Система обчислює інтегральний показник ризику та автоматично запускає захисні сценарії для мінімізації збитків.*

Наукова новизна. *Новизна полягає в розробці проактивної системи прогнозування ризиків для ICN на основі машинного навчання, яка передбачає потенційні блекаути, замість реактивного реагування. Інтегральний показник ризику, що враховує енергетичні, метеорологічні та операційні дані, є унікальним інструментом для автоматичного запуску захисних сценаріїв, що знижує залежність від людського фактора та дорогого обладнання. Це рішення підвищує фізичну та кіберзахищеність мереж, мінімізуючи вразливості до каскадних збоїв, що є новим у порівнянні з традиційними підходами.*

Висновки. *Зростання частоти та масштабів блекаутів вимагає переходу до проактивних рішень. Запропонована система прогнозування на основі машинного навчання забезпечує своєчасне реагування на загрози, мінімізує збитки для інформаційних, програмних і апаратних компонентів ICN, підвищує кібербезпеку та забезпечує безперервність роботи в умовах енергетичних збоїв.*

Ключові слова: *інформаційно-комунікаційні мережі, стійкість інформаційно-комунікаційних систем, енергетичні збої, блекаут, кібербезпека, проактивне управління, прогнозування ризиків, машинне навчання, критична інфраструктура.*

Viktor BOYKO, Valeriia SLATVINSKA, Yevgeny PSHENYCHNY. THE PROBLEM OF STABILITY OF INFORMATION AND COMMUNICATION SYSTEMS IN CONDITIONS OF ENERGY FAILURES

Abstract. Scientific novelty. *The novelty lies in the development of a proactive risk forecasting system for ICN based on machine learning, which predicts potential blackouts, instead of a reactive response. An integral risk indicator, considering energy, meteorological and operational data, is a unique tool for automatically launching protective scenarios, which reduces dependence on the human factor and expensive equipment. This solution increases the physical and cyber security of networks, minimizing vulnerabilities to cascading failures, which is new compared to traditional approaches.*

Purpose. *The purpose of the article is to analyze the threats to Information-Communication Networks (ICN) due to power outages and develop a proactive system to increase their resilience.*

Methodology. *The study is based on the analysis of statistical data on the increase in the frequency of blackouts (64% more outages in the USA from 2011 to 2021 compared to the previous decade) and the assessment of their consequences, such as economic losses (over 400 million euros in the Iberian Peninsula) and data loss in volatile random access memory (RAM), leading*

to corruption of system files and cascading failures in cloud data centers. Traditional protection methods (UPS, generators) are assessed as insufficient due to high cost, operating costs, equipment degradation and dependence on the human factor. A proactive risk forecasting system is proposed that uses machine learning methods (ARIMA, LSTM) to analyze historical power grid data (voltage, frequency), meteorological factors, and power system operator data. The system calculates an integral risk indicator and automatically launches protective scenarios to minimize losses.

Conclusions. *The increase in the frequency and scale of blackouts requires a transition to proactive solutions. The proposed machine learning-based forecasting system provides a timely response to threats, minimizes damage to information, software and hardware components of ICN, increases cybersecurity and ensures continuity of work in conditions of energy failures.*

Key words: *information and communication networks, information and communication system resilience, power outages, blackouts, cybersecurity, proactive management, risk prediction, machine learning, critical infrastructure.*

Постановка проблеми в загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. У сучасних умовах інформаційно-комунікаційні мережі (Information-Communication Networks – ICN) є основою критичної інфраструктури, що забезпечує функціонування економіки, державного управління та суспільного життя. Їх безперебійна робота – ключовий фактор сталого розвитку. Однак, попри прогрес у галузі технологій, ICN залишаються дуже вразливими до зовнішніх впливів, зокрема, до великомасштабних збоїв в електропостачанні, відомих як блекаути (blackouts) [15], [4]. Ці інциденти демонструють тривожну тенденцію до зростання частоти та масштабів, що підтверджується не лише емпіричними спостереженнями, а й статистичними даними. Наприклад, згідно з розрахунками аналітичного центру Climate Central [7], у Сполучених Штатах за період 2011–2021 років сталося на 64% більше великих збоїв в електромережах, ніж за попереднє десятиліття (2000–2010). Подібна динаміка спостерігається і в інших регіонах світу, включно з Європою та Азією, де зростання споживання та старіння інфраструктури створюють підвищені ризики.

