УДК 004.91

О. В. Иванченко, кандидат технических наук, доцент кафедры информационных систем и технологий Университета таможенного дела и финансов
К. В. Смоктий, кандидат экономических наук, доцент кафедры прикладной математики и теории систем управления Донецкого национального университета
О. Д. Смоктий, кандидат физико-математических наук, доцент кафедры прикладной математики и теории систем управления Донецкого национального университета
В. С. Харченко, доктор технических наук, заведующий кафедрой компьютерных систем и сетей Национального аэрокосмического университета им. Н. Е. Жуковского "Харьковский авиационный университет"

КОНЦЕПЦИЯ УПРАВЛЕНИЯ ГОТОВНОСТЬЮ КРИТИЧЕСКИХ ИНФРАСТРУКТУР НА ОСНОВЕ ПРИМЕНЕНИЯ ОБЛАЧНЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В работе изложены основные положения концепции управления готовностью критических инфраструктур, базирующиеся на комплексном решении задач мониторинга и контроля технического состояния критических инфраструктур (далее – КИ). Детальный анализ проблем обеспечения функциональной и информационной безопасности КИ подтвердил целесообразность использования аппарата аналитико-стохастического моделирования процессов изменения уровня надежности компонентных составляющих инфраструктурного образования. С целью обеспечения требуемого вычислительного ресурса и быстродействия выполняемых операций было предложено перейти из сферы традиционных информационных технологий в сферу облачных вычислений.

Ключевые слова: *критические инфраструктуры; облачные вычисления; критически важный объект.*

Наведено основні положення концепції управління готовністю критичних інфраструктур, що базуються на комплексному вирішенні завдань моніторингу і контролю технічного стану критичних інфраструктур (далі – КІ). Детальний аналіз проблем забезпечення функціональної та інформаційної безпеки КІ підтвердив доцільність використання апарату аналітико-стохастичного моделювання процесів

зміни рівня надійності компонентних складових інфраструктурного утворення. З метою забезпечення необхідного обчислювального ресурсу та швидкодії операцій було запропоновано перейти зі сфери традиційних інформаційних технологій до сфери хмарних обчислень.

Ключові слова: *критичні інфраструктури; хмарні обчислення; критично важливий об'єкт.*

The work is devoted to main features of availability management conception of the critical infrastructures. Authors proposed to use overall monitoring and control technical states system in order to solve this task. Detail analysis of ensuring of safety and security problems for critical infrastructures are used. Analytical and stochastic approach is performed as one of the best technique in order to determine reliability level of critical infrastructures components. Authors also proposed to transform the traditional information technologies management into cloud, because cloud computing faster and cloud infrastructures components have more power resource to solve different tasks.

Key words: *critical infrastructures; cloud computing; critical important object.*

Постановка проблемы. Одним из важнейших аспектов обеспечения национальной безопасности государства является эффективное использование по назначению критических инфраструктур (далее – КИ). Последствия аварий и инцидентов, произошедшие с участием КИ за последнее десятилетие, свидетельствуют о серьёзных проблемах, связанных с их функциональной безопасностью и надёжностью.

Дополнительным отрицательным фактором является ухудшение возможностей оперативного управления различными инфраструктурными образованиями в условиях враждебного несанкционированного информационного воздействия на кибернетические активы КИ. Это связано с тем, что хакерские атаки и различные виды информационного вмешательства, включая создание вредоносных ботсетей, целевой фишинг, создают условия, когда злоумышленникам удается влиять на общий процесс управления КИ. Как правило, такое негативное воздействие приводит к отключениям контура управления, возникновению опасных отказов компонентных составляющих КИ. Известно, что наиболее опасными являются отказы, обладающие каскадным эффектом, ущерб от которых может исчисляться сотнями миллионов долларов и в случае возникновения чрезвычайных ситуаций сопровождается человеческими жертвами.

Устранить эти серьезные проблемы, которые возникают фактически на "стыке" между функциональной и информационной безопасностью предлагается путём создания соответствующего научно-методического аппарата мониторинга информационно-технического состояния, оценки и контроля уровня готовности КИ. Для комплексной реализации подхода, базирующегося на совместном использовании данных оперативного и долгосрочного управления готовностью компонентных составляющих (активов) КИ, рекомендуется использовать облачные информационные технологии.

Анализ последних исследований и публикаций. Проанализируем результаты исследований по поддержанию требуемого уровня функциональной готовности на примере критической энергетической инфраструктуры (далее – КЭИ).

Известно [1], что по степени важности и приоритетности задач, решаемых в интересах обеспечения национальной безопасности, КЭИ занимают одно из лидирующих положений. Об этом свидетельствуют последствия крупнейших аварий, произошедшие за последние годы на АЭС Фукусима-1 (Япония, 2011 г.), Саяно-Шушенской ГЭС (Россия, 2009 г.) и др. Осознание того факта, что отказ элементов энергетической инфраструктуры может привести к человеческим жертвам, серьезным экологическим последствиям или финансовым потерям, обусловило актуальность применения формальных методов, основанных на выявлении потенциальных опасностей и оценке рисков их возникновения [2].

Серьёзные трудности, которые возникают в данной области, ещё раз подчёркивают необходимость углубленной проработки проблематики формализации задач управления готовностью КЭИ с учётом их структурного и иерархического построения [3]. Вопросы, связанные с разработкой формальных методов оценки уровня готовности инфраструктуры на основе аналитико-стохастических моделей надежности и функциональной готовности КЭИ, изложены в работах [4; 5].

Формализованное описание критической инфраструктуры в терминах генетической инженерии на основе комплементарного взаимодействия её систем и устройств, базирующееся на общих принципах анализа и управления безопасностью КИ [6], выполнено в работах [7; 8]. Следует отметить, что использование предложенного формального подхода осложняется динамичным развитием КЭИ. Это происходит вследствие наблюдающейся общей тенденции глобального роста объёмов потребляемой электроэнергии, что сопровождается расширением масштабов, сложности задач по её генерации, транспортировке, преобразованию и потреблению (рис. 1). В этих условиях чрезвычайную актуальность приобретают исследования, направленные на повышение энергоэффективности, профилирование спроса на электроэнергию, снижение затрат на её производство и контроль вредных выбросов в атмосферу [9].

