DOI: https://doi.org/10.15407/emodel.45.03.116
УДК 004.056.53

Р.І. Драгунцов, аспірант, **В.Ю. Зубок**, д-р техн. наук
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України
Україна, 03164, Київ, вул. Генерала Наумова, 15
тел. 044 4641063; e-mail: draguntsow@yahoo.com; vitaly.zubok@gmail.com

Моделювання загроз кібербезпеці у зв'язку з масовими відключеннями електропостачання та потенційні заходи протидії

Під час російсько-української війни в Україні відбувались масові відключення електропостачання, спричинені російськими атаками на цивільну інфраструктуру, а саме на генеруючі та розподільчі потужності енергосистеми. Ризики, пов'язані з такими відключеннями, охоплюють не лише питання безперебійного функціонування господарства напряму, а і більш складніші аспекти, пов'язані з кібербезпекою. Розглянуто вплив подібних відключень на кібербезпеку інформаційно-комунікаційних систем, а саме ефекти другого порядку, такі як перебої зі спостережністю інформації, порушення цілісності інфраструктури захисту, перевантаження команд моніторингу та реагування хибними тривогами. Всі ці фактори змінюють ландшафт загроз для системи та мають бути враховані в політиці безпеки і, відповідно, при моделюванні загроз. Проведено аналіз прихованих ризиків кібербезпеки, що виникають у зв'язку з масовими відключеннями електропостачання. Наведено можливі підходи до врахування таких факторів ризику при проведенні моделювання загроз, а також способи протидії.

К л ю ч о в і с л о в а: блекаут, відключення електропостачання, кібербезпека, спостережність інформації, CSIRT, російсько-українська війна.

Використання російськими військами засобів стратегічного нападу, таких як крилаті ракети та БПЛА великої дальності для ураження компонентів критичної цивільної інфраструктури, а саме генеруючих та розподільчих потужностей енергосистеми України, стало черговим кроком у ході російсько-української війни. Дана практика є, безперечно, черговим військовим злочином, здійсненим російськими військовими, однак не можна виключати, що подібні операції не будуть здійснюватись в інших військових конфліктах з метою руйнування економіки, деморалізації суспільства, унеможливлення нормального функціонування держави, пору-

шення логістичних спроможностей [1]. В умовах сучасної високоінтегрованої економіки більшості світових держав, подібні атаки впливають одразу на всі сектори господарства. Інформаційно-комунікаційна система (ІКС) більшості сучасних підприємств, як енергозалежні системи, страждають як напряму, так і внаслідок так званих каскадних ефектів.

Досліджувана проблематика є відносно новою (у відкритому доступі наявна незначна кількість робіт на дану тему), як в контексті наукових досліджень, так і в рамках інженерних рекомендацій щодо практичних засобів протидії. Дослідження впливу масштабних відключень електропостачання на економіку та господарство в цілому, існують, але такі, що фокусуються на ефектах другого порядку, зокрема впливі на кібербезпеку, тому потребують додаткової роботи. Натомість з моменту усвідомлення реальності масового удару по енергосистемі цілої держави, такі події мають досліджуватись вже не в світлі стійкості проти малоймовірних подій з великими наслідками (resilience to HILP events), а бути перенесеними в управління ризиками інформаційної безпеки. Зважаючи на ці причини, розгляд прихованих ризиків та загроз вважається важливим завданням для управління ризиками підприємств. На базі проведених досліджень, можливе прийняття рішень щодо контрзаходів. Отримання наукового підґрунтя для вирішення цих питань потребує проведення відповідних досліджень.

Головною метою цього дослідження є виявлення загроз кібербезпеки узагальненої ІКС в умовах відключення електропостачання, а також врахування цих факторів при моделюванні загроз та надання рекомендацій щодо заходів протидії.

Основним фактором, що розглядається, є проблема перевантаження команд реагування на кіберінциденти внаслідок появи хибнопозитивних спрацювань. Для досягнення цієї мети проводиться ідентифікація впливу масових відключень електропостачання на системи ІКС, аналізуються прямі наслідків відключення електропостачання для середньої ІКС, виявляються фактори впливу стосовно кіберстійкості та кібербезпеки, ідентифікація впливу на процеси контролю та забезпечення кібербезпеки, визначення потенційних способів врахування даних проблем під час моделювання загроз та ідентифікація можливих засобів протидії.

