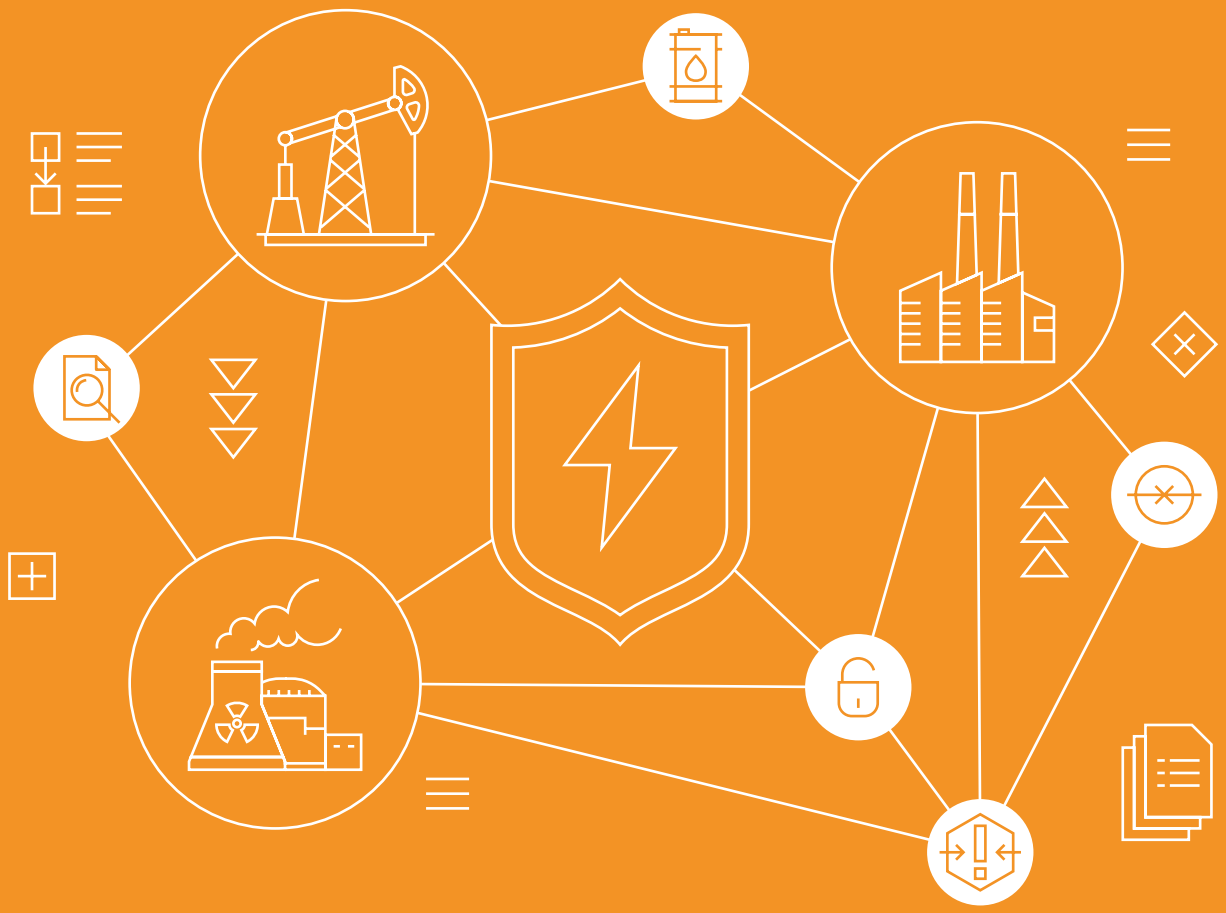


ОЦІНКА СТІЙКОСТІ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

АНАЛІТИЧНИЙ ЗВІТ

Автори дослідження:
Павленко Олена, Антоненко Антон, Ніцович Роман, Євтушок Сергій, Суходоля Олександр
Команда проєкту «Стійкість України: комплексна оцінка ризиків і загроз для держави, бізнесу і громад»
((Булах Анна, Клімкін Павло, Кадигроб Володимир, Тарасюк Антон, Гаврилюк Олександр).

ЗМІСТ

ВСТУП

Це дослідження, що виконувалося протягом травня-червня 2021 року проводить аналіз стійкості української енергетичної системи до ризиків, що можуть бути спричинені фізичними та кібер загрозами.

Аналітичний продукт призначений для українських центральних та місцевих органів влади, громадського сектору та бізнесу, що відповідальні або зацікавлені у розбудові системи стійкості української енергетичної інфраструктури.

Під час дослідження експерти спиралися на відриті джерела (дані американських органів влади, Міненерго, НКРЕКП, РНБО та інші українські органи влади), а також дослідження, статті та інші аналітичні продукти, опубліковані в Україні та за кордоном.

Дослідження складається з трьох розділів та додатків. Перший розділ містить методологічний підхід до дослідження та опис української енергетичної системи. Визначаються основні поняття та модель реагування енергетичної системи на кризи.

У другому розділі досліджується досвід США з робудови системи енергетичної стійкості та захисту критичної інфраструктури. Проводиться огляд законодавства США із захисту критичної інфраструктури та забезпечення стійкості енергетичного сектору. Наводиться модель реагування енергетичного сектору США на фізичні та кібер загрози.

У третьому розділі аналізується практика реагування на загрози електроенергетичного сектору в Україні та порівнюються системи захисту електрозабезпечення США та України та виокремлюються «пробіли» української «екосистеми». Пропонується підхід до реагування на загрози учасниками енергетичної системи України.

РОЗДІЛ І.
МЕТОДОЛОГІЧНІ ОСНОВИ ДОСЛІДЖЕННЯ ТА ОПИС УКРАЇНСЬКОЇ ЕНЕРГЕТИЧНОЇ «ЕКОСИСТЕМИ»

1.1 КОНЦЕПТУАЛЬНИЙ ПІДХІД ДОСЛІДЖЕННЯ ДО ОЦІНКИ ЕНЕРГЕТИЧНОЇ СТІЙКОСТІ УКРАЇНИ ТА ВИРОБЛЕННЯ РЕКОМЕНДАЦІЙ

Метою дослідження є запропонувати інструменти реагування **екосистеми енергозабезпечення** потреб країни на ситуації, коли виникатимуть критичні загрози стійкості функціонування енергетичного сектору України.

Енергетичний сектор охоплює сфери газу, електроенергії (у т.ч. видобутку та генерації), нафти та нафтопродуктів, а також суміжних сфер, що забезпечують функцію енергозабезпечення життєдіяльності людини, суспільства, економіки та держави.

Екосистема енергозабезпечення передбачає побудову екосистеми окремих складових функцій, як то електропостачання, теплопостачання, газопостачання, безперервності господарювання, безперервності управління тощо та являє собою синтез окремих складових функцій на системній основі.[1]

Складність опису екосистеми енергозабезпечення шляхом вичерпного та конкретного опису системи взаємозв'язків між елементами, що забезпечують реалізацію різних складових функцій (підсистем), зумовлює доцільність на початковому етапі дослідження енергетичної стійкості України проведення аналізу стійкості окремих підсистем окремо.

Система електропостачання може слугувати прикладом оцінки *стійкості функції забезпечення споживачів електричною енергією* та завдань діяльності елементів екосистеми.

Систему електропостачання, яка включає у себе окремі технологічні елементи (об'єкти виробництва сировини та електроенергії, передачі та розподілу електроенергії), а також сервісні елементи (зв'язок, управління, збут та розрахунки за спожиту електроенергію) відносять до критичної інфраструктури. Всі зазначені елементи системи електропостачання поєднані між собою безперервним виробничим процесом виробництва і споживання електроенергії, а порушення функціонування будь-якого із елементів буде впливати на стійкість *функції забезпечення споживачів електричною енергією*.

Завданням даного дослідження є визначення, опис та аналіз впливу *зовнішніх факторів на екосистему електропостачання*, а також аналіз здатності її елементів реагувати та протистояти цим факторам. Розроблена попередня оцінка впливу факторів на екосистему та напрацьовано рекомендації для кожного із типів елементів.

Основними елементами для екосистеми електропостачання є інституції, які формують законодавче і нормативно-правове поле, і забезпечують функціонування фізичного ланцюжка процесу від етапу залучення сировинних матеріалів до задоволення потреб кінцевих споживачів у електричній енергії.

Оцінка стійкості екосистеми електропостачання буде здійснюватися через оцінку спроможності та готовності елементів ефективно діяти щодо загроз протягом всіх етапів циклу кризового реагування.

Загалом під стійкістю розуміється спроможність системи передбачати, поглинати, адаптуватись до та відновлюватись від руйнівних подій (шкідливих впливів, загроз).

---

1 Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України / за ред. О. М. Суходолі. К. : НІСД, 2019. – с. 224.

Забезпечення стійкості систем, є одним із сучасних світових трендів забезпечення безпеки, зокрема національної безпеки і безпеки критичної інфраструктури країни.

В частині безпеки критичної інфраструктури **Національний план захисту критичної інфраструктури США[2] визначає метою** забезпечення безпеки та стійкості країни через посилення захищеності національної критичної інфраструктури шляхом: **запобігання, стримування, нейтралізації або пом'якшення наслідків цілеспрямованих дій з боку терористів** спрямованих на знищення, виведення з ладу або експлуатації критичної інфраструктури, **посилення національної готовності, своєчасне реагування та швидке відновлення критичної** інфраструктури в разі атаки, стихійного лиха або інших надзвичайних ситуацій».

Спроможність елементів екосистеми ефективно діяти протягом всіх етапів циклу кризового реагування (передбачати, поглинати, адаптуватись, відновлюватись) забезпечуючи виконання цільової функції системою є основною властивістю стійкої системи.

В частині забезпечення стійкості екосистеми електропостачання дана концепція може бути визначена наступним чином: «стійкість - це здатність енергетичної системи витримувати порушення роботи системи та продовжувати надавати споживачам доступні енергетичні послуги. Стійка енергетична система може швидко відновитися від потрясінь та може запропонувати альтернативні способи задоволення потреб енергетичних послуг у разі зміни зовнішніх обставин»[3,4].

Тобто, під стійкістю екосистеми енергопостачання будемо розуміти її здатність забезпечувати потреби споживачів у послугах (електроенергії) за будь-яких обставин, тобто її спроможність надійно функціонувати у штатному режимі, протистояти загрозам, адаптуватися до умов, що постійно змінюються, та швидко відновлюватися після реалізації загроз будь-якого виду[5].

Елементи для забезпечення стійкості системи мають мати необхідні регламентовані процедури дій, взаємодії та обміну інформацією на етапах реагування відповідно до наступної моделі реагування системи для забезпечення стійкості цільової функції [6].

---

2 National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience. URL: https://www.dhs.gov/publication/nipp-2013-partnering-criticalinfrastructure-security-and-resilience

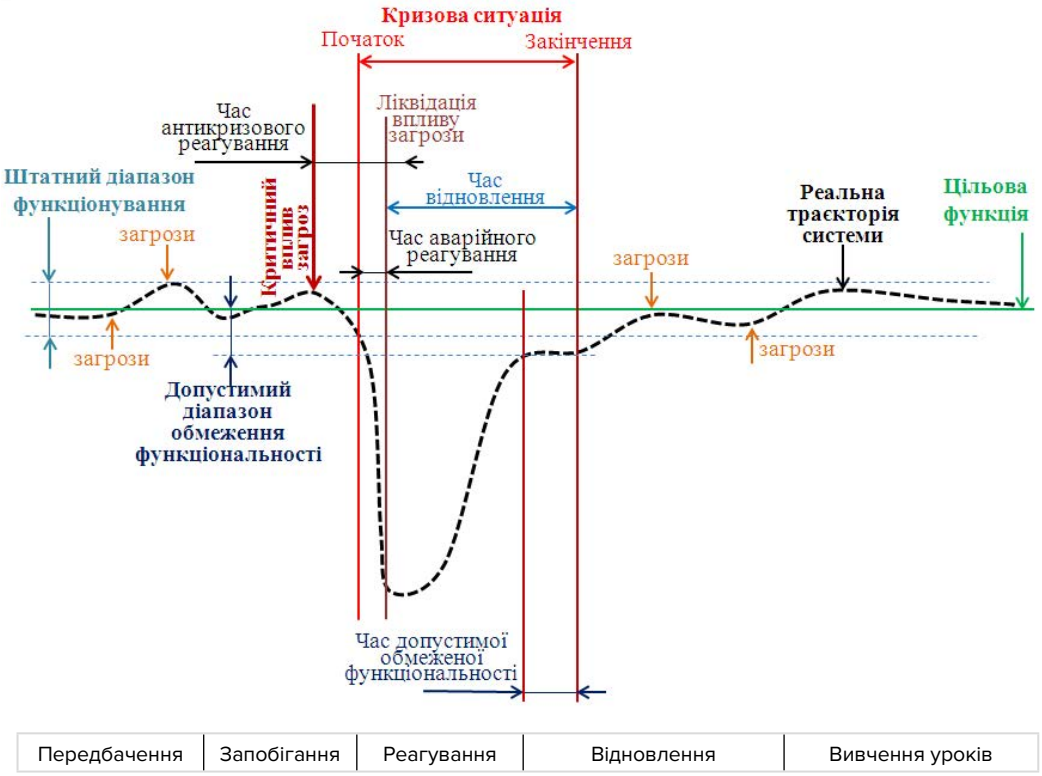
3 The Resilience of the Electricity System. Science and Technology Select Committee. Published by the Authority of the House of Lords London : The Stationery Office Limited. 2015. URL: https://publications.parliament.uk/pa/ld201415/ldselect/ldsctech/121/121.pdf

4 Building a Resilient UK Energy System. Research Report. 2011. UKERC/RR/HQ/2011/001. URL: http://www.ukerc.ac.uk/publications/building-a-resilient-uk-energy-system-research-report.html

5 Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України / за ред. О. М. Суходолі. К. : НІСД, 2019. – с. 224.

6 Суходоля О.М. Стійкість функціонування енергетичної системи чи стійкість енергозабезпечення споживачів: постановка проблеми // Стратегічні пріоритети. – 2018. – № 2. – С.101-117

Рис.1. Модель реагування системи для забезпечення стійкості цільової функції



Необхідність виділення параметрів цільової функції/послуг, як вихідного продукту системи є необхідною з точки зору аналізу критичності факторів впливу (загроз) на систему та оцінку ризиків. Ризики це є вплив невизначеності (загроз) на цілі системи.

Загалом, діяльність елементів екосистеми на різних етапах циклу кризового реагування передбачає такий предмет:

1) штатний режим (передбачення) — елементи екосистеми здійснюють діяльність щодо оцінки можливих загроз системі електропостачання та інформування щодо них. Функціонування фізичної інфраструктури електропостачання здійснюється відповідно до проектного цільового призначення;

2) режим запобігання реалізації загроз — елементи екосистеми проводять до готовності забезпечити захист системи від визначеного набору загроз та реагування на випадок реалізації загрози. Функціонування фізичної інфраструктури електропостачання здійснюється відповідно до проектного цільового призначення. Водночас запроваджуються додаткові режими «готовності» окремих установок та обладнання (stand-by), посилюється контроль та вводяться обмеження на доступ до об'єктів;

3) режим реагування на виникнення кризової ситуації — елементи екосистеми застосовують наперед підготовлені заходи реагування на критичну загрозу з метою запобігання кризової ситуації. За необхідності елементи екосистеми запроваджують додаткові заходи оперативного характеру для реагування на розвиток ситуації в залежності від конкретних обставин. Функціонування інфраструктури відбувається в режимі кризової ситуації, вводяться обмеження на режими роботи об'єктів інфраструктури, економічні умови господарювання, доступу до об'єктів;

4) режим відновлення штатного функціонування — елементи екосистеми застосовують заходи щодо повернення параметрів функціонування системи до цільового рівня. За необхідності здійснюються заходи «перебудови» системи відповідно до нових обставин. Функціонування інфраструктури здійснюється з обмеженнями відповідно до визначених термінів ліквідації наслідків кризи.

Окремо доцільно виділити етап діяльності пов'язаний із вивченням уроків.

У цьому режимі елементи екосистеми здійснюють оцінку ефективності та адекватності вжитих заходів, визначають недоліки реагування та вносять зміни у процедури своєї діяльності та фізичну інфраструктуру системи електропостачання відповідно до нових знань, наявних ресурсів тощо. Функціонування фізичної інфраструктури електропостачання здійснюється відповідно до проектного цільового призначення.

З точки зору регламентації діяльності екосистеми із забезпечення стійкості, законодавством та нормативно-правовими актами має забезпечуватись визначення/регулювання набору окремих важливих параметрів:

- штатний діапазон, рівень допустимих відхилень від цільових параметрів штатного (проектного) діапазону, штатна процедура реагування (інформування та взаємодії);
- перелік та параметри критичних загроз системі, процедури взаємодії та надання допомоги від інших систем, час необхідний для надання/отримання допомоги;
- процедури взаємодії та реагування на кризу, час реагування;
- вимоги резервування (ресурси, обладнання тощо) та дублювання/заміщення, процедури відновлення, час відновлення;
- допустимий діапазон та час обмеження функціональності, процедури адаптації до нової ситуації;
- процедури аналізу реагування; підготовка та оприлюднення звіту.

На основі такого концептуального підходу до забезпечення стійкості, у дослідженні проведено оцінку законодавства та практичних дій США щодо забезпечення стійкості екосистеми енергозабезпечення споживачів.

Для визначення рекомендацій до підходу до забезпечення стійкості буде виокремлено прогалини у українській екосистемі, які поділяються на дві основні групи:

Комунікаційні прогалини (communication gaps). У цю групу виокремлені прогалини української екосистеми, що відповідають за формування та реалізацію комунікаційних та операційних стратегій між учасниками екосистеми. На основі визначених прогалин сформовано рекомендації.

Прогалини у компетенціях (capacity gaps). Ця група у свою чергу поділяється на технічні можливості (technical capacities) та людський потенціал (human capacities). У цю групу виокремлені рекомендації стосовно покращення технічних аспектів формування підходу до стійкості, а також покращення людського потенціалу у цьому процесі.

1.2 ОПИС ЕЛЕМЕНТІВ УКРАЇНСЬКОЇ «ЕКОСИСТЕМИ»

Відповідно до методології, «екосистема» українського енергетичного сектору складається з 3 елементів:

1. Прийняття рішень та лідерство
2. Економіка та суспільство
3. Інфраструктура

1.1.1 ПРИЙНЯТТЯ РІШЕНЬ ТА ЛІДЕРСТВО

До частини «екосистеми» прийняття рішень та лідерство належать регулятори, парламент, органи місцевого самоврядування та місцеві органи виконавчої влади.

В українській енергетичній «екосистемі» влада виконує наступні функції:

1. Вироблення та втілення стратегічних політик, концепцій.

Центральну виконавчу роль виконують **Кабінет Міністрів** та **Міненерго**.

Міненерго як профільне міністерство відповідальне за реалізацію політики в енергетичному секторі. Відомство розробляє концепції, стратегічні документи, що впливають на розвиток енергетики та здійснює контроль над паливно-енергетичним сектором (електроенергетичному, ядерно-промисловому, вугільно-промисловому, торфодобувному, нафтогазовому та нафтогазопереробному комплексі). Міністерство слідкує за збалансованим розвитком енергетичної сфери через розроблення та впровадження державних інвестиційних програм, розробляє прогнозний енергетичний баланс. Уряд та Міненерго несуть відповідальність за питання національної безпеки у сфері енергетики, особливо, у сфері атомної енергії[7]. Міненерго здійснює управління державними видобувними підприємствами, НАЕК «Енергоатом» та вузькогалузевими контролюючими та науковими підприємствами.

Кабмін здійснює управління та представляє інтереси держави в державних підприємствах та підприємствах, де держава має свою частку акцій (НАК «Нафтогаз», АТ «Магістральні газопроводи України», Держгеонадра). Міндовкілля, Мінфін, Мінрегіон своєю діяльністю теж дотично впливають на енергетичну сферу через державні програми розвитку, концепції реформування соціальних та екологічних сфер.

Верховна Рада законодавчо формує політику стосовно розвитку енергетичного сектору України, ратифікує міжнародні угоди, що в тому числі стосуються енергетики. Парламент фактично визначає відповідальних (призначає керівника уряду та профільних міністерств) за здійснення політики та законодавчо встановлює правила функціонування енергетичних ринків в Україні, відносини між державою, виробниками та споживачами енергії та іншими державами.