Руйнівні наслідки блекаутів виходять далеко за рамки короткочасної незручності. Прикладом може слугувати інцидент, що стався 28 квітня 2025 року на Піренейському півострові [19]. Цей збій, що охопив Іспанію, Португалію, Андорру, частину Франції та Марокко, призвів не тільки до колапсу транспортної системи та зупинки метрополітену у великих містах, таких як Лісабон і Мадрид, а й до трагічних людських жертв – щонайменше одна людина загинула в Португалії, а вісім – в Іспанії внаслідок пожеж, спричинених спробами аварійного освітлення. Економічні збитки від цього інциденту, за різними оцінками, перевищили 400 мільйонів євро. Ці збитки складалися з безлічі факторів: втрати прибутку підприємств через простій, збитків від псування продукції, порушень логістичних ланцюжків і витрат на відновлення пошкодженого обладнання. Основні причини таких масштабних збоїв, як правило, мають комплексний характер, включно зі зносом інфраструктури, зростанням енергоспоживання, низькою автоматизацією управління та людським фактором [4].

Аналіз останніх досліджень і публікацій. Проблема стійкості інформаційно-комунікаційних систем (ICN) в умовах енергетичних збоїв стає дедалі актуальнішою через зростання частоти блекаутів, спричинених кліматичними змінами, старінням інфраструктури та залежністю від відновлювальних джерел енергії, що впливає на роботу дата-центрів, телекомунікаційних мереж і критичних сервісів. У роботах останніх років значна увага приділяється аналізу тенденцій збоїв і розробці проактивних рішень для підвищення живучості ICN [15, с. 1–8; 20, с. 428–431]. Так, P. Hines, J. Apt та S. Talukdar досліджують історичні дані про великі блекаути в США, вказуючи на їх стабільну частоту та power-law розподіл розмірів [15, с. 1–8], тоді як Y.-K. Wu, S. M. Chang та Y.-L. Hu підкреслюють комплексні причини збоїв, включаючи перевантаження мереж і каскадні відмови [20, с. 428–431]. Звіт ASCE 2021 року оцінює енергетичну інфраструктуру США на D+, зазначаючи зростання попиту від дата-центрів і вразливість до погодних факторів [4], а Climate Central фіксує 78% зростання погодних збоїв за 2011–2021 рр. [7]. B. A. Carreras та ін. аналізують ризики блекаутів при високому проникненні ВДЕ, акцентуючи на флуктуаціях і каскадних ефектах [5, с. 132663–132674], а E. L. Ratnam та ін. пропонують диверсифікацію для підвищення стійкості до кліматичних і кіберзагроз [18]. Конкретні інциденти, як-от блекаут на Піренейському півострові 2025 р. [19], збої Google Cloud 2023 р. через відмови ДБЖ [2; 9; 13; 14] та проблеми в дата-центрі 2025 р. [17], ілюструють вразливість ICN до перебоїв живлення. В. Бойко, М. Василенко та В. Слатвінська розробили моделі живучості ICN з використанням графового підходу для симуляції відновлення після збоїв [1, с. 13–19], а M.-G. Florin та ін. класифікують ризики енергетичних криз за матрицею ймовірність-вплив [11]. Застосування машинного навчання для прогнозування збоїв досліджується в роботах U. Farooq та R. B. Bass [10, с. 61494–61519], A. K. Onaolapo та ін., які пропонують колаборативні нейронні мережі для передбачення збоїв [16, с. 3079–3087], а також у дослідженнях Aalto University [3] та B. Ghasemkhani та ін., де розроблено моделі для оцінки тривалості збоїв [12].

Метою даної статті є обґрунтування та розробка концепції системи проактивного прогнозування ризиків для забезпечення стійкості інформаційно-комунікаційних мереж (ICN) в умовах енергетичних

збоїв. Для цього зроблено наступні кроки: аналіз існуючих загроз, спричинених блекаутами, для ICN; критичний огляд обмежень традиційних методів захисту; обґрунтування необхідності переходу від реактивних до проактивних методів реагування; опис методології та архітектури системи, що використовує методи машинного навчання для прогнозування інцидентів; деталізація етапів впровадження та експлуатації запропонованої системи.

Виклад основного матеріалу. *Загрози для інформаційно-комунікаційних мереж: Технічні та організаційні аспекти.* Припинення електропостачання є критичною загрозою для ICN з кількох ключових причин. Найсуттєвішими є: втрата даних, що зберігаються в енергозалежній оперативній пам'яті (ОЗП), і порушення зв'язності мережі, особливо в централізованих ієрархічних системах.