Аналіз загроз та ризиків для ІКС, пов'язаних з атаками на енергосистему. В державі, енергосистема якої піддається цілеспрямованим атакам та має суттєві пошкодження, для будь-якої ІКС утворюється певна сукупність загроз, до яких можна віднести:

• Планові відключення електропостачання на об'єктах ІКС.

• Аварійні (неочікувані) відключення електропостачання на об'єктах ІКС.

• Перепади напруги в електричній мережі на об’єктах ІКС.

Дані загрози можуть створювати певну кількість ризиків для функціонування системи [2]. Вважаємо за необхідне їх розглянути докладніше.

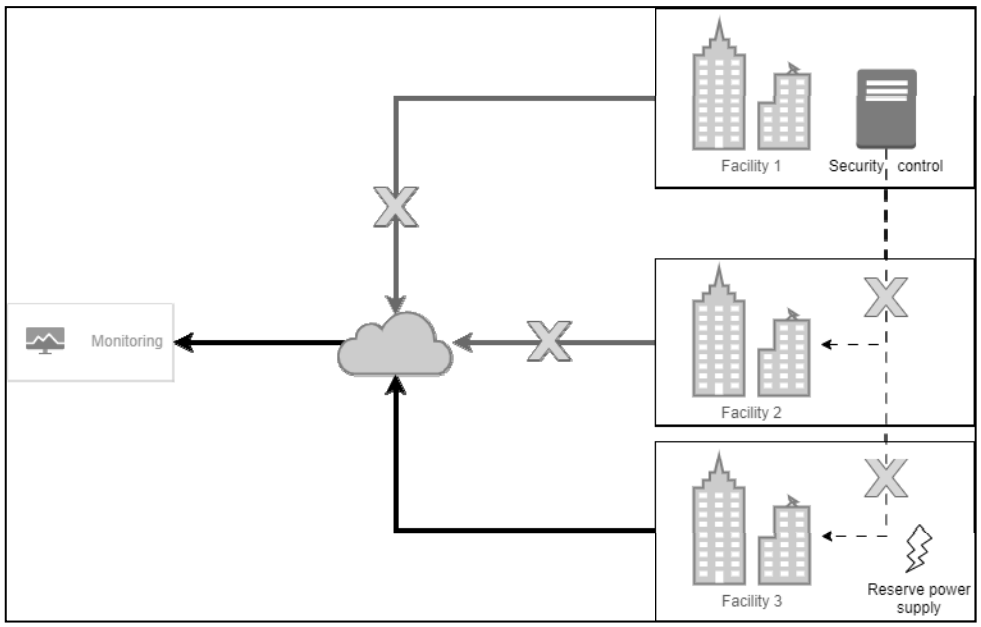
Прямим та очевидним ризиком відключень електропостачання для ІКС є фізичне відключення певної частини сервісів, простій та складність у відновленні їх функціонування. Відключення навіть частини сервісів в загальному випадку може призвести до зупинки функціонування всієї системи, що призводить до прямих втрат внаслідок недоотриманого прибутку. Окремим фактором ризику в даному випадку можна вважати можливість неповного або некоректного відновлення роботи сервісу в автоматичному режимі після відновлення живлення [2].

Відновлення роботи сервісів після аварійного відключення потребує додаткових ресурсів з боку команди технічного супроводу системи. В той же час, для систем, географічно розподілених відносно великого масштабу, утворюється додаткова проблема у вигляді необхідності моніторингу перерв у надходженні журналів. Ситуація, в якій певна система перестає надсилати інформацію про події безпеки, може розглядатися як інцидент та потребувати розслідування. В ситуації відключень електропостачання даний стан буде зустрічатись відносно часто, що відволікає увагу персоналу інформаційної безпеки та потребує від них додаткових ресурсів на розслідування.

Для розподілених географічно та структурноскладних ІКС може розглядатись додатковий ризик у вигляді відключення лише окремих систем безпеки, у разі розміщення їх на локаціях, вразливих до відключень. Отже, може виникнути ситуація, коли основна частина системи продовжує функціонувати стабільно, але відімкнений контроль не застосовується, що може спричинити втрату спостережності та послабити захист певного компонента системи.

