НАУЧНО-ИЗДАТЕЛЬСКИЙ ЦЕНТР «АКАДЕМИЯ ЕСТЕСТВОЗНАНИЯ»

SCIENTIFIC PUBLISHING CENTER «ACADEMY OF NATURAL HISTORY»

НАУЧНОЕ ОБОЗРЕНИЕ • ТЕХНИЧЕСКИЕ НАУКИ № 4

SCIENTIFIC REVIEW • TECHNICAL SCIENCES 2019

Журнал Научное обозрение. Технические науки зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций. Свидетельство ПИ № ФС77-57440
ISSN 2500-0799

Учредитель, издательство и редакция: НИЦ «Академия Естествознания», Почтовый адрес: 105037, г. Москва, а/я 47 Адрес редакции: 410056, г. Саратов, ул. им. Чапаева В.И., д. 56

Founder, publisher and edition: SPC Academy of Natural History, Post address: 105037, Moscow, p.o. box 47 Editorial address: 410056, Saratov, V.I. Chapaev Street, 56

Подписано в печать 02.08.2019
Дата выхода номера 02.09.2019
Формат 60×90 1/8

Типография НИЦ «Академия Естествознания», 410035, г. Саратов, ул. Мамонтовой, д. 5

Signed in print 02.08.2019
Release date 02.09.2019
Format 60×90 8.1

Typography SPC «Academy Of Natural History» 410035, Russia, Saratov, 5 Mamontovoi str.

Технический редактор Байгузова Л.М.
Корректор Галенкина ЕС.

Тираж 1000 экз.
Распространение по свободной цене
Заказ НО 2019/4

Журнал «НАУЧНОЕ ОБОЗРЕНИЕ» выходил с 1894 по 1903 год в издательстве П.П. Сойкина. Главным редактором журнала был Михаил Михайлович Филиппов. В журнале публиковались работы Ленина, Плеханова, Циолковского, Менделеева, Бехтерева, Лесгафта и др.

Journal «Scientific Review» published from 1894 to 1903. P.P. Soykin was the publisher. Mikhail Filippov was the Editor in Chief. The journal published works of Lenin, Plekhanov, Tsiolkovsky, Mendeleev, Bekhterev, Lesgaft etc.

М.М. Филиппов (M.M. Philippov)

С 2014 года издание журнала возобновлено Академией Естествознания

From 2014 edition of the journal resumed by Academy of Natural History

НАУЧНОЕ ОБОЗРЕНИЕ • ТЕХНИЧЕСКИЕ НАУКИ

SCIENTIFIC REVIEW • TECHNICAL SCIENCES

www.science-education.ru

2019 г.

В журнале представлены научные обзоры, литературные обзоры диссертаций, статьи проблемного и научно-практического характера

The issue contains scientific reviews, literary dissertation reviews, problem and practical scientific articles

СОДЕРЖАНИЕ

CONTENTS

СТАТЬЯ

УДК 004.4

ПРОЕКТИРОВАНИЕ ВЕБ-ПРИЛОЖЕНИЯ «SKYINFO» ДЛЯ УЧЕТА И НАПОМИНАНИЯ ПРИЕМА ЛЕКАРСТВ

Гребнева Д.М., Медведев К.А.

Нижнетагильский государственный социально-педагогический институт (филиал) Российского государственного профессионально-педагогического университета, Нижний Тагил, e-mail: grebdash@gmail.com

В статье описан процесс проектирования веб-приложения «SKYINFO» для учета и напоминания приема лекарств в терминах объектно-ориентированного подхода. Актуальность проектирования такого рода веб-приложения заключается в его востребованности разными целевыми аудиториями. Цель статьи – предложить проект веб-приложения в нотации UML. Концептуальная модель веб-приложения представлена в виде диаграммы вариантов использования. Обозначенные варианты использования описаны и детализированы в форме диаграмм последовательности. Структура backend веб-приложения представлена в виде диаграммы, на которой выделены четыре класса (администратор, пользователь, уведомления, лекарства) с необходимыми атрибутами, функциями и связями. Диаграмма классов была взята за основу создания базы данных, которая реализована в системе управления базами данных MySQL с помощью веб-интерфейса PhpMyAdmin. Пользовательский интерфейс спроектирован в виде набора связанных между собой веб-страниц: в работе представлена логическая модель, а также стилевое оформление веб-приложения для учета и напоминания приема лекарств. Представленные в статье материалы могут быть интересны студентам, изучающим проектирование и разработку веб-приложений, и использованы как основа для реализации подобного рода веб-приложений для уведомления пользователей о значимых событиях.

Ключевые слова: проектирование, веб-приложение, объектно-ориентированный подход, универсальный язык моделирования, UML

DESIGNING THE WEB APPLICATION «SKYINFO» FOR ACCOUNTING AND REMINDING FOR MEDICATIONS

Grebneva D.M., Medvedev K.A.

Nizhny Tagil State Social and Pedagogical Institute (branch) of Russian State Vocational Pedagogical University, Nizhny Tagil, e-mail: grebdash@gmail.com

The article describes the process of designing a web application «SKYINFO» for accounting and reminding for medications in terms of the object-oriented approach. The urgency of designing the web application of such type lies in its relevance to different target audiences. The purpose of the article is to propose a web application project in UML notation. The conceptual model of a web application is presented in the form of the use-case diagram; the indicated use cases are described and detailed in the form of sequence diagrams. The backend structure of the web application is presented in the form of the class diagram, which identifies four classes (administrator, user, notifications, medications) with the necessary attributes, functions and connections. The class diagram is taken as the basis for creating the database, which was implemented in the MySQL database management system with the help of PhpMyAdmin. The user interface is designed as a set of interconnected web pages: the work presents a logical model, as well as the styling of a web application for accounting and reminder for medications. The materials presented in the article may be of interest to students studying the design and development of web applications and to be used as the basis for the implementation of this kind of web applications to notify users about significant events.

Keywords: design, web application, object-oriented approach, universal modeling language, UML

В настоящее время большинство людей регулярно принимают различные лекарственные препараты и витамины. Как известно, в большинстве случаев для получения оптимального эффекта от приема лекарств требуется их употребление по определенной схеме, графику. Как показывает проведенный нами опрос среди различных возрастных категорий, многие люди периодически забывают вовремя принять препарат, что может привести к снижению эффективности от его приема, а также отразиться на здоровье человека в целом.

Современные информационные технологии способствуют решению обозначенной проблемы. Например, уже сегодня на рынке программных продуктов представлены такие мобильные приложения, как Roundhealth, Mr. Pillster, Mytherapy и другие, цель которых напоминать пользователю о необходимости приема лекарств [1–3]. Недостатком рассмотренных приложений является отсутствие мультиплатформенности. В свою очередь, веб-приложения лишены данного недостатка и могут использоваться на мобильных устройствах с любой операционной системой. Таким образом, можно сделать вывод об актуальности разработки специализированного веб-приложения «SKYINFO» с системой

отправки уведомлений о необходимости принять лекарство.

Цель исследования: проектирование веб-приложения для учета и напоминания приема лекарств «SKYINFO».

Материалы и методы исследования

Для разработки проекта «SKYINFO» используется объектно-ориентированная методология проектирования информационных систем, основу которой составляет объектно-ориентированная концепция представления моделей предметной области в форме классов, обладающих структурными свойствами и поведением [4].

Результаты исследования и их обсуждение

В результате анализа предметной области было составлено формальное описание процесса напоминания пользователю о необходимости приема лекарственных средств посредством веб-приложения. Этапы данного процесса визуально представлены в виде комплекса UML-диаграмм.

Для определения функциональных требований к веб-приложению была разработана диаграмма вариантов использования (рис. 1).

Диаграмма вариантов использования содержит три действующих лица: «Посетитель», «Пользователь» и «Администратор». Действующие лица системы, в свою очередь, инициируют различные варианты использования: «Зарегистрироваться», «Войти», «Посмотреть график приема лекарств», «Создать уведомление», «Вести учет приема лекарств», «Редактировать данные о приеме лекарств», «Удалить данные», «Выбрать данные из базы», «Отправить уведомление», «Редактировать данные». Подробно описание выделенных вариантов использования представлено ниже.

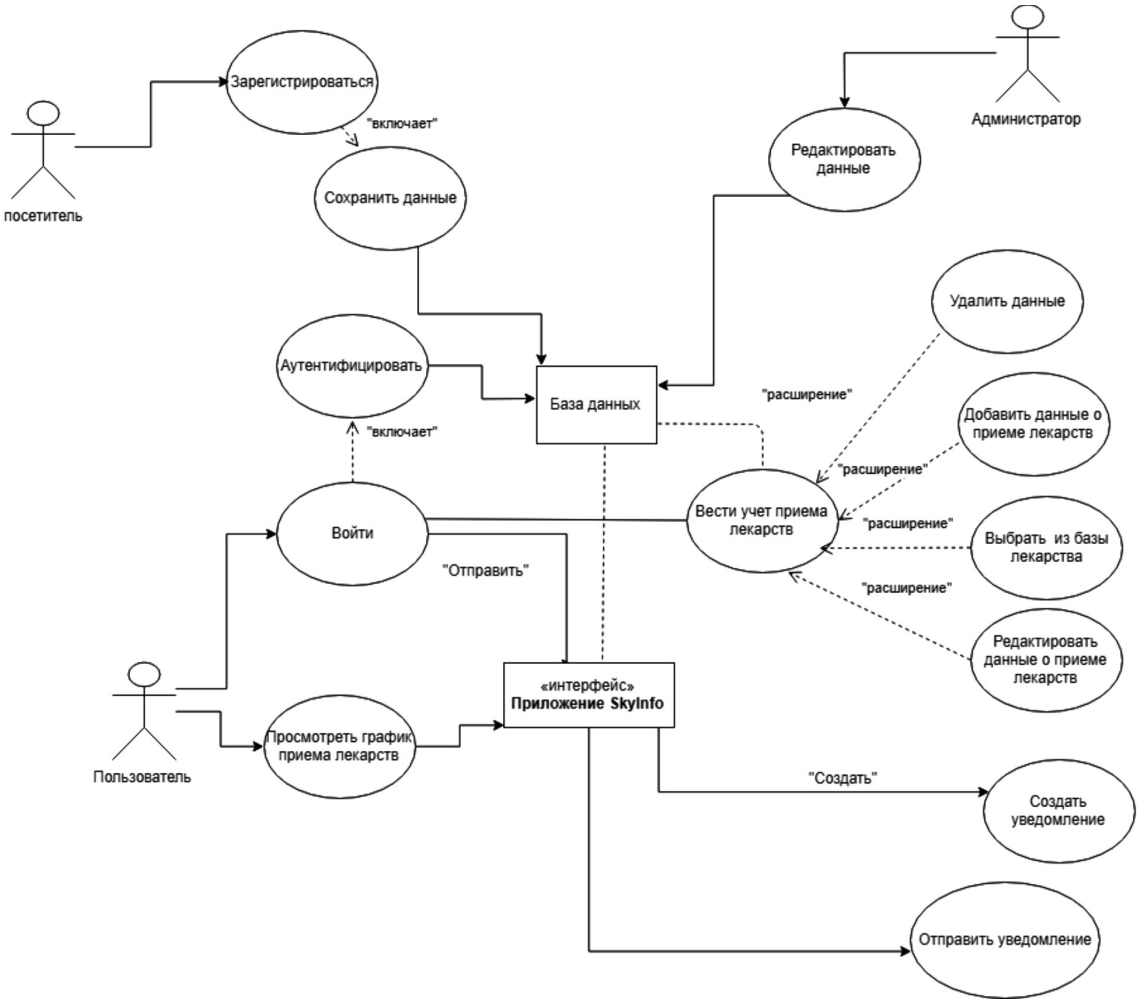

Рис. 1. Диаграмма вариантов использования

«Зарегистрироваться». Вариант использования включает в себя одно расширение: «Сохранить данные». Для регистрации посетитель вводит необходимые данные (логин, пароль, подтверждение пароля, e-mail) в форму и нажимает кнопку «Отправить». Регистрационные данные пользователя сохраняются в базу данных. Выводится уведомление об успешном сохранении, после чего происходит переадресация на страницу авторизации.

«Войти». Вариант использования включает в себя одно расширение: «Аутентифицировать». Пользователь вводит данные для входа в соответствующие поля и нажимает кнопку «Войти». Введенные пользователем данные сравниваются с базой данных. Если данные совпадают, то выводится уведомление об успешном входе и происходит переадресация на главную страницу. Если данные не совпадают, то выводится соответствующее уведомление и пользователю нужно их проверить или зарегистрироваться.

«Посмотреть график приема лекарств». Пользователь заходит на главную страницу. Из базы данных выводится информация о графике приема лекарств.

«Создать уведомление». Пользователь нажимает на кнопку «создать уведомление», открывается форма для ввода данных о приеме лекарств.

«Вести учет приема лекарств». Вариант использования включает в себя четыре расширения: «Добавить данные о приеме лекарств», «Удалить данные», «Выбрать лекарства из базы», «Редактировать данные о приеме лекарств».

Расширение «Добавить данные о приеме лекарств». Пользователь открывает форму для ввода данных о приеме лекарств. Заполняет поля «название лекарства», «кратность приема», «срок приема», «время приема». Нажимает кнопку «Сохранить». Данные сохраняются в базу. Выводится уведомление об успешном сохранении и происходит переадресация на главную страницу со сформированным графиком приема лекарств.

Расширение «Редактировать данные о приеме лекарств». Пользователь нажимает на кнопку «Редактировать данные», открывается форма для редактирования. Пользователь вносит изменения в нужные поля. Данные обновляются в базе данных. Выводится сообщение об успешном уведомлении и происходит переадресация на главную страницу с изменённым графиком приема лекарств.

Расширение «Удалить данные». Пользователь нажимает кнопку «Удалить». Запись о приеме лекарства удаляется из базы данных. Выводится уведомление об успешном удалении и происходит переадресация на главную страницу.