2. Регулювання енергетичного сектору

Незалежним регулятором в енергетиці є **НКРЕКП** (Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг). Регулятор контролює роботу енергетичних ринків та комунальних послуг. НКРЕКП видає ліцензії на виробництво, постачання, розподіл енергії, контролює виконання ліцензійних умов, накладає штрафні санкції та в окремих випадках анульовує ліцензії. НКРЕКП регулює роботу енергетичних підприємств, що виробляють, транспортують, постачають енергію споживачам через встановлення тарифів на передачу, розподіл, постачання енергії. Також Регулятор відповідальний за забезпечення захисту прав споживачів товарів та послуг у сферах енергетики та комунальних послуг[8].

РНБО є координаційним органом при Президентові України, який покликаний координувати дії різних гілок влади у ситуаціях, що можуть загрожувати національній безпеці країни, в тому числі стосовно енергетичної безпеки країни. Рішення РНБО можуть стосуватися будь яких сфер енергетики задля попередження або вирішення кризових ситуацій. Прийняті на засіданнях РНБО рішення є обов'язковими до виконання для усіх гілок

---

7 Згідно положення про Міністерство енергетики. URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennya-polozhennya-pro-ministerstvo-energetiki-ukrayini-i170620-507

8 Завдання та функції НКРЕКП. Сайт НКРЕКП. URL: https://www.nerc.gov.ua/?id=11804

виконавчої влади[9]. Наприклад, рішенням РНБО 19 лютого 2021 року уряду було доручено повернути під контроль держави частини нафтопродуктопроводів Самара – Західний напрямок і Грозний – Армавір – Трудова, що проходять через територію України[10].

Місцеві органи влади

Місцеві органи влади та місцевого самоврядування відповідальні за ефективне вироблення та використання енергетичних ресурсів на підпорядкованій їм території. Місцеві органи самоврядування встановлюють тарифи на теплову енергію для генеруючих підприємств та інші види комунальних послуг[11].

У випадку надзвичайних ситуацій місцеві адміністрації/ОТГ здійснюють заходи задля попередження та подолання негативних наслідків. Місцеві органи влади також працюють над розробкою комплексних планів постачання енергії для споживачів, розробляють системи заходів щодо об'єктів енергетики в надзвичайних умовах. Якщо на місцеві органи виконавчої влади покладені обов'язки здійснювати заходи надзвичайного стану, то енергетичні підприємства та інші об'єкти зобов'язані виконувати розпорядження визначених органів[12].

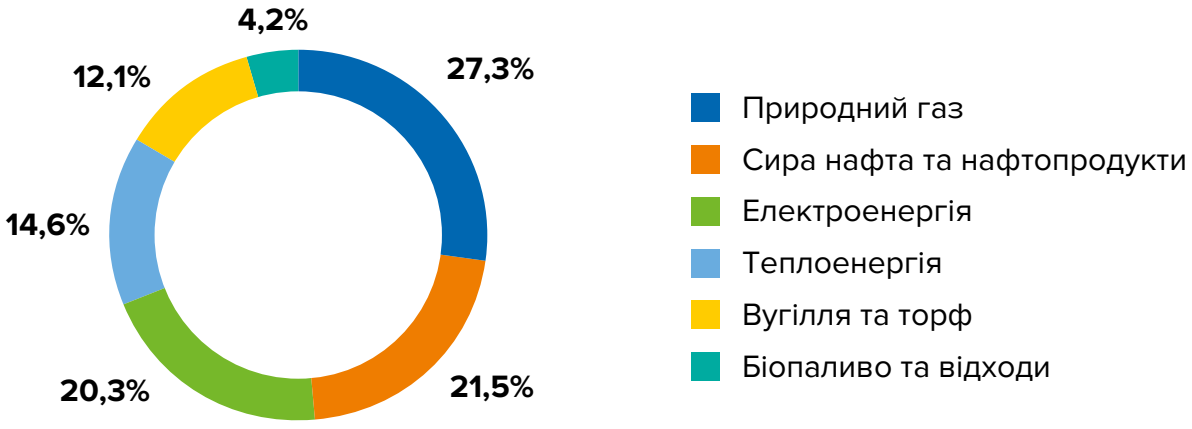
1.1.2 ЕКОНОМІКА ТА СУСПІЛЬСТВО

До елементу «екосистеми» економіка та суспільство належать:

- Державні та приватні компанії, що працюють в енергетичному секторі
- Компанії великі та середні споживачі енергії
- Домогосподарства

В Україні 29,04% всієї спожитої енергії вироблено з природного газу. Також важливими сферами є електроенергія та нафтопродукти (Рис2).

Рис. 2. Споживання енергії за джерелом енергії, %



Джерело: Держстат[13]

9 Закон України про Раду національної безпеки та оборони України. URL: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text

10 Рішення Ради національної безпеки і оборони України від 19 лютого 2021 року "Про вжиття заходів для захисту майнових інтересів держави". URL: https://www.rnbo.gov.ua/ua/Ukazy/4818.html

11 https://zakon.rada.gov.ua/laws/show/z1172-18#Text

12 https://zakon.rada.gov.ua/laws/show/2501-12#Text

13 http://www.ukrstat.gov.ua/express/expr2020/11/148.pdf

Компанії, що працюють в енергетичному секторі

Стратегічним сектором в Україні є атомна енергетика. Усі українські атомні станції зосереджені в одному державному підприємстві **«Національна атомна енергогенеруюча компанія «Енергоатом». НАЕК «Енергоатом»** традиційно генерує більше 50% від загальної генерації електроенергії в Україні[14]. В підпорядкуванні компанії знаходяться 4 діючі атомні електростанції (Запорізька, Рівненська, Южно-Українська, Хмельницька), на яких експлуатується 15 енергоблоків, загальною потужністю 13885 МВт[15]. Діяльність НАЕК «Енергоатом» регулюється спеціальним органом, Держатомрегулювання, який слідкує за безпечним використанням ядерної енергії та відповідає за фізичний захист атомних станцій[16].

ПАТ «Центренерго» є важливою державною компанією для генерації електроенергії та балансування енергосистеми. До складу компанії входять три теплові електростанції (Трипільська, Вуглегірська, Зміївська ТЕС) сумарною встановленою потужністю 7665 МВт. ПАТ «Центренерго» є основним споживачем вугілля, видобутого на державних шахтах. Важливу роль компанія зіграла в кінці 2020, коли в енергетичній системі існував дефіцит потужностей. Блоки ПАТ «Центренерго» змогли збільшити свою потужність та виробити третину всієї теплової генерації протягом листопада-грудня 2020 року .

Група компаній ДТЕК одна з найбільших приватних енергетичних компаній в Україні, що займається видобутком та збагаченням вугілля, генерацією електроенергії на ТЕЦ та ТЕС, розподілом електроенергії, активно розвивають альтернативні джерела енергії. В медійному полі неодноразово зазначалось, що ДТЕК займається лобіюванням власних інтересів у владних колах[17].

Група компаній ДТЕК є найбільшими видобувними підприємствами в країні. У їх власності 8 вугледобувних підприємств (у 2019 році видобуток компанії склав 24511 тис тонн)[18]. У сфері видобутку газу компанія «ДТЕК Нафтогаз» має частку 40% видобутку серед приватних компаній (у 2019 році компанія видобула 1,66 млрд куб газу)[19]. Провідну роль ДТЕК відіграє на ринку генерації електроенергії та тепла. Генерація ТЕС компаній ДТЕК складає приблизно чверть від усієї виробленої електроенергії в Україні.

Лідером на ринку відновлюваних джерел енергії є група компаній «ДТЕК ВДЕ, яка у своїй власності має сонячні та вітрові електростанції загальною встановленою потужністю 1 ГВт (станом на кінець 2019 року)[20].

Група компаній **НАК «Нафтогаз»** є найбільшими видобувниками газу та нафти в Україні. Окрім цього компанія займається розподілом і постачанням природного газу населенню, також постачає природний газ для підприємств ТКЕ в рамках ПСО на ринку газу.

У 2020 році в Україні видобуто 20,2 млрд куб газу, з яких державні компанії видобули 15,3 млрд куб (76%), а приватні 4,9 млрд куб (24%). Переважну більшість газу було видобуто компанією АТ «Укргазвидобування» (14,9 млрд куб)[21], яка є дочірньою компанією НАК «Нафтогаз». Ще однією дочірньою компанією «Нафтогазу» є ПАТ «Укрнафта», яка є лідером у видобутку нафти в Україні. Разом з **АТ «Укргазвидобування»** ПАТ «Укрнафта» у 2019 році видобули майже 90% усієї видобутої нафти в країні[22]. В підпорядкуванні «Нафтогазу» також є АТ«Укртрансгаз» та АТ «Укртранснафта», які займаються зберіганням та транспортуванням нафти та природного газу.

14 https://www.iea.org/data-and-statistics?country=UKRAINE&fuel=Energy%20supply&indicator=ElecGenByFuel

15 https://www.energoatom.com.ua/ua/about-6/misia-7

16 https://zakon.rada.gov.ua/laws/show/363-2014-%D0%BF#n8

17 https://www.epravda.com.ua/news/2020/05/21/660781/

18 https://dtek.com/media-center/press/dtek-group-key-performance-indicators-for-2019/

19 https://expro.com.ua/novini/dolya-vidobutku-gazu-dtek-naftogaz-dosyagla-40-sered-privatnih-vidobuvnikv

20 https://renewables.dtek.com/

21 https://expro.com.ua/novini/ukrana-u-2020r-skorotila-vidobutok-prirodnogo-gazu-na-2-do-202-mlrd-kub-m

22 http://eiti.org.ua/wp-content/uploads/2021/02/Abbreviated-EITI-Report_2019_final-1.pdf

В Україні активно розвивається **«зелена» енергетика**. З 2014 по 2019 рік частка відновлюваних джерел енергії в кінцевому споживанні збільшилася в два рази, а протягом 2020 року було введено в експлуатацію близько 1,5 ГВт нових потужностей[23]. В Україні діє спеціальний «зелений» тариф для виробників електроенергії з ВДЕ. Проте, існували серйозні проблеми з ліквідністю ринку через зависокі ставки тарифу в середині 2020 року[24]. Через це уряд був змушений переглянути ставки тарифу в сторону зменшення, що викликало невдоволення серед виробників електроенергії з ВДЕ.

Важливим елементом в постачанні електроенергії та газу для побутових споживачів є **постачальники**. Це компанії, які утворилися протягом двох останніх років в результаті реформування ринків газу та електроенергії в Україні, коли було законодавчо відокремлено функції постачання та розподілу енергетичних ресурсів.

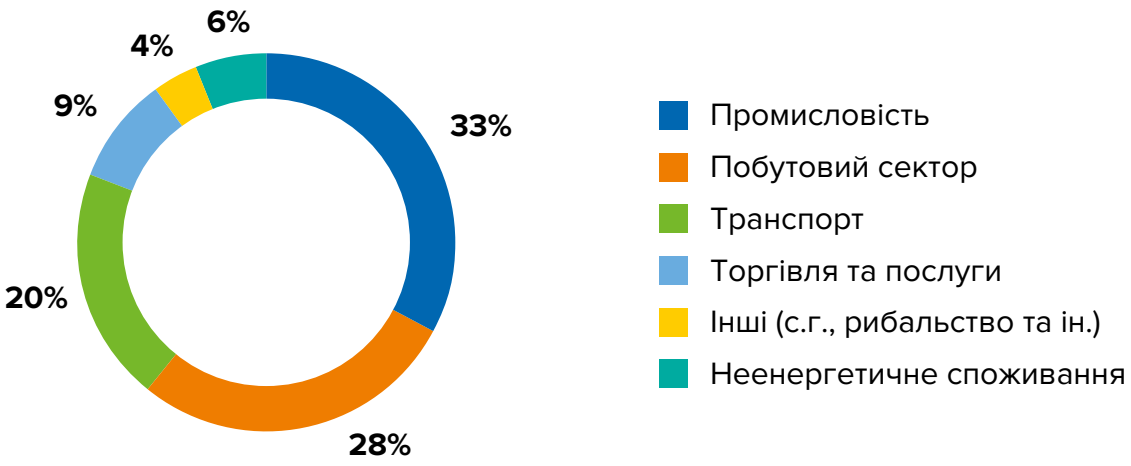
Лібералізація ринків газу та електроенергії створили умови для розвитку **трейдерів**, які займаються перепродажем енергоресурсів від виробників до промислових споживачів та постачальників енергії. Для трейдингу в Україні компаніям не потрібна ліцензія, тому нерідко різні компанії маніпулюють цінами, особливо в промисловому секторі[25].

Частина інфраструктурних енергетичних об'єктів знаходиться у приватній власності або орендовані у держави. Розподільні мережі газу та електроенергії (облгази та обленерго) є природніми монополістами у своїх регіонах та часто стають предметом розслідувань НКРЕКП, АМКУ[26,27,28].

Споживачі

Відповідно до даних Держстату найбільшими споживачами енергії в Україні є промисловість та домогосподарства, які споживають 2/3 всієї виробленої енергії в Україні. Достатньо високі відсотки споживання енергії мають транспорт і торгівля та послуги (20% та 9%)[29].

Рис. 3. Структура кінцевого споживання за напрямами (2019), %



Джерело: Держстат[30]

23 https://oilpoint.com.ua/za-pidsumkamy-roku-chastka-vde-v-strukturi-vyrobnycztva-e-e-perevyshhyt-planovu-na-2/?lang=uk

24 http://finbalance.com.ua/news/enerhoatoma-vidsudiv-u-harpoka-41-mlrd-hrn

25 https://daily.rbc.ua/ukr/show/shemnaya-pribyl-treydery-zloupotreblyayut-1605537115.html

26 https://ua-energy.org/uk/posts/nkrekp-oshtrafuie-7-hazzbutiv-ta-odyn-oblhaz-za-porushennia-pravyl-postachannia-hazu

27 https://ua-energy.org/uk/posts/nkrekp-oshtrafuvala-pat-cherkasyoblenerho-na-255-tys-hrn

28 https://amcu.gov.ua/news/amku-oshtrafuvav-18-oblgaziv-na-ponad-380-mln-grn-za-zlovzhivannya-monopolnim-stanovishchem

29 https://www.iea.org/data-and-statistics?country=UKRAINE&fuel=Energy%20consumption&indicator=TFCShareBySector

30 http://www.ukrstat.gov.ua/express/expr2020/11/148.pdf

Близько 10% всього споживання електроенергії припало на 17 промислових компаній, більшість з яких знаходяться у Східній та Південній частинах України. Найбільшими споживачами, на яких припало 5% всього споживання, є Нікопольський та Запорізький завод феросплавів. Також великі об'єми електроенергії споживаються АрселорМіттал Кривий Ріг, Дніпросталь, Маріупольський меткомбінат ім. Ілліча, Полтавський ГЗК[31]. Більшість промислових підприємств належать до впливових фінансових груп та компаній, які мають вплив на прийняття політичних рішень і лобіювання власних інтересів в енергетичній сфері також[32].

У 2019 році промисловість спожила 8,1 млрд куб газу (27% від усього споживання), що дещо менше, ніж побутові споживачі (9,5 млрд куб та 31,8% відповідно). Майже чверть від усього спожитого газу використали ТКЕ (теплокомуненерго) для виробництва теплової енергії (7,4 млрд куб газу та 24,7% відповідно[33].

Домогосподарства споживають 32,3% всієї виробленої енергії в країні. В Україні приблизно 12,5 млн побутових споживачів газу та приблизно 17 млн споживачів електроенергії[34]. Відповідно до даних Держстату за 2019 рік, на опалення житлових приміщень побутові споживачі витрачають 52,9% всієї спожитої енергії, 14,1% використовують на підігрів води, 16,6% для приготування їжі, та 15,8% на освітлення та живлення побутових пристроїв[35].

Важливою проблемою як для домогосподарств так і для всього муніципального сектору є низький рівень енергоефективності будівель. Щорічні втрати від низької енергоефективності можуть складати до 1,5 млрд доларів на рік[36].

1.2.3 ІНФРАСТРУКТУРА

До елементу «екосистеми» інфраструктура належать оператори транспортних та розподільних енергетичних систем.

ОГТСУ

ОГТСУ незалежний оператор газотранспортної системи, який здійснює транспортування природного газу українським споживачам, а також має систему магістральних газопроводів, через яку здійснює транзит газу з РФ до інших країн Європи.

ОГСТУ виконує функції балансування системи, чим забезпечує надійне постачання та транспортування природного газу. ОГТСУ керує магістральними газопроводами протяжністю 33 тис км, 1389 газорозподільними станціями та 57 компресорними станціями[37].

НЕК «Укренерго»

У сфері електроенергії управління енергетичною системою здійснює НЕК «Укренерго». Компанія забезпечує передачу електроенергії від генеруючих підприємств до мереж операторів систем розподілу (які забезпечують постачання електроенергії споживачам), технічне обслуговування мереж. Основною є функція диспетчеризації енергетичної системи. «Укренерго» балансує виробництво та споживання електроенергії. В управлінні «Укренерго» 19 тис км магістральних та міждержавних ЛЕП та 103 електричні підстанції[38].

---

31 https://biz.censor.net/resonance/3214503/reyiting_nayiblshih_spojivachv_elektroenerg_ukrani

32 https://www.epravda.com.ua/columns/2020/12/15/669204/

33 https://www.naftogaz.com/files/Zvity/Naftogaz_2019_UA.pdf

34 https://www.nerc.gov.ua/data/filearch/Catalog3/Richnyi_zvit_NKREKP_2019.pdf

35 http://ukrstat.gov.ua/operativ/operativ2021/energ/skse_domogosp_19ue.xlsx

36 https://www.ukrinform.ua/rubric-economy/2538060-mert-soricni-vtrati-ukraini-cerez-nizku-energoefektivnist-15-milarda.html

37 https://tsoua.com/gts-infrastruktura/mozhlyvosti-gts/tehnichni-dani/

38 https://ua.energy/

ОЕС (Об'єднана енергетична система) складається з основної частини, яка займає більшість території України та «острів Бурштинської ТЕС». Основна частина енергосистеми з'єднана з країнами СНД та Балтії, а «Бурштинський енергоострів» з країнами ЄС (ENTSO-E).

АТ «Укртрансгаз», яка входить до групи «Нафтогазу» є **оператором газових сховищ**. В управління компанії 12 газових сховищ загальною місткістю 31 млрд куб газу. Газосховища використовуються для зберігання газу українських та іноземних компаній та є одним з інструментів енергетичної безпеки[39].

В структурі «Нафтогазу» також є **АТ «Укртранснафта»**, яка управляє 19-ма магістральними нафтопроводами протяжністю 3500 км. Компаніє керує також морським нафтовим терміналом та перекачувальними станціями. Основна функція нафтового трубопроводу це транзит[40].

Функції транспортування природнього газу побутовим та непобутовим споживачам виконують **оператори газорозподільних мереж (ГРМ)**. Протяжність газорозподільних мереж складає приблизно 350 тис км. В сфері електрики існують аналогічні оператори розподілу. Основною задачею цього елементу «екосистеми» є транспортування газу або електроенергії споживачу та обслуговування мереж.

Стосовно захисту критичної інфраструктури важливо зазначити, що в Україні немає повноцінного законодавства, яке регулює захист критично важливої інфраструктури країни. Лише в жовтні 2020 року Кабмін прийняв постанову, якою затвердив порядок визначення об'єктів, які відносяться до критичної інфраструктури та визначив відповідальних по секторах. Згідно постанови, Міненерго також відповідальне за формування переліку об'єктів критичної інфраструктури[41].

Залежно до загрози в подальшому будуть визначатися додаткові елементи в кожній підсистемі. Даний перелік є набором основних стейкхолдерів.

1.3 ЗАГРОЗИ ТА ЇХ ВПЛИВ НА ЕЛЕМЕНТИ «ЕКОСИСТЕМИ» УКРАЇНИ.

Серед основних типів загроз, що можуть порушити стале задоволення потреб кінцевих споживачів у електричній енергії слід виділити:

- фізичні загрози (загроза військового втручання з боку Росії, фізичне пошкодження інфраструктури внаслідок умисних дій, катастроф);
- кібер-загрози (атаки на інфраструктуру, застосування AI);
- біологічні загрози (пандемії, хімічні атаки);
- економічні загрози (торговельні обмеження, деструктивна поведінка компаній, відтік інвестицій);
- кліматичні і природні загрози (зміна клімату);
- інформаційні загрози (дезінформація, маніпуляція інформаційним простором);
- інші.

