doi:https://doi.org/10.15407/emodel.41.01.081

УДК 621.3.51

В.А. Гуреев, канд. техн. наук, **Е.Н. Лысенко**, аспирант, **Е.В. Аветисян**
Институт проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины
(Украина, 03164, Киев, ул. Генерала Наумова, 15,
тел. +380 44 424 91 60, e-mail:viktor.gurieiev@ipme.com.ua)

Моделирование и визуализация кибератак в энергетике с использованием компьютерных распределенных тренажерных систем

Рассмотрены вопросы синтеза статических и динамических видеограмм для параллельного отображения результатов моделирования режимов работы больших электроэнергетических систем и потенциальных кибератак с использованием распределенных тренажерных систем подготовки оперативно-диспетчерского персонала в энергетике. Предложена учебно-методическая база и дистанционные курсы по тематике киберугроз на объектах критической инфраструктуры, а также организация обучения и тренажерной подготовки по киберзащите.

К л ю ч е в ы е с л о в а: методы визуализации, режимы энергосистем, принципиальные схемы, видеограммы киберугроз.

В настоящее время не только в Украине, но и во многих развитых странах мира существуют большие угрозы несанкционированного воздействия на объекты критической структуры. В 2015 г. в результате кибератаки на электроснабжающие компании Западной и Центральной электроэнергетических систем (ЭЭС) Объединенной электроэнергетической системы Украины были выведены из работы одновременно несколько подстанций напряжением 110/10 кВ, в результате чего без электроэнергии остались 230 тысяч жителей [1—3].

В этой кибератаке были использованы все классические этапы киберразведки, а именно разведка и сбор данных с использованием вируса трояна BlackEnergy, перехват команд системы управления и сбора данных ((SCADA) System Control And Data Acquisition) на управление выключателями, создание условий для отключения потребителей в разных местах одновременно. На этапе ликвидации следов преступления осуществлялось отключение систем бесперебойного питания, удаление всей инфор-

мации с жестких дисков, повреждение архива SCADA для исключения возможности восстановления всего процесса кибератаки. Кибератака сопровождалась большим числом ложных телефонных звонков оперативно-диспетчерскому персоналу. Отсутствие в составе SCADA энергоснабжающих компаний надежных механизмов контроля за доступом к оперативной информации и мониторинга событий в реальном времени привело к успешной реализации кибератаки.

Как правило, цель кибератак — разрушить нормальную работу систем энергоснабжения посредством воздействия на различные системы управления энергетическим оборудованием объектов энергетики. В связи с важностью этой проблемы для всех сфер экономики страны принят Закон Украины «Об основных принципах обеспечения кибербезопасности Украины», вступивший в силу 9 мая 2018 г. [4]. Законодательный акт был разработан во исполнение требований Стратегии национальной безопасности Украины, утвержденной указом президента Украины от 15.03.2016 № 96 «О решении Совета национальной безопасности и обороны Украины» от 27 января 2016 г. «О Стратегии кибербезопасности Украины». В законе сформулированы основы национальной системы кибербезопасности и определены основные объекты критической инфраструктуры страны. Согласно закону президент Украины координирует деятельность в сфере кибербезопасности через возглавляемый им Совет нацбезопасности и обороны Украины.

Под кибербезопасностью понимают свойство защищенности активов от угроз конфиденциальности, целостности и доступности в киберпространстве [5, 6]. Киберпространство — это абстрактная виртуальная среда, не имеющая физического воплощения и сформированная в результате деятельности людей, функционирования программ и сервисов в сети Интернета с использованием виртуальных и коммуникационных технологий.

Вероятность повторных и более тяжелых кибератак на энергетику Украины очень высока. К сожалению, в настоящее время в энергетике отсутствует цельная стратегия обеспечения кибербезопасности объектов критической инфраструктуры. Не уделяется также должного внимания разработке программ тренажерной подготовки и обучения персонала методам распознавания, предотвращения и быстрой ликвидации кибератак.

Существующие методы визуализации результатов моделирования основаны на правилах динамического и (или) статического графического представления информации. Эти методы предназначены для адекватного отображения результатов моделирования событий и процессов в сложных системах управления и должны способствовать формированию и принятию оперативно-диспетчерским персоналом (ОДП) эффективных управ-

ляющих решений в нормальных штатных ситуациях, в сложных аварийных ситуациях и в случаях тщательно спланированных кибератак.

