ЗАСТОСУВАННЯ МЕТОДІВ ТА ЗАСОБІВ МОДЕЛЮВАННЯ

DOI: <https://doi.org/10.15407/emodel.43.02.068>
УДК 621.3.51

В.О. Гурєєв, канд. техн. наук, **Є.М. Лисенко**, аспірант
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України,
Україна, 03164, Київ, вул. Генерала Наумова, 15,
тел. +380 44 424 91 60, e-mail: viktor.gurieiev@ipme.com.ua

Топологічний метод оцінки чутливості до виявлення кібернетичних загроз в енергосистемах ОЕС України

Розглянуто теоретичні питання побудови топологічного методу оцінки чутливості до виявлення кібернетичних загроз в електричних мережах енергосистем за допомогою моделювання режимів роботи окремих (виділених) підсистем. Описано основні етапи побудови моделей топології енергосистем, запропоновано та реалізовано методи формування інформаційних моделей об'єктів енергосистем. Досліджено методи візуалізації результатів моделювання умов виникнення кіберзагроз. Визначено способи використання запропонованого підходу до створення системи протидії кіберзагрозам в електричних мережах енергосистем і побудови сценаріїв їх ліквідації за допомогою навчального дистанційного режимного тренажера.

К л ю ч о в і с л о в а: режимні кіберзагрози, моделювання кіберзагроз, оперативні перемикання, сценарії протикібернетичних тренувань.

За оглядом наслідків наявних прикладів кібернетичних атак на об'єкти енергосистем України, зважаючи на критичний стан систем управління енергетичним обладнанням, доцільно проаналізувати умови створення таких загроз і запропонувати підходи до захисту об'єктів критичної інфраструктури економіки країни, включаючи методи попередження, швидкої протидії і ліквідації аварій [1, 2]. Виникнення умов для кібератак в енергосистемах певною мірою обумовлено розвитком систем автоматизації енергетичного устаткування генерації і підстанцій на основі новітніх мікропроцесорних пристроїв та ускладненням режимів роботи енергосистем.

Створення методів ранньої діагностики умов виникнення кіберзагроз за допомогою автоматизованих систем та оперативного захисту електричних мереж на різних рівнях ієрархії управління енергетикою є склад-

© Гурєєв В.О., Лисенко Є.М., 2021

ним науково-технічним завданням. Сучасна технологія вироблення і розподілу електричної енергії в нормальних (штатних) режимах вимагає безперервної зміни конфігурації (топології) електричних мереж для створення безпечних умов роботи енергосистем у разі виведення в ремонт енергетичного обладнання. Дозвіл на заявлені ремонтним персоналом оперативні перемикання в електричних мережах і на підстанціях надає диспетчер об'єднаної електроенергетичної системи (ОЕС), електроенергетичної системи (ЕЕС) або енергопостачальної компанії (ЕК) після перевірки допустимості таких комутацій.

Перевірка допустимості необхідних оперативних перемикань здійснюється режимною групою на етапі розгляду заявок на перемикання за допомогою програм розрахунку усталених режимів. Перевірці підлягають рівень напруги в контрольованих вузлах електричної мережі, струми ліній електропередач, величина перетікання потужності по контрольованих перерізах для знову виникаючих конфігурацій електричних мереж. Дозвіл на виконання отриманої диспетчером заявки залежить також від результатів аналізу ремонтного режиму, який іноді не співпадає з поточним в цій же мережі. Часто це призводить до технологічних порушень в роботі енергетичного устаткування і великих аварій.