Водночас, для цілей дослідження аналіз впливу загроз на функцію енергозабезпечення зосереджено на фізичних та кібер загрозах, що на даний час є найбільш актуальними для України.

---

39 http://utg.ua/utg/about-company/utg-today/

40 https://www.ukrtransnafta.com/#

41 https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#n42

Аналіз впливу загроз на стійкість функціонування енергосистеми

Активні військові дії Росії на Сході України та АР Крим продемонстрували важливість захисту енергетичного сектору. Порушення стабільності функціонування енергетичного сектору України стало одним з основних інструментів гібридної агресії Росії проти України в 2014 році[42].

Росія активно використовувала різні методи порушення стійкості функціонування інфраструктури життєдіяльності України: від опосередкованого впливу (економічні, інформаційні методи) до прямого фізичного впливу[43]. Детальний аналіз впливу фізичних загроз на енергетичний сектор країни, під час активної фази агресії Росії проти України, наведений у дослідженні Центру передового досвіду НАТО з енергетичної безпеки, виділяє цілий ряд методів зловмисного впливу у воєнний час[44]:

- фізичне захоплення об'єктів при збереженні їхньої функціональності[45];
- припинення функціонування об'єктів;
- пошкодження[46] чи блокування маршрутів постачання[47];
- фізичне знищення об'єкта[48];
- перешкоджання діяльності з відновлення функціональності[49];
- здійснення кібератак на електроенергетичну систему країни[50].

---

42 Sukhodolia O. The energy dimension of war. The Ukrainian experience: An overview of the Ukrainian events in 2014–2016. Energy Security: Operational Highlights. 2017. N° 11. P. 25-34.

43 Світова гібридна війна: український фронт/ за редакцією Горбуліна В.П. К. : НІСД, 2017, 496 с.
Суходоля О. М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України. Стратегічні пріоритети. 2016. N° 3. С. 62–76.

44 Hybrid Warfare Against Critical Energy Infrastructure: The Case of Ukraine. NATO ENSEC COE, 2020, 87 p. URL:https://enseccoe.org/data/public/uploads/2020/11/hybrid-warfare-against-critical-energy-infrastructure-the-case-of-ukraine.pdf

45 Втрата активів енергетичного сектору у Криму, на шельфі Чорного моря, на окупованій території Донеццької та Луганської областей. Потенційні втрати України внаслідок захоплення Росією активів лише в Криму і на шельфі оцінюють в 300 млрд дол. США.

46 У Карпатах на газопроводі сталося три вибухи. Основна версія інциденту – теракт. URL: http://tyzhden.ua/News/109919; ПАТ «Укртрансгаз»: Надзвичайна ситуація на газопроводі «Уренгой-Помари-Ужгород» не вплине на транзит природного газу в країни Європи. URL: http://mpe.kmu.gov.ua/minugol/control/publish/article?art_id=244942377; Обстрел боевиков снова обесточил Донецкую фильтровальную станцию – штаб. URL: http://zn.ua/UKRAINE/obstrel-boevikov-snova-obestochil-doneckuyu-filtrovalnuyu-stanciyu-shtab-220647_.html; Боевики умышленно взорвали газопровод, снабжающий Мариуполь – МВД. URL: http://news.liga.net/news/politics/5983963-boeviki_umyshlenno_vzorvali_gazoprovod_snabzhayushchiy_mariupol_mvd.htm

47 Продан: на кордоні із РФ вже п'ять днів заблоковані 200 вагонів із вугіллям. URL: http://www.pravda.com.ua/news/2014/12/2/7046178/; Россия заблокировала поставки угля в Украину. URL: http://biz.liga.net/all/tek/novosti/2894100-rossiya-zablokirovala-postavki-uglya-v-ukrainu.htm; Росія знову повністю зупинила постачання вугілля в Украину. URL: http://www.theinsider.ua/business/54c228c7d6654/

48 Боевики обстреливают инфраструктуру Донбасса: «Такое впечатление, что это их ключевая задача», - Жебривский. URL: http://censor.net.ua/news/360085/boeviki_obstrelivayut_infrastrukturu_donbassa_takoe_vpechatlenie_chto_eto_ih_klyuchevaya_zadacha_jebrivskiyi; Миномётный обстрел Счастья: ТЭС горит, в трёх городах нет света. URL: http://www.mediaport.ua/minomyotnyy-obstrel-schastya-tes-gorit-v-tryoh-gorodah-net-sveta; Бойовики серйозно пошкодили Вуглегірську ТЕС. URL: http://uainfo.org/blognews/1437999336-boyoviki-seryozno-poshkodili-vuglegirsku-tes-foto.html; Заява МЗС України у зв'язку із обстрілом Вуглегірської ТЕС. URL: http://mfa.gov.ua/ua/press-center/comments/3818-zajava-mzs-ukrajini-u-zvjazku-iz-obstrilom-vuglegirsykoji-tes

49 Боевики «ЛНР» не дают электрикам осматривать перебитые линии электропередач. URL: http://novosti.dn.ua/news/242050-boevyky-lnr-ne-dayut-ehlektrykam-osmatryvat-perebytye-lynyy-ehlektroperedach; Боевики обстреляли ремонтников в Маринке. URL: http://rus.newsru.ua/ukraine/11mar2016/obstrilialy_remontnu_brygadu.html; Генералы РФ блокируют ремонт теплоснабжения в Авдеевке. URL: http://news.liga.net/news/incident/14681528-generaly_rf_blokiruyut_remont_teplosnabzheniya_v_avdeevke.htm; Украинская сторона СЦКК обвиняет боевиков в затягивании восстановления инфраструктуры на Донбассе. URL: http://politkuhnya.info/novosti/ukrainskaya-storona-sckk-obvinyaet-boevikov-v-zatyagivanii-vosstanovleniya-infrastruktury-na-donbasse.html.

50 Confirmation of a Coordinated Attack on the Ukrainian Power Grid. URL: https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid#; Міненерговугілля. Повідомлення щодо запобігання несанкціонованому втручанню в роботу енергомереж. URL: http://mpe.kmu.gov.ua/minugol/control/publish/article?art_id=245086886; В Укренерго пояснили масштабний збій в енергосистемі під Києвом кібератаками. URL: http://economics.unian.ua/energetics/1689781-v-ukrenergo-poyasnili-masshtabniy-zbiy-v-energosistemi-pid-kievom-kiber-atakami.html

Фізичні загрози можуть призводити до наступних наслідків:

1. **Втрата контролю над об'єктами енергетичної інфраструктури, енергогенеруючих підприємств, їхнього майна, захоплення родовищ та видобувних підприємств.** Починаючи з 2014 року український уряд не контролює Старобешівську та Зуївську ТЕС[51], 1200 км магістральних газопроводів, 15 родовищ нафти та газу, 3 перспективні площі покладів нафти і газу, Глібовське підземне газосховище, 43 газорозподільчі станції, 29 одиниць плавзасобів, 4 плавучі бурові установки[52]. Також уряд втратив доступ до 67 державних вугледобувних шахт[53].

   Втрата контролю над об'єктами енергетичної інфраструктури потребує негайного реагування силовим блоком уряду (Генштаб, СБУ, МВС), місцевих органів виконавчої влади та інфраструктурних операторів (ОГТСУ, Укренерго, місцеві розподільчі компанії). Водночас Кабмін та Міненерго залучені до вирішення проблем можливого розбалансування енергетичної системи.

2. **Фізичне знищення об'єктів енергетичної інфраструктури, підприємств, приведення їх до непрацюючого стану.** Якщо під час анексії Кримського півострову здебільшого енергетичні об'єкти захоплювалися, то на території материкової України відбувалося знищення або вивезення працюючого обладнання до Росії. Вцілілі підприємства, які залишаються на непідконтрольній українському уряду території можуть зазнавати актів мародерства[54].

   Підприємства та інфраструктура, які вціліли потребують висококваліфікованих фахівців та обслуговування. Внаслідок спорадичних бойових дій на території Донецької та Луганської областей відбувається часте пошкодження ЛЕП, газогонів. За даними Харківської правової групи, станом на серпень 2017 року лише у Донецькій області за весь час конфлікту було пошкоджено або зруйновано 789 ліній передач або підстанцій, 176 об'єктів теплопостачання, 26 об'єктів газопостачання[55].

   Знищення об'єктів енергетичної інфраструктури вимагає негайного реагування з боку інфраструктурних стейкхолдерів (ОГСТУ, Укренерго, місцеві розподільчі компанії) та силового блоку уряду. Уряд в особі Кабміну та Міненерго підключається до нівелювання наслідків загроз.

3. **Розбалансування енергетичної системи країни та дефіцит енергетичних ресурсів.** Наслідком втрати масштабних енергетичних активів з 2014 року відбулось відчутне розбалансування енергетичної системи у всьому ланцюжку від видобування сировини до поставок енергії споживачам. Втрата вугледобувних підприємств, які постачали антрацитове вугілля на українські ТЕС та ТЕЦ спричинили дефіцит вугілля. Це змусило державні та приватні енергетичні компанії імпортувати вугілля та переобладнувати потужності на інші типи сировини, що потребувало нових інвестицій.

   Внаслідок втрати сировинної бази та пошкоджень в інфраструктурі, у 2014 році український уряд змушений був вводити графік віялових відключень електроенергії через неможливість забезпечити попит в пікові навантаження в системі[56].

   У випадку раптового розбалансування енергетичної системи негайно реагують інфраструктурні стейкхолдери (ОГТСУ, Укренерго), які забезпечують безперебійне постачання енергії. Кабмін та Міненерго реагують на загрозу в частині мінімізації втрат

51 https://www.radiosvoboda.org/a/28641718.html

52 https://www.naftogaz.com/www/3/nakweb.nsf/0/F7F3CB4317B2C77CC2257D01005382CD?

53 https://dixigroup.org/wp-content/uploads/2021/02/dixi-coal-industry-web-2.pdf

54 https://mtot.gov.ua/starobeshivska-tes-pratsyuye-na-pivpotuzhnosti-cherez-ekonomichnyj-zanepad-regionu-shho-sposterigayetsya-na-tymchasovo-okupovanyh-terytoriyah

55 http://khpg.org/files/doc/1542887107.pdf

56 https://www.pravda.com.ua/news/2014/12/2/7046158/

для бізнесу та населення. Енергетичні компанії залучаються урядом на вирішення проблем диверсифікації джерел енергії, транспортування та постачання енергії споживачам.

4. **Аварії, що можуть призвести до людських втрат, шкоди довкіллю, функціонуванню суміжних сфер.** Державні вугледобувні підприємства, які залишились на непідконтрольній території здійснюють видобуток, а також велика кількість шахт закривається. Український уряд не може здійснювати контроль за дотриманням екологічних норм на вугледобувних підприємствах, які консервуються. Наприклад, через неправильну консервацію вугледобувних шахт існує загроза радіаційного забруднення питної води, що за оцінками експертів може перерости в міжнародну екологічну катастрофу[57,58].

   Аварії та відключення, які відбуваються поблизу проведення бойових дій часто не можуть бути вчасно вирішені. Як наслідок, кваліфікований персонал не може добратися до місця поломки для відновлення постачання енергії. Наприклад, у 2015 році збройні формування так званої «ДНР» обстрілювали ремонтні бригади, через що жителі двох населених пунктів протягом двох тижнів залишалися без електроенергії[59].

   Негайно реагують на аварії стейкхолдери з групи інфраструктури, місцеві органи виконавчої влади та за потреби силовий блок. Уряд залучається у випадку масштабних та довгострокових наслідків загрози.

5. **Інвестиційні та економічні втрати для економіки та енергетичного сектору вцілому.**

   Внаслідок втрати територій, активів, контролю над підприємствами зазнають збитків всі стейкхолдери в країні. Втрата нафтогазовидобувних родовищ та обладнання на території окупованого Криму спричинила зменшення видобутку. З 2014 року Російська федерація експропріювала потужності «Чорноморнафтогаз» та видобуває щорічно близько 2 млрд куб газу на території Криму. НАК «Нафтогаз», в структуру якого входить «Чорноморнафтогаз», оцінив збитки від втраченого майна на суму 5,2 млрд доларів[60].

   Відповідальним за вирішення інвестиційних та економічних втрат є уряд в особі Кабміну та профільних міністерств (Міненерго, Мінекономіки, Мінстратегпром). Стейкхолдери з групи бізнесу та домогосподарства також реагують на економічні загрози.

Аналіз впливу загроз на стейкхолдерів

Аналіз подій що впливали на порушення електропостачання в Україні у 2014-2015 роках дозволяє оцінити наслідки впливу загроз (зловмисних дій) та ідентифікувати застосовані дії в Україні у цей період та потенційно можливі дії стейкхолдерів щодо реагування.

57 https://www.bbc.com/ukrainian/features-43845187

58 https://www.ukrinform.ua/rubric-regions/3197844-do-pitnoi-vodi-na-donbasi-skoro-moze-potrapiti-radiacia-reznikov.html

59 https://censor.net/ru/news/340864/snayipery_terroristov_dnr_ustroili_ohotu_na_elektrikov_ne_dopuskaya_ih_k_vypolneniyu_remontnyh_rabot

60 https://chornomornaftogaz.com.ua/novyny/31-5-2-mlrd-dolariv-naftogaz-podav-do-sudu-otsinku-zbitkiv-vid-zakhoplennya-rosieyu-aktiviv-grupi-v-krimu

Таблиця 1. Заходи реагування на виділені загрози проти енергетичної системи України

Типові зловмисні дії	Наслідки пошкодження	Реагування операторів інфраструктури на пошкодження
Підрив/пошкодження електростанцій	Зупинка (перерва) роботи електростанцій, руйнування обладнання станції. Зниження резерву генеруючих потужностей та надійності роботи ОЕС України	Заходи забезпечення операційної безпеки ОЕС України, зокрема: • включення у роботу генеруючих потужностей («гарячого резерву»); • запровадження графіків обмеження енергопостачання. • У деяких випадках, вжиті заходи можуть забезпечити умови, при яких кінцеві споживачі не відчувають проблем.
Підрив/пошкодження трансформаторних підстанцій	Переривання постачання електроенергії по окремих лініях та/або в окремих регіонах (якщо пошкоджуються трансформатори розподільчих мереж). Зниження стійкості функціонування ОЕС України та виникнення проблем з енергопостачанням на окремих територіях.	Заходи: • включення додаткових генеруючих потужностей (аварійних, резервних); • перерозподілення потоків потужності та електроенергії в ОЕС України; • запровадження графіків обмеження енергопостачання; • сприяння добровільного скорочення енергоспоживання. • В окремих випадках при втраті електропостачання - переведення на альтернативні джерела, інші види палива та енергозабезпечення.
Підрив/пошкодження ліній електропередачі	Переривання постачання по окремих лініях, в окремих регіонах (якщо немає інших ліній постачання). Зниження стійкості функціонування ОЕС України та припинення енергопостачання на окремих територіях (окремих споживачів).	Заходи: • перерозподілення потоків потужності та електроенергії в ОЕС України; • запровадження графіків обмеження енергопостачання; • сприяння добровільного скорочення енергоспоживання споживачами; • переведення на альтернативні джерела, інші види палива та енергозабезпечення.
Блокування роботи (розукомплектування) об’єктів	Переривання постачання палива для електростанцій та виробництва/постачання електроенергії.	Заходи: • включення додаткових генеруючих потужностей (аварійних, резервних); • перерозподілення потоків потужності

Кібератаки проти об'єктів енергетичної інфраструктури	Припинення функціонування окремого обладнання та окремих систем управління Переривання постачання електроенергії по окремих лініях та/або в окремих регіонах. Зниження стійкості функціонування ОЕС України.	Заходи: • перерозподілення потоків потужності та електроенергії в ОЕС України; • переведення на альтернативні джерела, інші види палива та енергозабезпечення • переведення у ручний режим роботи обладнання

Вплив військових загроз на стійкість енергетичної системи є критичним. Найбільше страждають державні інститути та інфраструктура. Окрім реагування на військові дії, уряд відповідальний за стабільність енергетичної системи, збереження людських життів та забезпечення населення енергетичними ресурсами.

Зазначені дії справляли комплексний вплив на економіку, обороноздатність і спроможність України протистояти тиску агресора:

- **знижувався рівень обороноздатності країни** через руйнування транспортних комунікації, систем зв'язку й забезпечення ресурсами збройних формувань, правоохоронних сил і сил цивільного захисту тощо;
- **завдавалися економічні збитки** національній економіці та окремим суб'єктам господарювання через захоплення енергетичних об'єктів і ресурсів, формувалася потреба додаткових витрат на відновлення інфраструктури, потреба в додаткових постачаннях ресурсів, блокувалося постачання окремих товарів через кордон та чинилися перешкоду функціонуванню транскордонної інфраструктури;
- **отримувалися локальні (тактичні) переваги:** досягнення ліпшої позиції у проведенні окремих операцій (бойові зіткнення, контрактні умови постачання товарів чи політичні переговори, мирне врегулювання), примус до здійснення окремих дій (платежів за товари чи послуги, продажу чи закупівлі ресурсів);
- **здійснювався психологічний тиск на різні групи населення й політиків** через створення інформаційних приводів з метою поширення панічних настроїв, соціального напруження та невдоволення керівництвом країни;
- **формувався «необхідний» імідж на міжнародній арені** для досягнення зовнішньополітичних цілей Росії (скасування санкцій, зміна влади та федералізація України, нехтування іншими країнами транзитного потенціалу України, передусім щодо транспортування природного газу);
- **використовувалася інфраструктура**, зокрема транспортна та повітряна, **для провокацій**, блокувалося відновлення критичної інфраструктури в зоні бойових дій, блокувався транзит товарів через російський кордон, Україна звинувачувалася в блокуванні транзиту з Росії до країн Європи.

Вирішення проблем, пов'язаних із фізичними загрозами, залежить від швидкості та якості дій, насамперед, стейкхолдерів з групи уряду та інфраструктури.

Держава та державні компанії можуть втратити енергетичні ресурси та може скластися ситуація, що уряд не зможе підтримувати енергетичну систему стабільною та гарантувати безпеку постачань.

Інфраструктурним операторам потрібно негайно реагувати на кризові відключення/аварії, безперебійно постачати енергію на критичні об'єкти. При цьому, також існує ризик виникнення техногенних катастроф на об'єктах, які мають підвищений рівень небезпеки.

Приватні енергетичні компанії ризикують втратити свої активи та фактично припинити діяльність у разі втрати урядом території, де знаходиться підприємство. Існує загроза відсутності доступу ресурсів (якщо мова йде про енергогенеруючі компанії) для здійснення підприємницької діяльності та вироблення/постачання енергії.

Побутові споживачі та домогосподарства можуть втратити безпечний доступ до енергетичних ресурсів через аварії та перебої. Також під час фізичних пошкоджень існують ризики припинення обслуговування енергетичного обладнання, що може призвести до загроз життю людини.

РОЗДІЛ ІІ.
АНАЛІЗ ДОСВІДУ США У ПРОТИСТОЯННІ ЗАГРОЗАМ ЕНЕРГЕТИЧНІЙ СИСТЕМІ

2.1 ОГЛЯД ДОСВІДУ США: АНАЛІЗ ДОКУМЕНТІВ

Аналіз досвіду США стосовно захисту та забезпечення надійного постачання електроенергії

Законодавство США

Система забезпечення стабільності постачання електричної мережі та захисту критичної інфраструктури складається з ряду президентських директив та законів, прийнятих Конгресом США. Законодавчі акти можна поділити на три основні категорії:

1. Закони США та стратегічні документи
2. Президентські директиви
3. Директиви відомств та регіональні ініціативи

The Energy Policy Act of 2005[61]

Закон, що регулює всі сфери енергетики, включно з електроенергією. Вводить поняття «Electric Reliability Organization», «Reliability standard» та регулює їхню роботу. Reliability standards (стандарти стійкості) це вимоги до операційної роботи електроенергетичної системи США, що включають фізичну та кібербезпеку. Стандарти затверджує американський енергетичний регулятор (Federal Energy Regulatory Commision) у співпраці з Electric Reliability Organization (ERO). ERO це організація, яка сертифікована регулятором і її основної метою є розробка та впровадження стандартів стійкості для електроенергетичної сфери.

Energy Independence and Security Act of 2007 (EISA), Section 1301 (Smart Grid)[62]

Закон визначає національну політику стосовно розвитку енергетики, та модернізації електромереж зокрема (Section 1301). Задля підтримки надійної та безпечної електроенергетичної інфраструктури документ окреслює вимоги кібербезпеки для розумних мереж (Smart Grid).