Важным свойством технологии производства и распределения электроэнергии является необходимость адекватной реакции персонала и систем управления на постоянные изменения топологии (конфигурации) электрических сетей, а также величины генерации и нагрузки у потребителей. Поэтому на практике, в реальных условиях эксплуатации энергосистем, ОДП очень трудно определить момент начала киберугрозы.

Все планируемые штатные изменения конфигурации ЭЭС контролируются специалистами режимных групп относительно допустимости возникающих в процессе коммутаций новых режимов. Но степень достоверности таких проверок не всегда позволяет учитывать критерии проверки на кибербезопасность. Возникает необходимость в разработке дополнительных методов и средств для предотвращения кибератак и их последствий. Все произошедшие киберугрозы должны быть тщательно исследованы, а полученные результаты анализа условий возникновения и создания таких угроз должны быть использованы для разработки новых подходов к созданию систем противодействия.

Исследование возможностей существующих алгоритмов, методов и средств синтеза статических и динамических видеограмм (визуализации) для отображения не только результатов моделирования режимов работы больших ЭЭС, но и возможных кибератак на объекты этих ЭЭС является важнейшей задачей. Ее решение позволит использовать эффективные распределенные тренажерные системы для формирования у персонала навыков не только ликвидации аварий, но и навыков распознавания условий возникновения киберугроз.

Постановка проблемы. Подсистемы моделирования и визуализации являются главными компонентами современных тренажерных систем, используемых для эффективного обучения, контроля знаний и тренажерной подготовки персонала в энергетике, включая систему повышения квалификации. Объектами распределенной среды моделирования являются источники энергии (атомные, гидравлические, тепловые, ветровые и солнечные электростанции), подстанции, открытые распределительные устройства и объединяющие их на большой территории электрические сети различных классов напряжения. При этом существует важная особенность энергетики — одновременность производства и потребления энергии потребителями.

В энергетике широко используются мнемонические диспетчерские щиты контроля и управления, цифровые измерительные приборы и другое оборудование. Для принятия правильных решений ОДП постоянно выполняет визуальный контроль и анализ большого количества информации.