Расширение «Выбрать данные из базы». Пользователь нажимает кнопку «Выбрать лекарство», после чего следует переадресация пользователя на страницу «Лекарства». На данной странице пользователь может осуществлять более детальный поиск лекарств и ознакомиться с характеристиками лекарственных средств. Далее пользователь вводит название лекарства в поле поиска. Если лекарство найдено, то пользователь нажимает кнопку «Добавить». После чего выбранное пользователем лекарство добавляется в форму для ввода данных о приеме лекарств. Если лекарство не найдено, пользователь нажимает кнопку «Детальный поиск». Переадресация пользователя на форму с критериями поиска лекарства с различными фильтрами.

«Отправить уведомление». При наступлении необходимой даты и времени принятия лекарства пользователю отправляется уведомление о необходимости его принять.

«Редактировать данные». Администратор нажимает кнопку «Добавить лекарство». Открывается форма ввода данных. Администратор вводит все необходимые поля. Нажимает кнопку «Сохранить». Выводится уведомление об успешном сохранении и происходит переадресация на главную страницу. Администратор нажимает кнопку «Изменить лекарство». Открывается форма со список лекарств. С возможностью редактирования/удаления лекарств. Администратор нажимает кнопку «Редактировать пользователей». Происходит переадресация на страницу списка пользователей с возможностью редактирования/удаления пользователей.

При инициализации определенного варианта использования пользователем, выполняется определенная последовательность действий, которая описывается с помощью специальной диаграммы UML. Пример описания варианта использования «Зарегистрироваться» в виде диаграммы последовательности приведен на рис. 2.

После того как определены функции приложения и описаны варианты использования, необходимо создать диаграмму классов (рис. 3). Диаграмма классов является типом диаграммы статической структуры. Она описывает структуру системы, показывая её классы, их атрибуты и операторы, а также взаимосвязи этих классов [5].

Диаграмма классов проекта «SKYINFO» состоит из четырех классов: User (Пользователь), Notifications (Уведомления), Bank (Связующая таблица) и Lec (Лекарства).

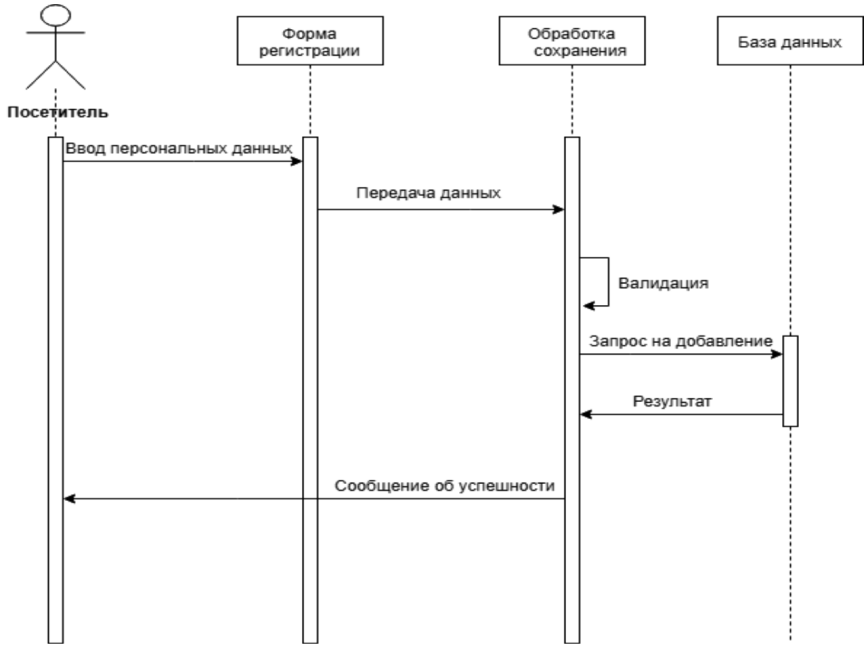

Рис. 2. Диаграмма последовательности «Зарегистрироваться»

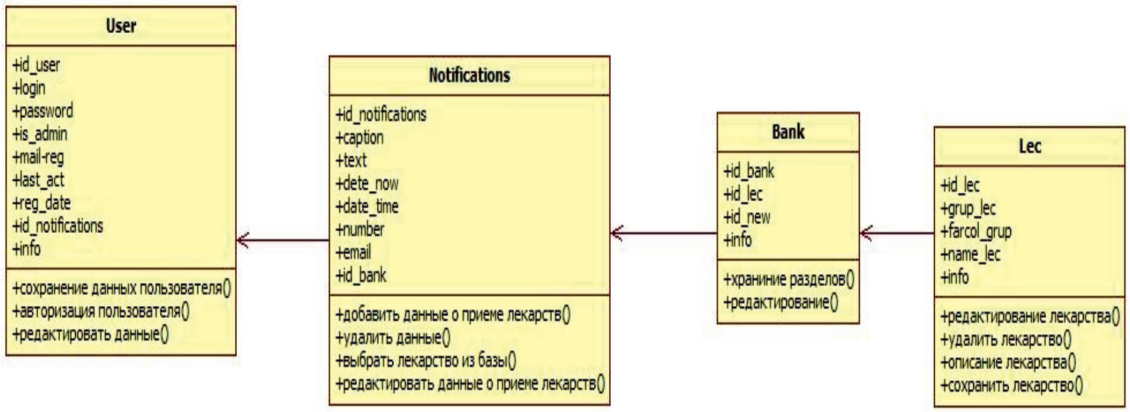

Рис. 3. Диаграмма классов

Диаграмма классов является основой для разработки базы данных, где будет храниться вся необходимая информация для работы веб-приложения.

База данных была реализована средствами системы управления базами данных СУБД MySQL с помощью веб-интерфейса PhpMyAdmin. Физическая модель – база данных проекта «SKYINFO» представлена на рис. 4.

Для обеспечения целостности информации, представленной в базе данных, были установлены связи между таблицами. Таблица «User» связана с таблицей «Notifications» с помощью связи «один ко многим», так как у пользователя может быть множество уведомлений. В одном уведомлении может храниться несколько лекарств, для хранения этой информации потребуется смежная таблица «Bank». В таком случае таблица «Notifications» будет связана с таблицей «Lec» связью «многие ко многим».

Для удобства использования веб-приложения «SKYINFO» также был разработан пользовательский интерфейс. Дизайн интерфейса базируется на «Material Design» – единой концепции построения логики работы и внешнего вида сервисов и приложений, унифицирующей все программное обеспечение с целью его максимально лёгкого и интуитивного восприятия пользователями [6].

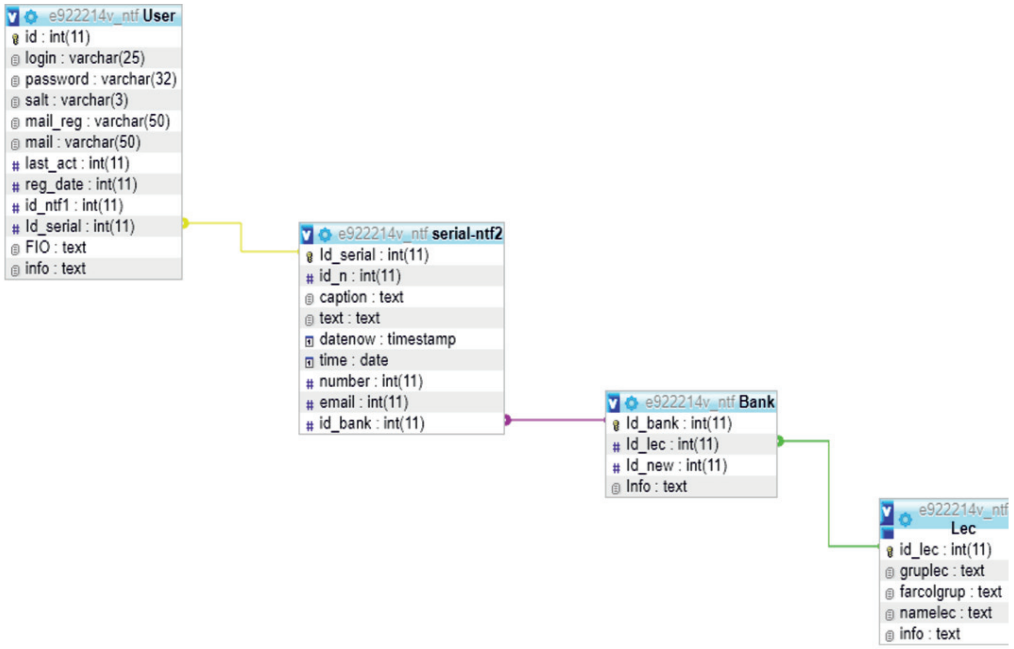

Рис. 4. База данных

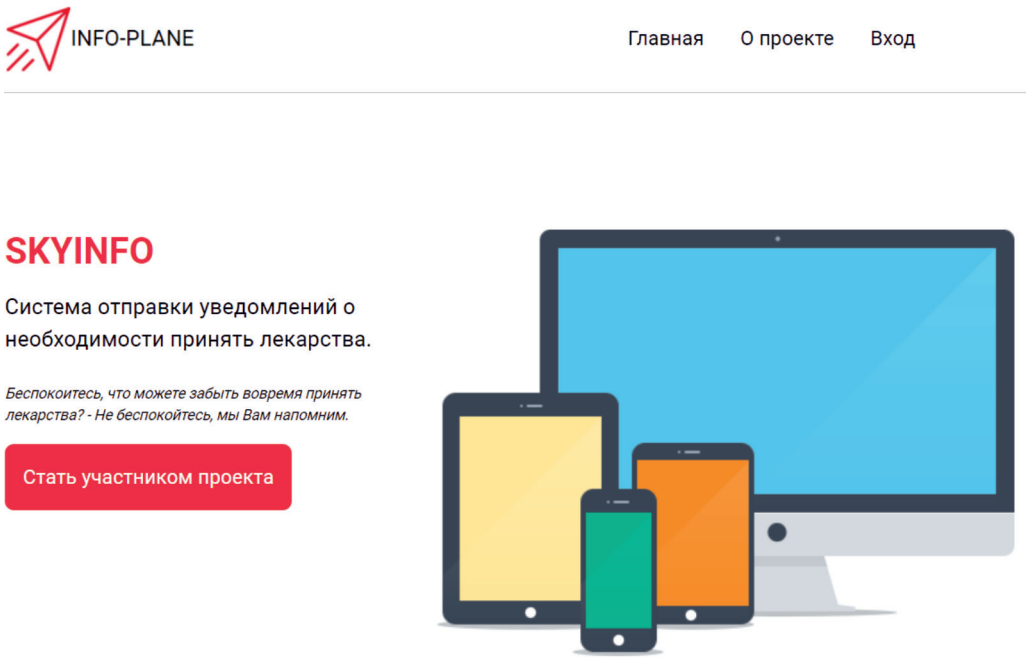

Рис. 5. Главная страница проекта «SKYINFO»

Интерфейс главной страницы веб-приложения представлен на рис. 5.

После авторизации пользователь попадает в личный кабинет, интерфейс представлен на рис. 6. В личном кабинете пользователь может создавать уведомления, нажав на кнопку «Создать уведомление». Также пользователь из личного кабинета имеет доступ в раздел «База лекарств», а также завершить активный сеанс с помощью кнопки «Выйти».

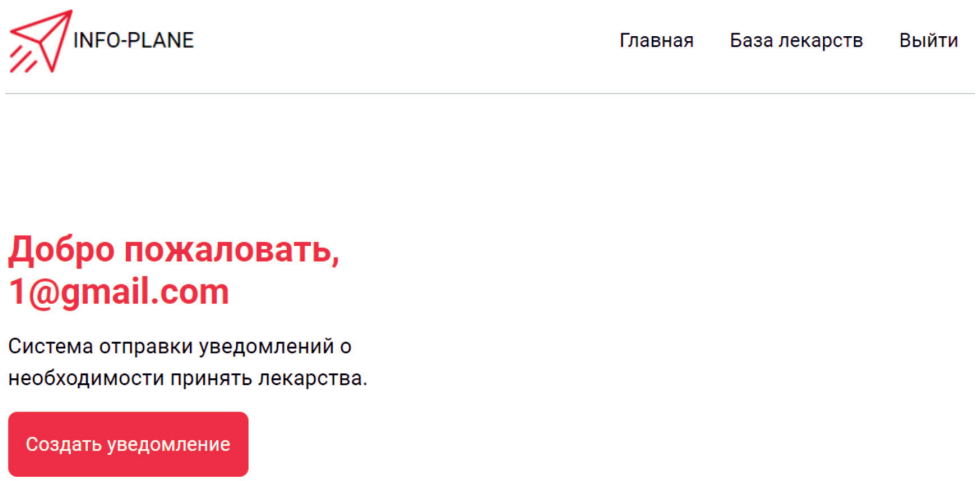

Рис. 6. Личный кабинет

Заключение

В результате выполнения данной работы было спроектировано веб-приложение «SKYINFO» с гибкой системой напоминания о необходимости приема лекарств. Проект был представлен в виде комплекса UML-диаграмм, позволяющих определить функционал и структуру веб-приложения и макетов веб-страниц со стилевым оформлением. Представленный в статье проект веб-приложения может использоваться как основа для реализации подобного рода веб-приложений для уведомления пользователей о значимых событиях.

Список литературы

1. MyTherapy – приложение для отслеживания приёма лекарств. [Электронный ресурс]. URL: https://droidnews.ru/mytherapy-prilozhenie-dlya-otslezhivaniya-priyoma-lekarstv (дата обращения: 06.05.2019).

2. Roundhealth – приложение для отслеживания приёма лекарств и состояния здоровья. [Электронный ресурс]. URL: https://appagg.com/ios/medical/round-health-17472058.html?hl=ru (дата обращения: 06.05.2019).

3. Mr. Pillster – напоминания о приеме таблеток. [Электронный ресурс]. URL: https://mr-pillster.ru.uptodown.com/android (дата обращения: 06.05.2019).

4. Леоненков А. «Самоучитель UML». СПб.: БХВ-Петербург, 2007. 576 с.

5. Мюллер Р. Базы данных и UML: Проектирование. М.: ЛОРИ, 2013, 422 с.

6. Дженифер Т. Разработка пользовательских интерфейсов. СПб.: Питер, 2011. 480 с.