Відповідно до закону DOE (Office of Electricity) відповідальний за впровадження Smart Grid у електроенергетичному секторі США. Встановлює національну політику стосовно модернізації електромереж для підтримки надійної та безпечної інфраструктури електроенергетики для задоволення майбутнього зростання попиту.

Section 215A of the Federal Power Act (FPA)[63]

Розділ 215A (a) визначає «надзвичайну ситуацію з безпекою мережі» та уповноважує Міністра енергетики надзвичайними заходами після того, як Президент оголошує надзвичайну ситуацію в галузі електроенергетичної безпеки. Надзвичайна ситуація мережі може бути наслідком фізичної атаки, кібератаки з використанням електронного зв'язку, електромагнітного імпульсу або геомагнітної бурі, що може пошкодити певні об'єкти інфраструктури електроенергетики та погіршити надійність енергетичної мережі країни. Екстрені накази, що реагують на надзвичайні ситуації, пов’язані з безпекою мережі, мають на

61 https://www.congress.gov/109/plaws/publ58/PLAW-109publ58.pdf

62 https://www.congress.gov/bill/110th-congress/house-bill/6

63 https://uscode.house.gov/

меті якомога швидше та ефективніше пом'якшити або усунути загрози надійності.

Визначається роль актора «Emergency & Incident Management Council» (EIMC). Це організація в структурі DOE та під головуванням заступника міністра енергетики, призначена для посилення співпраці та координації у Департаменті з метою підготовки, пом'якшення наслідків, реагування на ситуацію та відновлення від надзвичайних ситуацій. EIMC відіграє центральну роль у надзвичайних розпорядженнях щодо безпеки мережі.

План захисту критичної інфраструктури (2013)[64] та Енергетичний секторальний специфічний план (2015)[65]

Стратегічні документи, що визначають основні принципи політики стосовно захисту критичної інфраструктури, стейкхолдерів, окреслюють основні ризики для інфраструктури та визначають відповідальні органи за визначення та захист критичної інфраструктури

PRESIDENTIAL POLICY DIRECTIVE/PPD-21[66] Critical Infrastructure Security and Resilience

Директива про безпеку та стійкість критичної інфраструктури. Сприяє національній єдності зусиль щодо зміцнення та підтримання безпеки, функціонування та стійкої критичної інфраструктури.

Директива має три основні стратегічні цілі:

1) визначення функціональних взаємозв'язків у федеральному уряді для просування національної єдності зусиль щодо посилення безпеки та стійкості критичної інфраструктури;
2) забезпечення ефективного обміну інформацією шляхом визначення базових даних та системних вимог до федерального уряду;
3) впровадження функції інтеграції та аналізу для інформування про планування та оперативні рішення щодо критичної інфраструктури.

Директива передбачає залучення секторальних агентств (Sector-Specific Agencies), інших федеральних департаментів та відомств, а також співпрацю з власниками та операторами критичної інфраструктури.

Sector-Specific Agencies (в енергетиці Department of Energy)

Основні функції:

- координує роботу з Department of Homeland Security (DHS) та іншими відповідними федеральними департаментами та установами та співпрацює з власниками та операторами критичної інфраструктури, з незалежними регулюючими органами
- встановлення пріоритетів та координації секторних видів діяльності;
- управління інцидентами відповідно до статутних повноважень та інших відповідних політик, директив або положень;

Grid Security Emergency Final Rule, 10 CFR Part 205, (January 2018)[67]

Директива DOE, що встановлює процедури щодо того, як міністр здійснює дії щодо введення надзвичайних заходів після президентської декларації про надзвичайну безпеку мережі (GSE).

State Energy Assurance Plans

---

64 https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

65 https://www.cisa.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf

66 https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

67 https://www.govinfo.gov/content/pkg/FR-2018-01-10/pdf/2018-00259.pdf

Кожний уповноважений орган у своєму штаті розробляє регіональні Energy Assurance Plans. Це уніфіковані плани, що регламентують відповідальність та ролі регіональних посадовців під час надзвичайних ситуацій, спричинених природними катаклізмами, військовими та терористичними загрозами, непередбачуваними економічними факторами. У структуру таких планів входить:

- вказівки до процесу координації, заходів реагування та етапів реагування
- перелік основних принципів роботи під час надзвичайної ситуації для кожної відповідальної посадової особи у відомствах

2.2 ОПИС УЧАСНИКІВ ПРОЦЕСУ РЕАГУВАННЯ, ЇХНІ ФУНКЦІЇ ТА ЕТАПИ РЕАГУВАННЯ НА КРИЗУ

DOE/Office of Electricity

Проводить планування готовності до надзвичайних ситуацій національної безпеки, та проведення надзвичайних енергетичних навчань з енергетичною галуззю, федеральними партнерами та місцевими, штатними, племінними територіальними урядами.

DOE розробляє **North American Energy Resilience Model**, яка розширює здатність забезпечувати надійне та стійке постачання енергії в різних енергетичних секторах, враховуючи низку масштабних нових загроз. Модель знаходиться на етапі впровадження

Розробка системи NAERM буде організована у два етапи.

Етап 1 - Довгострокове енергетичне планування з використанням даних в режимі офлайн. Створення базової можливості планування в режимі офлайн для об'ємних систем передачі електроенергії та газу.

Етап 2 - Поінформованість про ситуацію та оперативне енергетичне планування.

Office of Cybersecurity, Energy Security, and Emergency Response (DOE)

Як секторальне агентство, що відповідає за енергетику DOE через Office of Cybersecurity, Energy Security, and Emergency Response:

- виявляє та оцінює життєво важливу енергетичну інфраструктуру;
- координує та проводить обмін інформацією з приватним сектором енергетики та з місцевими, державними, племінними та територіальними структурами;
- служить основним федеральним інтерфейсом для визначення пріоритетів та координації діяльності енергетичного сектору, включаючи, безпеку, ситуаційну обізнаність, планування, діяльність з підготовки, оцінку ризиків, секторну та національну звітність та навчання;
- проводить або підтримує заходи реагування на інциденти, що стосуються сектору енергетично важливої інфраструктури, відповідно до статутних органів та інших відповідних директив;
- координує та обмінюється інформацією з Electricity Sub-Sector Coordinating Council, NERC.

North American Electric Reliability Corporation

The Energy Policy Act 2005 року впровадив Організацію з надійності електричної енергії (ERO), незалежну, саморегульовану установу, яка застосовує обов’язкові «стандарти надійності» електричної енергії для всіх користувачів, власників та операторів національної системи передачі. Федеральна комісія регулювання енергетики (FERC) наділена повноваженнями нагляду за ERO. У липні 2006 року FERC сертифікував Північноамериканську корпорацію з електричної надійності (NERC) як ERO.

«Стандарт надійності» означає вимогу, затверджену Комісією щодо забезпечення надійної роботи системи. Цей термін включає вимоги до експлуатації існуючих об'єктів системи, включаючи захист кібербезпеки, та проектування запланованих доповнень або модифікацій таких об'єктів настільки, наскільки це необхідно для забезпечення надійної роботи системи.

Office of Energy Infrastructure Security (OEIS) (FERC)

Офіс у структурі FERC, який виконує наступні функції:

- розробка рекомендацій щодо виявлення, передачі та пом'якшення потенційних загроз та вразливостей, пов'язаних з кібер- та фізичною безпекою енергетичних об'єктів, що підпадають під юрисдикцію FERC, з використанням існуючих статутних повноважень Комісії;
- радання допомоги, експертних знань та порад іншим федеральним та державним установам, юрисдикційним комунальним службам та Конгресу у виявленні, передачі та пом'якшенні потенційних кібер- та фізичних загроз та вразливостей для енергетичних об'єктів, що підпадають під юрисдикцію FERC;

Electricity Sub-Sector Coordinating Council

Мета організації полягає у сприянні та підтримці координації діяльності та ініціатив, пов'язаних із політикою, у всіх підсекторах, спрямованих на підвищення надійності та стійкості підгалузі електроенергетики, включаючи фізичну і кібернетичну інфраструктуру та готовність до надзвичайних ситуацій у енергетичній галузі.

Місія ESCC базується на рекомендації Національної консультативної ради з питань інфраструктури (NIAC) ініціювати діалог на рівні виконавчої влади з керівниками секторів електроенергетики (CEO) та іншими вищими керівниками щодо ролей та відповідальності галузі у вирішенні інфраструктури з великим впливом ризиками та потенційними загрозами, і узгоджується з Директивою Президентської політики 21.

ESCC не регулюється жодним федеральним агентством, управляється самостійно та участь є добровільною.

Члени:

- представники підприємств генерації, передачі та розподілу е/е;
- регіональні розподільні оператори та незалежні системні оператори (ISO / RTO);
- NERC;
- Національна консультативна рада з питань інфраструктури (NIAC);
- Канадська асоціація електроенергетики (CEA), враховуючи взаємопов’язаний характер північноамериканської електричної мережі.

Electricity Information Sharing and Analysis Center (E-ISAC)

Аналітичний центр та інформаційний портал E-ISAC надає своїм членам та партнерам ресурси для підготовки та зменшення кібер- та фізичних загроз безпеці. E-ISAC управляється та тісно співпрацює з NERC, проте організаційно відокремлений. NERC та E-ISAC дотримуються суворого Кодексу поведінки (меморандум, де прописано, що NERC не впливає на результати роботи організації).

EAGLE-I

EAGLE-I - це веб-інструмент, який автоматично збирає дані про стан обслуговування електричної мережі в режимі реального часу з веб-сайтів компанії та упорядковує їх у зручну для читання картину стану електрообладнання по всій країні. Покриваючи 75 відсотків усіх споживачів електроенергії в США, він надає інформацію про мережу в режимі реаль-

ного часу, допомагаючи здійснити реагування на аварії та відновлення.

Місцеві органи влади

Місцеві органи влади безпосередньо відповідальні за організацію міжвідомчих органів для реагування на кризи у своєму штаті.

Місцеві органи влади, зокрема профільні відомства, що стосуються енергетики та захисту критичної інфраструктури (у кожному штаті назви відомств можуть відрізнятися) розробляють Energy Assurance Plans, що включають в себе покрокові інструкції стосовно реагування на кризу, інструкції стосовно створення міжвідомчих груп для реагування, комунікаційні настанови, роботу зі споживачами.

Для координації дій між штатами на випадок реалізації загроз існує Energy Emergency Assurance Coordinators Program, організована DoE, місцевими посадовцями з різних штатів.

Energy Emergency Assurance Coordinators Program

- Спільний координаційний орган з федеральними та національними зацікавленими сторонами
- Держава та території визначають первинний та вторинний контакт для кожного сектору (нафта, електроенергія, природний газ), щоб служити контактними точками у випадку надзвичайної ситуації в енергетиці.
- Забезпечує достовірне, точне та своєчасне джерело інформації та оновлення щодо вжитих дій.
- Мета полягає в покращенні обміну інформацією та комунікації, скороченні часу реагування та забезпеченні кращої координації між штатами та федеральними органами на етапі планування та операційних завдань.

Оператори енергосистеми

Оператори енергосистеми відповідальні за первинне реагування та усунення наслідків інцидентів. Оператори енергосистеми у електроенергетиці впроваджують розроблені регулятором (FERC) та NERC (North American Electric Reliability Corporation) стандарти операційної безпеки, що стосуються захисту від фізичних та кіберзагроз. Відповідно до стандартів, оператори енергосистеми розробляються власні операційні та плани на випадок надзвичайної ситуації, що включають у себе програми навчань для персоналу, комунікаційні настанови на випадок криз, покрокові інструкції для персоналу.

Таблиця 2. Аналіз дій державних органів США стосовно реагування на кризу

Елементи екосистеми (стейкхолдери)	Штатний режим (передбачення загроз)	Режим запобігання реалізації загроз	Режим реагування на виникнення кризової ситуації	Режим відновлення штатного функціонування	«Вивчення уроків»
Президент	Координація дій сектору безпеки та оборони, що можуть стосуватися забезпечення стійкого енергопостачання Моніторинг поточного безпекового стану Прийняття необхідних нормативно-правових актів для забезпечення захисту та стійкості критичної інфраструктури Президент затверджує директиви. Наприклад, Directive PPD-21, Critical Infrastructure Security and Resilience	Повідомлення для ЗМІ та міжнародного співтовариства, координація дій сектору безпеки та оборони у випадку військових загроз енергетичному сектору Приведення сил сектору безпеки та оборони у режим підвищеної готовності	Повідомлення для ЗМІ та міжнародного співтовариства Оголошення надзвичайного стану у енергетиці Координація дій сектору безпеки та оборони у випадку військових загроз енергетичному сектору Недопущення ескалації кризи та її використання у цілях, що загрожують національній безпеці держави Мобілізація всіх ресурсів для нейтралізації можливих загроз національній безпеці. За потреби здійснюють комунікацію з міжнародним співтовариством стосовно допомоги	За потреби здійснюють комунікацію з міжнародним співтовариством стосовно допомоги Координація дій сектору безпеки та оборони у випадку військових загроз енергетичному сектору	Внесення змін до нормативно-правових актів на основі «вивчених уроків»

Елементи екосистеми (стейкхолдери)	Штатний режим (передбачення загроз)	Режим запобігання реалізації загроз	Режим реагування на виникнення кризової ситуації	Режим відновлення штатного функціонування	«Вивчення уроків»
Департамент енергетики (Department of Energy (DoE)) Office of Electricity/ Office of Cybersecurity, Energy Security, and Emergency Response	Прийняття нормативно-правових актів, що стосуються захисту критичною інфраструктури та «цільової функції енергозабезпечення» Встановлення порядку взаємодії та обміну інформацією органів влади DoE видає директиви стосовно менеджменту надзвичайних ситуацій, кіберзахисту, моніторингу надзвичайних ситуацій Розробка секторального плану захисту критичної інфраструктури (DoE розробляє Sector specific Plan) Оцінка загроз енергозабезпечення	Забезпечення процесу інформування ЗМІ, міжнародного співтовариства. Координування дій інших секторів критичної інфраструктури відповідно до розроблених планів реагування Активація планів запобігання реалізації загроз, приведення до максимальної готовності системи захисту та реагування Оцінка сценаріїв розвитку кризової ситуації Забезпечення вчасного та ефективного процесу інформування усіх об'єктів реагування.	Розгортання антикризового штабу Забезпечення координації відомств, що залучені до процесу реагування Обмеження масштабу інциденту, локалізація наслідків загроз Оцінка масштабів загроз, потреб у ресурсах Активація планів забезпечення безпеки та стійкості енергопостачання Інформування інших учасників реагування Забезпечення управління в режимі кризової ситуації. Забезпечення стратегічної комунікації	Оцінка можливостей скасування режиму кризового реагування Припиняється робота антикризового штабу стосовно реагування Оцінка можливостей скасування режиму кризового реагування Прийняття рішення про перехід до відновлення нормального функціонування пошкодженої критичної інфраструктури. Виконання заходів з пом’якшення/ліквідації наслідків кризової ситуації.	Внесення змін до нормативно-правових актів та стратегічних документів на основі «вивчених уроків» Аналіз інциденту, «вивчення уроків», перегляд секторального плану забезпечення стійкості енергопостачання. Інформування учасників сектору стосовно причин та наслідків загрози, напрацювання рекомендацій до стратегічних документів.

Елементи екосистеми (стейкхолдери)	Штатний режим (передбачення загроз)	Режим запобігання реалізації загроз	Режим реагування на виникнення кризової ситуації	Режим відновлення штатного функціонування	«Вивчення уроків»
	Формування реєстру об'єктів критичної інфраструктури у електроенергетичній сфері Ведення комунікації з учасниками електроенергетичного сектору (виробники, оператори, споживачі) стосовно: їхніх прав та обов'язків Проведення навчання та вправ, що стосуються запобіганню загроз Встановлення вимог до забезпечення «цільовій функції енергозабезпечення» Підготовка плану заходів «запобігання» та реагування на загрози енергозабезпечення Моніторинг стану захисту критичної інфраструктури та «цільової функції енергозабезпечення»	У випадку оголошення Президентом надзвичайного стану у енергетиці керівник DoE організовує антикризовий штаб, що регулюється Section 215A of the Federal Power Act (FPA)			Розслідування інцидентів. DoE регулює процедури розслідування інцидентів через видачу директив

Елементи екосистеми (стейкхолдери)	Штатний режим (передбачення загроз)	Режим запобігання реалізації загроз	Режим реагування на виникнення кризової ситуації	Режим відновлення штатного функціонування	«Вивчення уроків»
Органи влади взаємодії (DHS, Federal Emergency Management Agency, Department of Transportation та інші)	Участь у оцінці загроз «цільовій функції енергозабезпечення» Обмін інформацією органів влади, що задіяні до захисту критичної інфраструктури та забезпечення стійкого енергопостачання Урядові відомства розробляють Specific Plans та регулюється Emergency Support Functions	Приведення сил сектору безпеки і оборони у режим підвищеної готовності, відповідно до розроблених планів реагування	Обмеження масштабу інциденту та стабілізація ситуації на місці подій Недопущення ескалації кризи Забезпечення безпеки громадян та команд реагування	Виконання заходів з пом'якшення/ліквідації наслідків кризової ситуації. Надання допомоги населенню Передача основної координуючої ролі до FEMA	Аналіз інциденту стосовно покращення захисту об'єктів критичної інфраструктури

Елементи екосистеми (стейкхолдери)	Штатний режим (передбачення загроз)	Режим запобігання реалізації загроз	Режим реагування на виникнення кризової ситуації	Режим відновлення штатного функціонування	«Вивчення уроків»
Місцева влада	Оцінка загроз енергозабезпечення місцевого рівня Підготовка місцевого плану заходів «запобігання» та реагування на загрози енергозабезпечення споживачів Проведення навчання та вправ для персоналу Місцеві органи влади розроблять Energy Assurance Plan, які регулюють діяльність органів влади під час кризи.	Приведення регіональних учасників реагування у режим «підвищеної готовності» Інформування населення регіону про можливі загрози енергозабезпечення споживачів та за потреби прохання зменшити споживання задля зменшення ймовірності настання загрози Впроваджуються дії щодо зменшення енергоспоживання державними установами	Обмеження масштабу інциденту та стабілізація ситуації на місці подій Недопущення ескалації кризи У разі неминучої ескалації кризи координування дій з центральними органами влади Координування/інформування дій з іншими залученими учасниками реагування Інформування населення стосовно загрози, надання рекомендацій, що зможуть зменшити наслідки загрози	Виконання заходів з пом'якшення/ліквідації наслідків кризової ситуації. Надання допомоги населенню Інформування населення стосовно переходу до етапу відновлення від кризової ситуації	Аналіз інциденту та внесення змін до місцевого плану заходів «запобігання» та реагування на загрози енергозабезпечення споживачів

Елементи екосистеми (стейкхолдери)	Штатний режим (передбачення загроз)	Режим запобігання реалізації загроз	Режим реагування на виникнення кризової ситуації	Режим відновлення штатного функціонування	«Вивчення уроків»
Регулятор (FERC) Office of Energy Infrastructure Security (OEIS) North American Electric Reliability Corporation NERC E-ISAC	Розробка, впровадження та перевірка стандартів «операційної безпеки». Програма E-ISAC забезпечує обмін інформацією між учасниками електроенергетичного сектору стосовно захисту від кібер та фізичних загроз. Відомства проводять навчання для учасників енергетичного сектору на випадок кібер та фізичних загроз енергетичній системі Діяльність відомств регулюється The Energy Policy Act of 2005, PPD-21	Інформування учасників реагування стосовно можливих загроз та «нагадування» стосовно дотримання стандартів «операційної безпеки» Оперативне введення стандартів «операційної безпеки» Програма E-ISAC забезпечує обмін інформацією між учасниками електроенергетичного сектору стосовно потенційної загрози	Забезпечення інформування усіх можливих учасників реагування стосовно етапів реагування на загрозу	Забезпечення інформування усіх можливих учасників реагування стосовно етапів реагування на загрозу	Внесення змін до стандартів «операційної безпеки» на основі аналізу інциденту