ISSN 0204-3572. Electronic Modeling. 2019. V. 41. № 1

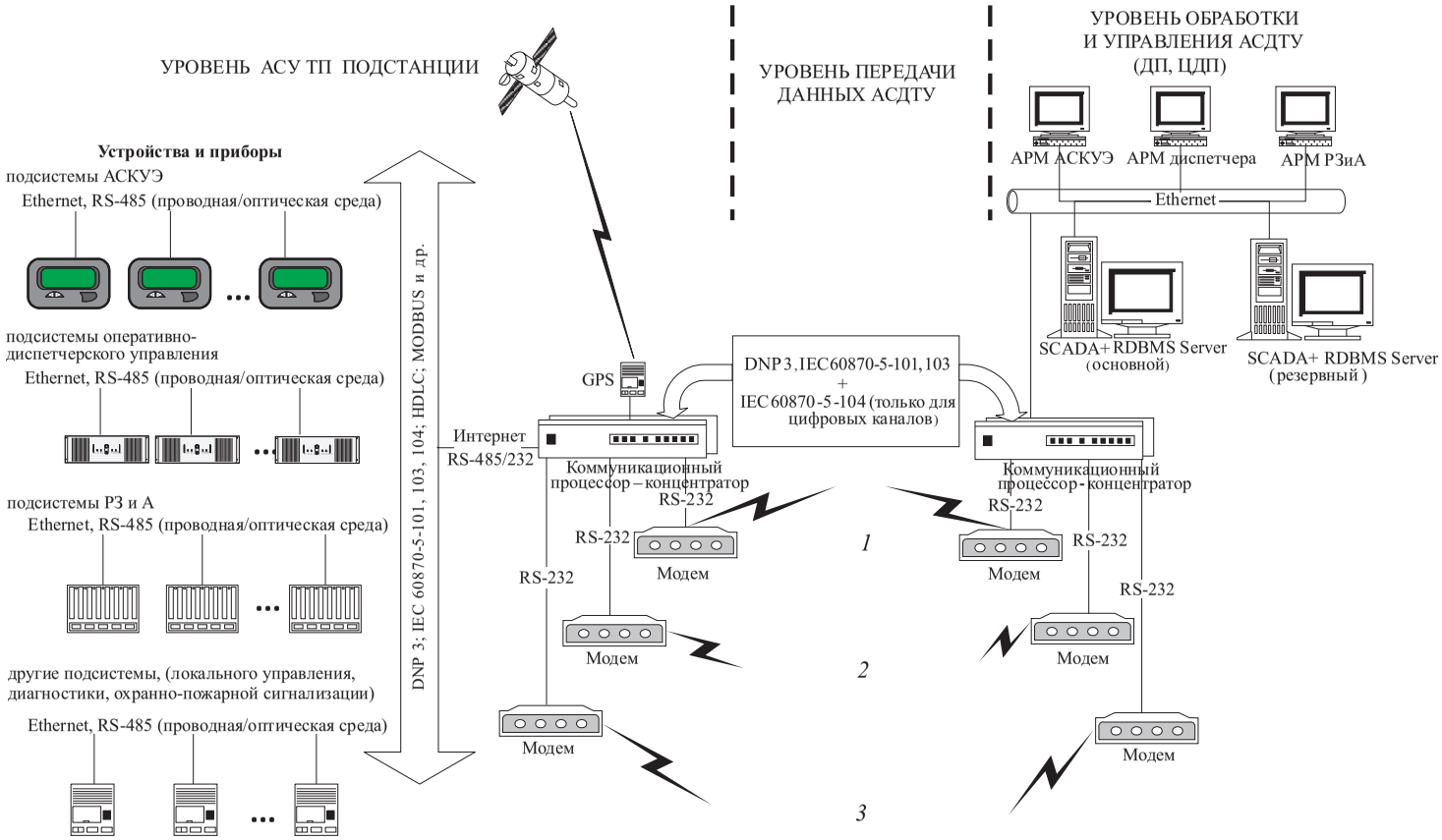

Рис. 1. Типовая архитектура системы управления в энергоснабжающих компаниях: *1*— радиоканалы (160-170 или 450 мГц) FSK 25/12 5 кГц 1200-9600 кбит/с криптозащита; *2* — ВЧ-каналы по ЛЭП (ТЧ-канал, 200-2400 бит/с; цифровой, 16-32 кбит/с и выше, криптозащита); *3* — кабельные каналы (ТЧ-канал, 1200-2400 бит/с; цифровой, 16-32 кбит/с и выше; Radio Ethernet; цифровой, 64 кбит/с и выше; сотовая связь; GSM, 9600 бит/с; GPRS, 14400 бит/с; CDMA, 9600 бит/с и выше криптозащита); АСКУЭ — автоматизированная система коммерческого учета электроэнергии; РЗ и А — релейная защита и автоматика

Типовая структура автоматизированной системы диспетчерского и технологического управления (АСДТУ) представлена на рис. 1.

Основные функции в реальном времени системы SCADA:

• сбор, обработка и хранение текущей информации от измерительных трансформаторов тока и напряжения, дискретной информации о состоянии коммутационных элементов подстанций;

• локальное и удаленное управление технологическим оборудованием на подстанциях;

• регистрация аварийных процессов;

• диагностика основного оборудования;

• ведение журналов системных событий, включая изменение параметров режима и состояние коммутационных элементов подстанций;

• визуализация информации в виде мнемосхем, графиков и др.;

• интерактивное взаимодействие с различными устройствами на подстанции с помощью стандартных интерфейсов и протоколов;

• интерактивное взаимодействие подсистемы SCADA с другими технологическими подсистемами с помощью стандартных баз данных.

Эксплуатация энергетического производства сопровождается формированием очень больших объемов самой разнообразной информации в реальном времени, которая с соответствующей отметкой времени сохраняется в SCADA архиве истории событий в виде срезов измеренных параметров режима и состояния коммутационных аппаратов. В процессе эксплуатации персонал непрерывно оценивает визуальную информацию, полученную от систем управления и сбора данных, которая позволяет уточнить цели и задачи управления. Для этого используется телефонная связь, результаты телеизмерений и телеинформация от SCADA систем в виде различных видеограмм.

Наиболее удобным является представление управляемого объекта в виде набора визуальных образов и принципиальных схем (рис. 2).