У складних розподілених ЕЕС відбувається велика кількість планових і нештатних технологічних комутацій (збурень), викликаних необхідністю виведення (введення) устаткування в ремонт, короткими замиканнями на лініях електропередач і підстанціях, відмовами облаштувань релейного захисту і автоматики, помилками обслуговуючого персоналу та ін. Частина цих збурень усувається засобами релейного захисту і протиаварійної автоматики. Проте дуже часто через відмову релейного захисту, помилки персоналу або в результаті зовнішніх і внутрішніх причин, що додатково виникають після поточних комутацій, можуть сформуватися умови для каскадного розвитку аварійних ситуацій. Ліквідацію каскадних аварій зазвичай забезпечує система протиаварійного управління більш високого рівня. При недостатній надійності системи або у разі несанкціонованого доступу виникають умови для розвитку важких системних аварій, часто з катастрофічними наслідками.

До таких аварій можна віднести системні аварії у Північній Америці і Європі (2003 р.), Росії (2005 р.), Європі (2006 р.), Україні (2014—2016 роки) та ін. [3—5]. Умови виникнення аварійних ситуацій можуть бути викликані рідкісним збігом випадкових обставин, а саме технологічними причинами, або в результаті ретельно спланованої кібератаки. Для виявлення дійсних причин аварій є доцільною розробка нових методів моделювання умов виникнення і розвитку прогнозованих аварій або аварій, що вже сталися.

Метою дослідження є аналіз існуючих підходів до вирішення проблеми виявлення кібератак на енергетичні об'єкти і розробка нової автоматизованої системи оперативного виявлення кіберзагроз (АСВК) технологічного походження (ТП) на основі інтегрованої системи серверів додатків і систем управління базами даних (СУБД), включаючи віртуальні [6]. Запропонована АСВК призначена для використання в умовах нормальної (штатної) роботи і в аварійних режимах в реальному часі. Передбачається цілодобове використання АСВК як порадики для оперативно-диспетчерського персоналу.

АСВК реалізовано з урахуванням особливостей розподіленого середовища моделювання режимів роботи енергосистем. До неї включено сервери додатків з вбудованими модулями (контролерами) аналізу наявності кібернетичних втручань, розподілені бази даних (БД) і тренажерні системи підготовки персоналу за тематикою захисту від кіберзагроз об'єктів енергетики [7].

Важливою функцією АСВК є структуризація представлення наявної інформації та існуючих знань про предметну область технології оперативних перемикачів в електричних мережах і ефективне застосування цих знань для формування таких навичок, які відповідають ключовим компетентностям оперативно-диспетчерського персоналу в області кіберзахисту. За допомогою АСВК можна вирішувати питання технології оперативних перемикачів в аварійних режимах електричних мереж і питання безпечної роботи з електроустановками.

Основними комутаційними апаратами на підстанціях електричних мереж є вимикачі, роз'єднувачі, короткозамикачі, відокремлювачі, трансформатори, системи шин та ін. Порядок і регламент комутацій визначається в службових інструкціях і заздалегідь підготовлених штатних програмах перемикачів. Проте на практиці стан комутаційних апаратів на підстанціях і в електричних мережах може суттєво відрізнятися від штатного (стандартного).

Для проведення потрібних операцій по введенню або виведенню устаткування в ремонт використовуються спеціальні бланки оперативних перемикачів, в яких враховано поточний стан устаткування на момент перемикачів. Навіть для невеликих ЕК потреба в створенні і використанні бланків оперативних перемикачів обчислюється десятками тисяч на рік. Наразі ручна підготовка бланків перемикачів зумовлює появу великої кількості помилок в діях оперативно-диспетчерського персоналу, а відсутність їх моніторингу призводить до створення умов для кібератак. Тому спрощення і автоматизація процесу підготовки бланків оперативних перемикачів в сучасних умовах є актуальною проблемою. Цим питанням присвячено багато публікацій в нашій країні і за кордоном [8—10]. У ба-

гатьох з них використовуються дерева оцінки ситуацій, плани дій і подібні їм алгоритми аналізу діяльності персоналу [10, 11].