ОБЗОР

УДК 004.048:004.032.26

ИНФОРМАЦИОННЫЕ НЕЙРОННЫЕ СЕТИ

Иванько А.Ф., Иванько М.А., Колесникова О.Д.

Московский политехнический университет, Москва, e-mail: alekfed@mail.ru, mihaleks@mail.ru, kod678@gmail.com

Предметом изучения данной статьи являются вопросы практического применения информационных нейронных сетей. Нейронная сеть – это алгоритм машинного обучения, основанный на модели человеческого нейрона. Эти нейроны связаны со специальной структурой, известной как синапсы. Синапсы позволяют нейронам передавать сигналы. Из большого количества моделируемых нейронов формируется нейронная сеть. Данная технология быстрыми темпами развивается в настоящее время. Информационные нейронные сети способны на анализ полученных данных, распознавание образов, классификацию информации и самообучение. Данная технология получила широкое распространение в программировании беспилотного транспорта, машинного обучения, создании медиа и аудиоинформации на основе полученных данных и многих других сфер информационных технологий. В статье исследуются, сферы применения нейронных сетей, их слоевая структура, модель каждого «нейрона», их совместная работа и базовые алгоритмы работы этой технологии. Приведен простейший пример работы ИНС, его поэтапный анализ. Также исследуются нейронные сети, которые функционируют в нынешнее время и очень полезны обществу и развитию многих передовых технологий. Результатами данной статьи являются: описание работы информационных нейронных сетей, их структура и механизм работы и рассмотрение примеров уже существующих ИНС.

Ключевые слова: нейронная сеть, машинное обучение, программирование, распознавание лиц, обработка изображений, информационные системы

INFORMATION NEURAL NETWORKS

Ivanko A.F., Ivanko M.A., Kolesnikova O.D.

Moscow Polytechnic University, Moscow, e-mail: alekfed@mail.ru, mihaleks@mail.ru, kod678@gmail.com

The subject of this article is the practical application of information neural networks. A neural network is a machine learning algorithm based on a model of a human neuron. These neurons are associated with a special structure known as synapses. Synapses allow neurons to transmit signals. A neural network is formed from a large number of simulated neurons. This technology is developing rapidly at the present time. Information neural networks are capable of analyzing the obtained data, pattern recognition, information classification and self-learning. This technology is widely used in programming of unmanned vehicles, machine learning, creation of media and audio information based on the data and many other areas of information technology. The article explores the spheres of application of neural networks, their layer structure, the model of each «neuron», their joint work and the basic algorithms of this technology. The simplest example of the work of the INS, its step-by-step analysis is given. Neural networks that function at the present time and are very useful to society and the development of many advanced technologies are also being investigated. The results of this article are the description of the work of information neural networks, their structure and mechanism of work and consideration of examples of already existing ANNs.

Keywords: neural network, machine learning, programming, face recognition, image processing, information systems

С недавних пор разработчики пытаются искуственно воссоздать биологический процесс мозга человека, основанный на нейронах.

Искусственные нейронные сети (ИНС) или нейронные сети являются вычислительными алгоритмами. Они предназначены для имитации поведения биологических систем, состоящих из «нейронов», и способны на машинное обучение, а также распознавание образов.

Целью исследования статьи являются: выявление закономерностей работы нейронных сетей, анализ области их применения и определение значения ИНС для развития других иновационных технологий.

Методами исследования данной статьи являются: аналогия работы нейронных сетей с биологическим процессом мозга человека, основанным на нейронах, описание структуры ИНС, анализ области применения данной технологии, описание современных, уже работающих нейросетей [1].

Нейронная сеть – это алгоритм машинного обучения, основанный на модели человеческого нейрона. Человеческий мозг состоит из миллионов нейронов. Он отправляет и обрабатывает сигналы в виде электрических и химических сигналов. Эти нейроны связаны со специальной структурой, известной как синапсы [2, 3]. Синапсы позволяют нейронам передавать сигналы. Из большого количества моделируемых нейронов формируется нейронная сеть.

Цель исследования: определить возможности нейронных сетей для анализа и синтеза информационных данных.

Эта технология может найти большое применение в интеллектуальном анализе

данных, а также для распознавания образов и классификации большого количества данных.

Искусственная нейронная сеть обычно организована по слоям. Слои состоят из множества взаимосвязанных «узлов», которые содержат «функцию активации».

Нейронная сеть может содержать следующие три слоя:

1. Входной слой.

Назначение входного слоя – получить в качестве входных данных значения объяснительных атрибутов для каждого наблюдения. Обычно количество входных узлов во входном слое равно количеству объясняющих переменных. «Входной слой» представляет шаблоны в сети, которая связывается с одним или несколькими «скрытыми слоями».

Узлы входного слоя являются пассивными, то есть они не изменяют данные. Они получают единственное значение на своем входе и дублируют значение на своих многочисленных выходах. Из входного слоя каждое значение дублируется и отправляется всем скрытым узлам [4].

2. Скрытый слой.

Скрытые слои применяют данные преобразования к входным значениям внутри сети. При этом входящие дуги идут от других скрытых узлов или от входных узлов, подключенных к каждому узлу. Они соединяются с исходящими дугами для выходных узлов или других скрытых узлов. В скрытом слое фактическая обработка выполняется через систему взвешенных «соединений». Скрытый слой может быть один или несколько. Значения, входящие в скрытый узел, умноженные на веса, представляют собой набор заранее определенных чисел, хранящихся в программе. Затем добавляются взвешенные входные данные для получения одного числа [5].

3. Выходной слой.

Затем скрытые слои связываются с «выходным слоем». Выходной слой получает соединения от скрытых слоев или от входного слоя, возвращает выходное значение, которое соответствует прогнозу переменной ответа. В задачах классификации обычно есть только один выходной узел. Активные узлы выходного слоя объединяют и изменяют данные для получения выходных значений [6].

Структура нейронной сети, называемая также «архитектурой» или «топологией», состоит из количества слоев, элементарных единиц и механизма регулировки веса.

Простейшей структурой принято считать структуру, в которой единицы распределяются по двум слоям: входной слой и выходной слой. При этом каждая единица входного слоя имеет один вход и один выход, который равен входу [7].

Рассмотрим внутреннюю структуру искусственного нейрона и процесс преобразования поступающаго на его входы сигнала [8]. На рисунке ниже представлена полная модель искусственного нейрона (рис. 1).

Обычные компьютеры используют алгоритмический подход, то есть компьютер выполняет набор инструкций для решения проблемы. Если не известны конкретные шаги, которые должен выполнить компьютер, то он не может решить проблему [9].

Способность нейронной сети обеспечивать полезные манипуляции с данными заключается в правильном выборе весов. Это отличает ее от обработки информации компьютером. Если весам связей присвоить случайные значения, то ничего осмысленного такая нейросеть делать не будет. То есть их надо еще как-то правильно подобрать. Иными словами, нейросеть надо обучить [10, 11].

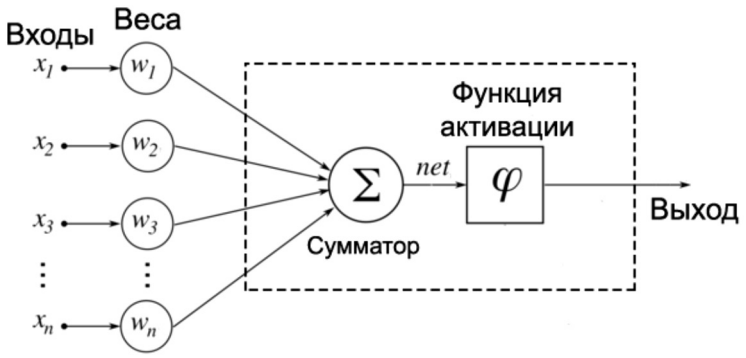

Рис. 1. Внутренняя структура искусственного нейрона

Обучение нейронной сети – это поиск такого набора весовых коэффициентов, при котором входной сигнал преобразуется в нужный нам выходной после прохода по сети.

Нейронные сети и обычные алгоритмические компьютеры не конкурируют, а дополняют друг друга. Есть задачи более подходящие для алгоритмического подхода, такие как арифметические операции, и задачи, которые больше подходят для нейронных сетей. Большое количество задач требует системы, использующей комбинацию двух подходов (чаще всего обычный компьютер используется для контроля нейронной сети), чтобы выполнять их с максимальной эффективностью [12].

Важным применением нейронных сетей является распознавание образов. Распознавание образов может быть реализовано с помощью нейронной сети с прямой связью (рис. 2), которая была обучена соответствующим образом. Во время работы сеть обучается связывать выходы с шаблонами ввода. Когда сеть используется, она идентифицирует входной шаблон и пытается вывести связанный выходной шаблон. Сила нейронных сетей приходит в себя, когда в качестве входных данных приводится шаблон, который не имеет выходных данных [13]. В этом случае сеть выдает выходные данные, которые соответствуют обученному шаблону ввода, который наименее отличается от данного шаблона.

Более сложным нейроном (рис. 3) является модель МакКаллоха и Питтса. Отличие от предыдущей модели состоит в том, что входные данные являются «взвешенными», а эффект, который каждый вход имеет при принятии решения, зависит от веса конкретного входа. Вес ввода – это число, которое при умножении на вход дает взвешенный ввод. Эти взвешенные входы затем складываются вместе, и, если они превышают предварительно установленное пороговое значение, нейрон срабатывает [14]. В любом другом случае нейрон не срабатывает [15].

В математических терминах нейрон срабатывает тогда и только тогда, когда

$$X 1 W 1 + X 2 W 2 + X 3 W 3 + ...> T.$$

Добавление входных весов и порога делает этот нейрон очень гибким и мощным. Нейрон Маккаллока – Питтса обладает способностью адаптироваться к конкретной ситуации, изменяя свои веса или порог [16].

Нейронные сети были изобретены еще многие десятилетия назад, но тогда не хватало вычислительной мощности для их использования. В настоящее время разработаны довольно мощные видеокарты, подходящие для работы ИНС.

Рассмотрим достижения современных нейронных сетей [17].

Нейросеть AlphaGo от Google DeepMind в марте 2016 г. обыграла в игру Го, логическую настольную игру с глубоким стратегическим содержанием, возникшую в Древнем Китае, лучшего игрока в мире – Ли Седоля. Вариантов ходов в ней в 10 раз больше, чем в шахматах, а число возможных партий больше количества атомов во вселенной. Сначала нейросеть просмотрела матчи лучших игроков, а потом стала играть сама с собой, становясь все совершеннее [18].

Также осенью 2016 г. компания DeepMind объявила, что их нейросеть научилась правдоподобно имитировать речь человека [19]. У этой технологии в совокупности с распознавателем речи и переводчиком есть перспектива создать приложение, с помощью которого с легкостью будут общаться носители разных языков. Нейронная сеть будет распознавать речь, переводить и транслировать голосом и интонацией, неотличимой от человеческой [20].

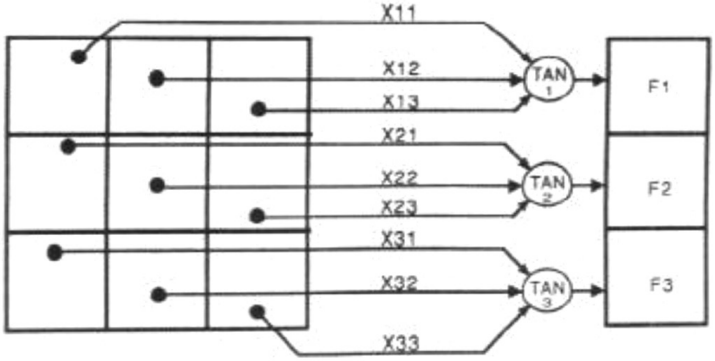

Рис. 2. Нейронная сеть с прямой связью

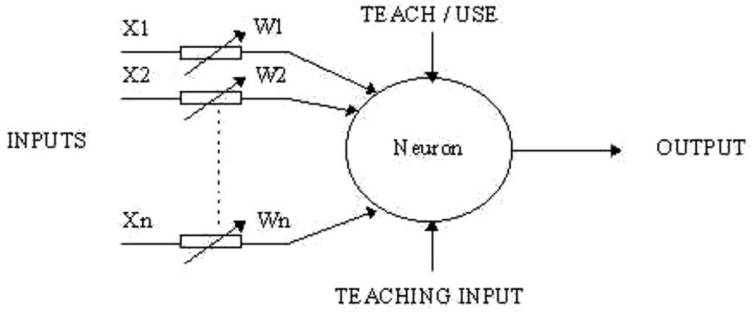

Рис. 3. Нейрон MCP

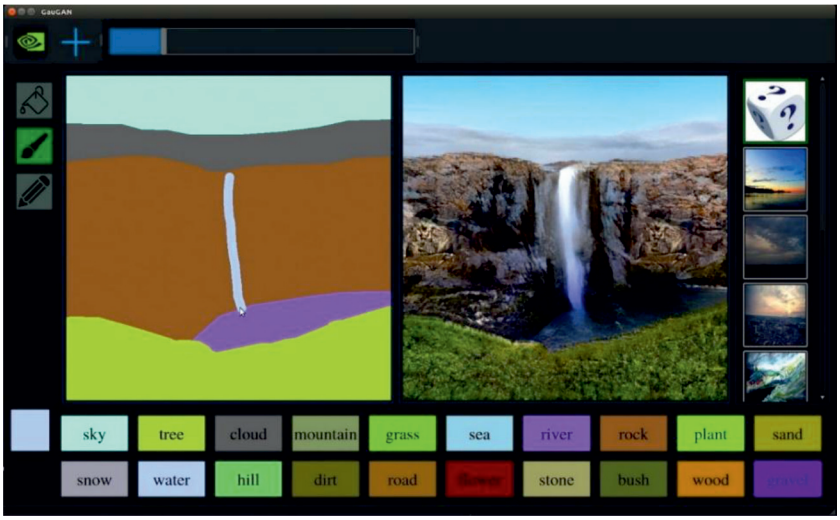

Рис. 4. Пейзаж, нарисованный нейросетью от Nvidia

Компания Nvidea разработала нейросеть для визуальных вычислений, с помощью которой возможно обучение вождению беспилотных автомобилей. Нейросеть уже умеет идеально водить даже на загруженной дороге, распознавая светофоры, знаки, другие машины и людей. Чем больше автомобили ездят по дорогам, тем больше обучается нейронная сеть [21].