Вопросам визуализации посвящено большое число исследований как в нашей стране, так и за рубежом [7—11]. Большинство из них посвящено локальной визуализации результатов моделирования или измерения, когда программы решения задач и исходные данные для них находятся на одном компьютере. В этом случае используются разнообразные встроенные стандартные графические средства визуализации (Microsoft VISIO, Adobe Illustrator, CorelDraw и др.). Эти инструментальные средства визуализации невозможно использовать в виртуальных распределенных средах моделирования, когда и программы моделирования и исходные данные находятся в разных местах и могут быть объединены только с помощью виртуальных информационных технологий и интернета.

Под виртуальной средой моделирующей системы, используемой для подготовки персонала в энергетике, будем понимать совокупность распределенных систем серверов приложений и систем управления базами

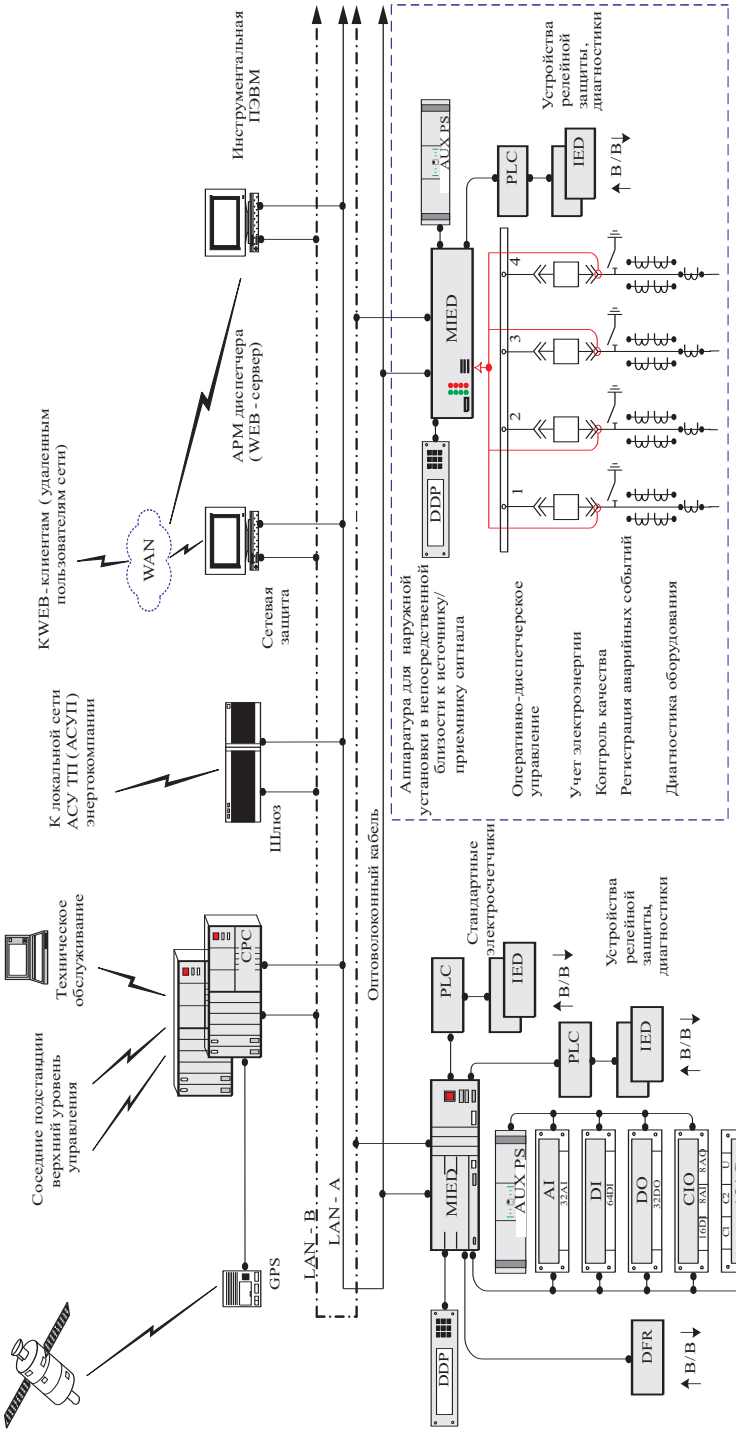

Рис. 2. Типовая архитектура систем управления подстанциями ЭЭС: AI, DI, DO, CIO, AIAC — семейство распределенных устройств ввода/вывода; CPC — коммуникационный процессор/концентратор; WAN — глобальная вычислительная сеть; PLC — контроллер с программируемой логикой; IED — интеллектуальное электронное устройство; MIED — многофункциональное интеллектуальное электронное устройство; DDP — дисплейная панель; AUX PS — источник питания для входных цепей; LAN — локальная вычислительная сеть; GPS — устройство ввода спутниковых сигналов точного времени; DFR — автономный регистратор аварийных событий

данных (СУБД), включая виртуальные, распределенную среду моделирования режимов работы ЭЭС, адаптивные интерактивные интерфейсы и учебно-методическое обеспечение для организации и проведения процессов обучения, повышения квалификации и тренажерной подготовки с учетом кибербезопасности.