• Втрата даних в оперативній пам'яті

Сучасні комп'ютерні системи, від персональних комп'ютерів до потужних серверів, побудовані на архітектурі фон Неймана. У її основі лежить принцип зберігання виконуваного програмного коду та оброблюваних даних в одній і тій самій пам'яті – оперативній пам'яті (RAM). RAM є енергозалежною, тобто її вміст повністю стирається при втраті електроживлення. Це зумовлено її фізичною природою – RAM використовує тригери та конденсатори, які вимагають постійного електричного заряду для підтримання стану «1» або «0». З одного боку, це дозволяє RAM досягати надзвичайно високої швидкодії, що набагато перевищує швидкість доступу до даних на енергонезалежних накопичувачах, таких як жорсткі диски (HDD) або твердотільні накопичувачі (SSD). З іншого боку, раптове відключення живлення, оминаючи штатні процедури завершення роботи операційної системи, призводить до миттєвої втрати всіх даних, які знаходилися в RAM у момент збою. В результаті можуть бути втрачені не тільки незбережені дані користувача, а й критично важливі системні файли, що потенційно веде до пошкодження операційної системи та необхідності її повної перевстановлення.

• Каскадні збої в централізованих системах

Розвиток ICN тяжіє до централізації та ієрархізації [1]. Поява потужних обчислювальних систем і дата-центрів призвела до широкого впровадження технологій віртуалізації та контейнеризації. Ці технології дозволяють оптимально використовувати ресурси потужних комп'ютерних кластерів: обчислювальні потужності можна «розділяти» між користувачами, створювати системи, які автоматично регулюють витрату ресурсів, та оптимізувати розгортання програмного забезпечення за допомогою заздалегідь створених образів операційних систем і контейнерів.

Однак, з точки зору стійкості, це створює додаткові ризики. У таких системах в RAM зберігаються не тільки дані операційної системи та користувацьких процесів, а й частини систем забезпечення віртуалізації та контейнеризації (гіпервізори, частини систем контейнеризації). Раптове відключення живлення може призвести до каскадного збою, коли відмова одного централізованого вузла тягне за собою втрату зв'язності та функціональності в масштабах усієї мережі [8]. Прикладом є збій у зоні us-east5-c дата-центру Google Cloud [2], спричинений відмовою джерела безперебійного живлення (ДБЖ) [9]. Цей інцидент призвів до порушення роботи понад двадцяти різних сервісів, зачепивши тисячі користувачів по всьому світу [13]. Інший подібний випадок – збій 25 квітня 2023 року в зоні europe-west9-a, де витік води та подальша пожежа призвели до відключень і вимагали понад доби на відновлення [14].

• Проблеми кібербезпеки під час енергетичних збоїв

Проблема енергетичних збоїв прямо впливає на кібербезпеку, створюючи нові вектори загроз, які виходять за межі простої відсутності зв'язку [20]. Раптове відключення живлення може призвести до незапланованого і некоректного завершення роботи систем, що порушує цілісність даних і конфігурацію програмного забезпечення. Під час блекауту критично важливі служби, які забезпечують кібербезпеку – системи виявлення вторгнень (IDS), системи протидії вторгненням (IPS), міжмережеві екрани (firewalls), системи моніторингу та логування – можуть вийти з ладу як і все інше програмне забезпечення. Оскільки зловмисники можуть скористатися ситуацією, щоб проникнути в систему, залишити шкідливе програмне забезпечення або скомпрометувати дані, це значно підвищує ризик інцидентів. Наприклад, якщо під час збою відключається система резервного копіювання, це може призвести не тільки до втрати даних, але й до потенційного збою в роботі системи відновлення [5].

Також блекаути можуть призвести до зниження контролю та втрати управління мережею [18]. У ситуації блекауту системи дистанційного моніторингу та управління можуть бути недоступними, що робить неможливим оперативне реагування на будь-які кіберінциденти [11]. Персонал може бути позбавлений можливості вчасно реагувати на попередження, виявлені в системах моніторингу, які ще продовжують працювати від ДБЖ або додаткових джерел живлення. Це може призвести до затримки в реагуванні на кібератаки і, як наслідок, збільшення збитків. Крім того, відновлення після збою може бути пов'язане з високим ризиком. Коли системи перезавантажуються після тривалої відсутності живлення, вони можуть бути вразливі до атак «нульового дня» або інших загроз, які зловмисники могли

ISSN 2786-5460 (Print), ISSN 2786-5479 (Online)

запустити під час збою. Наприклад, якщо зловмисники фізично отримали доступ до обладнання під час блекауту, вони можуть встановити шкідливе програмне забезпечення, яке спрацює під час відновлення живлення.

Тому перехід до проактивного управління енергетичною стійкістю, що включає прогнозування ризиків за допомогою машинного навчання є необхідним елементом комплексної стратегії кібербезпеки. Такий підхід дозволяє не просто реагувати на збій, а запобігти його негативним наслідкам, захищаючи цілісність даних і безперервність роботи критичних сервісів ще до того, як інцидент набуде критичного характеру.