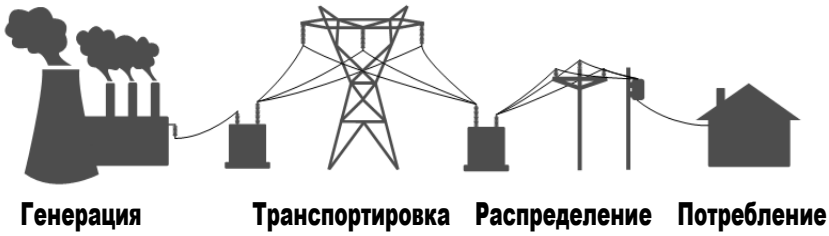

Рис. 1. Основные компоненты КЭИ [10]

Указанные проблемы и эволюционное развитие информационных технологий (далее – ИТ), реализуемых в информационно-управляющих системах КЭИ, послужили толчком для перехода к новому поколению Smart Grid энергосистем. По оценкам ведущих специалистов Smart Grid кластеры, представляющие собой интеллектуальную адаптивную распределенную сеть доставки энергии, позволяют существенно улучшить показатели энергоэффективности за счёт [11–13]:

1) повышения уровня информатизации сети, расширения её пропускной способности;

2) формирования справедливых сбалансированных цен на рынке розничной торговли электроэнергии, применения гибкой стратегии формирования тарифов;

3) оптимизации режимов использования электроэнергии на уровне различных потребителей, благодаря сглаживанию графиков пиковой нагрузки;

4) совместного применения технологий “умный счётчик” и интернета вещей;

5) предоставления потребителям возможности использовать различные восстанавливаемые источники энергии (солнечные батареи, ветрогенераторы и др.);

6) участия потребителей в процессе двухстороннего регулирования потоков энергии, то есть потребители принимают непосредственное участие в процессе управления режимами работы энергосистемы.

Реализация перечисленных возможностей базируется на результатах моделирования с использованием потоков данных о параметрах компонентных составляющих энергетической инфраструктуры, получаемых с помощью разветвленной сети датчиков (сенсоров). Элементами такой сети являются высокочувствительные датчики векторных измерений (далее – ДВИ) напряжения, тока и частоты сигналов, поступающих с выходных устройств подстанций КЭИ [14]. Использование ДВИ позволяет решать задачи мониторинга технических параметров объектов КЭИ в цифровом формате с высокой скоростью обновления информации от датчиков. Структурная схема измерительного модуля ДВИ представлена на рис. 2. Принцип функционирования ДВИ основан на измерении разности фаз между синхронизированными измерениями напряжения (тока) в точках передачи и приёма энергии [15]. Синхронизация показаний достигается применением устройств GPS навигации.

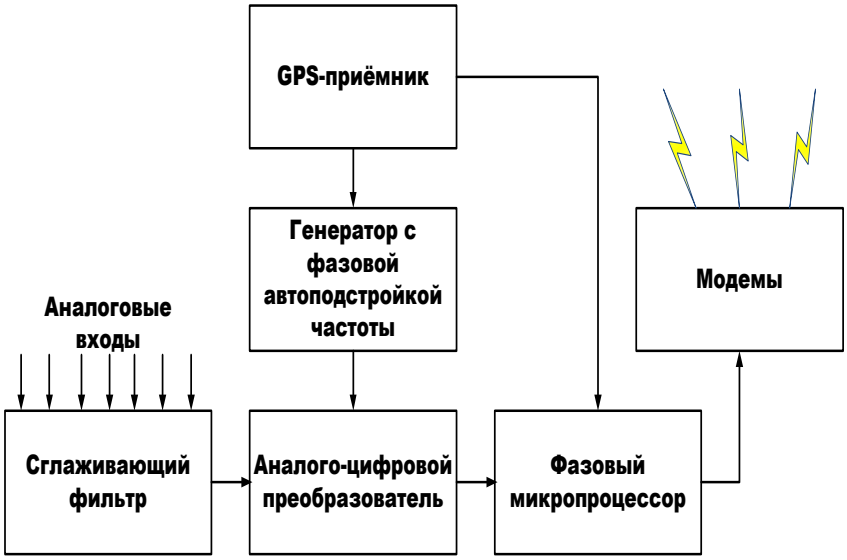

Рис. 2. Структурная схема измерительного модуля ДВИ [14]

Получив данные об изменении фазового угла между “стоком и истоком”, системный регулятор имеет возможность своевременно реагировать на негативные явления, происходящие в сети. В частности, на рис. 3 показано насколько увеличился фазовый угол для линии энергопередачи (далее – ЛЭП) Кливленд–Мичиган в течение 14 августа 2003 года, в период, когда произошла крупнейшая авария объединенной энергосистемы США и Канады.

Существенным преимуществом применения сети ДВИ является расширение возможностей использования данных мониторинга для решения задач оперативного управления готовностью КЭИ. Кроме того, эти данные могут быть записаны, сохранены и использованы для долгосрочного прогнозирования изменения уровня функциональной безопасности КЭИ. В перспективе данные сети ДВИ могут служить основой информационного обеспечения при разработке учебных сценариев, реализуемых на тренажно-имитационных комплексах и системах.

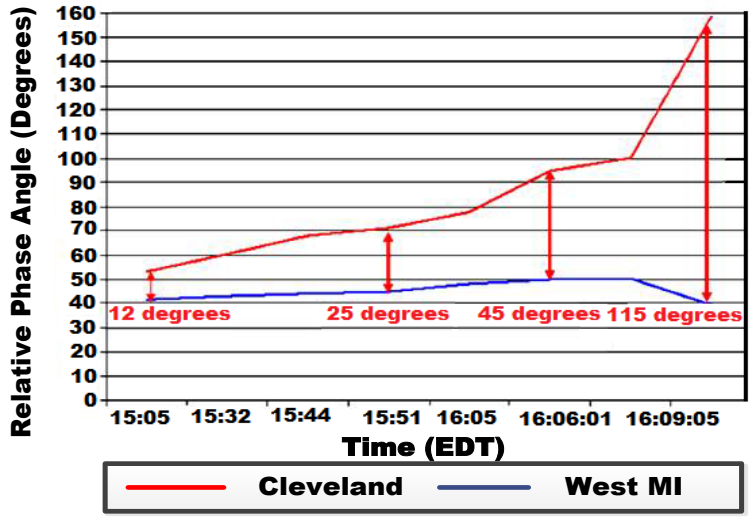

Рис. 3. Изменение фазового угла для ЛЭП Кливленд–Мичиган 14 августа 2003 г. [16]