В современных тренажерных системах подготовки персонала в энергетике используется принцип максимального подобия образов объектов визуализации реальным системам управления: диспетчерским щитам, панелям управления релейной защиты и автоматики, измерительным приборам, сигнализации и др. Визуальный анализ данных позволяет находить (идентифицировать) признаки и условия возникновения аварийных ситуаций (параметры и состояние) эксплуатируемого оборудования и выбирать степень детализации для получения необходимой дополнительной информации о вероятности возникновения аварии с требуемой точностью. Такие же признаки можно использовать для моделирования кибератак и обучения персонала методам противодействия им.

Важным условием успешной реализации программного инструментального продукта является правильный выбор базовых перечня и структур, динамически отображаемых на интерфейсных диалоговых видеограммах, элементов контроля и управления моделирующими системами. В разработанной распределенной тренажерной системе для ОДП высоковольтных подстанций и ЭЭС в качестве базовых динамических (контролируемых и управляемых) объектов визуализации выбраны все типы выключателей, заземляющих ножей, разъединителей, силовых шин подстанций, трансформаторов и др. Перечень и состав управляющих воздействий на динамические элементы определяется правилами оперативных переключений в электрических сетях и ЭЭС, а также должностными инструкциями. В тренажерной системе предусмотрена возможность расширения перечня управляемых объектов и систем управления до нужного уровня.

Человеко-машинный интерфейс реализованной системы тренажерной подготовки выполнен с помощью стандартных методов и средств типа диалоговых окон, выпадающих меню и всплывающих подсказок. Процесс подготовки сценариев штатных и противоаварийных тренировок автоматизирован и обеспечен встроенным редактором-конструктором. Визуализация результатов моделирования различных режимов работы энергосистем и этапов кибератак реализуется посредством отображения выбранных пользователем атрибутов элементов данных в свойства образов. Такое представление образов моделирования позволяет группировать большие объемы данных с целью более полного анализа исходных данных.

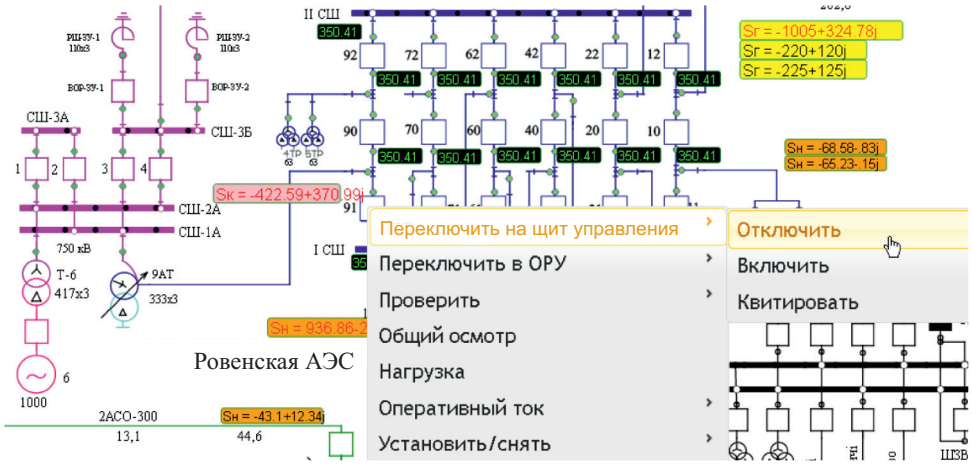

Рис. 3. Пример реализации человеко-машинного интерфейса в тренажерной системе: $S_г$ — заданная мощность генерации; $S_н$ — заданная мощность нагрузки; ОРУ — открытое распределительное устройство

Пример реализации разработанного метода визуализации представлен на рис. 3. Существующие полнофункциональные режимные тренажеры — самые эффективные средства обучения и тренажерной подготовки, но они очень дорогие и ориентированы, как правило, на моделирование конкретного энергетического оборудования (функционирующие АЭС, ТЭС, ЭС и др.). Это затрудняет перенос и применение полученных навыков и знаний по ликвидации аварий в подобные части больших ЭЭС.