Користувацькі системи, що мають надсилати журнали подій на log collector можуть тимчасово втрачати таку можливість або внаслідок розриву каналу зв’язку, або Тому аварійна ситуація відсутності подій від певної системи стає нормальним явищем. Внаслідок цього ситуація компрометації системи з відключенням логування подій може не бути вчасно виявлена [3].

Узагальнено проблеми нормального функціонування розподіленої ІКС за умови масового відключення електропостачання відображено на рисунку. При відключенні електропостачання перериваються зв’язки, що позначені хрестами, і частина даних не надходить на центр моніторингу та реагування, а засоби безпеки, розташовані на відключеному об’єкті, не застосовуються по відношенню до активних.



Принципова схема, що відображає фактори впливу відключення електропостачання на кібербезпеку розподіленої ІКС

Загальноприйняті контрзаходи. Переважна частина політик безпеки, що застосовуються в ІКС, передбачають можливість відсутності електропостачання протягом певного періоду часу та відповідні контрзаходи на випадок таких ситуацій [4—7]. Однак, дані розрахунки найчастіше не враховують ситуацію з систематичним руйнуванням зовнішніх енергосистем, вплив на які неможливо здійснити зсередини. Відключення в даних обставинах мають більш масовий, тривалий та регулярний характер, на противагу аварійним відключенням, які можуть відбуватись в мирний час, або під час стихійного лиха. Наприклад, під час дефіциту в енергосистемі України середня тривалість відключень електропостачання в Києві складала близько 4 годин три рази на добу, і з максимальними значеннями близько 72 годин відсутності електропостачання в окремих районах під час масштабного блекауту. Подібний стан найчастіше не сприймається як ймовірна загроза і тому не передбачаються відповідні контрзаходи при моделюванні загроз [4].

Розглянемо стандартні контрзаходи, що передбачаються під час моделювання загроз ІКС на випадок відключень електропостачання:

Під час масштабних відключень електропостачання використання однотипних каналів зв'язку може бути ризикованим, в особливості, якщо цей тип каналу є енергозалежним на останній ділянці від провайдера.

Дані типи каналів зв'язку передбачають наявність у провайдера обладнання щодо резервування електроживлення, що створює додаткові ризики відключень.

Встановлення батарей резервного живлення на обладнанні. Батареї резервного живлення (БРЖ) дозволяють підключеному обладнанню виконувати своє функціональне призначення певний час після відключення централізованого живлення [5, 8]. Дана схема резервування є суттєво обмеженою внаслідок ємності батарей: для забезпечення функціонування серверної інфраструктури тривалий час необхідне використання акумуляторів виключно великої ємності, що вимагає істотних фінансових вкладень. Крім того, регулярне використання батарей в режимі повного розряду призводить до їх зносу та необхідності у заміні, що несе за собою додаткові фінансові навантаження. Умови масових, регулярних та тривалих відключень електропостачання також накладають обмеження на використання БРЖ (період їхньої зарядки може бути більшим за період надання центрального електроживлення, тому батареї не будуть встигати перезаряджатись, а гарантії резервування будуть зменшені).

Встановлення резервних генераторів на локаціях ІКС Генератори є найбільш ефективним та надійним засобом резервування електропостачання для функціонування об'єкту ІКС [5]. Тривалість безперервної роботи визначається моторесурсом генераторної установки та запасом палива накопиченого на об'єкті [2]. Використання генераторів в якості резервного джерела живлення потребує залучення додаткового технологічного приміщення зі специфічними умовами для відповідної установки, що не є завжди можливим варіантом. Обладнання генераторами всіх локацій розгалуженої та географічно розподіленої ІКС потребує великих фінансових вкладень, є складним з організаційної точки зору процесом та потребує суттєвих логістичних зусиль з вчасного забезпечення паливом усіх локацій.