Аналіз існуючих рішень та їх обмежень. Традиційним і найбільш прямолінійним шляхом вирішення проблеми енергетичних збоїв є резервування – часто багаторазове – всіх існуючих систем енергоживлення та автоматизація переходу на аварійне електропостачання. Зазвичай вибудовується двоетапна система:

- Джерело безперебійного живлення (ДБЖ): Має вбудований акумулятор і розраховане на підтримання функціонування обладнання в проміжку від кількох хвилин до кількох годин. Це дозволяє коректно завершити роботу обладнання або переключитися на резервне джерело.
- Дизельний або газовий генератор: Паралельно з ДБЖ запускається додаткове джерело живлення, яке забезпечує автономне електроживлення протягом тривалого часу, до усунення основної проблеми.

Однак такий підхід, попри його очевидні переваги, пов'язаний з низкою суттєвих обмежень. По-перше, він пов'язаний з великими капітальними та експлуатаційними витратами на підтримання резервної інфраструктури. По-друге, його ефективність часто «впирається» в людський фактор. Автори неодноразово стикалися з ситуацією, коли за наявності генератора персонал не міг його запустити вчасно через помилки в процедурі, що призводило до втрати живлення – і пов'язаної з цим втрати даних і порушення робочих процесів.

Вартість повного резервування є значним бар'єром. Вона включає не тільки капітальні витрати на придбання обладнання, а й регулярні експлуатаційні витрати на паливо, технічне обслуговування та заміну компонентів. Акумулятори ДБЖ, наприклад, мають обмежений термін служби (зазвичай 3–5 років) і вимагають дорогої заміни. Їх ємність знижується з кожним циклом розряду-заряду, а також під впливом високих температур, що робить їх все менш надійними з часом. Ця природна деградація обладнання перетворює стаціонарні системи резервування на «одноразові» рішення, якщо не приділяти належної уваги їх своєчасному оновленню та обслуговуванню.

Додатковим ускладнювальним фактором є чутливість систем резервування до технічного обслуговування. Наприклад, експлуатація дизельних генераторів має тимчасові обмеження, після яких їх необхідно відключати для охолодження та/або профілактики. Самі генератори вимагають регулярного змащення, заміни фільтрів і контролю рівня палива. ДБЖ, своєю чергою, функціонують від акумуляторів, що перезаряджаються, які мають обмежену кількість циклів перезарядки, після чого їх ємність зменшується. На ємність і швидкість розряду акумуляторів може впливати температура навколишнього середовища, режим і швидкість перезарядки.

Таким чином, навіть система з «буферними» ДБЖ і довгостроковими резервними генераторами є складною системою, яка з часом може деградувати, особливо за відсутності належного обслуговування і регулярного тестування. Характерним прикладом є «одноразовий» ДБЖ, в якому не передбачено зміну акумулятора, що робить його ненадійним у довгостроковій перспективі.

Можливості прогнозування інцидентів. Інциденти з перебоями енергопостачання можна умовно розділити на дві категорії: прогнозовані та непрогнозовані. Якщо запобігти шкоді від раптових подій (наприклад, землетрусу) складно, то прогнозовані події, за умови адекватної та своєчасної реакції на них, дозволяють мінімізувати або повністю запобігти збиткам. Можливості прогнозування в сучасних умовах досить широкі, що пов'язано з характером функціонування енергосистеми.

Енергетичні мережі є складними та розподіленими системами. Суттєву роль у їх стійкості відіграє рівномірність і співмірність навантаження з генеруючими потужностями. Забезпечення цього балансу визначає стабільність мережі. Чим більша енергосистема (за умови її керованості), тим вища її живучість, оскільки великий розмір дозволяє в разі несприятливих впливів перерозподіляти потужності між різними ділянками, вирівнюючи навантаження. Крім того, важливим елементом є системи накопичення-віддачі енергії, такі як гідроакумулювальні електростанції (ГАЕС), які можуть змінювати режим роботи, виробляючи більше або менше енергії залежно від потреб.

Аналіз інцидентів показує, що настанню блекауту часто передують зміни в стані енергомережі та її параметрів (напруга, частота) [6], [19], [17]. Як правило, блекаут є наслідком проблем на якійсь ділянці, які намагаються скомпенсувати шляхом «маневрування» енергосистемою – зміною режиму роботи

генерації та перерозподілом потоків енергії. Такі дії можуть як увінчатися успіхом, так і призвести до більш глобального відключення, якщо ресурсів для «маневру» не вистачить. Важливо, що подібні дії впливають на стан енергомережі та можуть бути відстежені як зміни в стабільних до цього моменту параметрах [10], [17]. Точність прогнозування можна суттєво підвищити, враховуючи додаткові параметри [5], [16]:

- Метеорологічні дані: Погодні явища, такі як сильний вітер, грози, обмерзання, снігопади або спека, є частими причинами пошкоджень ліній електропередач (ЛЕП) і обладнання.
- Сезонні та тимчасові дані: Час року та доби, що впливають на загальний рівень споживання та виробництво електроенергії (наприклад, піки навантаження в літню спеку через кондиціонери або в зимові морози через опалення).
- Технічні дані: Дані від датчиків і систем моніторингу, які можуть вказувати на перевантаження обладнання або аномальні режими роботи.