В системе обучения и тренажерной подготовки большое значение имеют методы визуализации, которые в основном и определяют основные положения (принципы), содержание, формы и методы обучения. Обучение персонала (контроль знаний, тренажерная подготовка и формирование компетентностей) проводится с использованием разработанной для этой цели учебно-методической базы, которая включает рабочую программу организации обучения и семинаров, наборов дистанционных курсов по тематике оперативных переключений в электрических сетях, релейной защиты и автоматики, безопасных методов выполнения коммутационных операций в электрических сетях и на подстанциях, методов противопожарной безопасности и кибербезопасности [12]. Типовые сценарии штатных и аварийных противоаварийных тренировок дополняются результатами моделирования всех этапов несанкционированного доступа с требуемой степенью детализации.

Выводы

Существующие инструментальные программные методы и средства, используемые для визуализации результатов моделирования режимов работы различных объектов и систем энергетики, ориентированы в основном на локальное использование, т.е. в составе локального компьютера или группы сетевых компьютеров. В случае удаленного расположения компьютеров или баз данных необходимо использовать новые подходы к методам визуализации, основанные на новых возможностях виртуальных технологий для разработки алгоритмов удаленного синтеза и отображения видеограмм.

Разработанные алгоритмы, методы и средства визуализации могут быть использованы не только для формирования навыков ликвидации аварий на подстанциях и ЭЭС Украины, но и для формирования и поддержания навыков противодействия кибератакам в энергетическом секторе.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. *Analysis* of the Cyber Attack on the Ukrainian Power Grid. Інформаційний ресурс. Назва з екрану http://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
2. *Cyber-Attack* Against Ukrainian Critical Infrastructure Інформаційний ресурс. Назва з екрану https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01
3. *Inside* the Cunning, 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/
4. *Закон України* «Про основні засади забезпечення кібербезпеки України» від 05.10.2017. № 2163-VIII. Відомості Верховної Ради, 2017, № 45, ст.403.
5. *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.
6. *Кобец Б.Б., Волкова И.О.* Инновационное развитие электроэнергетики на базе концепции Smart Grid. М.: ИАЦ Энергия, 2010, 208 с.
7. *Аветісян О.В., Гурєєв В.О., Сангінова О.В.* Розробка та застосування віртуальних ієрархічних структур для моделювання режимів, навчання і тренажу персоналу ОЕС України // Вісн. Вінницького політехнічного інституту. 2016, 1(124), с. 101—107.
8. *Гуреев В.А., Сангинова О.В.* Построение обучающего дистанционного тренажера для подготовки персонала энергетической отрасли // Зб. наук. праць Ін-ту електродинаміки НАН України. Київ: ІЕД НАНУ, 2017, вип. 48, с. 52—58.
9. *Галактионов А.И.* Основы инженерно-психологического проектирования автоматизированных систем управления технологическими процессами. М.: Наука, 1978.
10. *Дозорцев В.М. и др.* Компьютерный тренинг операторов: непреходящая актуальность, новые возможности, человеческий фактор // Автоматизация в промышленности, 2015, № 7, с. 8—20.

11. *Kluge A. et al.* Designing training for process control simulators: a review of empirical findings and current practices // Theoretical issues in ergonomics science, 2009, Vol. 10, № 6, p. 489—509.
12. *The Art* of Computer Virus Research and Defense Інформаційний ресурс Назва з екрану https://www.amazon.com/The-Computer-Virus-Research-Defense/dp/0321304543/