В марте 2019 г. запущена открытая вебверсия «Paint эпохи искусственного интеллекта» работающая на нейросети GauGAN от Nvidia [22]. Данная нейросеть превращает простые наброски в реалистичные пейзажи (рис. 4). Достаточно лишь обозначить контуры объектов и цвета (голубые воспринимаются как вода, коричневые – горы, зеленые – трава). Нейросеть GauGAN не использует шаблоны, а каждый раз генерирует новые пейзажи.

Нейронные сети очень часто используют для систем создания и распознавания лиц. Например, нейросеть DeepFake накладывает выбранное лицо на лицо с видеоряда. В сети множество видео с лицами знаменитостей, которые были наложены данной ИНС. Они выглядят достаточно правдоподобно [23].

Нейронная сеть FindFace – лучшая в мире технология для распознавания лиц. По загруженному фото человека, даже не очень отчетливому, сайт выдает странички интернет-пользователей с похожими лицами. Эта система очень эффективна, ее использовали даже полицейские для поиска преступников в розыске, стоило только договориться о встрече с пользователем странички [24].

Разработчик Филипп Ванг создал сайт ThisPersonDoesNotExist.com, который генерирует реалистичное лицо несуществующего человека при каждом обновлении страницы (рис. 5). Для разработки ресурса Ванг использовал алгоритм генеративно-состязательной сети StyleGAN, работу которого в конце 2017 г. показала

компания Nvidia. StyleGAN комбинирует две нейросети: одна из них генерирует «образцы», а другая пытается отличить реалистичные изображения от неправдоподобных. Метод позволяет сети самой улучшать качество выдаваемых результатов.

Развитие ИНС полным ходом идет и в России. Нейросети Яндекса уже пишут стихи и музыку.

Нейросеть под именем «Зинаида Фолс» проанализировала по нескольку раз всю поэзию, написанную на русском языке, это примерно 130 Мб текста (полное собрание сочинений Уильяма Шекспира – примерно 5 Мб). Вот пример стихотворения, написанного Зинаидой Фолс с запросом наличия слов «будущее», «будет» и «время» (авторское название стихотворения, орфография и пунктуация сохранены):

Так будет завтра длиться
так будет завтра длиться
в темном сумраке сада
там где пляшет колесница
от радости бога награда
мы поняли что время от руки
не осилить не выйду не встану
не любя ни разу ни строки
кто кого из нас не выйдет замуж
кто же вы те дни и те ночи
да слабые мысли и вздохи о них
мой город прекрасен и скучен
покуда был первый жених

В 2017 г. нейронные сети Яндекса создали альбом в стиле группы «Гражданская оборона». Эти песни вышли под исполнителем «Нейронная оборона» и по стилю и тексту действительно похожи на оригинального исполнителя. Немного позже аналогично был сделан альбом на английском языке от исполнителя «Neurona», в стиле легендарной группы Nirvana.

А свою конференцию Yac-2017 Яндекс начали с музыки, написанной нейронной сетью в стиле произведений композитора Александра Скрябина.

Результатами данного исследования является обоснование работы нейронных сетей, их структуры и области применения, а также анализ существующих ИНС и оценка их значения для развития других инновационных технологий [25].

В заключение можно сказать, что существует множество других информационных нейронных сетей, помимо рассмотренных в данной статье. Многие из них очень полезны и продолжают совершенствоваться.

Выводы

Таким образом, с помощью нейросетей возможно реализовать невероятные технологии. Главное преимущество нейронных сетей – их самообучаемость. Нужен лишь достаточный объем данных и время системы на обучение. Методом проб и ошибок нейросеть поймет, как нужно работать. Используя способность обучения на множестве примеров, ИНС способна решать задачи, в которых неизвестны закономерности развития ситуации и зависимости между входными и выходными данными. То есть нейросети способны решить задачи, алгоритм решения которых не знает сам разработчик.

Рис. 5. Изображения сгенерированные на сайте ThisPersonDoesNotExist.com

Нейросети уже в нынешнее время получили огромное распространение во многих сферах машинного анализа и обучения. Будем надеяться, что со временем данная технология будет развиваться и дальше.

Список литературы

1. Рашид Тарик. Создаем нейронную сеть: Пер. с англ. Гузикевич А.Г., 2017. 272 с.

2. Нейронные сети для начинающих. Часть 1 [Электронный ресурс]. URL: https://m.habr.com/ru/post/312450/ (дата обращения: 15.06.2019).

3. Нейронные сети для начинающих. Часть 2 [Электронный ресурс]. URL: https://m.habr.com/ru/post/313216/ (дата обращения: 15.06.2019).

4. Хайкин С. Нейронные сети: Полный курс, 2-е изд. Пер. с англ. М.: Издательский дом «Вильямс», 2016. 1104 с.

5. Горбачевская Е.Н. Классификация нейронных сетей // Вестник Волжского университета им. В.Н. Татищева 2012. № 2 С. 23–24.

6. Горбачевская Е.Н. Обучение искусственной нейронной сети для задач прогнозирования // Вестник Волжского университета им. В.Н. Татищева 2012. № 2. С. 19–20.

7. Объясняем нейронные сети без математики [Электронный ресурс]. URL: https://zen.yandex.ru/media/reedr.ru/obiasniaem-neironnye-seti-bez-matematiki-596c4dade86a9e0873b24532 (дата обращения: 12.05.2019).

8. Искусственная нейронная сеть [Электронный ресурс]. URL: https://ru.m.wikipedia.org/wiki/%D0%98%D1%81%D0%BA%D1%83%D1%81%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BD%D0%B5%D0%B9%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C/ (дата обращения: 15.06.2019).

9. Фаустова К.И. Нейронные сети: применение сегодня и перспективы развития // Территория науки 2017. № 4. С. 83–87.

10. Ivanko A.F., Ivanko M.A., Kulikova E.V. Moscow Polytechnic University, Moscow, Security of information data. European journal of natural history. 2018. № 4. P. 118–120.

11. Иванько А.Ф., Иванько М.А., Сизова Ю.А. Нейронные сети: общие технологические характеристики // Научное обозрение. Технические науки. 2019. № 2. С. 17–23.

12. Нейронные сети [Электронный ресурс]. URL: https://hi-news.ru/tag/nejronnye-seti (дата обращения: 15.06.2019).

13. Нейросеть [Электронный ресурс]. URL: https://indicator.ru/tags/nejroset/ (дата обращения: 15.06.2019).

14. Николенко С.И., Кадурин А., Архангельская Е.В. Глубокое обучение. Погружение в мир нейронных сетей. СПб., 2018. 480 с.

15. Гусеев С.С. Искусственный интеллект как отражение действительности в XXI веке // Интерактивная наука 2016. № 8 С. 59–61.

16. Создаём простую нейросеть. Блог компании NIX Solutions [Электронный ресурс]. URL: https://m.habr.com/ru/company/nixsolutions/blog/423647/ (дата обращения: 15.06.2019).

17. Нейронные сети: на пороге будущего [Электронный ресурс]. URL: https://compress.ru/article.aspx?id=9663 (дата обращения: 15.06.2019).

18. Галушкин А.И. Нейронные сети: основы теории. М.: Горячая линия – Телеком, 2010. 496 с.

19. Искусственный нейрон [Электронный ресурс]. URL: https://ru.m.wikipedia.org/wiki/%D0%98%D1%81%D0%BA%D1%83%D1%81%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D1%8B%D0%B9_%D0%BD%D0%B5%D0%B9%D1%80%D0%BE%D0%BD/ (дата обращения: 15.06.2019).

20. Круглов В.В., Борисов В.В. Искусственные нейронные сети. Теория и практика. М.: Горячая линия – Телеком, 2002. 382 с.

21. DeepMind [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/DeepMind (дата обращения: 12.05.2019).

22. NVIDIA показала нейросеть для создания фотореалистичных пейзажей по наброскам [Электронный ресурс]. URL: https://tproger.ru/news/nvidia-gaugan/ (дата обращения: 12.05.2019).

23. Бодянский Е.В., Руденко О.Г. Искусственные нейронные сети: архитектуры, обучение, применения. Харьков: Телетех, 2004. 369 с.

24. Гудфеллоу Я., Бенджио И., Курвилль А. Глубокое обучение: Пер. с англ. А.А. Слинкин ДМК Пресс, 2017. 652 с.

25. Кулянин Е.М. Нейронные сети: история развития и перспективы применения // Научно-методический электронный журнал «Концепт». 2015. № 13 С. 2646–2650. [Электронный ресурс]. URL: http://e-koncept.ru/2015/85530.htm (дата обращения: 15.06.2019).

СТАТЬЯ

УДК 004.08

ИССЛЕДОВАНИЕ АРИФМЕТИЧЕСКИХ ПРОГРАММ

Попов С.В.

ООО «Научно-внедренческая фирма БП+», Москва, e-mail: s-v-popov@yandex.ru

Исследуются вычисления арифметических программ в зависимости от вида предметной области, над которыми вычисления осуществляются. Свойства предметных областей, определяющие сложность вычисления программ, описываются путем выделения так называемых разделимых означиваний префикса входной переменной программ. Каждое неполное означивание входной переменной программы в общем случае задает новую программу, вычисляемые значения которой зависят от вида окончательного продолжения означивания. Разделяемые означивания префикса характеризуются различными спектрами возможных продолжений вычислений. Тем самым разнообразие разделимых означиваний префиксов входной переменной программы служит характеристикой разнообразия вычислений над предметной областью. Из этого следует нижняя оценка сложности максимального вычисления в результате произвольного окончательного означивания входной переменной. Для исследования свойств вычислений программ используется сведение программ к так называемым обобщенным формулам, представляющим функции, вычисляемые программами. Каждая такая формула строится по программе единственным образом и позволяет исследовать ее вычисления логическими средствами. Обобщенная формула строится над расширенным логическим базисом, который помимо обычных логических связок содержит бесконечные дизъюнкцию и конъюнкцию. Обобщенные формулы представляют собой полное множество в том смысле, что всякая вычислимая функция представима обобщенной формулой.

Ключевые слова: арифметические программы, регулярные выражения, вычисления, сложность вычислений, обобщенные логические формулы

THE STUDY OF ARITHMETIC PROGRAMS

Popov S.V.

LLC «Nauchno-vnedrencheskaya firma BP+», Moscow, e-mail: s-v-popov@yandex.ru

The calculations of arithmetic programs depending on the type of the domain over which the calculations are carried out are investigated. The properties of the subject areas that determine the complexity of the calculation of programs are described by highlighting the so-called separable meanings of the prefix of the input variable of programs. Each incomplete denotation of the input variable of the program, in General, sets a new program, the calculated values of which depend on the type of the final continuation of the denotation. The separated values of the prefix are characterized by different spectra of possible extensions of calculations. Thus, the variety of separable meanings of prefixes of the input variable of the program is a characteristic of the variety of calculations over the subject area. This implies a lower bound on the complexity of the maximum computation as a result of arbitrary final signification of the input variable. To study the properties of program calculations, we use the reduction of programs to the so-called generalized formulas representing the functions calculated by programs. Each such formula is built according to the program in a unique way and allows to investigate its calculations by logical means. The generalized formula is constructed over an extended logical basis which, in addition to the usual logical bundles, contains infinite disjunction and conjunction. Generalized formulas are a complete set in the sense that every computable function is represented by a generalized formula.

Keywords: arithmetic programs, regular expressions, calculations, complexity of calculations, generalized logical formulas

Определение сложности вычислений актуально в связи с моделированием технологических, научных и социальных процессов и активным развитием искусственного интеллекта [1, 2]. Поэтому практически важно установление оценок сложности вычисления в зависимости от особенностей предметной области, над которой вычисление осуществляется [3, 4]. В статье рассматриваются арифметические двоичные программы над полным базисом $\boldsymbol{v} \Leftarrow \boldsymbol{v}+1$, $\boldsymbol{v} \Leftarrow 0$, $\boldsymbol{v} = \boldsymbol{u}$ операторов, обозначаемые соответственно $\boldsymbol{s}(\boldsymbol{x})$, $\boldsymbol{0}(\boldsymbol{x})$, $\boldsymbol{E}(\boldsymbol{v}, \boldsymbol{u})$. Каждая программа представляется орграфом с арифметическими вершинами $\boldsymbol{s}(\boldsymbol{x})$, $\boldsymbol{0}(\boldsymbol{x})$ и логическими ($\boldsymbol{E}$), обладает одной *входной* переменной $\boldsymbol{x}$ и конечным набором $\boldsymbol{y}_1$, $\boldsymbol{y}_2$, ..., $\boldsymbol{y}_m$ *рабочих*, среди которых одна – *выходная*. При этом одна вершина – входная; одна – выходная; в арифметических вершинах используются только рабочие переменные; в логических могут использоваться как рабочие, так и входная. Все определения, необходимые для детального понимания содержания статьи, приведены в [5]. В силу ограниченного объема статьи здесь приведены лишь пояснения к некоторым определениям, чтобы сделать изложение понятнее.

Пусть $\tau = \nu_1, \nu_2, \ldots, \nu_l$ – путь в программе π. Заменим каждый его предикат $P(z_1, z_2)$ предикатом $P^{\sigma}(z_1, z_2)$, где $\sigma \in \{0, 1\}$ так, что следующая в τ за $P(z_1, z_2)$ вершина является его σ-последователем. Полученную последовательность назовем *размеченным путем* и обозначим τ. Содержательно размеченный

путь представляет вычисление в программе. Если он начинается во входной вершине и заканчивается в выходной, то он представляет *полное вычисление* программы.