Система проактивного прогнозування ризиків. З урахуванням усіх перерахованих обмежень, пропонується впровадження додаткової міри безпеки – *системи проактивного прогнозування ризиків*. Цей інструмент буде відстежувати стан мережі енергопостачання та аналізувати вторинні параметри, такі як загальне навантаження на мережу в межах контрольованої інфраструктури, зміни в стані енергосистеми, вхідні повідомлення від служб оповіщення і навіть прогнози погоди [3]. В основі пропонованого рішення лежить концепція раннього попередження, реалізована за допомогою методів машинного навчання [12]. Замість того щоб пасивно реагувати на збій, система активно аналізує безліч параметрів, передбачаючи ймовірність його настання. Для цього можуть бути використані прогностичні моделі на основі часових рядів, такі як *ARIMA* (Autoregressive Integrated Moving Average) або *LSTM* (Long Short-Term Memory). Ці моделі навчаються на історичних даних про стан енергомережі (напруга, частота, навантаження) і здатні виявляти аномалії, що передують великим збоям.

Як додаткові параметри можуть бути використані:

- Дані від метеорологічних служб: Інформація про наближення штормів, сильних вітрів та обмерзання, які можуть пошкодити ЛЕП.
- Інформація від операторів енергосистем: Оповіщення про планові або позапланові роботи, аварії на підстанціях.

На основі аналізу цих даних, система обчислює інтегральний показник ризику. Чим вищий показник, тим вища ймовірність збою.

Система може функціонувати як система підтримки прийняття рішень (СППР) для персоналу, відповідального за забезпечення функціонування енергосистеми. Така система може бути реалізована у вигляді поєднання централізованого дашборду з інформацією для оператора та API для інтеграції з існуючою інфраструктурою.

Вона могла б видавати попередження про можливі відключення, дозволяючи оператору прийняти своєчасне рішення. Однак зважаючи на швидкоплинність подібних інцидентів, видається корисним, щоб така система працювала в автоматичному режимі. У такому режимі вона спочатку вживає необхідних заходів щодо недопущення втрати даних, а потім інформує оператора.

Ключовою особливістю системи є її здатність до «м'якого управління», що дозволяє уникнути помилкових спрацьовувань і невиправданого відключення обладнання. Залежно від величини ризику, система може переводити функціонування системи на кілька різних рівнів. Наприклад:

- Рівень 1 (Низький ризик): Відправка повідомлення адміністратору.
- Рівень 2 (Середній ризик): Підготовка резервних систем до роботи (наприклад, прогрів дизельного генератора, перевірка статусу ДБЖ).
- Рівень 3 (Високий ризик): Автоматичне виконання захисних сценаріїв, таких як збереження відкритих даних.
- Рівень 4 (Аварійне реагування): Коректне завершення роботи некритичних сервісів і переведення ключових систем на резервне живлення.

Це дозволяє мінімізувати збитки, не вдаючись до радикальних заходів при кожному незначному коливанні мережі.

Слід враховувати, що в такому режимі можливі помилкові спрацьовування та помилки в прогнозуванні, тому оптимальним буде «м'яке управління», що мінімізує можливий збиток від таких помилок. Система може приймати рішення про переведення обладнання в режим підвищеного ризику, про підготовку систем резервування тощо, залежно від розрахованих показників ризику. Це дозволяє уникнути непотрібних відключень і зберегти безперервність роботи при незначних коливаннях.

Система прогнозування: Методологія та реалізація. Сам по собі комп'ютер, як пристрій, не має спеціальних сенсорів для вимірювання параметрів енергомережі. Внутрішні сенсори вимірюють

ISSN 2786-5460 (Print), ISSN 2786-5479 (Online)

напругу та інші параметри роботи мікропроцесора та іншого апаратного забезпечення, які знаходяться «позаду» блока живлення. Блок живлення компенсує і згладжує коливання напруги та інших параметрів енергоживлення і таким чином нівелює можливість спостережень. Таким чином, до недавнього часу відстеження основних параметрів вимагало дорогої вимірювальної апаратури. Однак блекаути спричинили широке поширення та еволюцію систем безперебійної напруги. Наразі більшість професійних джерел безперебійного живлення забезпечені інформаційними інтерфейсами (мережеві карти, USB, послідовні порти), підключившись до яких, можна отримати показання параметрів мережі, таких як напруга, частота, навантаження та стан акумулятора. Регулярний збір цієї інформації дозволяє сформувати велику базу даних, яка і послужить основою для роботи системи прогнозування.