Таблиця 3. Участь недержавного сектору у процесі реагування на кризу

Елементи екосистеми (стейкхолдери)	Штатний режим (передбачення загроз)	Режим запобігання реалізації загроз	Режим реагування на виникнення кризової ситуації	Режим відновлення штатного функціонування	«Вивчення уроків»
Постачальники ресурсів	Участь у підготовці плану заходів «запобігання» та реагування на загрози енергозабезпечення Проведення навчання та вправ для персоналу Розробляють операційні та антикризові плани, відповідно до стандартів безпеки, запропонованих FERC та NERC. Беруть участь у субсекторальній електроенергетичній координаційній групі (Electricity Sub-Sector Coordinating Council)	Виконання плану заходів «запобігання» та реагування на загрози енергозабезпечення Беруть участь у субсекторальній електроенергетичній координаційній групі (Electricity Sub-Sector Coordinating Council)	Виконання плану заходів реагування на загрози енергозабезпечення Виконання штабу DOE або уповноваженого ним органу Беруть участь у субсекторальній електроенергетичній координаційній групі (Electricity Sub-Sector Coordinating Council)	Активація планів відновлення функціонування об'єктів критичної інфраструктури. Беруть участь у субсекторальній електроенергетичній координаційній групі (Electricity Sub-Sector Coordinating Council)	Надання рекомендацій до змін до плану заходів «запобігання» та реагування на загрози енергозабезпечення Беруть участь у субсекторальній електроенергетичній координаційній групі (Electricity Sub-Sector Coordinating Council)

Елементи екосистеми (стейкхолдери)	Штатний режим (передбачення загроз)	Режим запобігання реалізації загроз	Режим реагування на виникнення кризової ситуації	Режим відновлення штатного функціонування	«Вивчення уроків»
Субсекторальна електроенергетична координаційна група (Electricity Sub-Sector Coordinating Council)	Розробляє рекомендації до Energy Specific Plan, стандартів безпеки, регулювання ринку електроенергетики у цілому. Забезпечують обмін інформацією стосовно потенційних загроз та шляхів вирішення Регламентується Energy Specific Plan	Посилюють процес поширення інформації стосовно потенційних загроз, за можливості співпрацюють з урядом задля зменшення майбутніх наслідків кризи	Забезпечують поширення інформації між учасниками групи стосовно загрози та її наслідків. За потреби допомагають уряду у координації дій стосовно реагування на кризу	Забезпечують поширення інформації між учасниками групи стосовно загрози та її наслідків.	Розробляють рекомендації до стратегічних документів, стандартів безпеки, координаційних питань

Елементи екосистеми (стейкхолдери)	Штатний режим (передбачення загроз)	Режим запобігання реалізації загроз	Режим реагування на виникнення кризової ситуації	Режим відновлення штатного функціонування	«Вивчення уроків»
Виробники	Участь у підготовці плану заходів «запобігання» та реагування на загрози Проведення навчання та вправ для персоналу Розробляють операційні та антикризові плани, відповідно до стандартів безпеки, запропонованих FERC та NERC. Беруть участь у субсекторальній електроенергетичній координаційній групі (Electricity Sub-Sector Coordinating Council)	Виконання плану заходів «запобігання» та реагування на загрози Беруть участь у субсекторальній електроенергетичній координаційній групі (Electricity Sub-Sector Coordinating Council)	Виконання плану заходів реагування на загрози Виконання вказівок Міжвідомчого антикризового штабу або уповноваженого ним органу. Беруть участь у субсекторальній електроенергетичній координаційній групі (Electricity Sub-Sector Coordinating Council)	Активація планів відновлення функціонування об'єктів критичної інфраструктури. Беруть участь у субсекторальній електроенергетичній координаційній групі (Electricity Sub-Sector Coordinating Council)	Надання рекомендацій до змін до плану заходів «запобігання» та реагування на загрози Беруть участь у субсекторальній електроенергетичній координаційній групі (Electricity Sub-Sector Coordinating Council)

Елементи екосистеми (стейкхолдери)	Штатний режим (передбачення загроз)	Режим запобігання реалізації загроз	Режим реагування на виникнення кризової ситуації	Режим відновлення штатного функціонування	«Вивчення уроків»
Оператор (СП)	Участь у підготовці плану заходів «запобігання» та реагування на загрози енергозабезпечення Підготовка плану забезпечення операційної безпеки системи передачі Проведення навчання та вправ для персоналу Оператори системи передачі розробляють операційні та антикризові плани, відповідно до стандартів безпеки, запропонованих FERC та NERC. Беруть участь у субсекторальній електроенергетичній координаційній групі (Electricity Sub-Sector Coordinating Council)	Реалізація планів «запобігання» та реагування на загрози енергозабезпечення Створення команди для реагування та інформування інших учасників реагування Беруть участь у субсекторальній електроенергетичній координаційній групі (Electricity Sub-Sector Coordinating Council)	Активація планів «запобігання» та реагування на загрози енергозабезпечення Реалізація первинного реагування засобами та ресурсами персоналу об'єкта У разі неминучого збільшення масштабу інциденту, активація планів «реагування», що потребуються залучення інших учасників реагування. Застосування плану аварійної роботи Виконання вказівок DOE або уповноваженого ним органу Беруть участь у субсекторальній електроенергетичній координаційній групі (Electricity Sub-Sector Coordinating Council)	Активація планів відновлення функціонування об'єктів критичної інфраструктури Беруть участь у субсекторальній електроенергетичній координаційній групі (Electricity Sub-Sector Coordinating Council)	Надання рекомендацій до змін до стандартів «операційної безпеки» Беруть участь у субсекторальній електроенергетичній координаційній групі (Electricity Sub-Sector Coordinating Council)

Елементи екосистеми (стейкхолдери)	Штатний режим (передбачення загроз)	Режим запобігання реалізації загроз	Режим реагування на виникнення кризової ситуації	Режим відновлення штатного функціонування	«Вивчення уроків»
Оператор (СР)	Участь у підготовці плану заходів «запобігання» та реагування на загрози енергозабезпечення Підготовка плану забезпечення операційної безпеки системи розподілу Участь у підготовці місцевого плану заходів «запобігання» та реагування на загрози енергозабезпечення споживачів Проведення навчання та вправ для персоналу Оператори систем розподілу розробляють операційні та антикризові плани, відповідно до стандартів безпеки, запропонованих FERC та NERC. Беруть участь у субсекторальній електроенергетичній координаційній групі (Electricity Sub-Sector Coordinating Council)	Реалізація плану заходів реагування на загрози Забезпечення первинного реагування Забезпечення вчасного та повного інформування інших учасників реагування	Активація плану заходів реагування на загрози «цільовій функції енергозабезпечення» Забезпечення первинного реагування Забезпечення вчасного та повного інформування інших учасників реагування Застосування плану аварійної роботи Виконання вказівок Міжвідомчого антикризового штабу або уповноваженого ним органу	Активація планів відновлення функціонування об'єктів критичної інфраструктури	Надання рекомендацій до змін до плану заходів «запобігання» та реагування на загрози Надання рекомендацій до змін до стандартів «операційної безпеки»

Елементи екосистеми (стейкхолдери)	Штатний режим (передбачення загроз)	Режим запобігання реалізації загроз	Режим реагування на виникнення кризової ситуації	Режим відновлення штатного функціонування	«Вивчення уроків»
Споживачі промислові	Підготовка плану захисту критичної інфраструктури Участь у підготовці місцевого плану заходів «запобігання» та реагування на загрози енергозабезпечення споживачів Проведення навчання та вправ для персоналу.	Реалізація плану захисту критичної інфраструктури, плану заходів «запобігання» та реагування на загрози	Активація плану захисту критичної інфраструктури Виконання вказівок Міжвідомчого антикризового штабу або уповноваженого ним органу	Участь у планах відновлення функціонування об'єктів критичної інфраструктури	Надання рекомендацій до змін до плану заходів «запобігання» та реагування на загрози та плану захисту критичної інфраструктури
Домогосподарства	Участь у підготовці місцевого реагування на загрози енергозабезпечення	Виконання вказівок місцевої влади стосовно заходів реагування	Виконання вказівок місцевої влади стосовно заходів реагування	Виконання вказівок місцевої влади стосовно заходів реагування	Надання рекомендацій до місцевого реагування на загрози енергозабезпечення

2.3 АНАЛІЗ КІБЕРАТАКИ НА ТРУБОПРОВІДНУ СИСТЕМУ США «COLONIAL PIPELINE».

Загальний опис розвитку ситуації

У п'ятницю, 7 травня 2021 року було повідомлено про проведення кібератаки на трубопровідну систему США «Colonial Pipeline».

> *Трубопровідна система Colonial Pipeline доставляє бензин, дизельне та авіаційне паливо з Техасу, фактично майже в усі Східні штати аж до Нью-Йорка. Щоденно по нафтопроводу протяжністю 8850 км транспортується понад 2,5 млн барелів нафтопродуктів, що забезпечує 45% потреби у паливі всього Східного побережжя США.*
>
> *Атака сталася на тлі зростаючої стурбованості з приводу уразливості інфраструктури для кібератак, що виникла після кількох гучних атак, в тому числі злому SolarWinds в 2020 році, які вплинули навіть на кілька державних установ, включаючи Пентагон, Міністерство фінансів, Державний департамент і Міністерство внутрішньої безпеки.*

Робота трубопроводу повністю комп'ютеризована. При цьому систему управління технологічними процесами (operational technology (OT)) з'єднана з адміністративною інформаційною системою (information Technology (IT)), що відкриває потенційні можливості для проникнення через Інтернет, найчастіше, через електронну пошту. Саме цією вразливістю найчастіше користуються зловмисники.

Ransomware атак[68] зашифрувала інформацію на серверах компанії. Погрожуючи публічним оприлюдненням комерційної інформації, зловмисники вимагали плати за повернення Colonial Pipeline доступу до інформації. Зважаючи на неможливість ведення розрахунків із споживачами, керівництвом компанії було прийнято рішення:

- зупинити роботу трубопроводу до усунення шкідливих програм із IT та запобіганню ризику проникнення зловмисних програм в систему управління технологічними процесами (OT);
- виплатити викуп (75 біткойнів або майже 5 мільйонів доларів) протягом декількох годин після нападу;
- залучити для допомоги з подолання наслідків кібератаки приватну фірму з кібербезпеки FireEye, але не залучати Агентство з питань кібербезпеки та безпеки інфраструктури (CISA) до розслідування.

Атака зупинила роботу всіх трубопроводів системи на п'ять днів. Хакери надіслали Colonial Pipeline програмний додаток для відновлення IT мережі та повернення доступу до інформації, але відновлення інформації здійснювалось дуже повільно. 9 травня 2021 року компанія оголосила, що планує здійснити значний ремонт та відновити роботу трубопроводу до кінця тижня.

На Східному побережжі США почав виникати дефіцит палива на АЗС на тлі панічних покупок. На четвертий день (11 травня) через зупинку трубопроводу гострий дефіцит палива спостерігався в Алабамі, Флориді, Джорджії, Північній та Південній Каролініі. Найбільше постраждали райони від півночі Південної Каролініи до Вірджинії: в Шарлотті 11 травня 71% АЗС були закриті через відсутність палива, в окрузі Колумбія 14 травня не працювало 87% АЗС. Середні ціни на паливо зросли до найвищих з 2014 року, у понад 3 долари за галон.

---

68 Кібератака на Colonial Pipeline - приклад кібератаки Ransomware (тобто «програми-здирника»), націленої не просто проти бізнесу, а на важливий для країни елемент інфраструктури. Для цього злочинці використовували безпрецедентно масштабну комп'ютерну систему вартістю десятки мільйонів доларів.
Деякі експерти вважають, що успіх атаки на нафтопровід забезпечили «коронавірусне обмеження» - на робочому місці в компанії знаходилося менше мережевих інженерів, ніж зазвичай, велика їх частина працювала з дому. Зловмисники імовірно просто купила логін і пароль до утиліти віддаленого доступу, наприклад TeamViewer або Microsoft Remote Desktop, якою могли користуватись працівники.

Через зупинку трубопроводу зростали і ризики негативних економічних наслідків для США. Стали зростати об'єми нафти, що накопичувались для переробки на нафтопереробних заводах в Техасі, що спричиняло тиск на нафтодобувну галузь. Запаси бензину, дизельного палива США швидко падали, не тільки через зупинку трубопроводу, але й через зняття карантину і відновлення масового автомобільного руху.

13 травня 2021 року, Colonial Pipeline відновила роботу всієї мережі трубопроводів. Утім, в деяких регіонах на сході країни, після відновлення роботи, все ще відчувався дефіцит пального протягом декількох днів.

Реагування на надзвичайну ситуацію

7 травня Colonial Pipeline оголосила про кібератаку.

Міністерство транспорту США (US Department of Transportation (USDOT)) у неділю, 9 травня, оголосило регіональну надзвичайну ситуацію у Східних штатах США[69]. Даним розпорядженням в 18 штатах були ослаблені норми перевезення палива дорогами, зокрема щодо кількості годин робочого дня та тривалості роботи без перерви для водіїв компаній-перевізників нафтопродуктів.

10 травня губернатор штату Джорджія оголосив надзвичайний стан і тимчасово відмовився від збору податків на моторне паливо (дизель та бензин). Північна Кароліна, Південна Кароліна та Вірджинія також оголосили надзвичайний стан.

Адміністрація Д.Байдена створила міжвідомчу робочу групу для підготовки до різних сценаріїв, включно з необхідністю ухвалення додаткових заходів для пом'якшення будь-якого потенційного впливу на поставки пального. Загалом було запроваджено цілий ряд заходів реагування[70]:

- Федеральне управління безпеки автомобільних перевізників (USDOT's Federal Motor Carrier Safety Administration (FMCSA))[71] видало тимчасове звільнення від заборони роботи понаднормові години ("Hours of Service" waiver) для водіїв, які перевозять очищені нафтопродукти, включаючи бензин, дизельне паливо та авіаційне паливо, до постраждалих штатів уздовж Східного узбережжя;
- FMCSA і Федеральна адміністрація автомобільних доріг (USDOT's Federal Highways Administration (FHWA)) здійснювали моніторинг ситуації у штатах, а також видали накази про надзвичайну ситуацію і декларації, поширювали кращу практику реагування та можливості послабити вплив кризи.
- Ряд штатів (Північна Кароліна та Джорджія) підтримала заклик USDOT та надали дозвіл на збільшення ваги автоцистерн, що можуть пересуватись по дорогах штатів. Також штати запровадили обмін інформацією із DOT для узгодження зусиль з реагування на кризову ситуацію та поширення досвіду;
- Агентство захисту довкілля (The Environmental Protection Agency (EPA)) видало тижневий дозвіл використання нестандартного палива для 12 штатів, що знаходяться у зоні надзвичайної ситуації, намагаючись збільшити доступне постачання[72]. Дозвіл був продовжений на термін до 20 днів;

---

69 REGIONAL EMERGENCY DECLARATION UNDER 49 CFR § 390.23 No. 2021-002. https://www.fmcsa.dot.gov/emergency/esc-ssc-wsc-regional-emergency-declaration-2021-002-05-09-2021

70 The Biden-Harris Administration Has Launched an All-of-Government Effort to Address Colonial Pipeline Incident. https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/11/fact-sheet-the-biden-harris-administration-has-launched-an-all-of-government-effort-to-address-colonial-pipeline-incident/

71 https://www.transportation.gov/briefing-room/us-department-transportations-federal-motor-carrier-administration-issues-temporary

72 https://www.epa.gov/newsreleases/epa-issues-fuel-waiver-select-areas-impacted-colonial-pipeline-shutdown

- Федеральна залізнична адміністрація (The Federal Railroad Administration of DOT) активувала процедури щодо визначення спроможності залізничних операторів допомагати у транспортуванні палива з портів углиб країни, залучення залізничних операторів по всій країні до допомоги у транспортуванні палива з прибережних портів для потреб споживачів вглибині країни;
- Морська адміністрація (USDOT's Maritime Administration (MARAD)) розпочала оцінку наявності суден, які відповідно до законодавства (Jones Act) можуть бути додатково використані для перевезення нафтопродуктів у Мексиканській затоці та вздовж Східного узбережжя у кризовій ситуації. Морська адміністрація також готувала переліки відповідних суден для отримання дозволу від Міністерства внутрішніх справ (The Department of Homeland Security (DHS));[73]
- Адміністрація безпеки трубопроводів та небезпечних матеріалів (The Pipeline and Hazardous Materials Safety Administration of DOT (PHMSA)[74] видала тимчасове послаблення вимог до кваліфікації персоналу оператора трубопроводів, що був необхідний для допомоги у частковому поверненні в експлуатацію вручну;
- Проведено аналіз для визначення пріоритетів постачання пального до пунктів призначення для обслуговування районів з найбільшою потребою. Енергетичний Регулятор США (The Federal Energy Regulatory Commission - FERC) за необхідності мав повноваження запровадити такі вимоги для Colonial Pipeline;
- Підготовлено оперативні рекомендації щодо захисту критичної інфраструктури, зокрема від кібератак. ФБР (FBI) та Агентства з питань кібербезпеки та безпеки інфраструктури (The Cybersecurity and Infrastructure Security Agency (CISA)) опублікували[75] попередження FLASH для власників та операторів критичної інфраструктури та операторів із ідентифікаторами можливого враження та заходів пом'якшення впливу атак, якщо вони заражені.
- Запропоновано допомогу приватним операторам критичної інфраструктури, побідним до Colonial Pipeline посилити свою кібербезпеку завдяки долученню до ініціативи Кібербезпека промислових систем управління (the Industrial Control Systems Cybersecurity initiative), що реалізується спільними зусиллями між DOE, CISA та підприємствами електроенергетики для зміцнення стандартів кібербезпеки.

Після нападу на Colonial Pipeline компанії власників та операторів критичної інфраструктури звернулись до CISA для отримання інформації з питань кібербезпеки. CISA провело конференцію, в якій взяли участь понад 8500 учасників з 16 найважливіших секторів критичної інфраструктури, серед яких такі галузі, як енергетика, хімічна та ядерна галузі, а також представники штатів та місцевих органів влади. 12 травня CISA публічно оприлюднило набір технічних даних про інцидент, щоб допомогти іншим компаніям та комунальним службам критичної інфраструктури захиститися від подібної атаки.

Адміністрація Президента США Д.Байдена продовжувала щоденний моніторинг ситуа-

---

73 Statement on the Approval of an Additional Jones Act Waiver in Response to Eastern Seaboard Oil Supply Constraints. https://www.dhs.gov/news/2021/05/13/statement-approval-additional-jones-act-waiver-response-eastern-seaboard-oil-supply

74 PHMSA Stay of Enforcement - Colonial Pipeline Operator Qualification and Employment Testing Requirements https://www.phmsa.dot.gov/news/phmsa-stay-enforcement-colonial-pipeline-operator-qualification-and-employment-testing

75 Joint CISA-FBI Cybersecurity Advisory on DarkSide Ransomware. https://us-cert.cisa.gov/ncas/alerts/aa21-131a
May 11, 2021
If your organization is impacted by a ransomware incident, CISA and FBI recommend the following actions:

- **Isolate the infected system.** Remove the infected system from all networks, and disable the computer's wireless, Bluetooth, and any other potential networking capabilities. Ensure all shared and networked drives are disconnected, whether wired or wireless.
- **Turn off other computers and devices.** Power-off and segregate (i.e., remove from the network) the infected computer(s). Power-off and segregate any other computers or devices that shared a network with the infected computer(s) that have not been fully encrypted by ransomware.
- **Secure your backups.** Ensure that your backup data is offline and secure.

ції, аналізувала дію органів влади для забезпечення коригування процесу пом'якшення впливу кризи на життєдіяльність країни (american style of life)[76].

З метою недопущення паніки та ажіотажного попиту на автомобільне паливо, посадовці уряду США звертались через ЗМІ до бізнесу діяти відповідально та застерігали власників автозаправок від значного підвищення цін чи необгрунтованого закриття АЗС. «Федеральні чи державні чиновники розслідуватимуть ці дії, якщо побачать випадки маніпулювання цінами», - заявила Міністр енергетики США[77].

По закінченню кризи Д.Байден висловився за необхідність посилення вимог щодо підготовки критичної інфраструктури до впливу загроз різного типу[78]. 12 травня Президент США Д.Байден підписав[79] розпорядження про вдосконалення федеральної кібербезпеки, зазначивши, що агенції повинні брати активну роль у посиленні безпеки.

Розпорядженням Президента США передбачено[80] посилення процесу обміну інформації про загрози та інциденти із залученими компаніями, які будуть або є постачальниками послуг зі сфери кіберзахисту, впровадження більш жорстких стандартів кібербезпеки у федеральному уряді, запровадження методології багатофакторної автентифікація та шифрування, покращення безпеки ланцюжка постачання програмного забезпечення, вдосконалення системи захисту та реагування на інциденти, запровадження стандартизованого посібника щодо реагування на кіберінциденти федеральними департаментами та відомствами тощо. Також створено Раду з огляду рівня кібербезпеки (the Cyber Safety Review Board[81], якій доручається робити моніторинг загроз, ризиків та стану кібербезпеки.