Надійність роботи системи людина — автоматична або автоматизована система керування — енергетичний об'єкт визначається рівнем розуміння персоналом моделей функціонування об'єкту у вигляді уявної моделі об'єкту управління [12]. Уявна модель формується за допомогою інтеграції технологічної (суб'єктивно сформоване уявлення людини про структуру і топологію устаткування), функціональної (в образі наявних причинно-наслідкових взаємозв'язків в технологічному процесі), причинно-наслідкової (в образі змінних у часі причинно-наслідкових взаємозв'язків між можливими впливами і порушеннями в технологічному процесі) і іншими моделями [11, 12].

Результати ретельного аналізу діяльності персоналу лягли в основу процесу створення пропонованої АСВК, включаючи структуру бази знань для виявлення кіберзагроз.

Відомі два основні методичні підходи до формування уявної моделі об'єкту управління [9].

1. *Алгоритмічний підхід* забезпечує перетворення оперативних знань і рішень у відповідні оцінки чутливості до кіберзагроз. Основою цього методу є алгоритмічні способи опису експлуатаційних подій: дерева оцінки ситуацій і плани дій. Деревами оцінки ситуацій є графи (карти) усіх можливих умов і шляхів виникнення аварій і порушень в роботі устаткування. Головна мета полягає у можливості знати усі шляхи розвитку ситуації і знайти один або декілька найефективніших. Для цього використовуються плани дій у вигляді результатів реакції на можливі збурення. Плани дій допомагають знаходити і релевантно оцінювати шляхи досягнення мети за допомогою наявних засобів і з урахуванням існуючих обмежень.

Проте алгоритмічний підхід обмежує можливості розвитку самостійного оперативного мислення в нестандартних ситуаціях. Головною проблемою є складність процесу генерації достатньої кількості потрібних варіантів створення умов виникнення і розвитку аварій для формування ключових компетентностей персоналу, а саме розпізнавання цих умов і швидкої ліквідації аварій.

2. *Імітаційне моделювання* породжує ситуації і зміни стану систем. Цей підхід дозволяє генерувати різноманітні умови і варіанти розвитку аварійних ситуацій і моделювати складні екстремальні збурення, які викликають виникнення і розвиток аварій. Вважається, що чим неймовірніше поєднання подій у пропонованому сценарії розвитку аварії, тим більший вплив здійснюється на формування потрібних компетентностей персоналу в процесі тренажерної підготовки. Основною відмінністю такого підходу є можливість моделювання різних умов виникнення аварій

і подій, що дозволяє зосередити головну увагу на виявленні кіберзагроз, і здатність прогнозувати їх можливий вплив на об'єкти критичної інфраструктури. Генерація та ретельний аналіз різних можливих або прогнозованих варіантів кіберзагроз значною мірою доповнює алгоритмічний підхід.

Для моделювання і дослідження режимів роботи енергосистем широко використовуються так звані схеми заміщення енергетичного устаткування: лінії електропередачі, генератори, трансформатори, вимикачі, роз'єднувачі і тому подібне. Моделі окремих елементів утворюють більші об'єкти енергосистем, включаючи транзитні розподільні відкриті і закриті підстанції, теплові, атомні і гідроелектростанції, вітрові та інші джерела енергії. Великі енергосистеми можуть утворювати енергооб'єднання, призначені для забезпечення надійної статичної і динамічної стійкості. Методам дослідження великих енергосистем присвячено багато робіт, які є актуальними і сьогодні [13—15].

Для моделювання великих енергооб'єднань пропонується використовувати розподілене середовище і БД. На відміну від існуючих дискретних точкових методів розрахунку режимів енергосистем запропоновано перехід до апроксиматичних методів виконання розрахунків залежно від цілей, постановки завдань і вимог до результатів моделювання.

В основу АСВК покладено використання реляційної моделі структуризації оперативної інформації про параметри режимів і об'єкти ЕЕС у вигляді віртуальних реляційних таблиць у БД. Таке уявлення інформації про модель енергосистем та їх ЕК із вбудованою системою інтелектуальних тригерів сповіщення про кібератаки дозволить мінімізувати загальний час виявлення кібератак в різних місцях.