Однако спектр технических инноваций, рассматриваемых для КЭИ, будет неполным и экономически нерентабельным, если не предусмотреть переход к наиболее перспективным ИТ на основе облачного компьютинга. Это подтверждается последними достижениями в области разработки ДВИ. В частности, американской фирмой Power Standards Lab разработан микро-ДВИ, с помощью которого при условии развертывания распределенной сети датчиков выполняются измерения сдвига фаз по напряжению (то есть фазового угла) на объектах КЭИ с точностью до 0,002 градуса. Такая точность измерений обеспечивается на расстоянии свыше 500 километров с частотой 4 миллиона измерений в секунду [17]. Разумеется, потоки данных сети микро-ДВИ, помимо их использования в режиме автома-

тизированного оперативного управления готовностью КЭИ должны быть определённым образом обработаны, сохранены и визуализированы для их последующего применения по назначению. На решение этих задач с использованием интеллектуальных распределенных облачных информационных технологий ориентирован совместный проект Корнельского университета и Университета штата Вашингтон. В рамках этого проекта планируется создание сервис-ориентированной программной платформы (GridControl) для поддержки решений по мониторингу информационно-технических состояний и контроля уровня готовности компонентных составляющих КЭИ [18].

Использование ДВИ открывает новые горизонты для разработки новых ИТ на основе применения результатов математического и имитационного моделирования. Это связано с тем, что потоки данных, поступающие с модулей ДВИ, позволяют качественно улучшить решение следующих задач:

1) с точностью до долей секунд регистрировать время изменения технических параметров, моменты возникновения сбоев и отказов компонентов КЭИ, что немаловажно для выполнения последующего анализа на основе полной хронологии событий;

2) в синхронизированном режиме отслеживать изменения технических параметров для всей совокупности контролируемых компонентных составляющих инфраструктуры, определяя их вклад в изменение уровня функциональной безопасности и готовности КЭИ;

3) отслеживать причинно-следственные связи между взаимосвязанными нарушениями функциональной готовности элементов и нарушениями режима соблюдения кибербезопасности КЭИ, устанавливая таким об-разом всю последовательность событий, повлекших за собой негативные последствия;

4) обоснование величины входных параметров для аналитико-стохастического моделирования процессов изменения уровня готовности и функциональной безопасности КЭИ с использованием облачных информационных технологий записи, хранения и считывания информации.

Существуют различные подходы и математические методы анализа функциональной безопасности КИ. Они описаны в работах [1; 3; 5; 19; 20; 21] применительно к энергетическим, аэрокосмическим, облачным инфраструктурам (ОИ) и базируются на математическом аппарате марковских, полумарковских случайных процессов, байесовских сетях и методах риск-анализа. Например, анализ процессов взаимного влияния отказов на основе эффекта “перетекания” рисков КИ выполнен в [22]. Анализ аварий и инцидентов КЭИ на основе применения принципа причинно-следственной декомпозиции динамических систем [23; 24] выполнен в [25].

Цель статьи. Таким образом, целью статьи является формирование и изложение единой концепции управления готовностью критических энергетических инфраструктур для обеспечения функциональной и информационной безопасности их компонентных составляющих на основе комплексного применения облачных информационных технологий.

Изложение основного материала. Известно [26; 27], что таксономия инфраструктурной взаимозависимости (рис. 4) базируется на трёх основных компонентных составляющих.

1. Кибернетическая инфраструктура (или киберинфраструктура), которая представляет собой важный коммуникативный и информационный базис. Использование специализированных кибернетических активов позволяет организовать и контролировать функционирование компонентных составляющих таксономической схемы.

2. Критическая инфраструктура является фундаментальной основой секторальной деятельности по предоставлению конкретных сервисов (услуг) для объектов физической инфраструктуры. Фактически различные виды КИ формируют и распределяют ключевые ресурсы между критически важными объектами (далее – КВО).

3. Физическая инфраструктура (ФИ) состоит из КВО, которые потребляют ключевые ресурсы, вырабатываемые критическими инфраструктурами. По сути ФИ является инфраструктурной надстройкой, обладающей конкретными физическими активами.

Рис. 4. Таксономическая схема инфраструктурной взаимозависимости в кибернетическом пространстве

На основе таксономии инфраструктурной взаимозависимости рассмотрим схему функционирования КЭИ, которая описывает работу компонентных составляющих традиционной энергетики больших мощностей (далее – ТЭБМ). Формально можно предположить, что КВО, которые входят в состав каждой инфраструктуры, образуют

её активы. Тогда упрощенная схема функционирования отечественных КЭИ, работающих в струк-туре ТЭ-БМ, может быть представлена в соответствии с рис. 5.

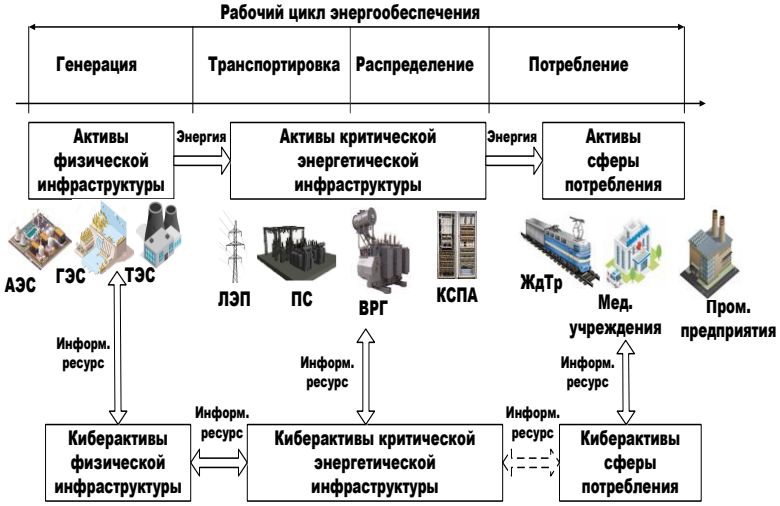

Рис. 5. Схема функционирования КЭИ в структуре ТЭБМ

Из рис. 5 видно, что каждый из этапов рабочего цикла ТЭБМ обеспечивается ограниченным информационно-вычислительным ресурсом, а именно:

1) этап генерации электроэнергии – кибернетическими активами ФИ;

2) этапы транспортировки и распределения электроэнергии – кибернетическими активами, используемыми для управления ключевыми ресурсами КЭИ;

3) этап потребления – кибернетическими активами, используемыми для управления физическими активами сферы потребления энергии.