27 травня Адміністрація транспортної безпеки своїм наказом запровадила (DHS Transportation Security Administration (TSA)) нові вимоги до компаній операторів трубопроводів[82]. Даний наказ спрямований на виконання розпорядження підписаного президентом Байденом.

Відповідно до наказу TSA компанії, які експлуатують трубопроводи, тепер повинні будуть попереджати уряд, коли вони зазнають кібератак. Протягом 30 днів компанії також повинні оцінити, як їхні практики кібербезпеки узгоджуються з існуючими керівництвом TSA, та розробити плани щодо виправлення будь-яких прогалин. TSA зможе накладати щоденні штрафи на компанії, які їх не виконують. Протягом семи днів оператори повинні також призначити основних та дублюючих працівників, відповідальних за забезпечення цілодобового зв'язку з TSA та CISA. За невиконання наказу передбачено застосування штрафів, починаючи з 7000 доларів на день.

---

76 https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/10/statement-by-press-secretary-jen-psaki-on-the-colonial-pipeline-incident/
https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/13/statement-by-press-secretary-jen-psaki-on-restart-of-colonial-pipeline-and-continued-federal-government-efforts-to-mitigate-impacts/

77 https://www.whitehouse.gov/briefing-room/press-briefings/2021/05/11/press-briefing-by-press-secretary-jen-psaki-secretary-of-energy-jennifer-granholm-and-secretary-of-homeland-security-alejandro-mayorkas-may-11-2021/

78 https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/

79 https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/

80 Executive Order on Improving the Nation's Cybersecurity. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
Серед інших заходів федеральний уряд має запровадити: security best practices; advance toward Zero Trust Architecture; accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS); centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks; invest in both technology and personnel to match these modernization goals; improve the security and integrity of the software supply chain, with a priority on addressing critical software.

81 Пропонована модель подібна the National Transportation Safety Board, яка аналізує безпеку авіатранспорту та розслідує авіаварії та інциденти.

82 DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators. https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators

Новий наказ TSA є суттєвою зміною політики США щодо кібербезпеки для трубопровідних компаній, які до цього часу стикалися лише з добровільними вказівками TSA для компаній операторів трубопроводів щодо організації захисту інфраструктури[83],[84], включаючи пропозицію повідомляти про порушення.

Найближчим часом TSA планує видати другий наказ із кібербезпеки трубопровідного транспорту з більш суттєвими вимогами.

Також, на політичному рівні обговорюються пропозиції щодо запровадження обов'язкової звітності про кіберінциденти для всіх компаній, які експлуатують критичну інфраструктуру або надають ключові технологічні послуги.

При цьому, деякі політичні діячі дискутують щодо ролі TSA у структурі DHS, і зокрема пропонують позбавити нагляду за безпекою трубопроводів з TSA. Керівники Комітету палати з питань енергетики та торгівлі наполягали на тому, щоб DOE енергетики взяло на себе портфель TSA[85]. Однак голова Комітету національної безпеки стверджував[86], що TSA має необхідний досвід, щоб зберегти свою роль.

Виявленні проблеми застосування процедур кризового реагування

Оцінка DOE та DHS ситуації виявили, що у випадку при невідновлені роботи Colonial Pipeline (зупинка роботи понад 10-12 днів), країна опинилась би перед необхідністю зупинити транспортне сполучення (автобусне та інші види транспорту) через відсутність дизельного палива. Також зазначається, що хімічні фабрики та нафтопереробні заводи припинили би роботу, оскільки неможливо розподілити продукцію, яку вони виробляють. І хоча у рамках кризового реагування було оголошено про організацію альтернативних шляхів для перевезення бензину та авіаційного палива по Східному узбережжю, підготовлених засобів для кризового реагування не виявилось у достатній кількості. Не вистачало водіїв вантажівок (бензовозів) та вагонів-цистерн для поїздів.

Аналіз дій залучених до реагування на кризову ситуацію суб'єктів показав, що оператор трубопроводу лише через кілька днів надав відповідальному за кібербезпеку державному органу (CISA) технічні дані про кібератаку. Компанія також не повідомила CISA про те, що заплатила багатомільйонний викуп, щоб відновити доступ до своїх даних.

Дана атака виявила недоліки сучасного підходу федерального уряду США до захисту критичної інфраструктури. Мало хто з 16 інфраструктурних секторів, за безпеку яких відповідають різні федеральні агентства, мають обов'язкові вимоги до організації кібербезпеки критичної інфраструктури.

Протягом багатьох років робота базувалась на запровадженні «добровільних програм», а керівники агенцій наголошували на співпраці, а не на регулюванні, як на засобі захисту інфраструктури від хакерів. Але багато компаній - у тому числі деякі, що керують електростанціями США, очисними спорудами та іншою життєво-важливою інфраструктурою - або ігнорують кібербезпеку, або приділяють їй занадто мало ресурсів та уваги.

Деякі відомства, відповідальні за нагляд за інфраструктурою, включаючи TSA та EPA, мають невеликий досвід роботи з кібербезпекою та виділяють мало ресурсів для цифрових загроз. У 2018 році в підрозділі безпеки трубопроводу TSA працювало лише шість штатних співробітників, які не мали достатнього рівня знань та досвіду для реагування на

83 TSA Pipeline Security Guidelines. https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf

84 Pipeline Security and Incident Recovery Protocol Plan. https://www.tsa.gov/sites/default/files/pipeline_sec_incident_recvr_protocol_plan.pdf

85 https://republicans-energycommerce.house.gov/news/pipeline-and-lng-cybersecurity-is-a-job-for-doe-not-tsa/

86 https://homeland.house.gov/news/press-releases/chairman-thompson-statement-on-new-tsa-security-directive-for-pipeline-cybersecurity-

сучасні кіберзагрози.[87]

Загалом даний випадок, спонукав адміністрацію Д.Байдена до більш жорсткого підходу щодо захисту життєво-важливої критичної інфраструктури, що і відобразилось у прийнятті нового розпорядження Президента США про вдосконалення федеральної кібербезпеки.

При цьому на оператора трубопроводу починає чинитися тиск, щоб пояснити свою практику реагування на кіберзагрози та наслідки, що призвели до дефіциту палива та зростання цін. Було навіть подано федеральний позов проти Colonial Pipeline, в якому стверджувалося, що неправильні дії оператора (хоча існуючі процедури вимагають від компанії припинити роботу[88]) призвели до таких наслідків.

Це демонструє необхідність також знайти технічні та правові рішення щодо дії операторів критичної інфраструктури коли виникають неврегульованості між діючим законодавством щодо забезпечення безпеки критичної інфраструктури та забезпечення національної стійкості з точки зору загальносуспільних інтересів.

87 Critical Infrastructure Protection:Actions Needed to Address Weaknesses in TSA's Pipeline Security Program Management. https://www.gao.gov/products/gao-19-542t

88 Стандартна процедура реагування на інциденти передбачає вимкнення систем, заражених шкідливим програмним забезпеченням.
Коли системи інфіковані шкідливим програмним забезпеченням, виконується ряд кроків для обмеження пошкодження та відновлення систем. Інститут SANS має навіть скорочення від цього процесу - PICERL. Це скорочення розшифровується як: Підготовка; Ідентифікація; Стримування; Викорінення; Одужання; Вивчені уроки. Фаза стримування передбачає виведення систем з режиму он-лайн, щоб вони не заражали інші системи. Прикладами невиконання цієї процедури, що призвело до величезної шкоди є: WannaCry або NotPetya, які поширилися по всьому світу та вивели з ладу системи, включаючи лікарні у багатьох країнах світу.

РОЗДІЛ III
ФОРМУВАННЯ ПІДХОДУ РЕАГУВАННЯ НА КРИЗИ В ЕНЕРГЕТИЧНОМУ СЕКТОРІ УКРАЇНІ

3.1 ПРАКТИКА РЕАГУВАННЯ НА ЗАГРОЗИ ПОСТАЧАННЯ ЕЛЕКТРОЕНЕРГІЇ В УКРАЇНІ

Приклад застосування моделі реагування системи для забезпечення стійкості цільової функції

Чинним законодавством визначено дії залучених суб'єктів управління та суб'єктів господарської діяльності до реагування на кризові ситуації. Так, при виникненні загроз стійкості функціонування ОЕС України Кабінетом Міністрів України, у встановленому законодавством порядку[89], запроваджуються тимчасові «надзвичайні заходи» щодо функціонування енергоринку»[90]. Критеріями запровадження заходів визначено:

1) пошкодження електроенергетичних установок та/або незаконне втручання третіх осіб, що можуть призвести до обмеження споживання електричної енергії більш як на 100 МВт;
2) зниження резерву енергогенеруючих потужностей ОЕС України нижче допустимого рівня протягом трьох діб;
3) критичний стан забезпечення паливом, зокрема зниження запасів палива на окремих теплових електростанціях енергогенеруючих компаній нижче 20-денного запасу;
4) відсутність протягом трьох місяців підряд повної оплати електричної енергії, або якщо оплата у розрахунковому місяці нижче 90 відсотків.

Рішення про вжиття тимчасових надзвичайних заходів приймається Кабінетом Міністрів України за поданням Міненерговугілля або НКРЕКП. Тимчасові надзвичайні заходи можуть вживатися на період, що не перевищує один місяць. При цьому, на період застосування тимчасових надзвичайних заходів суб'єкти електроенергетики незалежно від форми власності зобов'язані діяти відповідно до стандартів операційної безпеки функціонування ОЕС України та оперативних команд і розпоряджень Оператор системи передачі "НЕК "Укренерго". Вимоги щодо забезпечення безпеки об'єктів електроенергетики у надзвичайній ситуації є обов'язковими для виконання всіма суб'єктами ринку електричної енергії незалежно від форми власності.

У період 2014-2017 років такі надзвичайні заходи запроваджувались при виникненні аварійних ситуацій, спричинених цілеспрямованими зловмисними діями проти ОЕС України (внаслідок агресії Росії проти України): запроваджено 13 серпня 2014 року[91] із щомісячним подовженням до 1 травня 2015 року; запроваджено 9 грудня 2015 року[92] з терміном дії до 15 січня 2016; запроваджено 17 лютого 2017[93] року із щомісячним подовженням до 20 червня 2017 року.

89 Закон України "Про ринок електричної енергії України". https://zakon.rada.gov.ua/laws/show/2019-19#Text

90 Постанова Кабінету Міністрів України від 13 серпня 2014 р. N° 372 «Про затвердження Порядку вжиття тимчасових надзвичайних заходів з подолання наслідків тривалого порушення нормальної роботи ринку електричної енергії». http://zakon5.rada.gov.ua/laws/show/372-2014-%D0%BF

91 Розпорядження Кабінету Міністрів України від 13 серпня 2014 р. N° 764-р «Про вжиття тимчасових надзвичайних заходів на ринку електричної енергії». – Режим доступу : https://zakon.rada.gov.ua/laws/show/764-2014-%D1%80#Text

92 Розпорядження Кабінету Міністрів України від 9 грудня 2015 р. N° 1296-р «Про вжиття тимчасових надзвичайних заходів на ринку електричної енергії». – Режим доступу : https://zakon.rada.gov.ua/laws/show/1296-2015-%D1%80#Text

93 Постанова Кабінету Міністрів України від 15 лютого 2017 р. N° 103-р «Про вжиття тимчасових надзвичайних заходів на ринку електричної енергії». – Режим доступу : https://www.kmu.gov.ua/npas/249745986

У якості заходів запобігання виникнення кризової ситуації Міненерговугілля [94] здійснювало розроблення варіантів роботи ОЕС України у разі припинення генерації на вугільних ТЕС та плану дій для стабілізації роботи енергосистеми за зазначених умов; уточнення режимів роботи енергосистеми України та вжиття заходів для розвантаження генеруючих потужностей у нічному діапазоні роботи; встановлення допустимого рівня зниження резерву енергогенеруючих потужностей не нижче 700 МВт; встановлення граничних величини (лімітів) споживання потужності та електроенергії та забезпечення щоденного контролю за їх дотриманням;[95] аналізу ефективності заходів зниження споживання електроенергії та потужності та їх удосконалення.

Антикризовий координаційний штаб Міненерговугілля[96] *(створений в рамках реалізації положень Закону України «Про боротьбу з тероризмом» та працював в режимі **«ad hoc»**)*, щотижнево аналізував ситуацію, що забезпечило стале проходження осінньо-зимового періоду, оперативне вирішення проблемних питань щодо перевезень вугілля, потреб в енергоресурсах, вчасних розрахунків компаній за поставлене вугілля, проведення ремонтних кампаній тощо.[97] Задача полягала у забезпечені необхідних поставок енергетичного вугілля для потреб електростанцій (передусім антрацитового вугілля з окупованих територій) та реалізації проектів з розвитку ОЕС України, що забезпечить мінімізацію витрат дефіцитного антрацитового вугілля.

> *Положення про антикризовий штаб, затверджене лише у 2020 році,98 визначало цей елемент екосистеми «врегулювання проблемних питань діяльності енергетичної галузі», як тимчасовим консультативно-дорадчим органом Кабінету Міністрів України, який має право отримувати інформацію та залучати до роботи органів державної влади, органів місцевого самоврядування, НКРЕКП (за згодою), інших колегіальних органів (за згодою), установ, організацій та суб'єктів господарювання, зокрема енергетичних компаній (за погодженням з їх керівниками), а також незалежних експертів (за згодою).*

Для координації дій було створено Робочу групу з оперативного реагування та подолання наслідків порушення роботи ринку електричної енергії.[99] Для недопущення віялових відключень Україна приймала випереджаючі організаційні рішення[100] таким чином, щоб максимально завантажити ті блоки, які працюють на нашому газовому вугіллі та збільшити частку електроенергії, виробленої атомною генерацією до 60-61 %.

У практичному вимірі заходи реагування «елементів екосистеми» зводилися до: зменшення споживання електричної енергії на території України; обмеження експорту електричної

---

94 Наказ Міністерства енергетики та вугільної промисловості України від 21.12.2015 N°828 «Про затвердження Плану тимчасових надзвичайних заходів на ринку електричної енергії». – Режим доступу : http://mpe.kmu.gov.ua/minugol/doccatalog/document?id=245075221

95 Визначено порядок поетапного застосування вимушеного різних графіків обмеження/відключення в залежності від рівня загроз стійкості енергосистеми.
Наказ Міністерства енергетики та вугільної промисловості України від 23.11.2006 N°456 «Про затвердження Інструкції про складання і застосування графіків обмеження та аварійного відключення споживачів, а також протиаварійних систем зниження електроспоживання». – Режим доступу : http://zakon2.rada.gov.ua/laws/show/z0151-07

96 Наказ Міненерговугілля від 28 липня 2015 року N°474 «Про утворення Антикризового штабу при Міненерговугілля України». http://document.ua/pro-utvorennja-antikrizovogo-shtabu-pri-minenergovugillja-uk-doc237327.html

97 У Міненерговугілля проаналізували роботу Об'єднаної енергосистеми України та визначили напрямки подальших дій щодо проходження ОЗП за умов надзвичайних заходів в енергетиці. http://mpe.kmu.gov.ua/minugol/control/uk/publish/article?art_id=245188583&cat_id=245070636
Завдяки надзвичайним заходам в енергетиці буде зменшено споживання антрациту на ТЕС України. http://mpe.kmu.gov.ua/minugol/control/uk/publish/article?art_id=245188562&cat_id=245070636

98 Постанова Кабінету Міністрів України від 24 квітня 2020 р. N° 312 «Про утворення Антикризового енергетичного штабу» https://www.kmu.gov.ua/npas/pro-utvorennya-antikrizovogo-energetichnogo-shtabu-i240420-312

99 Наказ Міністерства енергетики та вугільної промисловості України від 10.10.2014 N°712 «Про створення робочої групи Міненерговугілля з оперативного реагування та подолання наслідків порушення роботи ринку електричної енергії». http://195.78.68.67/minugol/doccatalog/document?id=244965782

100 Наше завдання - зробити все, щоб віялових відключень не було, - Міністр Ігор Насалик. http://mpe.kmu.gov.ua/minugol/control/uk/publish/article?art_id=245188621&cat_id=24507063

енергії; додаткового імпорту електричної енергії; припинення генерації на окремих генеруючих потужностях (зокрема, на антрацитових вугільних ТЕС); збільшення генерації на інших потужностях (АЕС); встановлення граничних величини (лімітів) споживання потужності та електроенергії, а також забезпечення щоденного контролю за їх дотриманням.

Виходячи з наявних запасів палива для електростанцій, стану електричних мереж та іншого енергетичного обладнання, Оператор системи передачі (ДП «НЕК «Укренерго») здійснював серед іншого: встановлення допустимого рівня зниження резерву енергогенеруючих потужностей; встановлення графіків (добових, тижневих тощо) та обсягів виробництва електричної енергії за окремими енергогенеруючими компаніями (енергоблоків); забезпечення дотримання встановлених лімітів потужності; застосування у разі виникнення потреби графіків погодинного вимкнення електроенергії та графіків її аварійного вимкнення; встановлення тимчасових обмежень щодо пропускної спроможності міждержавних електричних мереж України, а також обсягів міждержавного перетікання електричної енергії.

Слід зазначити, що активування графіків обмеження енергопостачання стало оперативним та ефективним засобом забезпечення операційної функціональності енергосистеми України, водночас і найбільш ризикованим з точки зору непрогнозованого впливу на функціонування іншої критичної інфраструктури країни та ризиковим точки зору збереження соціально-економічної стабільності у країні в особливий період. При цьому, рішення щодо застосування графіків обмежень та аварійних відключень (найважливішого елемента із «надзвичайних заходів на ринку електроенергії») оперативно приймається головним диспетчером ОЕС України (Оператора системи передачі) за узгодженням з Міненерговугілля України, з позиції необхідності виконання завдання - забезпечення операційної безпеки функціонування ОЕС України.

Загалом, зазначені дії допомогли забезпечити стабільність роботи ОЕС України та зменшити споживання антрациту (100 % якого видобувається на окупованій території) на ТЕС України, однак суттєво вплинули на економіку країни.

Аналіз засвідчує (Рис. 4), що ***система забезпечення операційної безпеки функціонування енергосистеми України, яка була покладена в основу дій елементів «екосистеми електропостачання» у 2014-2015 роках виконувала своє завдання збереження синхронного режиму роботи всіх складових системи електропостачання, за рахунок адміністративного впливу на суб'єктів ринку (типи працюючої генерації) на обмеження споживачів (населення).***

Іншими словами, у відповідь на загрози військового та економічного характеру у 2014-2017 роках, елементи «системи електропостачання» реагували в рамках свої «вузьких» задач, і не було окремого відповідального за стійкість цільової функції, а саме задоволення потреб споживачів у електроенергії відповідно до проектних, штатних «параметрів».