Як початкова інформація для роботи АСВК використовується достовірна і адекватна інформація про поточні режими роботи ЕЕС і (або) ОЕС, яка формується в центральній системі управління збору даних SCADA (System Control and Data Acquisition) ОЕС України і періодично (з дискретністю приблизно 3 хв) передається на сервер АСВК у вигляді так званих зрізів параметрів режиму і стану комутаційного обладнання для певних моментів часу після оцінки ситуації.

Режим роботи ЕЕС для будь-якого моменту часу описується системою рівнянь

$$[\dot{I}_s(t)] = [\dot{Y}_{ss}] [\dot{U}_s(t)], \quad (1)$$

де $\dot{Y}_{ss}$ — матриця вузлової провідності електричної мережі з комплексними елементами; $\dot{U}_s(t)$ — вектор-стовпець напруги вузлів; $\dot{I}_s(t)$ — вектор-стовпець заданих струмів вузлів; s — кількість вузлів. Якщо відомі

або задані потужності вузлів, то формулу (1) подають у наступному вигляді:

$$[\dot{S}_s(t)]^T = ([I_s(t)]^T [\hat{U}_s(t)]_d), \quad (2)$$

де $[\dot{S}_s(t)]^T$ — транспонований вектор заданих потужностей вузлів;
 $[I_s(t)]^T$ — транспонований вектор-стовпець заданих струмів вузлів;
 $[\hat{U}_s(t)]_d$ — діагональна матриця спряжених векторів напруги вузлів.

Системи (2) вирішуються за допомогою різних варіацій методів Ньютона або Гауса, рідше використовуються ітераційні методи визначення контурних струмів. Основна вимога до цих методів — забезпечити максимально швидкий (комфортний) час отримання результатів моделювання для виявлення умов кібератак. Тому використано багатоопорний метод розрахунку контурних струмів [6], який є дуже швидким для моделювання великих розподілених енергосистем. Ідея методу полягає в ітераційній процедурі еквівалентної заміни замкнутої електричної мережі на розімкнену, режим якої повністю співпадає з режимом початкової електричної системи. Реалізація контурної розрахункової моделі для розрахунку режимів електричної мережі передбачає автоматичне виділення в розрахунковій схемі мережі дерев і хорд.

Відомо, що загальний час отримання кінцевого результату розрахунку параметрів режиму роботи енергосистем залежить також від місця розташування модулів розрахунку (локально або віддалено), БД (локальне або віддалене і кластерне) і від способу зберігання та подання результатів (у оперативній пам'яті або у віддалених БД та серверах додатків). Для прискорення рішення нелінійних систем рівнянь (2) використовується зазвичай оперативна пам'ять. Проте для моделювання великих енергосистем доводиться використовувати тільки розподілені системи управління БД. Це може збільшити час реакції моделюючої АСВК і підсистеми відображення результатів моделювання, але не дуже критично для отримання достовірних результатів у комфортний час (до трьох секунд).

Програми перемикачів обов'язково попередньо розробляються для кожної підстанції і є унікальними, їх кількість для підстанцій напругою 110/35/10 кВ обчислюється сотнями. Кількість операцій (перемикачів або дій) в кожній програмі коливається в діапазоні від 20 до 100. В енергетиці України нині функціонують близько 30 ЕК, і кожна з них має приблизно 600 підстанцій із вказаною вище напругою. Така велика кількість програм перемикачів і операцій перемикачів часто призводить до помилок і обумовлює необхідність ефективної перевірки коректності складання бланків оперативних перемикачів.

