Горбачук В. М.
доктор фізико-математичних наук,
завідувач відділом інтелектуальних інформаційних технологій,
Інститут кібернетики імені В. М. Глушкова
м. Київ, Україна
Ніколенко Д. І.
науковий співробітник,
Інститут кібернетики імені В. М. Глушкова
м. Київ, Україна
Ніколенко Я. Д.
аспірант,
Інститут кібернетики імені В. М. Глушкова
м. Київ, Україна

DOI: https://doi.org/10.36059/978-966-397-431-6-5

ПЛАНУВАННЯ ЗАХОДІВ І ОРГАНІЗАЦІЯ ВІДНОВЛЕННЯ ЕЛЕКТРОМЕРЕЖ ПІСЛЯ ТЕРОРИСТИЧНИХ АТАК

Система виробництва, транспортування, розподілу і постачання електроенергії покриває всю територію країни, її лінії електропередач простягаються на сотні кілометрів, а багато важливих об'єктів цієї системи такі, як великі трансформатори і електропідстанції, важко захистити від всіх можливих терористичних і військових загроз. Ретельно спланована терористична або військова атака на систему електроенергетичного живлення здатна позбавити значні частини країни доступу до системи постачання електроенергії на дні і тижні, а також суттєво обмежити потужність потоків електроенергії для певних регіонів країни на місяці і роки. Очевидно, що вся економіка, здоров'я і добробут людей залежать від електроенергії, тому наслідки цілеспрямованих пошкоджень можуть бути катастрофічними.

Героїчна робота українських енергетиків щодо відновлення електроенергетичної системи після терористичних атак російських окупантів дає багато інформації, аналіз та узагальнення якої і відповідні практичні висновки сприяють суттєвому покращенню стійкості електроенергетичної системи України до подібного руйнування. В той же час, корисно врахувати досвід інших країн щодо захисту енергетичних систем від терористичних загроз. Наприклад,

у 2004–2007 рр. *Комітет з покращення надійності і відмовостійкості нових ліній електропередач і систем розподілу електроенергії в США від терористичних атак* підготував Звіт з результатами відповідного дослідження. Цей Комітет працював під керівництвом Національної дослідницької ради Національних академій наук, інженерних наук і медицини (National academies of Sciences, Engineering and Medicine) – неурядових неприбуткових організацій США, чия діяльність спрямована на продукування порад для обґрунтування політики, стимулювання прогресу та інновацій і протистояння складним проблемам на благо суспільства [1; 2].

У 2012 році Департамент внутрішньої безпеки США (USA Department of Homeland Security) розсекретив Звіт і дозволив його публічне оприлюднення.

Названий Звіт основну уваге приділяє заходам, які зроблять можливим:

− Зменшення вразливості системи передачі електроенергії до атак;

− Швидке відновлення електропостачання після нападу;

− Підвищення стійкості і зменшення вразливості надання критично важливих комунальних послуг після порушення електропостачання.

Наведемо деякі види вразливості електроенергетичної системи.

Фізична вразливість. Проблеми в будь-якій частині системи можуть призвести до перебоїв у постачанні електроенергії до великої кількості споживачів. Особливо вразливими є високовольтні трансформатори і електро-підстанції, а виведення з ладу багатокілометрової лінії електропередач може бути спричинено руйнуванням декількох електроопор.

Кібервразливість. Автоматизовані системи управління, централізоване керування обладнанням, високошвидкісний зв’язок можуть стати об’єктами кібератак. Найбільш критичними є системи диспетчерського управління та збору даних (SCADA – Supervisory Control And Data Acquisition) [3]. За допомогою датчиків у складі систем SCADA вимірюються, передаються і обробляються показники функціонування об’єктів електроенергетичної системи в режимі реального часу, наприклад, автоматичні вимикачі. Потенційно, хакери можуть маніпулювати системами SCADA, передати помилкові сигнали операторам, заблокувати потік життєво важливої інформації або вивести з ладу захисні системи. Добре скоординовані кібератаки розглядаються, як підсилюючий елемент, який може збільшити шкоду від фізичної атаки. Наприклад, каскадне вимкнення збільшиться, якщо

оператори не отримають інформацію про його початок або якщо захисні пристрої були вимкнені за допомогою хакерів, що передувало фізичній атаці.

Напрацьовано ряд заходів для зменшення вразливості системи електропостачання. Назвемо деякі з цих заходів за видами вразливостей.

Фізична вразливість. Захист ключових підстанцій і центрів управління. Додавання анкерних (підсилених розтяжками) електроопор для запобігання обвалу веж за ефектом доміно. *Додатково*. Удосконалені датчики несанкціонованого вторгнення. Стратегії збільшення потужності електромереж. Широке використання розподіленої генерації (сонячні електростанції…) та мікромереж.