Географічне розподілення ІКС. Розташування об'єктів ІКС в різних географічних локаціях має на меті забезпечити диверсифікацію ризиків відносно відключення живлення для всієї інфраструктури. Даний підхід може бути оцінений як ефективний для однотипних компонентів системи, коли відключення частини знижує ефективність роботи цілого, але не зупиняє її, — але не може бути застосовним для компонентів різного класу, коли зупинка одного повністю зупиняє роботу системи. Масштабні та (або) непередбачувані відключення в рамках всієї країни також нівелюють ефективність географічного розподілу системи. В той же час, розподілення системи на міждержавному рівні може суттєво знизити ризики, пов'язані з відключенням електропостачання. Це особливо актуально, якщо для диверсифікації використовуються потужності гео-

графічно віддалених держав, енергосистеми яких не пов'язані з енергосистемою держави, в якій розміщується основна частина системи.

Розподілення ІКС з використанням потужностей хмарних провайдерів. Використання хмарних сервісів для диверсифікації частини функціоналу ІКС також може вважатись заходом протидії ризикам, пов'язаним з відключенням електропостачання [4]. Переважна більшість провайдерів хмарних сервісів широкого профілю, таких як Amazon, Google та Microsoft, мають розгалужену та розподілену по всьому світу фізичну інфраструктуру, забезпечену усіма необхідними засобами протидії надзвичайним ситуаціям, зокрема, і резервуванням електроживлення. Основну роль в забезпеченні надійності підтримки даних сервісів становить їхній географічний розподіл, тобто проблеми в енергосистемі окремо взятої держави не створюють підтверджених ризиків для функціонування хмарної інфраструктури. Це в свою чергу означає, що винесення окремого компоненту ІКС на потужності хмарного провайдеру дозволяє надійно захистити даний компонент від ризику відключення електропостачання, за умови достатнього географічного розподілу інфраструктури останнього [9]. Таке рішення може розглядатись як повністю ефективне по відношенню до захисту інформаційних бізнес-сервісів та окремих засобів кіберзахисту від відключень електропостачання. До останніх можна віднести окремі види (Web Application Firewall (WAF)), (Security Incident and Event Management system (SIEM)) та (Endpoint Detection and Response (EDR)).

Однак, на потужностях хмарного провайдера в загальному випадку не може бути розміщена абсолютно вся інфраструктура ІКС організації: робочі станції співробітників та деякі локальні сервіси будуть в будь-якому випадку розташовуватись локально. Використання потужностей хмарного провайдера для забезпечення роботи істотної частини ІКС потребує для доступу до неї надійного каналу зв'язку з високою пропускною спроможністю, що в умовах відключень електропостачання далеко не завжди є доступною опцією. Зокрема, термінали супутникового зв'язку в середньому можуть видавати швидкість з'єднання в 100 Мбіт/с, а термінали ADSL зв'язку — до 27 Мбіт/с. Така швидкість не може вважатись достатньою для повноцінного функціонування відносно великої організації з залученням хмарних компонентів ІКС.

Порівняльний аналіз контрзаходів з енергетичної безпеки ІКС. Розглядаючи наявні проблеми кібербезпеки, пов'язані з масовими відключеннями електропостачання, в поєднанні з існуючими контрзаходами щодо протидії періодичним відключенням, можна зробити висновки щодо того, які заходи можуть бути ефективні в нівелюванні ризиків саме в розглянутій ситуації.

Найефективнішим рішенням щодо протидії загрозам відключень електропостачання в ІКС представляється встановлення обладнання для резервного електропостачання — БРЖ та генераторів. В залежності від рівня критичності об'єкту та його енергоспоживання може бути зроблений вибір в сторону резервного акумулятора БРЖ або генератора.

Отже, встановлюється проміжок часу, під час якого об'єкт буде продовжувати функціонувати навіть під час масового відключення електропостачання. Важливим аспектом в такому випадку вважаємо наявність на обладнанні резервування можливості журналювання свого стану та відправки журнальних даних для аналізу та збереження. Даний функціонал дозволяє проводити кореляцію втрати надходження логів з об'єкту з подією розрядження акумуляторів резервного живлення.

Таким чином, зменшується навантаження на операційну команду безпеки, вирішується проблема додаткового вичерпання ресурсів сил моніторингу та реагування. Імплементація подібної практики зумовлює необхідність впровадження відповідного контролю на рівні моніторингу подій: втрата зв'язності з об'єктом ІКС, втрата журналів від такого об'єкту, або зафіксована перерва у його функціонуванні не має розглядатись як інцидент безпеки лише у випадках, прописаних в порядку виключення та, зокрема, у разі виявлення повідомлення від відповідного джерела резервного живлення про низький заряд акумуляторів, або, у разі використання генератора з можливістю віддаленого технічного моніторингу, низький рівень палива.