Параметри режиму та стан обладнання частини схеми підстанції 750 кВ

Програми оперативних перемикань, які обов'язково використовуються для комутацій в електричних мережах, структуруються у вигляді формальної системи логічних правил певних дій типу «включити», «відключити», «оглянути» та ін. Також зазначається місце таких дій, тобто номер комірки, панелі тощо. Це дозволяє створити базу знань про перевірку умов виконаних або запропонованих операцій у вигляді системи простих правил «якщо щось сталося або виконано, то результат буде наступним», яка в подальшому використовується для аналізу різноманітних сценаріїв кібератак та їх впливу на об'єкти критичної інфраструктури.

Запропоновано та реалізовано три типи правил діалогового формування бази знань. Перший тип належить до операцій з наявним устаткуванням на підстанції, другий — до операцій з телефонними переговорами персоналу і третій — до операцій, які прямо не пов'язані з перемиканнями, наприклад рапорт керівництву. Передбачено можливість формування переліку необхідних операцій від імені персоналу, який безпосередньо виконує комутації, і за допомогою моделюючого комплексу, що дозволяє перевіряти можливість фізичного існування режиму для заданих конкретних умов і параметрів, коректність роботи релейного захисту і автоматики та прийняття до уваги різних зовнішніх збурень або відмов устаткування в заданий час і залежно від ситуації, що склалася.

Загальний алгоритм роботи АСВК полягає в наступному. Отримані від SCADA ОЕС України дані використовуються для розрахунку поточного режиму ОЕС і створення моделі чутливості до кіберзагроз. Результати

розрахунку параметрів режиму ОЕС аналізуються відносно можливості його фізичного існування, обчислюються коефіцієнти запасу статичної та динамічної стійкості, проводиться аналіз режиму для виявлення виникнення умов певного рівня вірогідності потенційної кіберзагрози.

На рисунку наведено фрагмент принципової електричної схеми типової підстанції 750/330/110/35/10/0.4 кВ з комутаційними елементами, які аналізуються в АСВК. За допомогою автоматизованого конструктора-редактора реалізовано можливість виділення окремих груп обов'язкових послідовностей дій, передбачених в програмах перемикачів, введенням умовних або обов'язкових поточних операцій з комутаційним устаткуванням і побудови різноманітних сценаріїв розвитку аварій.

Висновки

Розроблена АСВК з вбудованими функціями конструювання, редагування, створення і виявлення потенційно можливих сценаріїв кіберзагроз для об'єктів критичної інфраструктури може бути використана як на енергетичних підприємствах всіх рівнів ієрархічної системи керування, так і в науково-навчальних віртуальних тренажерних центрах сучасної професійної електронної системи навчання для дослідження та створення ефективних методів протидії. Конструктор створення сценаріїв кіберзагроз призначений для послідовного накопичення навчально-методичної бази підготовки оперативно-диспетчерського персоналу методам попередження і ліквідації кіберзагроз. Середовище розподіленого моделювання забезпечує широкі можливості для ефективного використання АСВК і дозволяє навчати персонал, задіяний в енергетиці, методам попередження кіберзагроз. Об'єднання можливостей сучасних методів електронного навчання та інструментальних програмних засобів розподіленого віртуального моделюючого середовища для виявлення кіберзагроз дозволяє отримати нову якість систем протидії кіберзагрозам об'єктів критичної інфраструктури.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Понимание киберпреступности: Руководство для развивающихся стран. Проект. [Электронный ресурс]. Режим доступа: http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFR.pdf. - Название с экрана.
2. Кобец Б.Б., Волкова И.О. Инновационное развитие электроэнергетики на базе концепции Smart Grid. М.: ИАЦ Энергия, 2010, 208 с.
3. Снижение рисков каскадных аварий в электроэнергетических системах / Отв. ред. Н.И. Воропай. Новосибирск: Изд-во СО РАН, 2011, 303 с. (Интеграционные проекты СО РАН; вып. 29).
4. Cyber-Attack Against Ukrainian Critical Infrastructure. Інформаційний ресурс. Назва з екрану <https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01>.