Рассуждения в настоящей статье базируются на результате Ю.И. Янова (Проблемы кибернетики, вып. 32), который показал, что каждую арифметическую программу можно представить в виде конечного автомата, состояния которого суть логические и заключительная вершины, а входной алфавит образован следующими «буквами». Если из логической вершины E в логическую вершину E_1 ведет путь $E, \nu_1, \nu_2, \ldots, \nu_l, E_1$, где ν_1 есть σ-последователь вершины E, $\nu_1, \nu_2, \ldots, \nu_l$ суть арифметические вершины и $l \geq 0$, то переход из состояния E в состояние E_1 происходит под воздействием автоматной буквы $E^{\sigma}, \nu_1, \nu_2, \ldots, \nu_l$. Представимое таким автоматом событие состоит из всех полных размеченных путей программы. Регулярное выражение R_{π}, представляющее множество всех полных путей, представимо в виде суммы $R_1 \vee R_2 \vee \ldots \vee R_r$ членов, не содержащих операции суммирования. Очевидно, что *каждое выражение* R_i, $i = 1, 2, \ldots, r$ *представляет только полные вычисления*, а *всякое его регулярное подвыражение определяет совокупность целочисленных функций*.

В [5] показано, как по регулярному выражению $R_1 \vee R_2 \vee \ldots \vee R_r$ построить обобщенную логическую формулу, представляющую функцию, вычисляемую программой π. Построение основывается на том, что все базисные операторы представимы обобщенными формулами. Построенная формула вместо переменных содержит так называемые *метапеременные*, которые устанавливают соответствие между этой формулой и вычислениями. Дальнейшее содержание статьи состоит в исследовании свойств этой формулы.

Цель статьи состоит в установлении длины вычисления программы в зависимости от свойств предметной области, над которой вычисляется программа.

Соотношение обобщенных формул, регулярных выражений и размеченных путей

Построим *обобщенную* ДНФ (ОДНФ) по формуле, представляющей функцию, определяемой регулярным выражением R_{π}. Для этого отметим, что каждое регулярное выражение A^* определяет бесконечную дизъюнкцию. Если A не содержит оператора *, то соответствующая формула уже представлена в ОДНФ, с бесконечным числом конъюнктов, каждый из которых обладает конечной длиной. Если выражение A содержит оператор *, то индукцией по числу операторов * показывается, что определяемое им выражение эквивалентно преобразуется в бесконечную дизъюнкцию конъюнктов конечной длины, атомарными формулами в которых служат формулы $\mathbf{0}$, $\boldsymbol{S}$ и $\boldsymbol{E}$. Эту дизъюнкцию назовем обобщенной ДНФ.

Установим соответствие между ОДНФ и вычислениями программы, определяемыми размеченными путями. Индукцией по длине регулярного выражения доказывается теорема.

***Теорема* 1**. *Пусть формула F определяется регулярным выражением. Тогда по ней единственным образом строится ОДНФ, в которой каждый конъюнкт представляет в точности одну функцию, определяемую единственным размеченным путем программы*.

Будем исследовать так называемые *частичные вычисления*, которые определяются означиванием лишь конечного префикса входной переменной программы. В результате такого означивания σ_x программа $\pi(\boldsymbol{x})$ превращается в новую программу π', а первоначальная формула F, построенная по регулярному выражению R_{π}, в новую формулу F', представляющую функцию, вычисляемую программой π'. Преобразование формулы F в F' базируется на следующих эквивалентных преобразованиях.

Пусть обобщенная формула G построена по регулярному выражению. Введем так называемое *правильное означивание* метапеременных формулы G. Допустим, что означен некоторый префикс входной переменной, а рабочие метапеременные означиваются следующим образом.

1. Если в G встречается формула $\mathbf{0}(\alpha)$, где $\alpha = \alpha_0, \ldots, \alpha_m \ldots$, то $\alpha_0 = \ldots = \alpha_m = \ldots = 0$. Очевидно, это единственное означивание метапеременных, при котором формула $\mathbf{0}(\alpha)$ истинная.

2. Если в G встречается формула $S^l(\alpha, \beta)$, $\alpha = \alpha_0, \ldots, \alpha_m, \ldots, \beta = \beta_0, \ldots, \beta_m, \ldots$, то α, β – рабочие метапеременные. Следовательно, имеется самая правая единица в означивании компонентов $\alpha_0, \ldots, \alpha_m, \ldots$, за которой следуют бесконечный нулевой суффикс. Тогда означивание компонентов $\beta_0, \ldots, \beta_m, \ldots$ получается из двоичного представления числа $|\alpha| + l$. Здесь $|\alpha|$ – это двоичное число, определяемое значениями метапеременных $\alpha_0, \ldots, \alpha_m, \ldots$ отбрасыванием бесконечного нулевого суффикса правее последнего единичного компонента. При таком означивании метапеременных α, β формула S^l истинная, при любом другом означивании метапеременных $\beta_0, \ldots, \beta_m, \ldots$ она ложна.

3. Если α и β суть рабочие метапеременные, то формула $E(\alpha, \beta)$ истинная при означиваниях, соответственно $\boldsymbol{\sigma}_{\alpha}$ и $\boldsymbol{\sigma}_{\beta}$ лишь в случае, когда $\boldsymbol{\sigma}_{\alpha} = \boldsymbol{\sigma}_{\beta}$, т.е. $\boldsymbol{\sigma}_{\alpha}$ и $\boldsymbol{\sigma}_{\beta}$ суть рав-

ные двоичные числа. А формула $E^{-1}(\alpha, \beta)$ истинная лишь в случае, когда $\boldsymbol{\sigma}_\alpha \neq \boldsymbol{\sigma}_\beta$, т.е. $\boldsymbol{\sigma}_\alpha$ и $\boldsymbol{\sigma}_\beta$ суть равные двоичные числа.

Пусть $G(\alpha_1, \alpha_2, \ldots, \alpha_q)$ есть конъюнкция формул, представляющих арифметические и логические операторы, содержащая только рабочие метапеременные $\alpha_1, \alpha_2, \ldots, \alpha_q$. Тогда при означивании ее метапеременных она истинная тогда и только тогда, когда означивания *правильные*, т.е. удовлетворяют условиям из пунктов 1–3. Если конъюнкция G построена по регулярному выражению, определяемому размеченным путем, то значения ее метапеременных полностью соответствуют вычисленным значениям рабочих переменных. То есть вычисление, определяемое размеченным путем, совпадает с правильным означиванием, и наоборот, всякое правильное означивание совпадает с вычислением, определяемым размеченным путем. Такой вывод справедлив лишь при условии, когда размеченный путь не включает логической вершины, содержащей входную переменную программы. Рассмотрим, что происходит, если в размеченном пути встречаются логические операторы, содержащие входную переменную программы. Легко показать, что *формула* $E(\alpha, \beta)$ *может быть либо ложной, либо неопределенной*, а $E^{-1}(\alpha, \beta)$ – *либо истинной либо неопределенной*. *Формула* $E^{\sigma}(\alpha, \beta)$ *после означивания ее метапеременных представляет собой конъюнкт или дизъюнкт литер, лишь когда она содержит частично означенную входную переменную и означенные префиксы метапеременных* α и β *совпадают*. Таким образом, если логический оператор не содержит частично означенной переменной, то его логическое значение совпадает с логическим значением представляющей формулы. Но если логический оператор содержит частично означенную входную переменную, то не является константой, и его окончательное значение зависит от дальнейшего означивания входной переменной.

Расширение означивания префикса входной переменной программы

Естественно возникает вопрос, что происходит с формулой, которая строится по регулярному выражению R_π, если расширяется означиваемый префикс входной переменной. В [5] показано, что при расширении α_2 начального означивания α_1 входной переменной вычисление для α_2 включает вычисление для α_1. При этом возможны следующие случаи.

1. Оно либо завершается с тем же результатом, что и при вычислении с означиванием α_1. Это происходит в случае, когда вычисление с начальным означиванием α_1 завершилось.

2. Оно может завершиться, хотя вычисление с начальным означиванием α_1 не завершилось.

3. Оно может не завершиться, при этом вычисление с означиванием α_1 также не завершается.

Действительно, увеличение длины означиваемого префикса входной переменной программы приводит к исключению ряда конъюнктов из ОДНФ, построенной по формуле, определяемой регулярным выражением.

***Пример* 1.** Рассмотрим означивания префикса длины $n > 0$ входной переменной $\boldsymbol{x} = x_0x_1x_2x_3 \ldots x_i \ldots$ в формуле $0(\alpha_0)$ $(E(\alpha_0, \boldsymbol{x})$ $E(\alpha_0, \boldsymbol{Out}) \vee \cup_{j=1,\omega} (\cap_{h=0,j-1} E(\alpha_h, \boldsymbol{x})\, S(\alpha_h, \alpha_{h+1}))$ $E(\alpha_j, \boldsymbol{x})\, E(\boldsymbol{x}, \boldsymbol{Out}))$.

Нетривиальным значением эта формула обладает, когда формула $0(\alpha_0)$ истинная, т.е. значение метапеременной α_0 нулевое.

Базис индукции. При $n = 1$ возможны только два случая $x_0 = 0/\ \underline{x}_0 = 1$. При $x_0 = 0$ формула $E(\alpha_0, \boldsymbol{x}) = \cap_{i=1,\omega}\, x_i$. Выходная метапеременная ***Out*** в этом случае нулевая. В оставшейся бесконечной дизъюнкции каждый конъюнктивный член содержит выражение $E(\alpha_j, \boldsymbol{x})$, $j = 1, 2, \ldots$. Каждый такой член ложный в том случае, когда j – нечетно. Следовательно, бесконечная дизъюнкция эквивалентно преобразуется в бесконечную дизъюнкцию, в которые входят выражения $E(\alpha_j, \boldsymbol{x})$, где j – четно. Выражение α_j представляет число j. Следовательно, результирующая бесконечная дизъюнкция представляет предикат «число $\boldsymbol{x}$ – четно», и эквивалентно преобразуется в x_0. Случай, когда $x_0 = 1$, эквивалентно преобразует исходное выражение в формулу, представляющую предикат «число x – нечетно», представляемый формулой x_0. Итак, начальные означивания $x_0 = 0$ / $x_0 = 1$ порождают две формулы: x_0 и x_0.

Индукционные рассуждения. Если $n > 0$, то, рассуждая как в предыдущем случае, можно показать, что при означивании $\sigma_x = \sigma_0\sigma_1 \ldots \sigma_{n-1}$ префикса переменной $\boldsymbol{x}$ исходное выражение эквивалентно преобразуется в формулу $x_0^{\sigma_0} x_1^{\sigma_1} \ldots x_{n-1}^{\sigma_{n-1}}$, представляющую предикат «число $\boldsymbol{x}$ имеет своим префиксом σ_x». Таким образом, все эти наборы образуют 2^n классов эквивалентности.

***Пример* 2**. Рассмотрим программу, вычисляющую функцию $\boldsymbol{x} + \boldsymbol{y}$, в которой $\boldsymbol{u}$, $\boldsymbol{v}$ суть рабочие переменные, причем $\boldsymbol{u}$ – выходная. Первая вершина есть функция присваивания $\boldsymbol{u} \Leftarrow \boldsymbol{x}$, следующий за ней цикл осуществляет прибавление к переменной $\boldsymbol{u}$ еще $\boldsymbol{y}$ единиц. Таким образом, на выходе программы формируется сумма $\boldsymbol{x} + \boldsymbol{y}$. Регу-

лярное выражение, порождаемое этой программой, таково: $0(\boldsymbol{v})\ E(\boldsymbol{u}, \boldsymbol{x})\ (\ E(\boldsymbol{v}, \boldsymbol{y})\ s(\boldsymbol{v})\ s(\boldsymbol{u}))^{*}\ E(\boldsymbol{v}, \boldsymbol{y})$. Нетрудно убедиться, что для него справедливы приведенные выше рассуждения.

Классы неполных означиваний входной переменной программы

В этом разделе введем классификацию означиваний префиксов входной переменной программы. Справедлива следующая теорема.

***Теорема* 2**. *Пусть* $F(\boldsymbol{x})$ *есть формула, представляющая функцию, вычисляемую программой* $\pi(\boldsymbol{x})$, и *означивания* α_1 и α_2 *префиксов входной переменной находятся в отношении* $\alpha_1 < \alpha_2$. *Тогда справедлива импликация* $F(\alpha_2) \supset F(\alpha_1)$.

Следствие. *Пусть* $\Im_1$ *есть множество вычислений, которые определяются программой* $\pi(\alpha_1)$ и $\Im_2$ *– множество вычислений, которые определяются программой* $\pi(\alpha_2)$. *Тогда справедливо включение* $\Im_2 \subseteq \Im_1$.

Таким образом, программа $\pi(\alpha_1)$ вычисляет функцию, которая является *обобщением* функции, вычисляемой программой $\pi(\alpha_2)$.

Говорим, что логические формулы A и B находятся в отношении $A \# B$, если неверны обе импликации $A \supset B$ и $B \supset A$.

***Теорема* 3**. *Пусть формула* $F(\boldsymbol{x})$ *представляет функцию, вычисляемую программой* $\pi(\boldsymbol{x})$, и α_1, α_2 *суть означивания префиксов входной переменной, причем формулы* $F(\alpha_1)$, $F(\alpha_2)$ *находятся в отношении* $F(\alpha_1) \# F(\alpha_2)$. *Тогда*:

1) имеются размеченные пути t_1 и t_2, *такие, что* t_1 *принадлежит программе* $\pi(\alpha_1)$ и *не принадлежит программе* $\pi(\alpha_2)$, а t_2 *– принадлежит программе* $\pi(\alpha_2)$ и *не принадлежит* $\pi(\alpha_1)$;

2) имеются конъюнкты C_1 и C_2, *такие, что* C_1 *принадлежит ОДНФ формулы* $F(\alpha_1)$ и *не принадлежит ОДНФ формулы* $F(\alpha_2)$, а C_2 *– принадлежит ОДНФ формулы* $F(\alpha_2)$ и *не принадлежит ОДНФ формулы* $F\ (\alpha_1)$.

Доказательство. Упомянутые конъюнкты C_1 и C_2 различаются подформулами E^{σ}, в которых один аргумент есть не полностью означенная входная переменная программы, а второй – рабочая метапеременная. Эти же конъюнкты определяют различные размеченные пути t_1 и t_2.

О длине вычисления программ

В этом разделе покажем, что длина вычисления программы определяется ее свойствами образовывать различные вычисления при означивании префикса ее входной переменной. Введем такое определение.