Существенным недостатком ТЭБМ является фактическое отсутствие возможности обмениваться информационно-вычислительным ресурсом (далее информационным ресурсом) в цифровом формате между компонентными составляющими сферы потребления и КЭИ. Это оказывает негативное влияние на весь рабочий цикл энергообеспечения и порождает комплекс проблем, связанных: а) со снижением энергоэффективности; б) с отсутствием возможности оптимизировать режимы потребления электроэнергии; в) с необоснованным повышением тарифов на электроэнергию.

Серьёзной проблемой является дисбаланс между видом и объёмом производимой электроэнергии, определяющими её стоимость. Для устранения этой проблемы необходимо использовать сбалансированный комплексный подход, учитывающий экономическую и научно-техническую составляющие. Подтверждением этому являются действия правительства США в сфере энергетики после глобального отключения энергетической инфраструктуры в 2003 г. (Blackout) [16]. В частности, в период с 2003 по 2007 гг. были реализованы крупномасштабные инфраструктурные проекты и разработаны новые наукоёмкие стандарты для КЭИ [17; 18].

Анализ тенденций развития энергетического рынка Украины по данным ГП “Энергорынок” (рис. 6 и 7) свидетельствует, что, несмотря на лидерство атомной энергетики (АЭС) в объёмах производимой энергии (54 %), её вклад в формирование цены на энергию составляет всего 29,32 %, в то время как вклад тепловых электростанций (ТЭС, ТЭЦ) – почти 46 %.

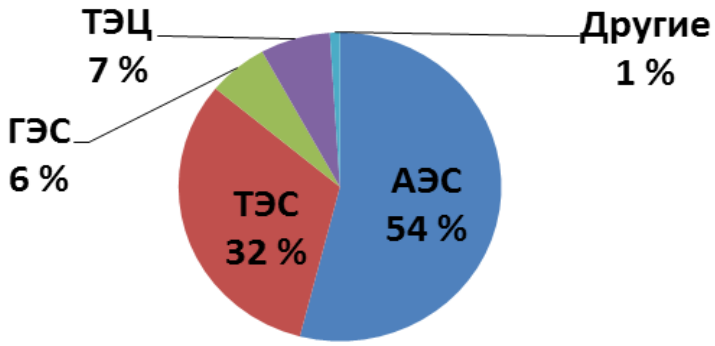

Рис. 6. Вклад видов генераций в общий объём производимой электроэнергии

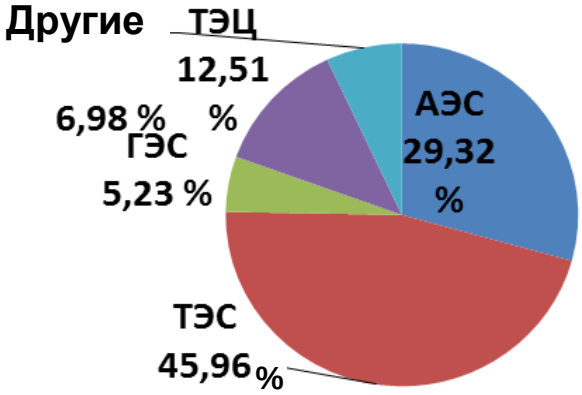

Рис. 7. Вклад видов генераций в стоимость электроэнергии

В сложившейся ситуации, когда особенно остро стоит вопрос обеспечения ТЭС, ТЭЦ антрацитовой группой угля, решить эту проблему может только реализация крупных инфраструктурных проектов, базирующихся на перспективной финансово-инвестиционной основе. К сожалению, в краткосрочной перспективе создать новые генерирующие мощности и соответствующее инфраструктурное обеспечение не представляется возможным. Но вполне реально в течение определённо-

го переходного периода внедрить отдельные элементы Smart Grid для КЭИ и инфраструктуры сферы потребления. На рис. 8 представлена упрощённая схема функционирования КЭИ в переходный период к ТЭБМ – Smart Grid.

Из рис. 8 видно, что главной отличительной особенностью такого инфраструктурного образования является расширенное применение модулей ДВИ, охватывающих основные объекты КЭИ (ЛЭП, подстанции, реакторные группы, коммутируемые вакуумными выключателями). Сеть ДВИ информационно обеспечивает работу двух систем, а именно:

1) системы мониторинга и контроля информационно-технического состояния критически важных объектов КЭИ и ФИ;

2) системы децентрализованного оперативного управления готовностью критически важных объектов КЭИ и ФИ.

Как было отмечено выше, существенной экономии будет способствовать оптимизация режимов энергопотребления благодаря применению smart-счётчиков, используемых в рамках концепции “умный дом” и “умный город”. В переходный период планируется также перевести все физические киберактивы в виртуальную часть облачной инфраструктуры. Операция трансформации ИТ менеджмента в сферу облачных вычислений реализуется в виде миграции киберактивов в облачную инфраструктуру [28]. В качестве облачного ресурса на основании известного опыта [18] были выбраны сервисы Amazon EC2 [29].

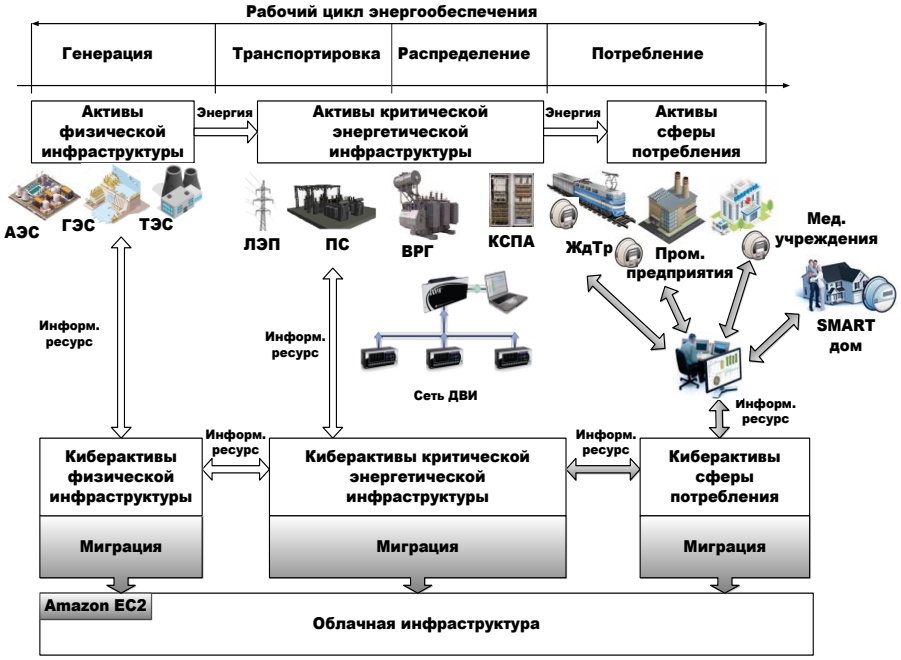

Рис. 8. Схема функционирования КЭИ в переходный период к ТЭБМ – Smart Grid

Использование сервисов ОИ Amazon EC2 позволит сэкономить значительную часть средств на содержание киберактивов инфраструктурных образований и расширит объём задач, решаемых с использованием информационного ресурса. Среди множества задач, которые предстоит решить, используя ОИ, наиболее актуальными являются:

1) создание информационно-вычислительного ресурса на основе модели виртуального приватного облака, в последующем разворачиваемого в виртуальную сеть (VPN) [30];

2) организация сбора данных и транспортной инфраструктуры VPN, архивация, фильтрация, пакетная обработка, хранение, обновление и визуализация данных в ОИ Amazon EC2 [18];

3) реализация комплекса мер по обеспечению кибербезопасности ОИ Amazon EC2 с использованием инструментария Splunk [31; 32].

Заключительный этап эволюционного развития КЭИ связан с реализацией концепции Smart Grid с комбинированными формами генерации, распределения, потребления потоков большой и малой мощности. Потоки малой мощности формируются с помощью возобновляемых источников энергии. На рис. 9 представлена упрощённая схема функционирования КЭИ в единой структуре ТЭБМ – Smart Grid.

Сравнительная оценка традиционной и активно-адаптивной сетей, используемых в ТЭБМ и Smart Grid энергетике, выполнена в [33]. Как видно из рис. 9 с переходом к единой структуре ТЭБМ – Smart Grid – весь информационный ресурс трансформируется в ОИ, что существенно расширяет возможности по оперативному управлению потоками мощности и регулированию частоты. Кроме того, предоставление облачного сервиса позволит записывать и хранить большие объёмы информации о технических параметрах всех участников рабочего цикла энергообеспечения, включая информацию о погодных условиях, солнечной активности, влажности, давлении в любой точке расположения элементов КЭИ. Благодаря использованию облачного ресурса и хранилищ появляется возможность отслеживать данные о выполняемых технологических операциях буквально на каждом объекте КЭИ в виде информации “полного контекста” с точностью до секунды.

Применение облачных сервисов Amazon EC2 в структуре ТЭБМ – Smart Grid – качественно улучшит информационную составляющую решения проблемы обеспечения функциональной и информационной безопасности КЭИ, поскольку появляется возможность получать в режиме реального времени (фактически без задержек) данные от сети ДВИ о параметрах критических важных объектов инфраструктуры, записывать, хранить, визуализировать и использовать их по назначению. В соответствии с [34] ОИ Amazon EC2 предоставляет широкий спектр сервисов на основе развёрнутого ресурса виртуальных машин (далее – ВМ). Поэтому эффективность облачных сервисов зависит от динамики роста цен на ресурс ВМ (высокая или низкая), от скорости подключения ВМ (высокая или низкая), а также от степени масштабируемости вычислительной мощности виртуальных машин (точная или грубая) [35].

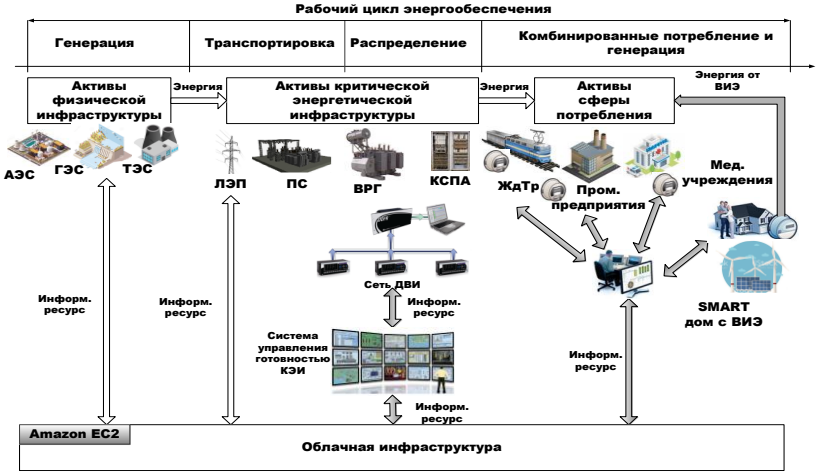

Рис. 9. Схема функционирования КЭИ в единой структуре ТЭБМ – Smart Grid

В табл. 1 представлена характеристика задач систем управления готовностью (далее – СУГ), мониторинга и контроля информационно-технического состояния (далее – ИТС) КЭИ (ФИ), решаемых с использованием ресурса виртуальных машин облачной инфраструктуры Amazon EC2.

Таблица 1

Характеристика задач, решаемых системами управления, мониторинга и контроля ИТС КЭИ (ФИ) с использованием ресурса облачной инфраструктуры Amazon EC2

№ п/п	Название системы	Выполняемые функции	Управляющее воздействие	ВМ Amazon EC2	
				Скорость подключения [35]	Степень масштабируемости [35]
1	2	3	4	5	6
1	Система децентрализованного оперативного управления готовностью КВО КЭИ	Техническое обслуживание и текущий ремонт по комбинированным стратегиям, изменение нагрузочных режимов и т. д.	Решение принимает обслуживающий персонал по результатам оценки и контроля уровня готовности КВО КЭИ	Высокая	Грубая

Окончание табл. 1

1	2	3	4	5	6
2	Система централизованного оперативного управления готовностью КВО КЭИ	Техническое обслуживание и текущий ремонт по регламентированным стратегиям, перераспределение нагрузки между ЛЭП для предотвращения каскадных отключений и т. д.	Команды управления вырабатываются в автоматизированном режиме АСУ ТП типа SCADA	Высокая	Грубая
3	Система централизованного долгосрочного управления готовностью активами КЭИ	Оценка рисков несанкционированного информационного воздействия на отдельные КВО инфраструктуры, тренинги обслуживающего персонала по конкретным сценариям протекания аварий и инцидентов и т. д.	Команды управления вырабатываются в автоматизированном режиме АСУ ТП типа SCADA	Высокая	Грубая
4	Система мониторинга и контроля ИТС КВО КЭИ (ФИ)	Анализ потоков данных, поступающих от сенсорных сетей ДВИ для / поддержания требуемого уровня готовности КВО КЭИ (ФИ), выявления фактов несанкционированного воздействия на кибератывы КЭИ (ФИ)	Решение на блокирование вредоносных кодов, программ, сетей принимает обслуживающий персонал АСУ ТП типа SCADA. Информационная поддержка обеспечивается с помощью инструментария Splunk	Высокая	Точная

В дополнение к табл. 1 следует отметить, что команды управления вырабатываются в автоматизированном режиме с использованием АСУ ТП типа SCADA с программным обеспечением, реализующим алгоритмы анализа причинно-следственных комплексов (далее – ПСК) протекания аварий, инцидентов КЭИ [25], а также алгоритмов оценки, контроля уровня функциональной готовности инфраструктуры по результатам марковского и полумарковского моделирования [2; 3; 5; 20; 21].