5. Inside the Cunnning. Unprecedented Hack of Ukraine's Power Grid. Інформаційний ресурс. Назва з екрану <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>
6. Аветисян Е.В., Гуреев В.А., Сангінова О.В. Розробка та застосування віртуальних ієрархічних структур для моделювання режимів, навчання і тренажу персоналу ОЕС України // Вісник вінницького політехнічного інституту, 2016, 1(124), с. 101—107.
7. Гуреев В.А., Сангінова О.В. Построение обучающего дистанционного тренажера для подготовки персонала энергетической отрасли // 36. наук. праць Ін-ту електродинамики НАН України, 2017, вип. 48, с. 52—58.
8. Чачко А.Г. Подготовка операторов энергоблоков: Алгоритмический подход. М.: Энергоатомиздат, 1986, 232 с.
9. Дозорцев В.М., Агафонов Д.В., Назин В.А и др. Компьютерный тренинг операторов: непреходящая актуальность, новые возможности, человеческий фактор // Автоматизация в промышленности, 2015, № 7, с. 8—20.
10. Kluge A., Sauer J., Schüler K., Burkolter D. Designing training for process control simulators: a review of empirical findings and current practices // Theoretical issues in ergonomics science, 2009, Vol. 10, No. 6, p. 489—509.
11. Крумм Л.А. Уравнения стационарного режима электрических систем с учетом статических характеристик нагрузки и генераторов и автоматического регулирования частоты, напряжения и мощности // Труды Таллинского политехнического института, 1957, № 12.
12. Фазылов Х.Ф., Удовиченко В.Б., Крамер Ю.М. Вопросы расчета установившихся режимов с учетом изменения частоты. Исследование решения на ЦВМ уравнений установившегося режима электрических систем. Ереван: Арм. НИИЭ, 1976.
13. Калюжный А.Х. Расчет режимов и статической устойчивости электроэнергетических систем с учетом изменения частоты. // Электричество, 1976, № 8.
14. Галкина Н.В., Ильина В.П., Конторович А.М. Методика и алгоритм определения предельных по статической устойчивости послеаварийных режимов с учетом изменения частоты. Труды ЛПИ «Электроэнергетика», 1976, № 350.
15. Баринев В.А., Совалов С.А. Определение установившихся режимов и апериодической устойчивости сложных электроэнергетических систем при учете частоты // Электричество, 1978, № 11.

Отримано 06.01.21

REFERENCES

1. Project “Understanding Cybercrime: A Guide for Developing Countries” (2009), available at: http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFR.pdf (accessed February 15, 2021).
2. Kobec, B.B. and Volkova, I.O. (2010), *Innovatsionnoye razvitiye elektroenergetiki na baze kontseptsii Smart Grid* [Innovative development of the electric power industry based on the concept Smart Grid], IAC Energiya, Moscow, Russia.
3. Voropai, N.I. (2011), *Snizheniye riskov kaskadnykh aviariy v elektroenergeticheskikh sistemakh* [Reducing the risks of cascade accidents in power systems], SO RAN, Novosibirsk, Russia.
4. Cybersecurity & Infrastructure Security Agency (2016), Cyber-Attack Against Ukrainian Critical Infrastructure, available at: <https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01> (accessed February 15 2021).
5. Inside the Cunnning. Unprecedented Hack of Ukraine's Power Grid (2016), available at: <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/> (accessed February 15 2021).