Пусть σ_x' есть означивание префикса входной переменной программы $\pi(\boldsymbol{x})$. Тогда двоичное число σ_x называется *окончательным продолжением* означивания σ_x', если $\sigma_x'\sigma_x$ есть двоичное число. Два означенных префикса σ_x' и σ_x'' входной переменной программы π называются *разделимыми*, если имеется окончательное продолжение σ_x такое, что вычисления $\pi(\sigma_x'\sigma_x)$ и $\pi(\sigma_x''\sigma_x)$ различные.

***Теорема* 4**. *Пусть* σ_x' и σ_x'' *суть два разделимых означивания и формула* $F(\boldsymbol{x})$ *получена по регулярному выражению* R_{π}. *Тогда выполняется отношение* $F(\sigma_x') \# F(\sigma_x'')$.

Доказательство. Пусть окончательные означивания $\sigma_x'\sigma_x$ и $\sigma_x''\sigma_x$ определяют разные вычисления программы, т.е. им соответствуют разные размеченные пути. Тогда этим путям в ОДНФ формул $F(\sigma_x')$ и $F(\sigma_x'')$ соответствуют две разные конъюнкции, которые истинны при различных означиваниях $\sigma_x'\sigma_x$ и $\sigma_x''\sigma_x$ входной переменной и при соответствующих правильных означиваниях метапеременных.

Следствие. *Пусть формула* $F(\boldsymbol{x})$ *получена по регулярному выражению* R_{π}, и $\{\sigma_x', \sigma_x'', \ldots, \sigma_x^{(m)}\}$ *попарно разделимые означивания префикса входной переменной программы*. *Тогда формулы* $F(\sigma_x')$, $F(\sigma_x'')$, …, $F(\sigma_x^{(m)})$ *попарно находятся в отношении* #.

Справедлива теорема.

***Теорема* 5**. *Пусть* $\{\sigma_x', \sigma_x'', \ldots, \sigma_x^{(m)}\}$ *попарно разделимые означивания префикса входной переменной программы* $\pi(\boldsymbol{x})$. *Тогда при всяком окончательном продолжении* σ_x *средняя длина вычислений* $\pi(\sigma_x^{(i)}\ \sigma_x)$ *не меньше* $log_2 m$, $i = 1, 2, \ldots, m$.

Доказательство. Пусть формула $F(\boldsymbol{x})$ представляет функцию, вычисляемую программой $\pi(\boldsymbol{x})$. Каждое означивание $\sigma_x^{(i)}$ определяет совокупность конъюнктов в ОДНФ формулы $F(\sigma_x^{(i)})$, которые содержат в качестве переменных не означенный суффикс входной переменной программы. При окончательном продолжении σ_x в точности один из них становится тождественно истинным и определяет значение программы $\pi(\sigma_x^{(i)}\ \sigma_x)$. Из соответствия конъюнктов ОДНФ формул $F(\sigma_x^{(i)})$ и размеченных путей следует, что при окончательном продолжении σ_x существуют не менее m размеченных путей соответственно $t_1, t_2, \ldots, t_m$, начинающихся во входной вершине программы и оканчивающихся в заключительной. В совокупности они определяют однокорневое бинарное дерево $T(\sigma_x)$ вычислений, в котором будет не менее m бинарных узлов, разделяющих эти размеченные пути $t_1, t_2, \ldots, t_m$. Поэтому средняя длина всех путей в нем не менее $log_2 m$.

Следствие. *Пусть* $\{\sigma_x', \sigma_x'', \ldots, \sigma_x^{(m)}\}$ *попарно разделимые означивания префикса входной переменной программы* $\pi(\boldsymbol{x})$. *Тогда*

для всякого окончательного продолжения σ_x *длина некоторого вычисления программы* $\pi(\sigma_x^{(i)}\ \sigma_x)$ *не меньше* m, $i = 1, 2, \ldots, m$.

Доказательство. Для получения 1 в l-м разряде, начиная с 0, оператору $\boldsymbol{x}+1$ требуется не менее 2^l применений. В каждой совокупности конъюнктов, выделяемых означиваниями σ_x', σ_x'', …, $\sigma_x^{(m)}$, имеется по меньшей мере одна подформула, которая имеет вид $E^{\sigma}(\sigma_x^{(i)}\boldsymbol{x'}, \alpha)$, где $\boldsymbol{x'}$ – не означенный суффикс входной переменной программы и α – рабочая метапеременная, означенный префикс которой совпадает с $\sigma_x^{(i)}$.

Заключение

Приведена нижняя оценка вычислений арифметических программ в зависимости от предметной области, над которой вычисление осуществляется. Свойства предметной области описываются как совокупность попарно разделимых означиваний префикса входных переменных программ. При такой характеристике найдется вычисление, длина которого не меньше, чем мощность множества попарно разделимых означиваний префикса входа программы.

Список литературы

1. Кормен Т.Х., Лейзерсон Ч.И., Ривест Р.Л., Штайн К. Алгоритмы: построение и анализ. М.: Вильямс, 2016.

2. Хопкрофт Д., Мотвани Р., Ульман Д. Введение в теорию автоматов, языков и вычислений. М.: Вильямс, 2012. 528 с.

3. Верещагин Н.К., Успенский В.А., Шень А. Колмогоровская сложность и алгоритмическая случайность. М.: МЦНМО, 2013. [Электронный ресурс]. URL: http:// www.mccme.ru/free-books/shen/kolmbook.pdf (дата обращения: 27.06.2019).

4. Goldreich O. P, NP, and NP-Completeness: The Basics of Complexity Theory. Cambridge University Press, 2011.

5. Попов С.В., Брошкова Н.Л. Длина вычисления арифметических программ. LAP Lambert Academic Publishing, Saarbrucken, Deutschland. 2014. 250 с.

СТАТЬЯ

УДК 621.64:519.8

ОПТИМИЗАЦИЯ ПЕРЕРАСПРЕДЕЛЕНИЯ ПОТОКОВ НА МАГИСТРАЛЬНЫХ ГАЗОПРОВОДАХ

Ильичев В.Ю., Юрик Е.А., Антипов В.С.

Калужский филиал ФГОУ ВО «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет), Калуга, e-mail: patrol8@yandex.ru

Статья посвящена обзору современных, наиболее передовых, методов оптимизации перераспределения потоков добываемого природного газа среди газодобывающих пунктов и по веткам газотранспортной системы. Рассмотрены принципы организации и основные составляющие новых систем компьютерной симуляции функционирования оборудования газоперекачивающих станций и магистральных трубопроводов. Проведённый анализ позволил предложить направления совершенствования процесса оптимизации с целью получения наиболее достоверных результатов. Отмечено, что данная работа обладает актуальностью, а выбранное направление научных исследований имеет потенциал для дальнейшей разработки, так как обобщённая методика, используемая при перераспределении потоков газа, позволяет добиться качественного повышения технико-экономических показателей предприятий и организаций топливно-энергетического комплекса (ТЭК) России, и в конечном итоге минимизации стоимости природного газа для конечного потребителя. Также важным следствием применения новых математических методов с использованием современных компьютерных мощностей является повышение бесперебойности обеспечения предприятий и частных потребителей природным газом, а также совершенствования самих процессов производства и повышения качества жизни населения. Применение разработанной методики помогает решать задачи, поставленные руководством нашего государства в рамках программы социально-экономического развития. При подведении итогов проведённой работы и по результатам анализа литературных источников предложены меры дальнейшего совершенствования организации газотранспортной сети и снижения потерь природного газа при транспортировке.

Ключевые слова: природный газ, топливно-энергетический комплекс, магистральные трубопроводы, компьютерная симуляция, линейное программирование

OPTIMIZATION OF REDISTRIBUTION OF STREAMS ON MAIN GAS PIPELINES

Ilichev V.Yu., Yurik E.A., Antipov V.S.

Kaluga Branch of Bauman Moscow State Technical University, Kaluga, e-mail: patrol8@yandex.ru

Article is devoted to the review modern, most front lines, methods of optimization of redistribution of flows of the extracted natural gas among gas points and on branches of the gas transmission system. The principles of the organization and the main components of new systems of computer simulation of functioning of the equipment of gas-distributing stations and trunk pipelines are considered. The carried-out analysis allowed to offer the directions of improvement of process of optimization for the purpose of obtaining the most reliable results. It is noted that this work has relevance, and the selected direction of scientific research has the potential for further development as the generalized technique used at redistribution of gas flows allow to achieve high-quality increase in technical and economic indicators of the enterprises and organizations of the fuel and energy complex (FEC) of Russia, and finally minimization of cost of natural gas for the end user. Increase in uninterrupted operation of providing the enterprises and private consumers with natural gas and also improvement of processes of production and improvement of quality of life of the population is also important consequence of application of new mathematical methods with use of modern computer capacities. Application of the developed technique helps to solve the tasks set by the leaders of our state within the program of social and economic development. When summing up the carried-out work and by results of the analysis of references measures of further improvement of the organization of gas transmission network and decrease in losses of natural gas when transporting are proposed.

Keywords: natural gas, fuel and energy complex, trunk pipelines, computer simulation, linear programming

Данная статья посвящена проблеме, имеющей высокую значимость в настоящее время – разработке технически и экономически обоснованной методики перераспределения потоков газа на трубопроводах газотранспортных систем. Эта методика будет полезной для применения как при эксплуатации чрезвычайно разветвлённой системы газопроводов России, так и при проектировании и закладке строительства новых веток трубопроводов. Разработанная методика является обобщённой и учитывает основные действующие факторы. Эта обобщённая методика сможет помочь разработать более детальные математические модели функционирования газотранспортных систем, с минимальным количеством допущений и упрощений. Данная методика с некоторой переработкой может стать полезной также при проектировании и эксплуатации нефтепроводов и иных трубопроводных сетей.

Цель исследования: совершенствование методики проектирования магистральных газопроводов с целью повышения их технико-экономических показателей, а также снижение затрат при добыче и транспортировке природного газа.

Материалы и методы исследования

При разработке методики необходимо произвести математическое моделирование [1], заключающееся в оптимизации управления транспортированием продуктов по трубопроводам при нормальной эксплуатации, при реконструкциях и аварийных ситуациях (экстремальная задача линейного программирования). Взаимосвязь между элементами проектируемой системы целесообразно осуществлять с помощью формирования систем равенств и неравенств, содержащих основные эксплуатационные параметры оборудования и граничные условия (ограничения) для каждого элемента транспортной системы. Обобщённые технико-экономические характеристики каждого узла газотранспортной системы также описываются в виде систем равенств и неравенств.

Целевой оптимизируемой функцией задачи линейного программирования (объектом оптимизации) будут являться экономические показатели, характеризующие рассматриваемую часть газодобывающей и газотранспортной системы в целом. Наиболее целесообразно и удобно в качестве такого показателя принять себестоимость газа для заказчика (продавца природного газа).

Для формирования исходных данных для задачи оптимизации необходимо определить основные составляющие себестоимости газа в пределах затрат на добычу и на транспортировку. Принято производить расчёт себестоимости добычи и транспортировки 1000 куб. м газа.

Согласно [2, 3] себестоимость добычи газа складывается из следующих основных составляющих:

а) затраты при добыче и промысловой подготовке газа, зависящие от используемых технологий и организации процессов (в том числе затраты топлива и электроэнергии);

б) затраты на подготовку, освоение и совершенствование производственных процессов;

в) затраты при эксплуатации очистных сооружений;

г) дополнительные затраты, связанные с осуществлением работ вахтовым методом;

д) отчисления на воспроизводство минерально-сырьевой базы;

е) затраты по обеспечению нормируемых условий труда и техники безопасности;

ж) затраты на управление производством;

з) затраты, связанные с подготовкой и переподготовкой кадров;

и) платежи банкам по кредитам и т.п.;

к) отчисления в отраслевые, внебюджетные фонды;

л) затраты на содержание производственных и вспомогательных помещений;

м) отчисления на социальные нужны, налоги, сборы, платежи и другие обязательные отчисления.

Среди рассмотренных затрат крупной газодобывающей компании сильно зависят от её месторасположения лишь пункты а)–г), поэтому при разработке методики перераспределения потоков газа в первом приближении остальные пункты затрат можно считать постоянными на 1000 куб. м добытого газа.

Согласно [4], себестоимость транспортировки газа складывается из затрат на техническое обслуживание и ремонт магистральных и вспомогательных газопроводов, а также оборудования, с помощью которого осуществляется транспорт, очистка газа и т.п.

Расход перекачиваемого газа можно рассчитать следующим образом:

$$G = G_{const} – G_{sn} – G_{pot},$$

где G_{const} – расчётный расход поступающего в трубопроводы газа;

G_{sn} – расход газа на собственные нужны транспортной сети;

G_{pot} – потери газа при транспортировке.

Себестоимость транспортировки газа складывается из тех же составляющих, что и себестоимость добычи, кроме пунктов а)–г), остальные пункты можно также считать в первом приближении постоянными на 1000 куб. м транспортируемого газа. К остальным пунктам добавляются:

– стоимость химических добавок;

– затраты на транспорт газа;

– неизбежные потери расхода при хранении и транспорте газа, расход на собственные нужды.

При расчёте потерь газа при транспортировке необходимо учитывать утечки газа из хранилищ и из трубопроводов.

При расчёте расхода газа на собственные нужды учитывается потребление газа газовыми турбинами и прочим энергетическим оборудованием, котельными, химическими лабораториями, механическими мастерскими и другими подразделениями.

К собственным нуждам также относится расход газа, стравливаемого при пусках и остановках компрессорных агрегатов, при заправке метанола в газопроводы, при продувке пылеуловителей, сепараторов и конденсатоотводчиков, расходуемый на продувку трубопроводов для освобождения его от конденсата, воды, грязи и т.п.

Таким образом, можно обобщить, что себестоимость добычи и транспортировки

газа состоит из совокупности постоянных затрат, на которые влиять практически невозможно, и переменной части затрат, которая зависит главным образом от месторасположения пунктов добычи газа, конструкции и протяжённости трубопроводных систем и режимов работы газоперекачивающего и прочего оборудования (собственно транспортные затраты).

Для проведения расчётов по стоимости транспортировки газа по различным участкам сети вначале необходимо построить топологическую схему рассматриваемой сети. В настоящее время такие построения производятся с помощью так называемых компьютерных симуляторов [1].