Пропонована нами система захисту використовує наявну інфраструктуру для відстеження основних параметрів і доступ до інтернету для моніторингу вторинних. Для прогнозування використовуються методи машинного навчання, які на основі аналізу отриманої інформації обчислюють значення величини ризику. Залежно від величини ризику, система приймає рішення про режим роботи. Слід зазначити, що в різних випадках можуть мати місце різні набори режимів роботи та сценаріїв реагування. Також розумно надати користувачеві можливість визначати свої власні сценарії на основі вже заданих. Така система в разі експлуатації POSIX-сумісних веб-серверів може спиратися на використання частково реалізованих сценаріїв (наприклад, unit-ів у рамках systemd підходу). Якщо розглянута або контрольована система є розподіленою, слід забезпечити централізований дашборд, можливість управління і включення-виключення робочих станцій і дистанційне управління ними. Пропонована система швидкого реагування при розгортанні буде деякий час збирати інформацію в пасивному режимі, формуючи інформаційно-часовий ландшафт поведінки енергомережі та зіставляючи його з вторинними параметрами.

Пропонована система прогнозування енергетичних збоїв складається з трьох основних частин: блоку збору даних (Data Collection Unit), блоку обробки та аналізу даних (Processing and Analytics Unit), блоку проактивного реагування (Proactive Response Unit).

Блок збору даних – це «сенсорний» рівень, який відповідає за збір інформації з різних джерел. До нього входять модулі-агенти та мережеві інтерфейси/API-шлюзи. Модулі-агенти являють собою програмне забезпечення, встановлене на пристроях або серверах, під'єднаних до ДБЖ. Вони в реальному часі збирають дані про напругу, частоту, навантаження і стан акумуляторів. Мережеві інтерфейси/API-шлюзи забезпечують підключення до зовнішніх джерел, таких як метеорологічні сервіси, API операторів енергомереж і новинні стрічки.

Зібрані дані перетворюються та аналізуються для прогнозування ризиків за допомогою блоку обробки та аналізу даних. Цей блок функціонально поділяється на базу даних, модуль обробки даних і модуль прогнозування. База даних використовується для зберігання історичної та поточної інформації про стан енергосистеми. Структура оптимізована для швидкого аналізу даних часових рядів. Як така база може використовуватися DuckDB.

Модуль обробки даних очищає, нормалізує та агрегує дані, готуючи їх для моделі машинного навчання. Модуль прогнозування (Prediction Engine) являє собою ядро системи, де розгорнуто модель машинного навчання (наприклад, LSTM або ARIMA). Вона аналізує дані та обчислює інтегральний показник ризику в реальному часі.

Блок проактивного реагування складається з модулів прийняття рішень, модуля автоматичного реагування та інтерфейсу оператора (dashboard). Він відповідає за прийняття рішень і взаємодію з оператором або іншими системами. Модуль прийняття рішень на основі показника ризику визначає необхідний рівень реагування (низький, середній, високий). Модуль автоматичного реагування виконує заздалегідь задані сценарії (скрипти для коректного завершення роботи, перемикання на резервне живлення) залежно від рівня ризику. Візуальний дашборд відображає поточний стан системи, рівень ризику, історію збоїв і прогнози, слугуючи основним інструментом для оператора.

Розгортання системи проактивного реагування. Процедуру впровадження та розгортання такої системи можна розділити на кілька ключових етапів, що забезпечують поетапне та контрольоване впровадження. Послідовність має включати в себе підготовчий етап, етап розгортання, етап навчання і тестування, етап експлуатації та моніторингу – основний етап роботи системи.

На підготовчому етапі проводиться аналіз і планування, необхідні для успішного старту проєкту. Зокрема, етап включає в себе визначення цілей і вимог проєкту. Слід визначити, які саме ICN будуть захищені, і які критичні сервіси необхідно захистити насамперед. Далі визначаються допустимі ризики та цільові показники стійкості. Потім розробляються сценарії реагування для кожного рівня ризику (наприклад, що буде відбуватися при «низькому», «середньому» і «високому» ризику).

Після цього проводиться аналіз існуючої інфраструктури: проводиться аудит ДБЖ, генераторів та іншого обладнання. У процесі слід визначити, що ДБЖ мають необхідні інформаційні інтерфейси (USB, мережеві порти) для збору даних і передбачити їх заміну або встановлення додаткових датчиків у разі відсутності таких. Також цей аналіз має включати оцінку можливостей існуючої мережі для передачі даних і віддаленого управління.