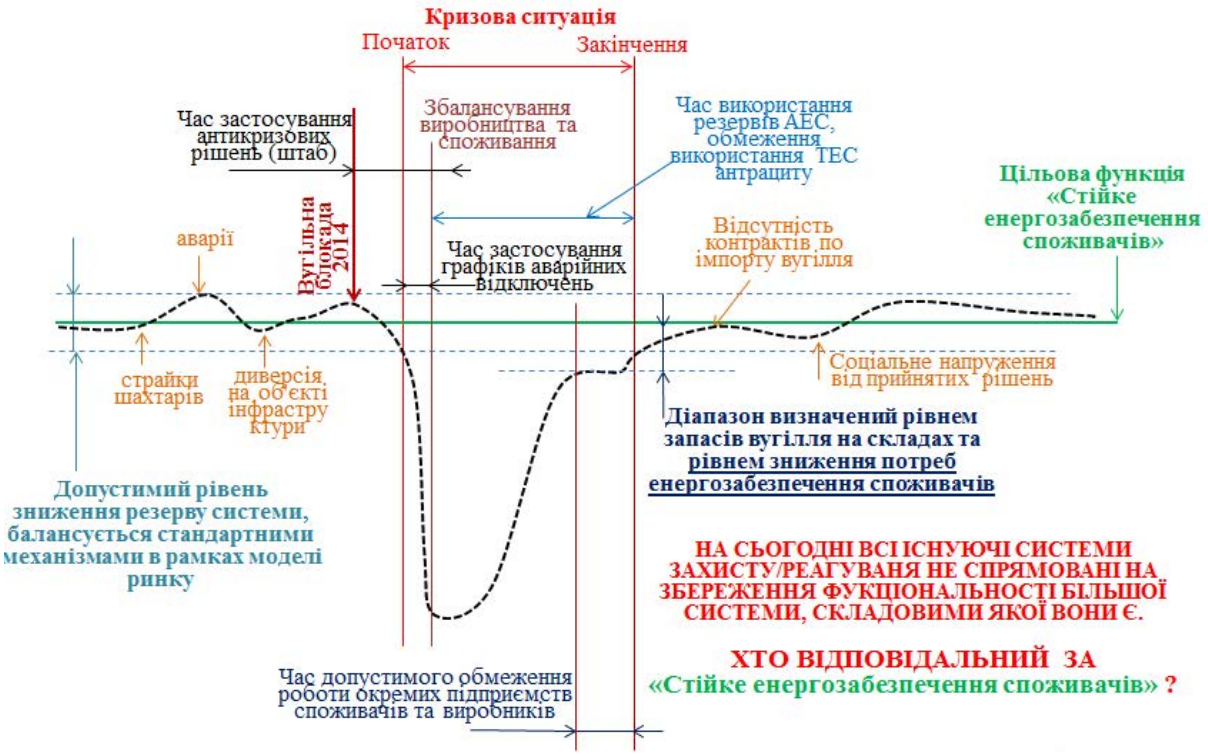


Рис. 4. Застосування моделі реагування системи для забезпечення *стійкості функції «забезпечення споживачів електричною енергією»*

До реагування на загрози порушення енергопостачання переважно залучаються лише Оператор системи передачі («Укренерго») та оператори системи розподілу (обленерго). Опосередковано, на етапі складання списків для застосування графіків обмеження та аварійного відключення споживачів (ГАВ) до заходів реагування залучаються найбільші споживачі (групи споживачів "Промисловість") електроенергії в регіонах (зонах відповідальності «обленерго»). Водночас інші категорії споживачів (середні та малі підприємства, домогосподарства, бюджетні установи) практично не беруть участь у розробці заходів запобігання та реагування на загрози порушення функції електропостачання.

Слід зазначити, що застосування графіків обмеження та аварійного відключення, як і процедура їх застосування є фактичним порушенням нормального режиму функціонування ринку електроенергії. Хоча модель ринкового регулювання передбачає механізми «управління попитом» та «допоміжні послуги», які можуть бути використані у якості «ринкового» механізму реагування, вони не застосовуються для запобігання виникнення кризових ситуацій.

Загалом, кризова ситуація 2014-2015 років, продемонструвала той факт, що системи запобігання виникнення кризової ситуації на ринку електроенергії, яка б не змушувала блокувати ринкові механізми не існувало на той час. Всі запровадженні заходи та відповідні рішення були здійснені адміністративними методами регулювання ринку. Аналізуючи ситуацію, що виникла на ринку електроенергії у 2020 році можна стверджувати, що такої системи в Україні не існує й досі.

Не створено також надійної системи інформування споживачів, передусім домогосподарств, щодо реагування на загрози, та систем обміну інформацією щодо дій у кризових ситуаціях. Дана функція покладається на місцеві органи влади, які не мають достатніх можливостей це забезпечити.

Не є достатнім, з точки зору централізованого планування (на рівні ОЕС України чи розподільчих систем), рівень підготовки заходів запобігання кризи «енергозабезпечення

кінцевих споживачів», зокрема заходів «заміщення» джерел та видів енергопостачання (резервні потужності та маршрути, альтернативне палива тощо).

Окрім того, спостерігається також спрощення трактування завдань щодо забезпечення стійкості функції *«забезпечення споживачів електричною енергією»*. Дана функція, яку слід розглядати у якості складової забезпечення національної стійкості, підміняється завданням щодо забезпечення операційної безпеки ОЕС України, а саме забезпечити її надійне функціонування з нормативними показниками якості послуг з розподілу та постачання електричної енергії. Відтак завдання щодо розроблення заходів реагування на загрози функціонування ОЕС та їх імплементацію покладається на Оператора система передачі (Укренерго), який обмежений у своїх повноваженнях. При цьому, специфіка впливів загроз різного типу (фізичні, кібер-, економічні, природні тощо) не враховується, а всі дії зводяться виключно до «організаційно-технічних» корегувальних впливів щодо дотримання балансу виробництва та споживання електроенергії в системі.

Таким чином, даний аналіз свідчить про необхідність удосконалення існуючих підходів до забезпечення «стійкості електрозабезпечення». Розвиваючи стійкість необхідно передбачити узгоджену систему дій, відповідальності та повноважень елементів екосистеми (органів влади, суб'єктів ринку тощо) з метою:

- забезпечення «безперервності» виконання системою цільових функцій/послуг (зокрема функції «електрозабезпечення споживачів»), що може виходити за межі відповідальності окремих елементів, на різних етапах циклу кризового реагування;
- формування єдиних процедур реагування на загрози різних типів, що у свою чергу потребуватимуть залучення різних елементів екосистеми

Створення узгоджених та єдиних для всіх суб'єктів реагування процедур, на загальнодержавному рівні[101] покликана виконати державна система захисту критичної інфраструктури.[102] У свою чергу, система забезпечення захисту критичної інфраструктури стане основою побудови системи національної стійкості.[103] Відповідні положення щодо уніфікації процедур кризового реагування передбачені у проекті Закону України «Про критичну інфраструктуру та її захист», винесеного на розгляд Верховної Ради України.[104]

3.2 ПОРІВНЯННЯ ЕКОСИСТЕМ ЗАХИСТУ ЕЛЕКТРОЗАБЕЗПЕЧЕННЯ США ТА УКРАЇНИ

В Україні відсутнє **єдине відомство**, яке відповідальне на захист критичної інфраструктури, що виконує аналіз загроз, ризик менеджмент впливу різних типів загроз, оцінку потреб/вразливих сторін стейкхолдерів, затвердження безпекових стандартів для учасників сектору.

В Україні функції забезпечення стійкого постачання електроенергії покладені на Міненерго, яке відповідальне за стратегічний розвиток галузі.

Оскільки перелічені вище функції відсутні у українських державних органів, тому можна сказати, що в Україні відсутня загальнонаціональна система **попередження (prevention)**

---

101 Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України / за ред. О. М. Суходолі. К. : НІСД, 2019. – с. 224.

102 Рішення РНБО України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури». https://www.rnbo.gov.ua/ua/Ukazy/435.html
Постанова КМУ «Про схвалення Концепція створення державної системи захисту критичної інфраструктури». https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text

103 У Києві за підтримки США почалися семінари з розбудови системи національної стійкості за принципами НАТО. https://www.kmu.gov.ua/news/u-kiyevi-za-pidtrimki-ssha-pochalisya-seminari-z-rozbudovi-sistemi-nacionalnoyi-stijkosti-za-principami-nato

104 Проект Закону про критичну інфраструктуру та її захист. http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=71442

загроз критичній інфраструктурі та у сфері електроенергії зокрема.

У існуючих державних органах, що частково своїми функціями відповідають та безпеку критичної інфраструктури та забезпечення надійного електропостачання відсутні конкретні профільні департаменти стосовно реагування, відновлення та вивчення уроків від загроз. В Україні лише у РНБО існує Служба захисту критичної інфраструктури, проте цей орган не є органом виконавчої влади, тому не може повноцінно здійснювати державну політику стосовно захисту критичної інфраструктури. Така ситуація спричинена відсутністю законодавчої основи, національних програм та стратегічних документів стосовно захисту критичної інфраструктури.

Важливим елементом на етапі попередження загроз є створення уніфікованих стандартів безпеки для учасників ринку. Досвід США говорить про важливість імплементації «стандартів надійності», що стосуються кібербезпеки та фізичної безпеки, які обов'язкові для впровадження В Україні уніфіковані стандарти безпеки існують на рівні НЕК «Укренерго» (стандарти операційної безпеки функціонування ОЕС України), проте на рівні регіональних операторів таких зобов'язань впроваджувати уніфіковані протоколи кібербезпеки немає.

Хоча в Україні нещодавно і запроваджено вимогу для Оператора СП розробити План забезпечення безпеки для захисту критичної інфраструктури, не врегульовано питання щодо можливостей забезпечення постачання електроенергії кінцевим споживачам у кризових ситуаціях, коли оператори в рамках реагування на надзвичайну ситуацію, з метою забезпечення операційної безпеки електромереж отримують право відключати споживачів від електропостачання.

В Україні відсутнє поняття Організації з надійності електричної енергії (ERO) та «стандартів надійності». У США визначення такої організації та затвердження стандартів надійності покладене на енергетичного регулятора, в той час як в Україні у НКРЕКП таких функцій немає. Окрім цього, ERO разом зі специфічними аналітичними центрами та порталами обміну інформації проводять загальнодержавні навчання на випадок фізичних або кіберзагроз у енергетичному секторі.

У разі виникнення ризиків стійкості енергетичної системи України **(етап Preparedness, Response)** функції попередження та реагування на загрози покладено на Кабінет Міністрів України, у якого існують повноваження запроваджувати «надзвичайні заходи» щодо електроенергетичної галузі. Надзвичайні заходи впроваджуються за подання Міненерго або НКРЕКП.

Критеріями запровадження заходів визначено:

1) пошкодження електроенергетичних установок та/або незаконне втручання третіх осіб, що можуть призвести до обмеження споживання електричної енергії більш як на 100 МВт;

2) зниження резерву енергогенеруючих потужностей ОЕС України нижче допустимого рівня протягом трьох діб;

3) критичний стан забезпечення паливом, зокрема зниження запасів палива на окремих теплових електростанціях енергогенеруючих компаній нижче 20-денного запасу;

4) відсутність протягом трьох місяців підряд повної оплати електричної енергії, або якщо оплата у розрахунковому місяці нижче 90 відсотків.

Тимчасові надзвичайні заходи можуть вживатися на період, що не перевищує один місяць. При цьому, на період застосування тимчасових надзвичайних заходів суб'єкти електроенергетики незалежно від форми власності зобов'язані діяти відповідно до стандартів операційної безпеки функціонування ОЕС України та оперативних команд і розпоряджень Оператор системи передачі "НЕК "Укренерго". Вимоги щодо забезпечення без-

пеки об'єктів електроенергетики у надзвичайній ситуації є обов'язковими для виконання всіма суб'єктами ринку електричної енергії незалежно від форми власності.

Запровадження надзвичайних заходів в Україні відбувалося протягом 2014-2017 років як засіб реагування на аварійні ситуації, спричинені військовими діями та агресією РФ.

Схожа систему реагування має і США, де президент запроваджує надзвичайний стан, а секретар DOE отримує повноваження видавати надзвичайні накази. Проте система реагування на загрози на етапах попередження та реагування є набагато грунтовнішою і базується не лише на показниках збереження системи, а орієнтується також на інші сфери та приватний сектор.

Також в Україні існує Антикризовий енергетичний штаб під головуванням прем'єр-міністра, куди входять представники уряду (входять обов'язково, наступні учасники – за згодою), регулятора, найбільших енергетичних підприємств.

Завданнями штабу є:

Антикризовий енергетичний штаб відповідно до покладених на нього завдань:

1) проводить аналіз стану справ в енергетичній галузі;
2) вивчає результати діяльності центральних і місцевих органів виконавчої влади, органів місцевого самоврядування, підприємств, установ та організацій з питань, що належать до його компетенції;
3) опрацьовує шляхи та механізми щодо врегулювання питань в енергетичній галузі;
4) бере участь у розробленні проектів нормативно-правових актів з питань, що належать до його компетенції, та в разі потреби подає відповідні пропозиції;
5) подає Кабінетові Міністрів України розроблені за результатами своєї роботи рекомендації та пропозиції з питань, що належать до його компетенції.

Звідси можна зробити висновок, що в Україні відсутні урядові та міжурядові органи, що спеціалізуються на захисті критичної інфраструктури та у сфері електроенергії, зокрема.

В Україні існує серйозна проблема крос-секторальної комунікації та у самому енергетичному секторі. У США існує ряд державних (EGSCC) та приватних (ESCC) органів, які координують між собою зусилля для попередження, реагування та відновлення від загроз.

У США існує специфічний досвід створення інформаційних аналітичних центрів та порталів, що координують співпрацю державних та приватних органів та операторів інфраструктури. Такі аналітичні портали виконують функції інформування стосовно потенційних загроз, проводять case study інцидентів та надають рекомендації для державних органів та приватних компаній.

У профільних міністерств США (DOE, DHS) існує розгалужена система місцевого представництва або ж налагоджена співпраця з місцевими органами влади, які відповідальні за координацію та обмін інформації на місцевому рівні у випадку загроз електроенергетичній інфраструктурі.

Місцеві органи влади у США регулюють свій процес реагування на кризові явища в енергетиці через Energy Assurance Plans. Ці документи передбачають аналіз можливих загроз енергетичному сектору штату, інструкції взаємодії місцевих посадовців на випадок кризи та комунікаційні настанови.

3.3 ПРОПОЗИЦІЇ ДО ПІДХОДУ РЕАГУВАННЯ НА КРИЗУ УЧАСНИКАМИ ЕНЕРГЕТИЧНОЇ СИСТЕМИ УКРАЇНИ

МОЖЛИВІ ЗАГРОЗИ ЕНЕРГЕТИЧНІ СИСТЕМІ УКРАЇНИ

Аналізуючи можливі загрози енергетичній системі України, ми виокремили дві основні групи загроз: кіберзагрози та фізичні загрози.

Можливі **кіберзагрози** включають в себе три основні групи:

1. Атаки на IT системи об'єктів енергетичної системи.

Атаки на інформаційні системи об'єктів енергетичної системи, що можуть блокувати роботу персоналу, комерційні процеси на ринку

2. Атаки на OT системи об'єктів енергетичної системи.

Кібератаки, що блокують або виводять з ладу операційні системи об'єктів енергетичної системи.

3. Інформаційні атаки.

Може виражатися у розповсюдженні дезінформації, яка тягне за собою можливі збої у роботі інформаційних, операційних систем.

Фізичні загрози

1. Порушення функціонування об'єктів енергетичної системи

- Порушення функціонування може виражатися через фізичний вплив на системи управління та системи комунікації об'єктів енергетичної системи
- Відключення від електропостачання/живлення окремих об'єктів електроенергетики
- Умисне перевантаження окремого елемента енергетичної системи

2. Руйнування об'єктів енергетичної системи

- Вибухи та диверсії на об'єктах енергетичної системи
- Крадіжки частин інфраструктури

3. Блокування роботи окремих об'єктів енергетичної системи

- Блокування постачання ресурсів для енергетичних об'єктів
- Недопущення персоналу до об'єктів
- Диверсії, спрямовані на блокування роботи спеціального обладнання, блокування постачання спеціалізованого обладнання

Об'єкти, на які можуть здійснюватися атаки:

- Оператори систем розподілу
- Оператори системи передачі
- Електрогенеруючі підприємства
- Великі промислові споживачі
- Системи зберігання енергії (storages)
- Об'єкти транспортної інфраструктури (залізниця, морські порти)
- Персонал компаній
- Ресурси
- Міждержавні енергетичні мережі

Підхід до реагування на кризу учасниками енергетичного сектору України

Ми пропонуємо підхід до реагування на кризи в енергетичній системі на прикладі потенційного фізичного пошкодження системи електропередачі ОЕС України, що призвело до пошкодження ліній електропостачання та знеструмлення декількох областей більше, ніж на 50%.

Таблиця 4. Розподіл функцій учасників енергетичної системи України у разі настання кризової ситуації

Учасник	Режим нормального функціонування	Реагування	Відновлення	Вивчення уроків
Оператор системи передачі	Забезпечує стабільну роботу ОЕС України. Розробляє та затверджує внутрішні протоколи реагування на кризові явища. Надає рекомендації для Міненерго стосовно процедури реагування на кризові явища Розробляє стандарти операційної безпеки оператора. Впроваджує стандарти безпеки, розроблені Регулятором та Міненерго	Оператор реагує на інцидент, забезпечує електропостачання у залежності від своїх можливостей та пошкодженої інфраструктури. Оператор системи передачі інформує міністра енергетики про настання кризового явища, за потреби інформує ДСНС. Застосовує внутрішні розроблені протоколи реагування. Забезпечує енергопостачанням життєво важливі функції. Бере участь у Антикризовому енергетичному штабі.	У координації з Міненерго та Антикризовим штабом розробляє та втілює план відновлення електропостачання	За потреби оновлює внутрішні протоколи реагування. Надає рекомендації для Міненерго стосовно покращення процедури реагування на кризові явища

Міненерго	Розробляє план енергетичної стійкості (за прикладом США - Energy Specific Plan) Розробляє та затверджує процедури комунікації між органами влади, енергетичними підприємствами, іншими можливими учасниками (стандарти безпеки, пропозиції див Додаток 1). Проводить аналіз/ моніторинг ресурсів, спроможностей учасників енергетичної сфери, ризик менеджмент. Встановлює вимоги до учасників енергетичної системи стосовно реагування на кризові явища. Розробляє та проводить програми навчань для учасників енергетичної системи. Координує роботу органів міжсекторального та приватно-державного партнерства	У разі можливого настання загрози енергосистемі, скликає штаб кризового реагування при Міненерго. Інформує Кабмін. Координує роботу відомств та учасників ринку стосовно реагування на загрозу. Бере участь у Антикризовому енергетичному штабі Кабміну. Впроваджує плани реагування на кризову ситуацію.	За потреби залучає державні/недержавні ресурси та інструменти для відновлення нормального режиму електропостачання	Проводить розслідування інцидентів, аналіз уроків. Оновлення плану енергетичної стійкості, впровадження нових стандартів.

Кабмін	Затверджує план енергетичної стійкості, встановлює вимоги до регіональних антикризових планів.	Розпочинає роботу Антикризового енергетичного штабу Координує роботу відомств уряду	В рамках Антикризового енергетичного штабу розробляють план відновлення пошкодженої інфраструктури та забезпечує необхідними ресурсами.	Затверджує оновлений план енергетичної стійкості (за прикладом США - Energy Specific Plan) Оновлення регламентів роботи Антикризового енергетичного штабу
Регулятор	Розробляє стандарти енергетичної стійкості у координації з Міненерго (пропозиції стосовно стандартів див. Додаток 1) Контролює дотримання учасниками енергетичного сектору стандартів енергетичної стійкості Разом з Міненерго розробляє програми навчань, що включають в себе сценарії фізичних та кібер атак на енергетичну інфраструктуру	Бере участь у Антикризовому енергетичному штабі Кабміну.	Бере участь у Антикризовому енергетичному штабі Кабміну.	Розробляє оновлення стандартів енергетичної стійкості Контролює дотримання учасниками енергетичного сектору стандартів енергетичної стійкості
Регіональні системи розподілу	Розробляють антикризовий план забезпечення мінімального рівня електропостачання для свого регіону	Забезпечують мінімальний рівень постачання електроенергії	За потреби, беруть участь у відновленні об’єктів пошкодженої інфраструктури (персонал, ресурси)	Надають рекомендації до регіонального плану реагування (Energy Assurance Plan)

Регіональна влада (ОДА, місцеві адміністрації	Розробляють регіональний антикризовий план (Energy Assurance Plan): • Покрокові інструкції для персоналу • Комунікаційні інструкції • План забезпечення автономного електропостачання на випадок кризи Розробити план забезпечення ресурсів на випадок збоїв у системі електропостачання	Комунікація з населенням стосовно кризової ситуації, надання інструкцій Впровадження антикризового плану (Energy Assurance Plan)	Комунікація з Антикризовим енергетичним штабом, виконання вказівок Комунікація з населенням стосовно вирішення проблеми, надання інструкцій	Надання рекомендацій стосовно оновлення стратегічних документів (регіональний план реагування (Energy Assurance Plan))
Великі підприємства споживачі	Великі підприємства споживачі електроенергії розробляють плани та формують базу ресурсів для автономного забезпечення електроенергії. Впроваджують стандарти стосовно енергетичної стійкості, розроблені Міненерго. Забезпечують безпеку персоналу	Забезпечують власні потреби в енергопостачанні За потреби забезпечують безпечну зупинку виробництва За потреби надають допомогу у ліквідації кризової ситуації (персонал/ресурси), підтримці населення	Запускають процес відновлення енергопостачання власних потреб. За потреби надають допомогу місцевій владі (персонал/ресурси), населенню	Оновлюють власні протоколи реагування
Споживачі	Формують певні запаси ресурсів для забезпечення себе енергоресурсами на випадок кризи	Зменшення споживання	Зменшення споживання	

Міжсекторальна координаційна група

З досвіду США важливим елементом системи попередження та реагування на кризові явища є міжсекторальна координація та державно-приватне партнерство, задля реалізації якого існує ряд координаційних органів. Українська ж система попередження та реагування на кризові явища не включає в себе розвиток такого партнерства.