Рассматривая аспекты марковского, полумарковского моделирования (далее – ПММ) поведения критически важных объектов КЭИ, особо важное внимание следует уделить вопросам правильного понимания режимов стационарного и нестационарного

функционирования компонентных составляющих инфраструктуры. В тех случаях, когда на изделии (или КВО) проводится полный комплекс мероприятий технического обслуживания, мониторинга, контроля ИТС и ремонта, можно считать, что наблюдается процесс регенерации его уровня готовности, что приводит к разрежению участков с нестационарными выбросами. Соответственно, это способствует увеличению продолжительности участков со стационарным поведением. Кроме того, имеющие место потоки отказов и восстановлений разрежаются, что приводит к их трансформации в потоки Пуассона [5]. Только в этом случае можно сказать, что изделие находится на стационарном участке своего жизненного цикла, и применять аппарат моделирования эргодических марковских цепей [1; 4]. Оценку вероятностных показателей получают в результате решения уравнений Колмогорова для финальных вероятностей [20]. В противном случае, когда изделие находится на нестационарном участке, а изменение его ИТС описывается с помощью графа с поглощающими состояниями, необходимо решать систему дифференциальных уравнений Колмогорова. Только таким образом можно получить корректные количественные оценки вероятностных показателей КВО КЭИ [5]. Иной подход следует использовать при выполнении ПММ. Как правило, этот вид моделирования используется при сочетании явно выраженных детерминированных и стохастических интервалов времени. Например, интервалы мониторинга и контроля ИТС между сезонными предупредительно-профилактическими работами. В этом случае рекомендуется использовать аппарат моделирования ПММ с вложенными марковскими цепями [3; 21].

Взаимозависимость функциональной и информационной безопасности КЭИ [17] порождает новый класс задач, для решения которых необходимо применять принципиально новые подходы. Один из них основан на использовании причинно-следственных связей (далее – ПСС) [23; 24] между отказами, сбоями, инцидентами, авариями компонентов КЭИ и факторами несанкционированного воздействия (в виде хакерских атак, целевого фишинга) на киберактивы инфраструктуры. Предлагаемый подход реализуется в виде трёхфазного процесса.

1 фаза. Потоки данных от систем мониторинга и контроля ИТС (МКИТС) критически важных объектов КЭИ (ФИ) поступают в VPN, которая осуществляет сбор данных и выполняет функции транспортной инфраструктуры [18].

2 фаза. С выхода VPN данные поступают в ОИ Amazon EC2, где осуществляется их обработка с целью адаптации для участия в вычислительном процессе с использованием трёх подсистем ВМ (горячий, тёплый и холодный пулы). Результаты вычислительного процесса локализуются для визуализации на интерфейсах системы централизованного долгосрочного управления готовностью (СУГ ЦД) КЭИ.

3 фаза. Данные интерфейсов СУГ ЦД КЭИ используются специалистами по информационной безопасности (структурное подразделение входит в состав обслуживающего персонала АСУ ТП типа SCADA) для причинно-следственного анализа в соответствии с выполняемыми функциями (табл. 1). Возможные варианты действий обслуживающего персонала формируются в виде ПСК и отрабатываются для приобретения практических навыков, включая действия в нештатных ситуациях. Результаты применения ПСК регистрируются для дальнейшего применения в качестве сценариев тренингов обслуживающего персонала в экстремальных условиях. На рис. 10 представлена таксономическая схема управления готовностью КЭИ в структуре ТЭБМ – Smart Grid – на основе использования сервисов ОИ Amazon EC2.