Компьютерный симулятор состоит из трёх взаимосвязанных систем. Первой системой является интерактивный интерфейс для воспроизведения на компьютере реальной системы газопроводов, с учетом их диаметров, материалов, топологии прокладки, состава и месторасположения компрессорных станций, вентилей, регулирующих клапанов и т.д.

Как и в любой системе обработки информации, в компьютерном симуляторе присутствует база данных, состоящая из структурированной информации, полученной из первой системы (интерактивного интерфейса) и динамически изменяющейся информации по текущему расчёту перераспределения загрузки оборудования, расходов газа по веткам газотранспортной сети и т.д.

Двумя рассмотренными системами компьютерного симулятора управляет программно-расчётный комплекс, реализующий метод решения экстремальной задачи линейного программирования.

Таким образом, для проведения анализа работы реальной системы магистральных трубопроводов и компрессорных станций, с помощью визуальных редакторов топологии задаются паспортные характеристики и режимные параметры элементов исследуемой системы: турбоприводов, нагнетателей, данные об условиях транспортирования природного газа, о техническом состоянии оборудования и т.д. Параметры оборудования задаются исходя из проектной и технической документации, результатов испытаний.

Пример интерфейса компьютерного симулятора AMADEUS, работающего в многопользовательском режиме, приведён на рис. 1. Этот симулятор использовался для управления трубопроводной сетью Международной газотранспортной компании «SPP» [5].

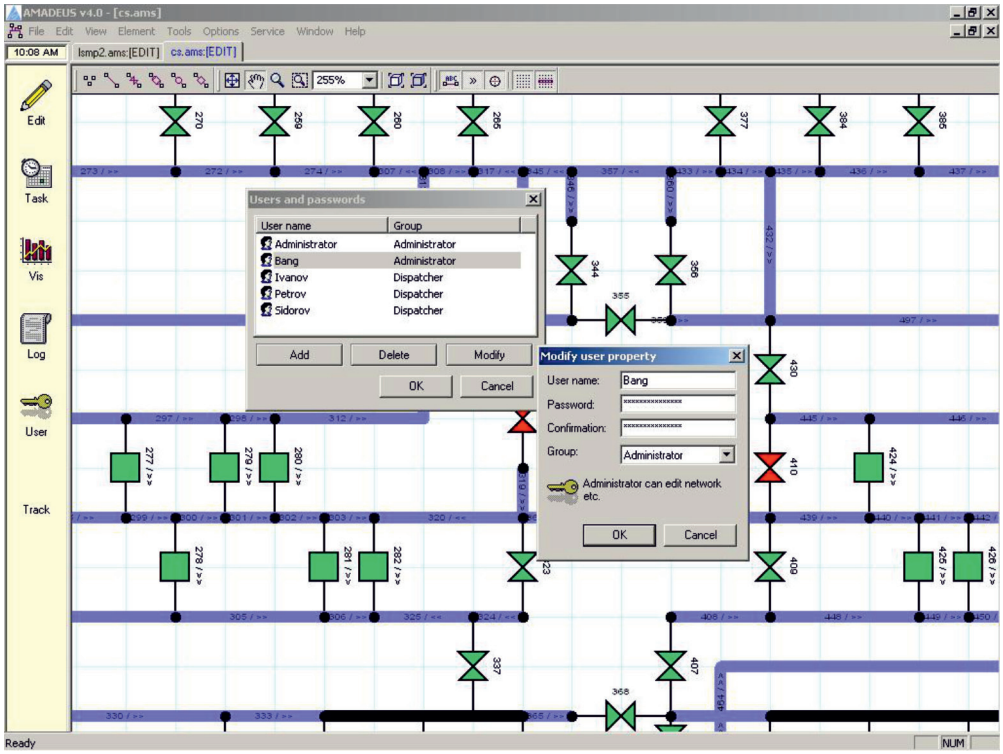

Рис. 1. Интерфейс компьютерного симулятора AMADEUS

Оптимизация транспортирования газа через трубопроводную сеть газотранспортного предприятия осуществляется путём использования газодинамического симулятора для построения и решения задачи оптимизации путём численного анализа параметров и режимов работы магистральных газопроводов и станций компримирования газа.

Ядро компьютерного симулятора создано путём формализации математических моделей механики и газодинамики для описания процессов, происходящих в трубопроводах и прочем газотранспортном оборудовании при эксплуатации в паспортном режиме, испытаниях и при проведении модернизации. Конкретнее используются следующие хорошо отработанные физико-математические модели: система уравнений механики жидкостей и газов, система уравнений равновесия деформируемого твердого тела. Так как системы уравнений, описывающих данные процессы, являются очень громоздкими и сложными для вычисления, для решения задачи нахождения оптимума приходится вводить необходимые упрощения и допущения. Глубина упрощений ещё больше увеличивается в случае, если необходимо исследовать модель функционирования системы транспорта газа в динамике, тем более при необходимости обеспечения режима работы компьютерного симулятора в реальном времени.

Оптимизация, производимая симулятором, заключается в подборе параметров работы оборудования и загрузки газотранспортных веток с целью достижения максимума или минимума заданного параметра оптимизации (чаще всего, это минимум себестоимости транспортировки газа от начального пункта в конечный, рассчитанная только по стоимости потребляемой оборудованием энергии).

Результаты оптимизации параметров работы оборудования и загрузки магистральных трубопроводов отображаются графически на составленном при задании исходных данных изображении расчетной схемы (мнемосхемы) с помощью гистограмм, эпюр, текста и т.п.

Также можно вывести на экран результаты расчёта стоимости транспортировки газа до и после оптимизации (рис. 2).

К сожалению, используемые в настоящее время симуляторы при оптимизации не учитывают иных затрат, кроме затрат на энергию и поэтому требуют дальнейшего совершенствования. Для этого в структуру учитываемых факторов необходимо включить дополнительные затраты, указанные выше в данной статье. Это потребует увеличения вычислительной мощности компьютеров либо проведения вычислений в течение довольно длительного времени, но результаты расчётов преобретут гораздо большую достоверность.

Результаты исследования и их обсуждение

Преимущество рассмотренной методики с учётом её доработки состоит в том, что она на протяжении всего жизненного цикла оборудования магистральных трубопроводов (при проектировании, эксплуатации и реконструкции) позволит более точно корректировать перераспределение потоков газа, а также состав и загрузку оборудования.

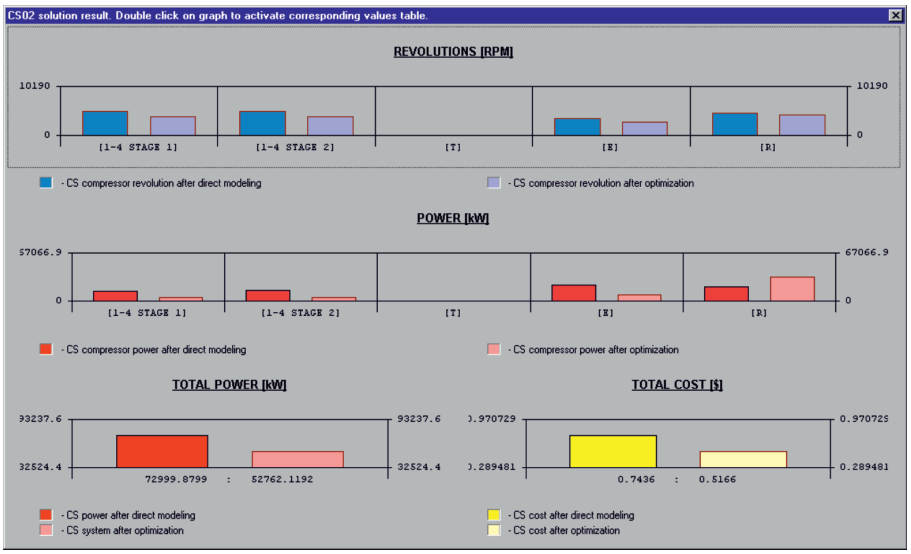

Рис. 2. Результаты оптимизации системы транспортировки газа

Для внедрения в процесс расчёта и оптимизации магистральных трубопроводов предложенной методики необходимы будут дополнительные расходы. Потребуется разработка нового, более совершенного, программного обеспечения, существенное повышение мощности используемой компьютерной техники, на обучение инженеров-проектировщиков и техников применению компьютерных симуляторов и т.д.

Предложенный метод проектирования позволит повысить глубину оптимизации за счёт учёта описанных выше дополнительных статей затрат и уменьшения количества допущений, поэтому затраты на внедрение новых методик, безусловно, окупятся.

Окупаемость метода достигается за счет повышения безопасности эксплуатации и большего срока службы газотранспортных систем, а также сокращения затрат на строительство и эксплуатацию трубопроводных веток [6].

Для снижения расхода газа на собственные нужды (и тем самым минимизации материальных затрат) можно порекомендовать безусловное внедрение рационализаторских предложений и технических усовершенствований. Уменьшение расхода газа на собственные нужды и потери также позволяет обеспечить бесперебойный режим обеспечения газом потребителей, из-за чего эффективность работы газотранспортной сети существенно повышается. Это является одним из путей решения народнохозяйственных задач, сформулированных Правительством РФ.

Одновременно необходимо стремиться к постоянному сокращению потерь природного газа за счет внедрения следующих мероприятий:

– своевременное проведение ремонтов и технического обслуживания агрегатов и оборудования с целью улучшения их характеристик, в частности КПД;

– эксплуатация скважин добычи, газоперекачивающего оборудования и газопроводов без сброса газа в атмосферу.

Заключение

Таким образом, цель данной работы выполнена – произведён обзор и анализ наиболее современных методов оптимизации перераспределения потоков природного газа по участкам транспортной системы. Выработан ряд рекомендаций по дальнейшему совершенствованию и отработке данных методов на практике. Также даны рекомендации по уменьшению потерь природного газа при добыче и транспортировке.

Список литературы

1. Селезнев В.Е., Алешин В.В., Прялов С.Н. Основы численного моделирования магистральных трубопроводов. Москва – Берлин: Директ-Медиа, 2014. 436 с.

2. Босова И.Ю., Орлов Ю.Н., Семенцова В.А. Расчет показателей экономической эффективности нефтегазовых проектов в нестационарных сценариях внешних условий // Препринты ИПМ им. М.В. Келдыша, 2010. № 19. 26 с.

3. Методика по планированию, учету и калькулированию себестоимости добычи нефти и газа от 29.12.1995. М.: Минтопэнерго России, 1995. 32 с.

4. Вовк В.С., Новиков А.И., Глаголев А.И., Орлов Ю.Н., Бычков В.К., Удалов В.А. Мировая индустрия и рынки сжиженного природного газа: прогнозное моделирование. М.: ООО «Газпром экспо», 2009. 312 с.

5. Селезнев В.Е., Алешин В.В., Прялов С.Н. Основы численного моделирования магистральных трубопроводов / Под ред. В.Е. Селезнева. Изд. 2-е, перераб. и доп. М.: МАКС Пресс, 2009. 436 с.

6. Селезнев В.Е., Прялов С.Н. Технологии высокоточного компьютерного моделирования для управления жизненными циклами трубопроводного транспорта // Управление развитием крупномасштабных систем: труды Пятой международной конференции. Учреждение Российской академии наук Институт проблем управления им. В.А. Трапезникова. М.: РАН, 2011. С. 16–25.

СТАТЬЯ

УДК 007.52:551.46.06/.07/.08/.09

ЗАРЯДНЫЕ СТАНЦИИ АВТОНОМНЫХ РОБОТОТЕХНИЧЕСКИХ СИСТЕМ ОКЕАНОЛОГИЧЕСКИХ ИССЛЕДОВАНИЙ

Горлов А.А.

Институт океанологии им. П.П. Ширшова РАН, Москва, e-mail: oceangorlov@yahoo.com

В последние годы всё более востребованной научной общественностью и специалистами-практиками многих странах мира становится концепция «Цифрового океана» (Digital Ocean), разрабатываемая за рубежом во главе с Институтом океанографии Скриппса (США), а в России – Институтом океанологии им. П.П. Ширшова РАН (ИО РАН). Она направлена на всестороннее изучение Мирового океана путем расширения масштабов скоординированного использования различных новых средств океанской техники – автономных морских измерительных платформ с разнообразными датчиками, приборами и инструментами, а также распределенных робототехнических систем. Это позволяет внедрять новые научные программы и методики, основанных на сборе и анализе больших массивов данных (Big data). Для разработки программ использования средств океанской робототехники по многим научным направлениям ИО РАН необходимо изучение такого опыта в мировой практике наблюдений в морях и океанах. С этой целью в статье показаны преимущества зарубежных кабельных и автономных систем долговременных океанологических исследований. Особое внимание уделено одному из основных элементов таких автономных систем – узловым коммуникационным и зарядным станциям электроснабжения морских беспилотников и других средств океанотехники, предназначенных для решения широкого круга разнообразных океанологических, климатических и прикладных задач исследований Мирового океана с ограниченным использованием экспедиционных судов.

Ключевые слова: кабельные и автономные системы, океанологические исследования, морская робототехника, поверхностные и подводные беспилотники, АНПА, зарядные станции, Мировой океан

CHARGING STATIONS OF AUTONOMOUS ROBOT TECHNICAL SYSTEMS OF OCEANOLOGICAL RESEARCH

Gorlov A.A.

P.P. Shirshov Institute of Oceanology RAS, Moscow, e-mail: oceangorlov@yahoo.com

In recent years, the concept of the «Digital Ocean», developed abroad led by the Scripps Oceanography Institute (USA), and in Russia by the P.P. Shirshov Institute of Oceanology RAS (IO RAS), has become more and more popular among the scientific community and practitioners in many countries of the world. It is aimed at a comprehensive study of the oceans by expanding the scale of the coordinated use of various new means of ocean technology – autonomous marine measuring platforms with a variety of sensors, instruments and tools, as well as distributed robotic systems. This allows you to introduce new scientific programs and techniques based on the collection and analysis of large data arrays (Big data). To develop programs for using ocean robotics in many scientific fields of the IO RAS, it is necessary to study such experience in the global practice of observations in the seas and oceans. To this end, the article shows the advantages of foreign cable and autonomous systems for long-term oceanological research. Particular attention is paid to one of the main elements of such autonomous systems – nodal communication and charging stations for power supply of marine drones and other ocean engineering equipment, designed to solve a wide range of diverse oceanological, climatic and applied problems of ocean research with limited use of expeditionary vessels.