Для забезпечення безперебійного зв'язку об'єктів з центром, де проводиться накопичення та аналіз журналів, а також центром керування ІКС необхідне забезпечення резервного каналу зв'язку, стабільного та достатнього для здійснення, як мінімум, задач моніторингу та керування системою відповідно. В якості такого каналу може достатньо ефективно використовуватись як стабільний та відносно повільний ADSL, так і оптичний канал або супутниковий зв'язок.

Вибір конкретної технології залежить від можливостей реалізації в поточних умовах, але головним критерієм має залишатись стабільність та гарантованість зв'язку у ситуації відключення електроживлення протягом періоду, як мінімум, гарантованого системами резервування на об'єкті ІКС. Забезпечення такого каналу гарантує, що центр, в якому проводиться накопичення та аналіз журналів зможе отримати необхідні дані для забезпечення спостережності.

В свою чергу, винесення об'єктів ІКС на потужності стабільного та розподіленого хмарного провайдера дозволяє зменшити вимоги до забезпечення резервування електроживлення об'єкту, а також усунути проб-

лему відключення контролів безпеки, у разі перенесення відповідних контролів у «хмару». Особливість даного підходу полягає в тому, що в загальному випадку не представляється можливим перенесення всіх частин ІКС на потужності хмарного провайдера — певна частина буде фізично локалізуватись там, де знаходиться персонал, що робить дані частини вразливими до відключень електропостачання. Саме тому, можемо дійти двох висновків щодо застосовності «хмарного переходу» для подолання проблеми відключень електропостачання.

1. Перенесення об'єктів ІКС на будь-яку зовнішню платформу не вирішує проблему масових відключень для інфраструктури повністю, хоча і дозволяє нівелювати декілька вище названих ризиків. Подібні заходи у будь-якому випадку вимагають додаткових вкладень у резервування електропостачання для «нехмарних» об'єктів.

2. Чим більше внутрішніх сервісів є винесеними за межі периметру ІКС на потужності хмарного провайдера, тим більше значення отримує канал зв'язку, що забезпечує комунікацію «наземних» сервісів з «хмарними». Втрата зв'язку, що є одним з основним джерелом загроз в ситуації масових відключень електропостачання, в таких умовах призведе до більш серйозних порушень в роботі системи.

Таким чином, резервування каналів зв'язків представляється пріоритетною задачею для забезпечення доступності та нормального режиму функціонування для «гібридних» ІКС, тобто таких, частина компонентів яких дислокується на потужностях хмарних провайдерів.

Короткі результати порівняльного аналізу наводяться в таблиці.

Пропозиції підходів до моделювання загроз з урахуванням факторів масштабних відключень електропостачання. Виходячи з таких підходів до моделювання загроз як STRIDE [10], враховуючи вище викладене, можемо дійти висновку щодо можливих підходів до моделювання загроз пов'язаних з масштабними відключеннями електропостачання. Щоб врахувати цей фактор, можна використовувати наступні підходи:

1. Моделювання відключення електропостачання як окремої загрози: можна включити в модель загрозу відключення електропостачання як окрему загрозу, з оцінкою ймовірності та відповідними наслідками.

2. Врахування взаємозв'язку між електропостачанням та функціонуванням іншими системами: можна включити в модель взаємозв'язки між електропостачанням та іншими критичними системами, такими як мережі електрозв'язку, банківські системи, системи зберігання даних. Це дозволить оцінити, як відключення електропостачання може вплинути на роботу цих систем та які можуть бути наслідки.