Получена 26.11.18

REFERENCES

1. "Analysis of the Cyber Attack on the Ukrainian Power Grid", available at: http://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
2. "Cyber-Attack Against Ukrainian Critical Infrastructure Information resource", available at: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-0
3. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid", available at: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid
4. "The Law of Ukraine «On the Fundamental Ambush of the Firebugs of Ukraine»", *Vidomosti Verkhovnoi Radi*, No. 2163-VIII, (accessed 05.10.2017).
5. "Understanding Cybercrime: A Guide for Developing Countries. Project", available at: http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFR.pdf
6. Kobets, B.B. and Volkova, I.O. (2010), "Innovative development of electric power industry based on the concept of Smart Grid", IATs Energiya Moscow, Russia.
7. Avetisian, O.V., Gurieiev, V.O. and Sanginova, O.V. (2016), "Development and application of virtual hierarchical structures for modeling of modes, teaching and training of UES staff of Ukraine", *Visnyk Vinnytskogo politechnichnogo instytutu*, Vol. 1, no. 124, pp. 101-107.
8. Gurieiev, V.A. and Sanginova, O.V. (2017), "Construction of a training remote simulator for the training of personnel in the energy sector", *Zbirnyk naukovykh prats Instytutu elektodynamiky NAN Ukrainy*, no. 48, pp. 52-58.
9. Galaktionov, A.I. (1978), *Osnovy inzhenerno-psikhologicheskogo proektirovaniya avtomatizirovannykh system upravleniya tekhnologicheskimi protsessami* [Fundamentals of engineering and psychological design of automated process control systems], Nauka, Moscow, USSR.
10. Dozortsev, V.I., Agafonov, D.V. and Nazin, V.A. (2015), "Computing training of operator: nontransient urgency, new potentialities, human factor", *Avtomatizatsiya v promyshlennosti*, no. 7, pp. 8-20.
11. Kluge, A. (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.
12. "The Art of Computer Virus Research and Defense", available at: https://www.amazon.com/The-Computer-Virus-Research-Defense/dp/0321304543/

Received 26.11.18

В.О. Гурєєв, Є.М. Лисенко, О.В. Аветісян

МОДЕЛЮВАННЯ І ВІЗУАЛІЗАЦІЯ КІБЕРАТАК
В ЕНЕРГЕТИЦІ З ВИКОРИСТАННЯМ КОМП'ЮТЕРНИХ
РОЗПОДІЛЕНИХ ТРЕНАЖЕРНИХ СИСТЕМ

Розглянуто питання синтезу статичних і динамічних відеограм для паралельного відображення результатів моделювання режимів роботи великих електроенергетичних систем і потенціальних кібератак з використанням розподілених тренажерних систем підготовки оперативно-диспетчерського персоналу в енергетиці. Запропоновано навчально-методичну базу і дистанційні курси за тематикою кіберзагроз на об'єктах критичної інфраструктури, а також організація навчання і тренажерної підготовки по кіберзахисту.

К л ю ч о в і с л о в а: методи візуалізації, режими енергосистем, принципові схеми, відеограми кіберзагроз.

V.A. Gurieiev, Y.H. Lysenko, O.V. Avetisyan

SIMULATION AND VISUALIZATION OF CYBER ATTACKS IN THE ENERGY
SECTOR USING COMPUTER DISTRIBUTED TRAINING SYSTEMS

The article discusses current issues of the synthesis of static and dynamic video grams for a parallel display of the results of modeling the operation modes of large electric power systems (EPS) and potential cyber attacks using distributed training systems for training dispatch personnel in the power industry. An educational and methodical base and distance courses on cyber threats at critical infrastructure facilities are proposed. The organization of training and simulator training on the subject of cyber defense is focused on the use of the Scientific and Training Center Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine National Academy of Sciences of Ukraine. Refer. 12, fig. 3

K e y w o r d s: visualization methods, power system modes, schematic diagrams, videograms cyber threats.

ГУРЕЕВ Виктор Александрович, канд. техн. наук, докторант Ин-та проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины. В 1974 г. окончил Киевский политехнический ин-т. Область научных исследований — моделирование режимов работы больших электроэнергетических систем и энергообъединений для компьютерных тренажерных систем.

ЛЫСЕНКО Евгений Николаевич, аспирант Ин-та проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины. В 2002 г. окончил Национальный авиационный университет (г. Киев). Область научных исследований — моделирование методов автоматизации компьютерных тренажерных систем.

АВЕТИСЯН Елена Викторовна, инженер, директор учебного центра Научно-производственного общества с ограниченной ответственностью «Инфотех» (г. Киев). В 2002 г. окончила Национальный технический университет Украины «Киевский политехнический ин-т». Область научных исследований — моделирование режимов работы больших электроэнергетических систем, обучение и тренажерная подготовка оперативно-диспетчерского персонала, кибербезопасность электроэнергетических систем.