Звідси варто зосередити увагу над створенням постійних координаційних груп, куди будуть входити органи влади різних рівнів та приватного сектору. Залучення приватного сектору повинно відбуватися виключно на добровільній основі та мати рекомендаційний характер.

Рис. 5. Структура координаційних груп при Міненерго

Пропонується два рівні координаційних груп. Міжсекторальна координаційна група очолюється заступником міністра енергетики та включає представників уряду та спеціалізованих відомств. Функціями органу є забезпечення комунікації між органами влади стосовно розвитку системи захисту критичної інфраструктури, напрацювання рекомендацій до стратегічних документів, участь у Антикризовому енергетичному штабі при Кабміні.

Якщо Антикризовий енергетичний штаб при Кабміні стосується власне реагування на кризові явища і є тимчасовою, то Міжсекторальна координаційна група діє постійно та спрямована розвиток систем передбачення та запобігання загрозам.

Членами Міжсекторальної координаційної групи можуть стати:

- Регулятор;
- Міністерство транспорту та інфраструктури;
- Служба безпеки України;
- Міністерство внутрішніх справ;
- Державна служба спеціального зв'язку та захисту інформації України;
- Місцеві органи влади (ОДА)

У складі Міжсекторальної координаційної групи існують дві підгрупи, що стосуються електроенергії та нафти і газу.

Функції підгруп:

- Комунікація між учасниками сектору стосовно розвитку системи захисту критичної інфраструктури, обмін досвідом;
- Напрацювання рекомендацій до стратегічних документів, що стосуються захисту критичної інфраструктури та енергетичної стійкості;
- Вироблення спільних позицій щодо забезпечення безпеки і стійкості секторів.

Члени підсектору елетроенергетики:

- представники підприємств генерації;
- оператор системи передачі;
- оператори систем розподілу;
- найбільші постачальники елетроенергії

Члени підсектору нафти і газу:

- АТ «НАК «Нафтогаз»
- Оператор газотранспортної системи;
- Оператор газосховищ;
- Найбільші видобувні підприємства;
- Розподільні компанії (облгази);
- Найбільші постачальники газу.

Запропонований підхід до формування енергетичної стійкості та реагування на кризові явища передбачає покладення основних функцій захисту критичної інфраструктури та безпеки постачань на профільне міністерство. Роль Міненерго полягає у формуванні стратегічних документів стосовно енергетичної стійкості та їхнього впровадження.

Важливим елементом запропонованого підходу також є формування міжсекторальної комунікації між органами влади та приватним сектором. Роль Міненерго полягає у формуванні діалогу з приватним сектором через Міжсекторальну координаційну групу, та дві підгрупи.

Задля формування надійної системи реагування на кризові явища в енергетиці важливу роль повинні виконувати місцеві органи влади, які розробляючи чіткі покрокові регіональні плани реагування на загрози зможуть краще залучити місцеві ресурси до реагування.

РЕКОМЕНДАЦІЇ

Для формування надійної системи енергетичної стійкості України у частині вирішення комунікаційних прогалин (communication gaps) важливо:

1. **Зосередитися над формуванням комунікаційних стандартів та підходів** у спілкуванні з акторами поза функціональними межами енергосистеми, що пришвидшить процес реагування на кризу та дозволить мінімізувати наслідки. Процес комунікації між державними органами влади та учасниками сектору є чи не вирішальним у попередженні та зменшенні наслідків криз.
2. Необхідно змінити законодавство для **встановлення законодавчих вимог стосовно комунікаційних стандартів та стандартів звітування** щодо інцидентів.

Для формування надійної системи енергетичної стійкості у частині вирішення прогалин у компетенціях та спроможності української системи попередження та реагування на кризи важливо:

1. Визначити відповідальний орган за формування енергетичної стійкості, а саме Міненерго. Під час своєї діяльності Міненерго повинно виконувати наступні функції:
   - аналіз загроз (фізичних і кібер) та слабких сторін енергетичної системи країни;
   - ризик менеджмент впливу різних типів загроз на енергетичний сектор (ідентифіковані ризики);
   - оцінка потреб/вразливих сторін стейкхолдерів;
   - моніторинг, аналіз та превентивні дії стосовно можливих загроз;
   - розробка та затвердження стандартів енергетичної стійкості (разом з Регулятором).
2. Для формування стратегічних напрямів енергетичної стійкості Міненерго важливо розробити **стратегічні документи**, які окреслюватимуть основних стейкхолдерів, загрози, підходи до попередження і реагування на загрози та методи комунікації. План енергетичної стійкості України може виступати таким документом загальнодержавного рівня.
3. Для місцевих органів влади (в першу чергу обласні державні адміністрації) важливо розробити **регіональні плани енергозабезпечення споживачів на випадок кризи**, які включатимуть в себе відповідну координацію залучення суб'єктів реагування на регіональному рівні та покрокові інструкції для посадовців та комунікаційні настанови.
4. Оператору СП необхідно затвердити передбачений чинним законодавством План забезпечення безпеки для захисту критичної інфраструктури з врахуванням загроз різного типу;
5. У формуванні підходу до формування енергетичної стійкості важливо окреслити основними стейкхолдерами всіх можливих акторів сектору (постачальників ресурсів, виробників енергії, транспортування, розподіл, споживачі). Задля розширення кола зацікавлених осіб уряду важливо налагодити міжсекторальну співпрацю, яка може виражатися через **створення міжсекторальних та галузевих груп** при Міненерго. Залучення приватного сектору до формування підходів до енергетичної стійкості лише посилить українську енергетичну систему.
6. Міненерго разом з НКРЕКП важливо розробити систему **стандартів безпеки**, які по-

винні впроваджуватися на українських енергетичних підприємствах. Стандарти безпеки повинні включати в себе:

- фреймворки для внутрішньої оцінки загроз і потреб учасників сектору;
- формування операційних планів на випадок реалізації загроз будь-якого типу відповідно до етапів циклу кризового реагування;
- систему внутрішнього навчання персоналу;
- стандарти фізичної безпеки та кібербезпеки критичної енергетичної інфраструктури;
- стандарти звітування стосовно інцидентів;

7. Необхідно змінити законодавство для встановлення законодавчих вимог щодо безпеки функціонування енергетичної інфраструктури та дотриманням вимог суб'єктами усіх форм власності та визначення джерел фінансування суб'єктами виконання встановлених вимог.

Додаток 1. Рекомендації стосовно протоколів енергетичної стійкості (на прикладі сфери електроенергетики)

Напрямок	Учасник	Суть діяльності	Час/ періодичність	Ресурси	Нотатки
Плануван-ня ризиків, протоколів фізичного захисту	Оператори систем розпо-ділу, опера-тор системи передачі	Проводить оцінку ризиків раз в 30-60 місяців, пові-домляє про це регіональ-ного оператора з доказа-ми проведеної оцінки	Один раз в 30-60 місяців	Власними ре-сурсами	Контроль за виконанням здійснює регулятор або регіональні представ-ництва. Фреймворк для оцінки ризиків та плану фізичного захисту складає та надає регулятор
	Оператори систем розпо-ділу, опера-тор системи передачі	Залучає третю незалежну сторону до оцінки ризи-ків, яка надає обов'язкові рекомендації в управлінні ризиками	Один раз в 30-60 місяців	Залучення третьої сторо-ни, власними ресурсами	
	Оператори систем розпо-ділу, опера-тор системи передачі	Складає physical security plan	120 календар-них днів з мо-менту оцінки	Власними ре-сурсами	Physical security plan включає в себе: 1. Заходи щодо стійкості або безпеки, розроблені спільно для стримування, виявлення, затримки, оцінки, реагу-вання на потенційні фізичні загрози та вразливості, виявлені під час оцінки 2. Контактна та координаційна інформа-ція правоохоронних органів 3. Графік виконання модернізацій зазначених у плані фізичної безпеки 4. Положення щодо оцінки постійних фізичних загроз та відповідні заходи безпеки

Напрямок	Учасник	Суть діяльності	Час/ періодичність	Ресурси	Нотатки
	Оператор систем розподілу	Кожний оператор систем розподілу складає restoration plan, затверджує його з регулятором		Власними ресурсами, затверджується регулятором	Стратегії з відновлення включають в себе: 1. Покроковий опис відновлення системи, пріоритети відновлення. 2. Процедури відновлення роботи з іншими операторами. 3. Опис та ідентифікація ресурсів, з яких буде відновлено систему (Black start) 4. Інші технічні особливості
	Оператор систем розподілу, оператор системи передачі	Кожна сторона повинна мати детальний операційний план як вона буде здійснювати свої функціональні обов'язки після втрати функціональності його основного центру управління		Власними ресурсами, затверджується регулятором	Операційний план повинен мати наступні характеристики: Можливості обміну даними. Міжособистісні комунікації. Джерело (и) живлення. Фізична та кібербезпека
	Генерація, оператори системи розподілу, оператор системи передачі, Міненерго, місцеві органи влади (ОДА)	Кожна посадова особа оператора системи розподілу/передачі повинна мати можливості міжособистісного спілкування з оператором системи передачі/розподілу, місцевими органами влади. Як мінімум раз в місяць відбувається перевірка каналів зв'язку.	live	Укренерго, Міністерство, Регулятор.	Повинен існувати затверджений Міненерго порядок комунікації всього ланцюжка електропостачання на випадок надзвичайної ситуації

Напрямок	Учасник	Суть діяльності	Час/ періодичність	Ресурси	Нотатки
	Генерація, оператори системи розподілу, оператор системи передачі, Міненерго, місцеві органи влади (ОДА)	Кожна сторона розробляє протоколи реагування на інциденти.	live	Власними ресурсами	Регулятор подає приклади реагування на інциденти та встановлює чіткі правила та форми звітності.
Комунікація	Генерація, оператори системи розподілу, оператор системи передачі, Міненерго, місцеві органи влади (ОДА)	Кожний залучений орган повинен мати внутрішні протоколи комунікації для своїх працівників з чіткими інструкціями, проводити тренування	перегляд один раз в 12 місяців	Власними ресурсами	Контроль за виконанням здійснює регулятор або регіональні представництва.

Напрямок	Учасник	Суть діяльності	Час/ періодичність	Ресурси	Нотатки
	Генерація, оператори системи розподілу, оператор системи передачі, Міненерго, місцеві органи влади (ОДА)	Кожна залучена сторона має мати власні протоколи кібербезпеки	Кожні 15 місяців	Власними ресурсами	Протоколи кібербезпеки включають в себе такі складові: Кадри та навчання; Фізична безпека кіберсистем; Управління безпекою системи; Повідомлення про аварії та плануання реагування; Плани відновлення власних кіберсистем; Оцінка вразливості Захист інформації; Повідомлення та реагування на надзвичайні обставини. Фреймворк надає регулятор
	Генерація, оператори системи розподілу, оператор системи передачі, Міненерго, місцеві органи влади (ОДА)	Кожна залучена сторона має мати власні кіберсистеми, з можливими точками доступу до системи без авторизованого входу, яка знаходиться в обмеженому доступі	live	Власними ресурсами	

Напрямок	Учасник	Суть діяльності	Час/ періодичність	Ресурси	Нотатки
Кібер	Генерація, оператори системи розподілу, оператор системи передачі, Міненерго, місцеві органи влади (ОДА)	Кожна сторона повинна мати плани/системи відновлення даних	тестувати мінімум раз в 15 місяців	Власними ресурсами	
	Генерація, оператори системи розподілу, оператор системи передачі, Міненерго, місцеві органи влади (ОДА)	Здійснювати контроль за операційними системами обладнання/підібрати набір програмного забезпечення	live	Власними ресурсами	Контроль повинен включати: Операційні системи (включаючи версію) або мікропрограму, де не існує незалежної операційної системи; Будь-яке комерційне або прикладне програмне забезпечення з відкритим кодом (включаючи версію); Будь-яке спеціальне програмне забезпечення; Будь-які логічні мережеві порти Будь-які ПЗ безпеки

Напрямок	Учасник	Суть діяльності	Час/ періодичність	Ресурси	Нотатки
	Генерація, оператори системи розподілу, оператор системи передачі, Міненерго, місцеві органи влади (ОДА)	Процедури для захисту та надійної обробки інформації про кіберсистему, включаючи зберігання, транзит, і використання.	live	Власними ресурсами	
	Генерація, оператори системи розподілу, оператор системи передачі, Міненерго, місцеві органи влади (ОДА)	Кожна відповідальна організація повинна розробити один або кілька задокументованих планів управління ризиками кібербезпеки в ланцюжку поставок	переглядати раз в 15 місяців	Власними ресурсами	

Додаток 2. Приклад фреймворку для оцінки стабільності енергетичного сектору у випадку фізичних загроз

Прийняття рішень	Стратегічний аспект	Проведений аналіз військових загроз та слабких сторін енергетичної системи країни	РНБОУ, Міноборони (у т.ч. в рамках оборонного огляду), СБУ, Міненерго, оператори мереж Має бути частиною Національного плану захисту (National Energy Specific Plan)
		Визначені та розроблені варіанти впливу різних типів військових загроз на енергетичний сектор (ідентифіковані ризики), визначений процес оновлення таких ризиків	РНБОУ, Міноборони, СБУ, Міненерго, оператори мереж Має бути частиною Національного плану захисту (National Energy Specific Plan)
		Проведена оцінка потреб стейкхолдерів та можливих ризиків під час військових загроз (економіка та суспільство, інфраструктурні оператори). Під час розробки стратегічних документів відбувається залучення інших стейкхолдерів	РНБОУ, Міноборони, СБУ, Міненерго, оператори мереж, інших об'єктів критичної енергетичної інфраструктури Має бути частиною Національного плану захисту (National Energy Specific Plan)
		Визначені та класифіковані об'єкти критичної енергетичної інфраструктури	РНБОУ, Міноборони, Міненерго, Мінекономіки, оператори мереж, інших об'єктів критичної енергетичної інфраструктури Має бути частиною Національного плану захисту (National Energy Specific Plan), основа для Національного плану захисту інфраструктури (National Infrastructure Protection Plan)
		Визначений порядок фізичного захисту об'єктів критичної інфраструктури	РНБОУ, Міноборони, СБУ, НГУ, Міненерго, оператори мереж, інших об'єктів критичної інфраструктури частина Національного плану захисту інфраструктури (National Infrastructure Protection Plan)

		Визначений механізм моніторингу прогресу (наприклад, в частині навчання, досліджень) і частоти перегляду документів.	NESP, NIPP
	Операційні питання та комунікація між інституціями	Існують крос-секторальні координаційні органи, що відповідають за безпеку та стабільність енергетичної системи. Хто відповідальний за міжвідомчу комунікацію та реагування.	Координаційний орган в рамках КМУ із залученням РНБОУ (подивитись на нинішні штаби реагування під час надзвичайного стану, кризові енергетичні штаби) Пропозиція відповідального - Міненерго (відповідно до положення про міністерство)
		В програмах реагування на можливі військові загрози охоплені три етапи - попередження (запобігання), реагування та відновлення.	Усі три елементи мають бути присутні у всіх планах (NESP, NIPP)
		В рамках крос-секторальних координаційних органів розроблені програми та проводяться навчання (тренування, симуляції) дій в рамках потенційних кризових ситуацій.	Мають бути присутні у всіх планах (NESP, NIPP)
		Існують ефективні канали обміну інформації між стейкхолдерами (уряд, економіка та суспільство, інфраструктура). Комунікація між стейкхолдерами в енергетичному секторі у випадку військових загроз виписана окремо.	Частина положення про координаційний орган. Має бути присутня у всіх планах (NESP, NIPP)
		Визначені економічні механізми попередження наслідків військових загроз (фінансові компенсації, введення спеціальних економічних режимів, умов, страхування ризиків).	Мають бути присутні у всіх планах (NESP, NIPP)

	Місцевий рівень	Існують програми розвитку енергетики на регіональному рівні/програми захисту критичної інфраструктури.	Місцеві адміністрації, місцеві оператори мереж, місцеві органи влади (Local Energy Specific Plan). Як залучати військових на місцевому рівні?
		Об'єкти критичної інфраструктури та ризики впливу військових загроз на енергетику на місцевому рівні чітко ідентифіковані	Місцеві адміністрації, місцеві оператори мереж, місцеві органи влади (Local Energy Specific Plan). Як залучати військових на місцевому рівні?
		Органи виконавчої влади на місцях мають відпрацьовані механізми реагування на загрози критичної інфраструктури, програми безперебійного диверсифікованого постачання енергії. Місцеві органи влади мають достатній рівень ресурсів для ліквідації наслідків.	Міноборони (у т.ч. підрозділи територіальної оборони), місцеві адміністрації, спільно з місцевими органами влади (кошти у випадку надзвичайного стану будуть іти через адміністрації, але місцеві органи мають кращу інфраструктуру).
		Органи місцевої влади залучені до національного рівня розробки стратегій реагування на наслідки загроз у енергетичному секторі.	РНБОУ, Міноборони (у т.ч. в рамках оборонного огляду), СБУ, Міненерго, оператори мереж. Для постійної комунікації - Координаційний орган. Мають бути залучені до розробки NESP, NIPP
Економіка та суспільство	Компанії, що працюють в енергетичному секторі	Чи існують внутрішні протоколи безпеки компаній	Оператори мереж, інших об'єктів критичної інфраструктури (НПЗ, склади/бази/сховища, електростанції та ін.)
		Існує співпраця компаній, що відносяться до об'єктів критичної інфраструктури, з урядом та іншими стейкхолдерами	Міненерго, СБУ, оператори мереж, інших об'єктів критичної інфраструктури
		Чи існують механізми співпраці між компаніями та урядом стосовно попередження та зменшення наслідків військових загроз	Міненерго, СБУ, оператори мереж, інших об'єктів критичної інфраструктури

	Промислові та побутові споживачі	Проводиться навчання та роз'яснення для побутових споживачів можливих наслідків військових загроз. Бізнес розробляє власні механізми реагування на військові загроз (плани захисту працівників, диверсифікація джерел постачання енергії). Існують програми залучення бізнесу, експертів та побутових споживачів до швидшої ліквідації наслідків (волонтерство, меморандуми про співпрацю).	Місцеві адміністрації, спільно з місцевими органами влади, суб'єкти господарювання та їх об'єднання
Інфраструктура		Існують програми розвитку та підвищення безпеки постачань (диверсифікація джерел енергії, міжнародна безпекова співпраця). Проводиться регулярна оцінка стану безпеки постачань та готовності до реагування (напр., стандарту поведінки щодо об'єктів газової інфраструктури N-1).	Міненерго, КМУ, НКРЕКП - стратегічні документи (Енергетична стратегія?). Міненерго, НКРЕКП - операційні документи (плани розвитку мереж на 10 років, національні плани дій з безпеки постачання газу та електроенергії, правила про безпеку постачання газу та електроенергії).
		Існують протоколи реагування об'єктів критичної інфраструктури у випадку військових загроз на національному та регіональному рівнях	РНБОУ, Міноборони, СБУ, НГУ, Міненерго, оператори мереж, інших об'єктів критичної енергетичної інфраструктури частина Національного плану захисту інфраструктури (National Infrastructure Protection Plan)
		Хто відповідальний за фізичну охорону інфраструктурних об'єктів в енергетичному секторі	РНБОУ, Міноборони, СБУ, НГУ, Міненерго, оператори мереж, інших об'єктів критичної енергетичної інфраструктури частина Національного плану захисту інфраструктури (National Infrastructure Protection Plan)

		Проводиться підготовка інфраструктурних компаній та їхнього персоналу стосовно можливих військових загроз	Оператори мереж, інших об’єктів критичної інфраструктури, Міненерго. Механізми мають бути виписані в NIPP.
		Існують ефективні механізми реагування на наслідки військових загроз, що потребують специфічних технологій та ресурсів (меморандуми про співпрацю з приватними контрагентами, іншими країнами, спільні технологічні з’єднання з іншими компаніями та країнами).	Координаційний орган в рамках КМУ із залученням РНБОУ (додаткові ресурси потребуватимуть окремих урядових рішень на високому рівні). Механізм має бути виписаний в NIPP.