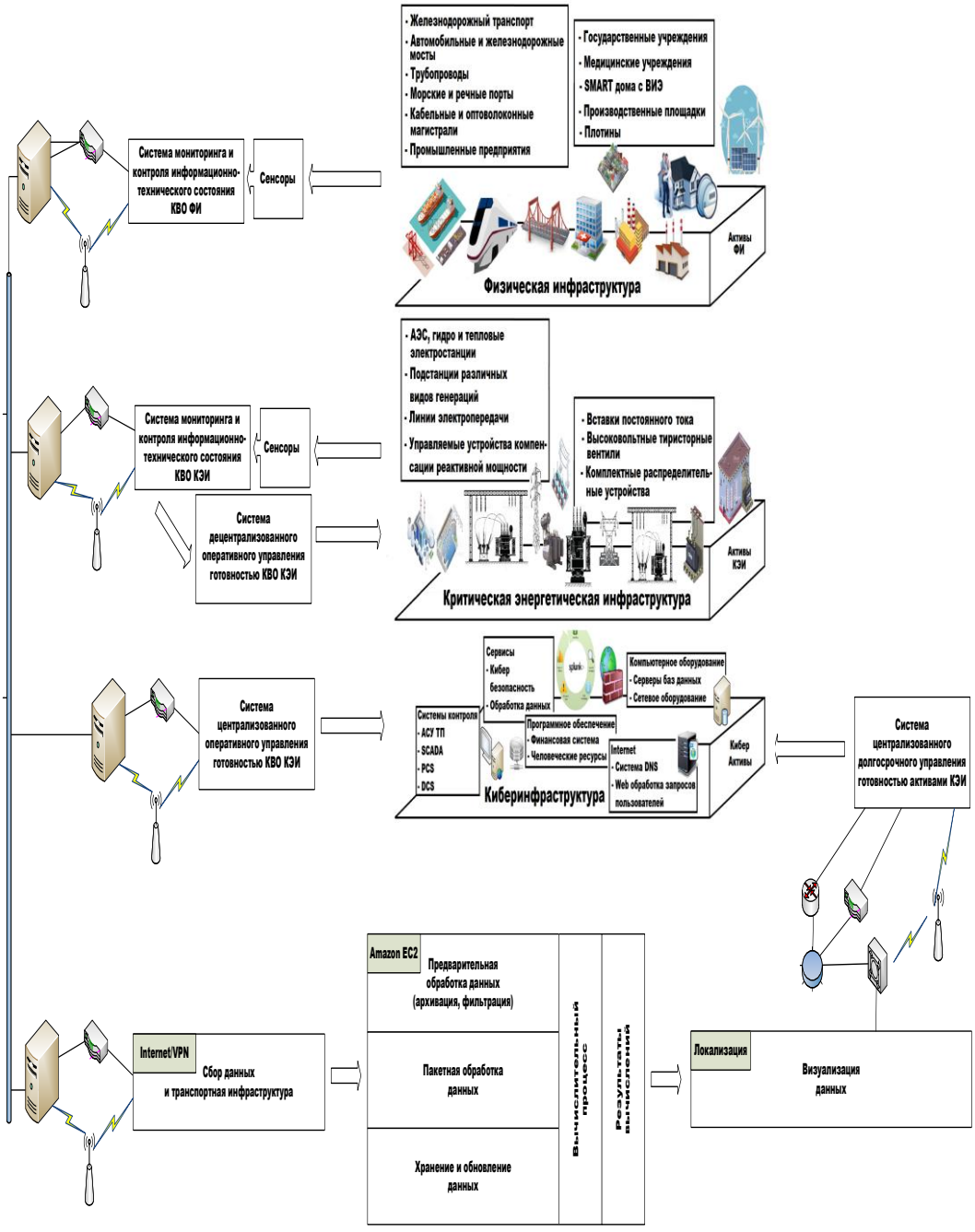

Рис. 10. Таксономическая схема управления готовностью КЭИ
в структуре ТЭБМ – Smart Grid

Объём дисковой памяти, который предоставляет Amazon, позволит записывать и хранить информацию в цифровом формате, поступающую от любой компонентной составляющей КВО КЭИ. Правильно структурированная цифровая информация может быть использована как для построения ПСК в масштабах КЭИ, так и для отдельно взятого блока, модуля и даже слота. Поэтому автоматизация процесса построения ПСК существенно расширит горизонты возможностей по обеспечению функциональной и информационной безопасности КЭИ.

Выводы из данного исследования и перспективы дальнейших исследований в данном направлении. Таким образом, сформулирована общая концепция управления готовностью критических инфраструктур, основные усилия от реализации которой направлены на обеспечение функциональной и информационной безопасности компонентных составляющих различных инфраструктурных образований. В рамках предложенной концепции рассмотрена возможность использования облачной инфраструктуры компании Amazon для архивации, фильтрации, пакетной обработки, хранения, обновления данных [18], поступающих от систем мониторинга и контроля ИТС инфраструктурных образований различного уровня.

Исходя из изложенного, перспективными являются следующие научные исследования и изыскания.

1. Анализ проблемы обеспечения надежности и безопасности критических инфраструктур.
2. Элементы методологии управления готовностью критических инфраструктур (на примере критической энергетической и облачной инфраструктур).
3. Модели и методы мониторинга информационно-технического состояния критических инфраструктур.
4. Аналитико-стохастические методы метамоделирования облачных инфраструктур.
5. Модели и методы управления готовностью критических инфраструктур с использованием облачных сервисов.
6. Облачные информационные технологии управления готовностью критических инфраструктур.

Список использованных источников:

1. Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения : монография / под ред. В. С. Харченко. – Х. : [Национальный аэрокосмический университет им. Н. Е. Жуковского “ХАИ”], 2011. – 641 с.

2. Ivanchenko O. Management of critical infrastructures based on technical megastate / O. Ivanchenko, V. Kharchenko, A. Skatkov // Information and Security. – 2012. – Vol. 28. – P. 37–51.

3. Скатков А. В. Информационные технологии для критических инфраструктур / под ред. А. В. Скаткова ; Министерство образования и науки Украины. – Севастополь : Севастопольский национальный технический университет, 2012. – 306 с.

4. Скопинцев В. А. Качество электроэнергетических систем: надёжность, безопасность, экономичность, живучесть / Скопинцев В. А. – М. : Энергоатомиздат, 2009. – 322 с.

5. Распределенные критические системы и инфраструктуры : учеб. пособие / О. В. Иванченко, В. С. Ловягин, Е. Н. Мащенко и др. ; под ред. А. В. Скаткова, В. С. Харченко. – Х. : Национальный аэрокосмический университет им. Н. Е. Жуковского "ХАИ", Севастопольский национальный технический университет, 2013. – 179 с.

6. Харченко В. С. Принципы анализа и управления безопасностью критических инфраструктур / В. С. Харченко, О. Н. Одарущенко, О. В. Иванченко // Вісник Хмельницького національного університету. – 2010. – № 5. – С. 218–221.

7. Паун Г. ДНК – компьютер. Новая парадигма вычислений : пер. с англ. / Паун Г., Розенберг Г., Саломаа А. – М. : Мир, 2003. – 528 с.

8. Харченко В. С. Методология FMECA: новая парадигма анализа видов и последствий отказов критических инфраструктур / В. С. Харченко, О. В. Иванченко, Е. Н. Мащенко // АПИР-2010 : материалы международной науч.-практ. конф. – Севастополь, 2010. – С. 142–145.

9. Xi Fang Smart Grid – The New and Improved Power Grid / A Survey, Xi Fang, Satyajayant Misra, Guoliang Xue // IEEE Communications Surveys & Tutorials. – 2012. – Vol. 14. – P. 944–980.

10. Scott Paul Distributed Coordination and Optimisation of Network-Aware Electricity Prosumers [Электронный ресурс] / Scott Paul // A thesis submitted for the degree of Doctor of Philosophy of the Australian National University. – Режим доступа : https://openresearch-repository.anu.edu.au/bit-ream/1885/110027/1/Scott%20Thesis%202016.pdf

11. Jianping He Optimal Investment for Retail Company in Electricity Market / Jianping He, Lin Cai, Peng Cheng, Jialu Fan // Industrial Informatics IEEE Transactions on. – 2015. – Vol. 11. – P. 1210–1219.

12. Hamid Gharavi Four-way Handshaking Protection for Wireless Mesh Network Security in Smart Grid / Hamid Gharavi, Bin Hu // Global Communications Conference (GLOBECOM) 2013 IEEE. – 2013. – P. 790–795.