Паралельно може виконуватися збір і підготовка первинних і вторинних даних – розгортається програмне забезпечення для збору даних з ДБЖ (наприклад, за допомогою протоколу SNMP), налаштовується підключення до метеорологічних служб, API операторів енергомереж та інших зовнішніх джерел даних. Визначається формат зберігання даних і планується структура бази даних для їх зберігання та обробки.

Далі розробляється та уточнюється архітектура системи: модулі збору даних, модуль прогнозування (модель машинного навчання), модуль прийняття рішень та інтерфейс для оператора (дашборд) тощо.

На етапі розгортання виконується безпосереднє встановлення та налаштування компонентів системи. За необхідності, якщо наявні ДБЖ не підходять, проводиться їх заміна на моделі з можливістю віддаленого моніторингу. Якщо потрібно (і є така можливість у проєкті), встановлюються додаткові датчики.

Далі виконується розгортання програмного забезпечення: встановлюються та налаштовуються модулі збору даних на серверах або виділених пристроях, перевіряється підключення до ДБЖ, встановлюється модуль машинного навчання на обчислювальному сервері або в хмарі, створюється та налаштовується база даних.

Далі настає етап навчання і тестування. Система працює в пасивному режимі, щоб зібрати дані та налаштувати модель. У процесі функціонування відбувається пасивний збір даних: відбувається безперервний збір даних про стан енергомережі та зовнішні параметри. Цей період має тривати достатньо довго (кілька тижнів або місяців), щоб накопичити репрезентативний обсяг даних, що відображає нормальні та аномальні режими роботи.

Далі в рамках цього етапу виконується навчання та валідація моделі: накопичені дані використовуються для навчання моделі машинного навчання. Виявляються закономірності, що передують збоям. Для оцінки точності та зниження помилкових спрацьовувань проводиться валідація та доналаштування моделі.

Після або паралельно з навчанням моделі проводиться розробка та налаштування сценаріїв реагування. На основі аналізу даних і поведінки моделі оптимізуються пороги спрацьовування для кожного рівня ризику. Тестуються сценарії реагування (скрипти для коректного завершення роботи, перемикання на резерв, відправлення повідомлень тощо). Також виконується навчання персоналу відповідального за ICN, роботі з новими інтерфейсами, розробляються схеми та інструкції з реагування на різні рівні ризику.

Після проходження трьох попередніх етапів, система починає працювати в режимі реального часу. Протягом цього етапу безперервно виконується моніторинг і аналіз роботи системи, регулярно проводиться рекалібрування та донавчання моделі для адаптації до нових умов. Також у процесі роботи системи регулярно формуються звіти про роботу, про ефективність системи та запобігання інцидентам.

Загалом, поетапне впровадження, починаючи з пасивного збору даних і навчання, дозволяє побудувати надійну та ефективну систему, яка мінімізує ризики та підвищує стійкість ICN.

Висновки. Збільшення частоти та масштабів блекаутів вимагає додаткових заходів для забезпечення стійкості ICN. Перебої з напругою можуть призводити не тільки до первинних наслідків, пов'язаних із простоєм ICN, а й до втрати цілісності збереженої інформації та, в деяких випадках, до псування обладнання. Рішення у вигляді додаткового дублювання систем електроживлення часто є недостатнім і економічно недоцільним, оскільки системи дублювання розраховані на порівняно недовгі терміни експлуатації і при тривалій і напруженій експлуатації самі починають виходити з ладу.

Тому, незалежно від використовуваних заходів, пропонується використання додаткової системи управління ICN, яка виконуватиме прогнозування можливих збоїв на основі аналізу поведінки енергомережі та вторинних параметрів. На основі розрахованого ризику система обиратиме режим роботи ICN так, щоб мінімізувати можливі втрати. Така система може працювати як самостійно, так і як доповнення до вже існуючих когнітивно-імітаційних моделей відновлення ICN.

Розгортання та функціонування такої системи управління дозволить вчасно реагувати на інциденти з втратами електроживлення, що, своєю чергою, істотно знизить ризики збитку для інформаційної, програмної та апаратної частини ICN, а також підвищить живучість і стійкість експлуатації в умовах, пов'язаних з перебоями в мережах напруги.

ISSN 2786-5460 (Print), ISSN 2786-5479 (Online)

Список використаних джерел:

1. Бойко В., Василенко М., Слатвінська В. Моделювання живучості та відновлення інформаційно-комунікаційних мереж в умовах дії кіберзагроз. *Інформаційні технології та суспільство*. 2024. № 1 (12). С. 13–19. URL: https://journals.maup.com.ua/index.php/it/article/view/3143.