6. Avetisyan, E.V., Gurieiev, V.O. and Sanginova, O.V. (2016), "Development and application of virtual hierarchical structures for modeling regimes, training and coaching of UES personnel in Ukraine", *Visnyk vinnytskoho politekhnichnoho instytutu*, Vol. 1, no. 124, pp. 101-107.
7. Gurieiev, V.A. and Sanginova, O.V. (2017), "Construction of a remote training simulator for training energy industry personnel", *Zbirnyk naukovykh prats Instytutu elektrodynamiky NAN Ukrainy*, Vol. 48, pp. 52-58.
8. Chahko, A.G. (1986), *Podgotovka operatorov energoblokov: Algoritmicheskii podkhod* [Power Unit Operator Training: An Algorithmic Approach], Energoatomizdat, Moscow, Russia.
9. Dozortcev, V.M., Agafonov, D.V., Nazin, V.A. and others (2015), "Computer training of operators: enduring relevance, new opportunities, human factor", *Avtomatizatsiya v promyshlennosti*, Vol. 7, pp. 8-20.
10. Kluge, A., Sauer, J., Schüler, K. and Burkolter, D. (2009), "Designing training for process control simulators: a review of empirical findings and current practices", *Theoretical issues in ergonomics science*, Vol. 10, no. 6, pp. 489-509.
11. Krum, L.A. (1957), *Uravneniya statsionarnogo rezhima elektriche skikh sistem s uchetom staticheskikh kharakteristik nagruzki i generatorov i avtomaticheskogo regulirovaniya chastoty, napryazheniya i moshchnosti* [Equations of stationary mode of electrical systems taking into account the static characteristics of the load and generators and automatic control of frequency, voltage and power], Izdatelstvo Tallinskogo politekhnicheskogo instituta, Tallinn, Estonia.
12. Fazilov, X.F., Udovichenko, V.B. and Kramer, Y.M. (1976), *Voprosy rascheta ustanovivshikhsya rezhimov s uchetom izmeneniya chastoty. Issledovaniye resheniya na TSVM uravneniy ustanovivshegosya rezhima elektricheskikh sistem* [Issues of calculating steady-state modes taking into account the change in frequency. Investigation of the solution of the equations of the steady-state mode of electrical systems on a digital computer], NIIE, Erevan, Armenia.
13. Kalyzhniy, A.X. (1976), "Calculation of modes and static stability of electric power systems taking into account frequency changes", *Elektrichestvo*, Vol. 8, pp. 8-13.
14. Galkina, N.V., Ilina, V.P. and Kotorovoch, A.M. (1976), "Method and algorithm for determining the limiting static stability of post-emergency modes taking into account the change in frequency", *Trudi LPI "Elektroenergetika"*, Vol. 350.
15. Barinov, V.A. and Sovalov, C.A. (1978), "Determination of steady-state modes and aperiodic stability of complex electric power systems taking into account the frequency", *Elektrichestvo*, Vol. 11, pp. 10-16.

Received 06.01.21

V.O. Gurieiev, Y.M. Lysenko

TOPOLOGICAL METHOD FOR ASSESSING THE SENSITIVITY TO THE DETECTION OF CYBERSECURITY IN ELECTRICAL NETWORKS

The article discusses the theoretical issues of constructing a topological method for assessing the sensitivity to identifying cybersecurity in electrical networks of power systems, the way of modeling the operation modes of individual (selected) subsystems that arise during the operations. The main stages of building an algorithm for modeling the topology of electrical networks and systems are described, methods for generating information models of power supply systems and visualizing simulation results for conditions of occurrence of cybersecurity are proposed and implemented, ways to use the proposed approach to creating a cybersecurity sys-

tem for electrical networks of power systems and building scenarios for their elimination using the outlined training remote full-scale simulator are marked.

Key words: cybersecurity from regimes, modeling cybersecurity, operational switching. scenarios of anti-cybersecurity training.

ГУРЄЄВ Віктор Олександрович, канд. техн. наук, ст. наук. співроб. Ін-ту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. В 1974 р. закінчив Київський політехнічний ін-т. Область наукових досліджень — моделювання режимів роботи великих електроенергетичних систем і енергооб'єднань для комп'ютерних тренажерних систем.

ЛИСЕНКО Євген Миколайович, аспірант Ін-ту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. В 2002 р. закінчив Національний авіаційний університет. Область наукових досліджень — моделювання методів автоматизації комп'ютерних тренажерних систем.