3. Моделювання відновлення електропостачання: можна включити в модель процес відновлення електропостачання після відключення, з оцін-

Контрзахід	Переваги	Недоліки
Резервне живлення від батарей	Забезпечення функціонування об'єкта в умовах відключення електропостачання	Час підтримки функціонування об'єкту відносно нетривалий
	Можливість моніторингу стану батареї, що зменшує ризики щодо спостережності	Потребує істотних фінансових вкладень для забезпечення усіх об'єктів, особливо стосовно серверного обладнання
Резервні генератори	Забезпечення функціонування об'єкта в умовах відключення електропостачання протягом потенційно необмеженого часу	Потребує істотних фінансових вкладень для забезпечення усіх об'єктів ІКС
		Створює логістичне та організаційне навантаження на підтримку функціонування
	Можливість резервування порівняльно більшої електричної потужності	Ускладнений централізований моніторинг стану генераторів
Географічне розподілення	Можливість нівелювати ризики відключень по відношенню до однотипних компонентів системи	Не вирішує проблему відключення унікальних компонентів ІКС
		Не забезпечує захисту від загальнодержавних відключень
	У разі міждержавного розподілу дозволяє забезпечити гарантований захист частини ІКС	
Перенесення в хмару	Гарантований захист від відключень електропостачання винесених компонентів	Неможливо перенести усі компоненти ІКС в хмару

кою тривалості та наслідків цього процесу. Це дозволить оцінити, який час може зайняти відновлення електропостачання і як це вплине на інші системи, зокрема такі, що стосуються засобів забезпечення кібербезпеки.

4. Використання симуляційного моделювання: пропонується використовувати симуляційне моделювання, щоб оцінити, як відключення електропостачання може вплинути на роботу інших систем і якими можуть бути наслідки, зокрема, для кібербезпеки.

Однією з основних загроз кібербезпеки в умовах масових відключень електропостачання є суттєве погіршення спостережності інформації, а також порушення цілісності системи кіберзахисту. Особливий вплив дана загроза має на інфраструктуру географічно розподілених ІКС. Врахувати подібні загрози в процесі моделювання загроз можливо викорис-

товуючи методологію STRIDE, а саме категорії Denial of Service та Tampering або Repudiation. Основними засобами протидії даним загрозам вбачається, окрім резервування джерел електропостачання та каналів зв'язку, створення додаткових способів відстежування факту відключення електроживлення об'єкту, розробка відповідних протоколів щодо аналізу інцидентів та перенесення частин ІКС на потужності хмарного провайдеру.

Висновки

В подальшому вбачається розвиток дослідження даної тематики. В першу чергу, на момент створення даної роботи у вільному доступі відсутні детальні статистичні дані щодо впливу масових відключень електропостачання на господарство, на функціонування ІКС та на кібербезпеку.

Для розробки ефективних конкретизованих методів моделювання загроз та протидії ним необхідне отримання та розгляд цих даних. Як пріоритетна задача розглянута розробка конкретних методів протидії, відповідних контролів та процесів безпеки, уніфікованих під різні можливі випадки, що спричиняють масові відключення. Не достатньо висвітленим залишається аспект реальної ситуації в кібербезпеці високо цифровізованої держави в умовах нестабільної роботи енергосистеми. Даний аспект вважається особливо важливим для подальшого дослідження на основі як статистичних даних так і результатів моделювання.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. КІБЕРАТАКИ, АРТИЛЕРІЯ, ПРОПАГАНДА. Загальний аналіз вимірів російської військової агресії. Державна служба спец. зв'язку та захисту інформації України. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=50692.
2. Petermann, T., Bradke, H., Lüllmann, A., Poetzch, M., & Riehm, U. (2011). What happens during a blackout (Technology Assessment Studies Series – 4). BoD – Books on Demand.
3. Cyber-Physical Observability for the Electric Grid / N. Jacobs та ін. 2020 IEEE Texas Power and Energy Conference (TPEC), м. College Station, TX, USA, 6–7 лют. 2020 р. 2020.
4. STRIDE-based threat modeling for cyber-physical systems / R. Khan та ін. 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), м. Torino, 26–29 верес. 2017 р. 2017. URL: https://doi.org/10.1109/isgteurope.2017.8260283 (дата звернення: 04.06.2023).
5. Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies / I. Zografopoulos та ін. IEEE Access. 2021. Т. 9. С. 29775–29818. URL: https://doi.org/10.1109/access.2021.3058403 (дата звернення: 04.06.2023).
6. Lars Halvdan F. Threat Modeling Framework for Smart Grids: Master thesis. Trondheim, 2021. 90 p. URL: https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2781029/no.ntnu:inspera:66462738:38097967.pdf?sequence=1 (дата звернення: 15.05.2023).
7. Muckin M., C. Fitch S. A Threat-Driven Approach to Cyber Security. Lockheed Martin Corporation, 2019. 45 с. URL: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Threat-Driven-Approach.pdf (дата звернення: 15.05.2023).