Кібервразливість. Ліквідація другорядних шляхів доступу до енергооб'єктів. Якісна кібербезпека на всіх ланках. *Додатково*. Кібербезпека датчиків, систем зв'язку та управління. Системи моніторингу та уникнення помилок оператора.

Вразливість персоналу. Перевірка співробітників та підрядників. Тренування навичок реагування на атаки. Координація з урядовими органами, в першу чергу, з правоохоронними. Забезпечення персоналу під час відновлювальних робіт всім необхідним (вода, харчування тощо). *Додатково*. Удосконалені тренажери для тренувань. Освітні програми в енергетиці.

Деградація системи з плином часу її експлуатації. Удосконалення інституційних механізмів для вчасної модернізації системи електропостачання. Високовольтні силові електронні технології. З'єднання постійного струму. Вибіркове управління попитом та автоматизація розподілу електроенергії [4]. *Додатково*. Імовірнісна оцінка вразливостей. Датчики, зв'язок, аналіз у реальному часі та візуалізація системи. Автоматичне керування. Острівне енергозабезпечення та самовідновлення. Зберігання енергії.

Прискорене відновлення. Планування великих вимкнень. Навчання деяких працівників комунальних служб навичкам рятувальників. *Додатково*. Накопичення запасів аварійних трансформаторів та ключового обладнання.

Забезпечення критичних комунальних послуг під час блекаутів. Прилади з електрозбереженням: світлодіоди (LED), світлофори з акумуляторами крапельного заряду тощо. Наближення електрогенеруючих потужностей до критичних споживачів (насосів водопостачання, лікарень тощо). Планування дій на випадок надзвичайних ситуацій. Незалежне енергоживлення, де воно можливе

(зарядка мобільних телефонів, газові насоси замість електричних на газопроводах тощо). *Додатково*. Розподілена архітектура системи електрозабезпечення. Покращене зберігання енергії.

Після слова «*Додатково*» названі заходи, які потребують проведення належних науково-дослідних і дослідно-конструкторських робіт.

Планування заходів з ліквідації наслідків терористичної атаки. Мета такого планування – забезпечити обслуговування клієнтів комунальних служб в умовах втрати одного або декількох компонентів енергоструктури, кількість яких не перевищує визначеного проєктного рівня, та знати наперед, що з певною імовірністю залишиться достатня кількість працездатного обладнання для задовільного обслуговування клієнтів. Зазвичай, комунальні служби розробляють плани дій на випадок виходу з ладу окремих одиниць обладнання. В умовах терористичної або військової атаки можливе пошкодження цілої лінії електропередач або декількох одиниць обладнання (трансформаторів тощо).

Для планування дій щодо відновлення електропостачання потрібно передбачити вирішення таких питань: 1) можливість аварійного запуску, тобто наявність зовнішнього джерела електроенергії для запуску роботи електрогенератора; 2) розподіл потоків електроенергії між лініями/кабелями та інші засоби контролю напруги та реактивної потужності з метою електропостачання високоприоритетним споживачам (лікарні, навчальні заклади, насоси водопостачання тощо) та тимчасового відімкнення від електромережі інших споживачів; 3) додаткове регулювання захисних систем, призначених для зниження напруги, частоти, контролю синхронізації тощо; 4) використання панелей відновлення; 5) розробка політик відновлення, включно з організацією роботи ізольованих енергетичних островів, моніторингу напруг, частот тощо.

Особливий наголос робиться не на адміністративних засобах впливу, а на організації добровільного співробітництва урядових органів, бізнесу і громадськості, а також на економічних важелях стимуляції енергозбереження і підвищення надійності та відмовостійкості енергосистем.

Література:

1. National Research Council. *Terrorism and the Electric Power Delivery System*. Report of the Committee On Enhancing The Robustness And Resilience Of

Future Electrical Transmission And Distribution In The United States To Terrorist Attack. National Academy of Sciences. Washington, DC: The National Academies Press. 2012. P. 164. DOI: https://doi.org/10.17226/12050

2. National academies of Sciences, Engineering and Medicine of USA. About Us. *Web site of National Academies of USA*. URL: https://www.nationalacademies.org/about

3. Wikipedia. *SCADA*. URL: https://en.wikipedia.org/wiki/SCADA

4. Horbachuk V., Havrylenko S., Holotsukov H., Nikolenko D. Economics of internet applications and digital content. In book: The role of technology in the socio-economic development of the post-quarantine world. M.Gavron-Lapuszek, A.Karpenko (eds.). P. 81–88. Publisher: Katowice: Katowice School of Technology.