13. Yu Wang Analysis of solar generation and weather data in smart grid with simultaneous inference of nonlinear time series / Yu Wang, Guanqun Cao, Shiwen Mao, R. M. Nelms // Computer Communications Workshops (INFOCOM WKSHPS) 2015 IEEE Conference. – 2015. – P. 600–605.

14. Kunkolienkar G. R. Phasor Measurement Units for Power System [Электронный ресурс] / G. R. Kunkolienka, Jayesh G. Priolkar. – Режим доступа : http://www.electricalindia.in/blog/post/id/8522/phasor-measurement-units-for-power-systems

15. Giani Anarita Cyber-Security of Wide Area Protection System [Электронный ресурс] / Giani Anarita. – Режим доступа : http://cnls.lanl.gov/~chertkov/ SmarterGrids/Talks/Giani.pdf

16. Final Report on the August 14, 2003 Blackout in the United States and Canda: Causes and Recommendation [Электронный ресурс] / U.S. – Canada Power System Outage Task Force. – Режим доступа : https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf

17. Fairley P. Sniffing Out Grid Attacks / P. Fairley // IEEE Spectrum. – September, 2016. – P. 13–15.

18. GridControl: A Software Platform to Support the Smart Grid [Электронный ресурс] / Cornell University Computer Science. – Режим доступа : http://www.cs.cornell.edu/projects/gridcontrol/index.html

19. Иванченко О. В. Анализ стохастических методов метамоделирования и оценивания готовности облачных инфраструктур / О. В. Иванченко, В. С. Харченко // Радіоелектронні і комп'ютерні системи. – 2016. – Вип. 6 (80) . – С. 6–10.

20. Основы зеленой ИТ-инженерии. Моделирование облачных систем : учеб. пособие / В. С. Харченко, А. В. Дрозд, Ю. Л. Поночовный и др. – Х. : Нац. аэрокосмический ун-т им. Н. Е. Жуковского "ХАИ", 2016. – 168 с.

21. Ivanchenko O. V. Semi-Markov Availability Models for an Infrastructure as a Service Cloud with Multiple Pools [Электронный ресурс] / O. V. Ivanchenko, V. S. Kharchenko. – Режим доступа : http://ceur-ws.org/Vol-1614/paper_116.pdf.c

22. Харченко В. С. Безопасность информационно-управляющих систем и инфраструктур. Модели, методы и технологии / Харченко В. С., Скляр В. В., Брежнев Е. В. – Германия : Palmarium Academic Publishing, 2013. – 528 с.

23. Резчиков А. Ф. Принцип причинно-следственной декомпозиции динамических систем / А. Ф. Резчиков, В. А. Твердохлебов. – Саратов : Наука, 2013. – 56 с.

24. Резчиков А. Ф. Причинно-следственные модели производственных систем / А. Ф. Резчиков, В. А. Твердохлебов. – Саратов : Наука, 2008. – 137 с.

25. Иванченко О. В. Метод причинно-следственной декомпозиции аварий и инцидентов критических инфраструктур / О. В. Иванченко, В. С. Харченко // Радіоелектронні і комп'ютерні системи. – 2014. – Вип. 5 (69). – С. 12–17.

26. Agcaoili Phil Cybersecurity: The Executive Order – Defining the Internet Security Ecosystem [Электронный ресурс] / Phil Agcaoili. – Режим доступа : https://www.slideshare.net/philipagcaoili/cy-sec3

27. Potii O. V. Cybersecurity in Ukraine: Problems and Perspectives [Электронный ресурс] / O. V. Potii, O. V. Korneyko, Yu. I. Gorbenko // Information and Security. – 2015. – Vol. 32. – Режим доступа : https://connections-qj.org/32.01_potii_ korneyko_gorbenko.pdf

28. Take Control of Your Data Center Migration and Consolidation Efforts with ExtraHop [Электронный ресурс] / White Paper. – Режим доступа : http://docs.media.bitpipe.com/io_13x/io_135695/item_1489885/Migration%20and%20Consolidation%20With%20ExtraHop%20Whitepaper.pdf

29. Amazon EC2 [Электронный ресурс] / Безопасные масштабируемые вычислительные мощности в облаке. – Режим доступа : https://aws.amazon.com/ru/ec2

30. Adding a Hardwar Virtual Private Gateway to Your VPC [Электронный ресурс] / Amazon Virtual Private Cloud. – Режим доступа : http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html

31. Gartner: Start security monitoring in the public cloud [Электронный ресурс] / NETWORKWORLD from IDG. – Режим доступа : http://www.networkworld.com/article/2167209/security/gartner--start-security-mo-nitoring-in-the-public-cloud.html

32. Enhance AWS Security with Splunk Solutions [Электронный ресурс] / An AWS and Splunk White Paper. – Режим доступа : http://docs.media.bitpipe.com/io_12x/io_127953/item_1384169/enhance-aws-security-with-splunk-solutions.pdf

33. Smart Grid или умные сети электроснабжения [Электронный ресурс] / ЭНЭКА инженерно-консалтинговая компания. – Режим доступа : http://www. eneca.by/ru_smartgrid0

34. Cheng Wang Identification and Empirical Analysis of Amazon EC2 Spot Instance Features for Cost-Effective Tenant Procurement [Электронный ресурс] : Technical report CSE-16-006 / Cheng Wang, Qianlin Liang, Bhuvan Urgaonkar. – Режим доступа : http://www.cse.psu.edu/research/publications/tech-reports/2016/CSE-16-006.pdf

35. Cheng Wang Navigating the public cloud labyrinth: A study of price capacity and scaling granularity trade-offs [Электронный ресурс] / Cheng Wang, Bhuvan Urgaonkar, Aayush Gupta, Qianlin Liang Technical report CSE-16-002. – Режим доступа : http://www.cse.psu.edu/research/publica-tions/tech-reports/2016/CSE-16-002.pdf

✧ ✧ ✧ ✧ ✧ ✧ ✧

UDC 004.054

B. I. Moroz, Doctor of Engineering Science,
Head of the Information System and Technology Department, University of Customs and Finance
A. O. Holtvianskyi, Postgraduate Student,
University of Customs and Finance

INDUSTRIAL GAS STOCK MANAGEMENT PROBLEM

This article outlines the problem of inventory management of industrial gases in the warehouses of enterprises that are engaged in their production as one of the key problems in economic activities of any enterprise of this kind. The analysis of modern approaches to address inventory management problems of industrial gases in the warehouses of the enterprise. The analysis of the formation of stocks of industrial gases, and the need to manage them in order to obtain the highest profit. Based on this analysis