8. Using a Reserve Power Architecture to Increase Data Center Infrastructure Utilization and Efficiency. Columbus: Emerson Network Power Global Headquarters, 2014.
9. Business Continuity Management for SMEs using the Cloud. Bonn: Federal Office for Information Security, 2013.
10. Conducting a STRIDE-based threat analysis. 1. United Kingdom Department for Science, Innovation & Technology. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1155778/Conducting_a_STRIDE-based_threat_analysis.pdf (дата звернення: 23.05.2023).

Отримано 23.05.2023;
після доопрацювання 04.06.2023

REFERENCES

1. CYBERATTACKS, ARTILLERY, PROPAGANDA. Common analysis of Russian aggression metrics. (2022). Center for Cybersecurity and Cybercrime Combatting under the State Service of Special Communication and Information Protection of Ukraine. https://cip.gov.ua/services/cm/api/attachment/download?id=50692
2. What happens during a blackout / T. Petermann et al. Norderstedt : BoD – Books on Demand, 2011.
3. Jacobs, N., Hossain-McKenzie, S., Summers, A., Jones, C. B., Wright, B., & Chavez, A. (2020) Cyber-Physical Observability for the Electric Grid. У 2020 IEEE Texas Power and Energy Conference (TPEC). IEEE. https://doi.org/10.1109/tpec48276.2020.9042494
4. Khan, R., McLaughlin, K., Laverty, D., & Sezer, S. (2017) STRIDE-based threat modeling for cyber-physical systems. У 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe). IEEE. https://doi.org/10.1109/isgteurope.2017.8260283
5. Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021) Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies. IEEE Access, 9, 29775–29818. https://doi.org/10.1109/access.2021.3058403
6. Halvdan Flå, L. (2021) Threat Modeling Framework for Smart Grids [Master thesis, Norwegian University of Science and Technology]. https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2781029/no.ntnu:inspera:66462738:38097967.pdf?sequence=1
7. Muckin, M., & C. Fitch, S. (2019) A Threat-Driven Approach to Cyber Security. Lockheed Martin Corporation. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Threat-Driven-Approach.pdf
8. Using a Reserve Power Architecture to Increase Data Center Infrastructure Utilization and Efficiency. (2014a). Emerson Network Power Global Headquarters.
9. Business Continuity Management for SMEs using the Cloud. (2013b). Federal Office for Information Security.
10. Conducting a STRIDE-based threat analysis. (2023) United Kingdom Department for Science, Innovation & Technology.

Received 23.05.2023;
after revision 04.06.2023

R. Drahuntsov, V. Zubok

MODELING OF CYBER THREATS RELATED TO MASSIVE POWER OUTAGES AND SUMMARY OF POTENTIAL COUNTERMEASURES

During the Russian-Ukrainian war, mass power outages occurred in Ukraine, caused by Russian attacks on civilian infrastructure, namely on the generating and distribution capacities of the power system. The risks associated with such outages cover not only the issue of uninter-

rupted operation of the economy directly, but also more complex aspects related to cyber security. The impact of such outages on the cyber security of information and communication systems is considered, namely, the second-order effects, such as interruptions with information observability, violation of the integrity of the protection infrastructure, overloading of monitoring teams and response to false alarms. All these factors alter the threat landscape for the system and must be considered in security policy and during the threat modeling process accordingly. An analysis of hidden cyber security risks arising in connection with massive power outages was conducted. Possible approaches to taking such risk factors into account when modeling threats, as well as methods of countermeasures, are given.

K e y w o r d s: blackout, power outage, cybersecurity, information observability, false positive, CSIRT, russo-ukrainian war.

ДРАГУНЦОВ Роман Игоревич, аспірант Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. В 2016 р. закінчив Державний університет телекомунікацій. Область наукових досліджень — кібербезпека, теорія ризиків, моделювання загроз інформаційній безпеці.

ЗУБОК Віталій Юрійович, д-р техн. наук, пров. наук. співробітник Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. В 1994 р. закінчив Київський політехнічний інститут. Область наукових досліджень — глобальні інформаційні мережі, Інтернет, теорія складних мереж, кібербезпека.