2. A major Google Cloud outage was caused by uninterruptible power supplies being interrupted. URL: https://www.techradar.com/pro/a-major-google-cloud-outage-was-caused-by-uninterruptible-power-supplies-being-interrupted, 2023.

3. Aalto University. Machine learning helps to predict blackouts caused by storms. URL: https://www.aalto.fi/en/news/machine-learning-helps-to-predict-blackouts-caused-by-storms-0, 2019.

4. American Society of Civil Engineers (ASCE). 2021 Report Card for America's Infrastructure: Energy. American Society of Civil Engineers; URL: https://infrastructurereportcard.org/cat-item/energy-infrastructure/, 2021.

5. Carreras B. A., Colet P., Reynolds-Barredo J. M., Gomila D. Assessing Blackout Risk With High Penetration of Variable Renewable Energies. *IEEE Access*. 2021. Vol. 9. P. 132663–132674.

6. Carreras B. A., Newman D. E., Dobson I. North American Blackout Time Series Statistics and Implications for Blackout Risk. *IEEE Transactions on Power Systems*. 2016. Vol. 31, No. 6. P. 4406–4414.

7. Central C. Surging Weather-Related Power Outages. URL: https://www.climatecentral.org/climate-matters/surging-weather-related-power-outages, 2021.

8. Connexion France. French mobile network operator SFR hit by major outage. URL: https://www.connexionfrance.com/news/french-mobile-network-operator-sfr-hit-by-major-outage/730194, 2023.

9. Data Center Dynamics. UPS issue caused Google Cloud's March outage. URL: https://www.datacenterdynamics.com/en/news/ups-issue-caused-google-clouds-march-outage/, 2023.

10. Farooq U., Bass R. B. Frequency Event Detection and Mitigation in Power Systems: A Systematic Literature Review. *IEEE Access*. 2022. Vol. 10. P. 61494–61519.

11. Florin M.-G., Iosif M. R., Daniel F. N., Mihai S. A., Mihai P.-S., Alin C. E., Ioan S., Eugen S. G., Obretenova M. I. Assessment of Vulnerabilities and Risks That May Generate Energy Crises – Blackout. *Preprints*, 2025. URL: https://doi.org/10.20944/preprints202504.0815.v1.

12. Ghasemkhani B., Kut R. A., Yilmaz R., Birant D., Arıkök Y. A., Güzelyol T. E., Kut T. Machine Learning Model Development to Predict Power Outage Duration (POD): A Case Study for Electric Utilities. *Sensors*. 2024. Vol. 24, No. 13.

13. Google Cloud. Incident Report for us-east5-c outage on March 14, 2023: Incident Report N3Dw7nbJ7rk7qwrtwh7X. Google Cloud; URL: https://status.cloud.google.com/incidents/N3Dw7nbJ7rk7qwrtwh7X, 2023.

14. Google Cloud. Incident Report for us-east9-a on April 25, 2023: Incident Report dS9ps52MUnxQfyDGPfkY. Google Cloud; URL: https://status.cloud.google.com/incidents/dS9ps52MUnxQfyDGPfkY, 2023.

15. Hines P., Apt J., Talukdar S. Trends in the history of large blackouts in the United States. 2008. IEEE Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century. 2008. P. 1–8.

16. Onaolapo A. K., Carpanen R. P., Dorrell D. G., Ojo E. E. Event-Driven Power Outage Prediction using Collaborative Neural Networks. *IEEE Transactions on Industrial Informatics*. 2023. Vol. 19, no. 3. P. 3079–3087.

17. Powerquality.blog. UPS Problem at Datacenter. URL: https://powerquality.blog/2025/03/17/ups-problem-at-datacenter/, 2025.

18. Ratnam E. L., Baldwin K. G. H., Mancarella P., Howden M., Seebeck L. Electricity system resilience in a world of increased climate change and cybersecurity risk. *The Electricity Journal*. 2020. Vol. 33, 9. 106833. URL: https://www.sciencedirect.com/science/article/pii/S1040619020301251.

19. Unipower. What Caused the Big Blackout in Spain and Portugal? URL: https://www.unipower.se/news/what-caused-the-big-blackout-in-spain-and-portugal/, 2025.

20. Wu Y.-K., Chang S. M., Hu Y.-L. Literature Review of Power System Blackouts. *Energy Procedia*. 2017. Vol. 141. P. 428–431. URL: https://www.sciencedirect.com/science/article/pii/S1876610217354619.

Дата надходження статті: 23.09.2025
Дата прийняття статті: 20.10.2025
Опубліковано: 04.12.2025