Keywords: cable and autonomous systems, oceanological research, marine robotics, surface and underwater drones, AUV, charging stations, the World Ocean

Современные средства робототехники могут использоваться для исследований и наблюдений в Мировом океане несколькими различными способами. Наиболее распространенными до сих пор являются традиционные экспедиции научно-исследовательских судов (НИС) с телеуправляемыми подводными аппаратами (ПТА) или автономными необитаемыми подводными аппаратами (АНПА) на борту. Последнее время к АНПА и ПТА часто добавляются поверхностные и подводные глайдеры и воздушные беспилотники (рис. 1), что позволяет выполнять комплексные исследования на достаточно больших площадях акваторий [1]. Однако использование НИС в качестве носителей средств океанской исследовательской робототехники обходится очень дорого, и поэтому длительность таких экспедиций обычно существенно ограничена.

Другим всё шире внедряемым направлением выполнения океанологических исследований является применение поверхностных и подводных беспилотников (глайдеров) повышенной автономности с малым энергопотреблением или с использованием бортовых возобновляемых источников энергии (ВИЭ). Такие средства робототехники эффективны, экономичны и способны работать автономно несколько месяцев или даже лет [1, 2]. Но для всесторонней оценки океанологических процессов требуется использование одновременно огромного количества таких беспилотников,

что существенно усложняет задачи исследований с организационной и финансовой стороны. Кроме того, их малые собственные размеры позволяют устанавливать на них только ограниченное количество датчиков и приборов, что часто делает их достаточно специализированными. Существенно большими функциональными возможностями обладают протяженные донные кабельные сети океанологических исследований, к которым присоединено множество приборов и средств робототехники, но их создание и эксплуатация требует огромных затрат. Наконец, наиболее перспективными являются активно разрабатываемые в настоящее время за рубежом автономные системы океанологических исследований с энергетическим обеспечением всех основных элементов за счет использования собственных зарядных станций на базе ВИЭ.

Океанологические исследования путем использования кратковременных единичных экспедиций НИС или подводных обитаемых аппаратов (ПОА) обычно не дают возможность получать непрерывные большие ряды данных. В свою очередь, это затрудняет проведение качественного анализа процессов, проходящих в океане, и создания их достоверных математических моделей. Перспективным направлением для решения задач долговременных широкомасштабных наблюдений в океане является создание и использование в прибрежных районах различных стран мира донных кабельных сетей большой протяженности. Примером такой кабельной сети может служить система «NEPTUN Canada» на шельфе Канады, доходящая до очень важных для ученых тектонических районов дна океана, с гидротермальными полями на глубинах более 2,7 км [3]. Сеть имеет общую длину оптоволоконных кабелей около 1000 км с встроенными в неё узловыми модулями (рис. 2), к которым присоединены различные исследовательские приборы и оборудование (блоки датчиков, сейсмографы, видеокамеры системы вертикального профилирования, ПТА и другое). Поступающие от них разнообразные данные по кабелям непрерывно передаются в Центр, а от него в систему передаются электроэнергия и команды управления.

С помощью мощной информационной онлайновой системы «Oceans 2.0» любой специалист может через интернет получать данные и наблюдать подводную картину непосредственно в интересующей его точке около кабельной сети. В рамках программы роботизированных исследований экстремальных сред (ROBEX), объединяющей космические и глубоководные исследования в Германии, были созданы донные гусеничные ПТА «Wally» (рис. 2). Эти аппараты, разработанные в привязном кабельном и автономном вариантах, в течение многих лет поочередно подключались к сети обсерватории «NEPTUNE Canada» и обеспечили сбор цифровых и видеоданных на больших глубинах [4].

Рис. 1. Средства робототехники для океанологических исследований на причале около научного судна Национального океанографического центра Великобритании

Особый интерес представляют автономные аппараты этой серии, типа «Viator» и «Tramper», оснащенные различными датчиками и микрозондами, видеокамерами с высоким разрешением, совершенными навигационными системами и манипуляторами. АНПА «Viator» способен отстыковываться от узлового модуля кабельной сети, работать автономно по заданной траектории, а затем возвращаться к узловому модулю для подзарядки бортовых аккумуляторов. Ещё более совершенным является АНПА «Tramper», автономность которого на дне между автоматическими подзарядками составляет около года. Большое значение при развертывании научного оборудования донной кабельной сети и получения информации о процессах в океане обеспечили также ПТА типа «ROPOS» (рис. 2), связанные с НИС или узловыми модулями гибкими оптоволоконными кабелями для энергоснабжения и передачи информации.

Комплексное совместное использование различных датчиков и измерительных приборов в определенном районе Мирового океана повышает эффективность сбора различного рода данных. Поэтому над кабельными сетями дополнительно регулярно работают НИС «Thomas G. Thompson» и другие суда, оснащенные разнообразными измерительными приборами, ПТА, АНПА и глайдерами для регистрации параметров на поверхности, в водной среде и на дне. Широкому распространению кабельных систем препятствуют огромные расходы, связанные с их развертыванием и эксплуатацией, и постоянная привязка к конкретному району исследования, без возможности перемещения её на новую акваторию.

Автономные сети океанологических исследований

В качестве альтернативы кабельным сетям нами в ИО РАН была разработана концепция долговременной автономной системы океанологических исследований, элементы которой получают питание от различных видов возобновляемой энергии океана (АСОИ ЭО) [5]. Конструктивно система АСОИ ЭО состоит из необходимого количества автономных стационарных узловых станций (СУП), вокруг базируются мобильные автономные измерительные платформы (АИП) и привязные измерительные платформы (ПИП), соединенные с СУП кабелями (рис. 3). В число АИП входят разнообразные плавучие зонды, АНПА и глайдеры, а к ПИП относятся блоки научных приборов, профилирующие зонды, обсерватории и ПТА.

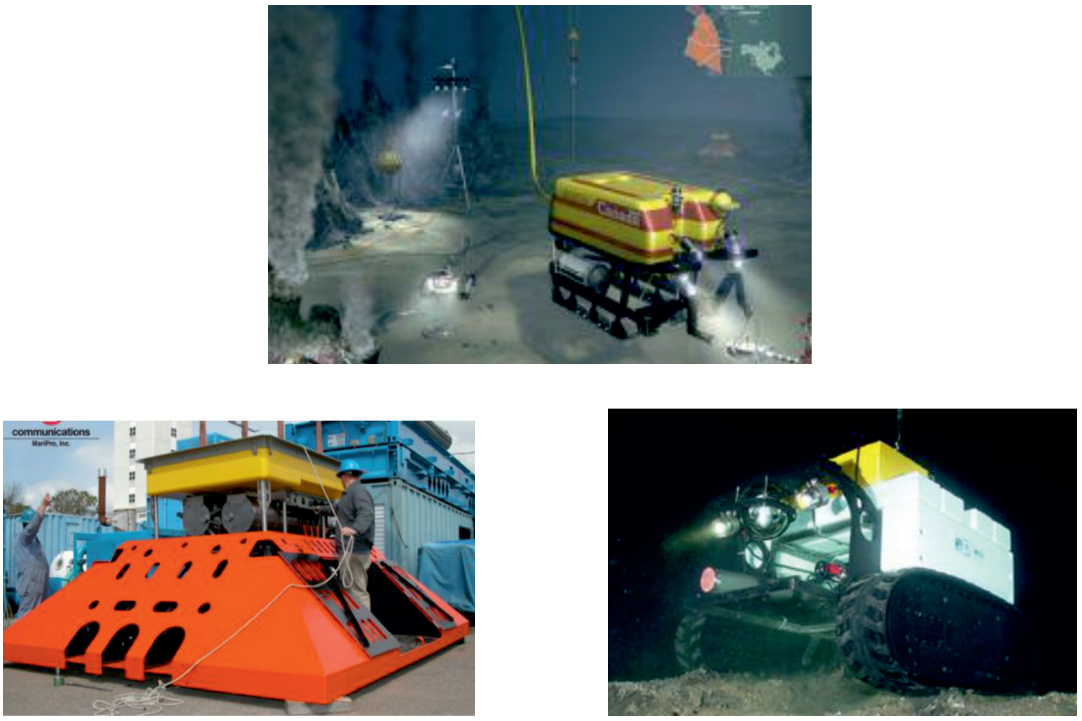

Рис. 2. Участок сети «NEPTUN Canada» с научным оборудованием и ПТА «ROPOS» (сверху), донный узловой модуль на берегу (внизу слева) и донный ПТА «Wally» около полей газогидратов (внизу справа)

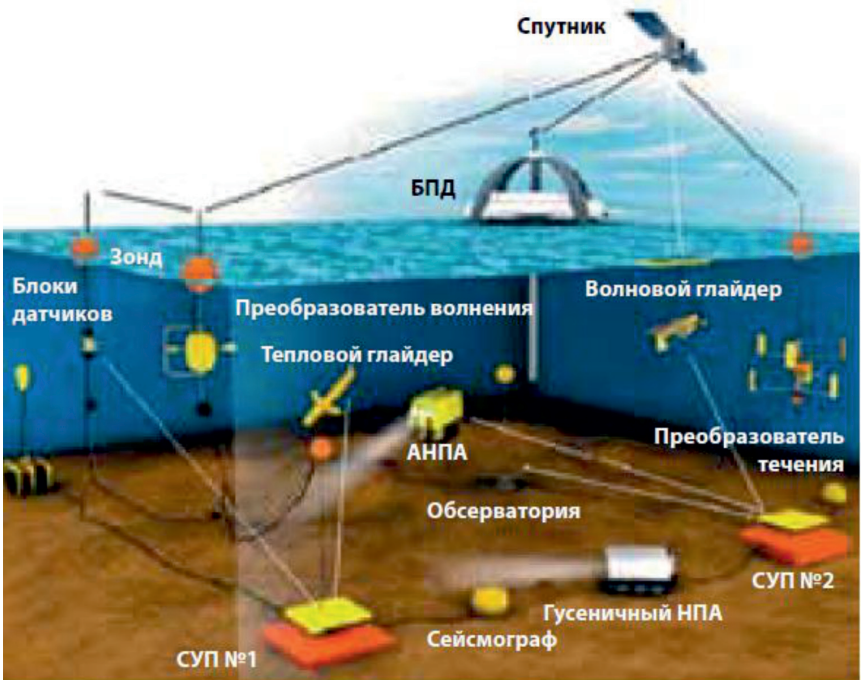

Рис. 3. Фрагмент системы АСОИ ЭО

Энергообеспечение такой системы обеспечивается блоками преобразователей различной мощности (от ватт до сотен киловатт), использующих энергию поверхностного волнения, солнечной радиации, подводных течений, теплового градиента океана и морского ветра. Для бесперебойного питания различных научных приборов, ПТА, АНПА и оборудования системы АСОИ ЭО необходимы разнообразные буферные накопители, аккумулирующие электроэнергию, поступающую от преобразователей. Одним из основных элементов системы АСОИ ЭО являются СУП, с одной стороны, представляющие собой узловые коммуникационные станции, обеспечивающие по гидроакустическим, кабельным и спутниковым каналам связь между всеми элементами системы, а с другой – узловые электростанции на базе морских ВИЭ, служащих для кабельного энергообеспечения, расположенных вокруг ПИП и для подводной подзарядки АИП путем стыковки с СУП или от неё через индукционные блоки. Обычно СУП состоит из автономного поверхностного стабилизированного буя и соединенного с донного модуля, аналогичного стационарному модулю системы «NEPTUN Canada» (рис. 2), Большим преимуществом по сравнению с кабельными системами является возможность, при необходимости, сравнительно легкого и дешевого переноса связок «буй – донный модуль» всех СУП, входящих в состав АСОИ ЭО в любой новый район Мирового океана. В свою очередь, все СУП региональной системы исследований должны располагаться на удалении в несколько миль вокруг мобильных базовых платформ управления и сбора данных (БПД), на которых будут расположены крупные дата-центры и где могут непрерывно работать вахтовым методом различные специалисты и ученые-океанологи. Такие БПД станут также местом постоянного базирования комплексов ПОА, ПТА, АНПА и воздушных дронов. В перспективе экологически чистые БПД, с полным обеспечением всех бортовых систем от возобновляемой океанской энергии, заменят существующие НИС для проведения экспедиционных исследований.

Зарядные станции для средств океанской робототехники в составе СУП АСОИ ЭО

Эффективность использования автономных поверхностных и подводных средств робототехники значительно повышается, если имеется возможность подзарядки их бортовых накопителей энергии непосредственно в районе проведения океанологических исследований. Использование НИС для этой цели обходится очень дорого, поэтому необходимы специальные автономные океанские зарядные станции, которые целесообразно интегрировать в состав оборудования стационарных узловых энергетических и коммутационных платформ (СУП) сетей АСОИ ЭО.

Наиболее часто на исследовательских подводных беспилотниках в качестве бортового источника энергии используются либо литий-ионные аккумуляторы – АНПА «Remus» (США), «Explorer» (Канада), «Alistar» (Франция), «Talisman» (Великобритания), либо литий-полимерные – АНПА «Bluefin» (США), «Hugin100» (Норвегии), «Seaotter MK II» (Германия), «AUV-150» (Индия), «Autosub6000» (Великобритания) и «Isimi6000» (Южная Корея) [6]. По сравнению с другими накопителями такие аккумуляторы отличаются высоким напряжением, значительной емкостью, малыми массой и габаритами, большим количеством циклов заряда-разряда и долговечностью. Именно использование такого типа бортовых накопителей в сочетании с автономными узловыми станциями их подзарядки обеспечивает широкие возможности для океанологических океанских исследований робототехническими средствами. Обычно автономная станция подводной зарядки получает энергию от дизеля, газовой турбины или накопителя большой мощности, что ограничивает её собственную долговременность работы. Эту проблему позволяет полностью решить использование различных видов возобновляемой энергии океана [5], которая способна обеспечить непрерывную работу зарядной станции в течение нескольких лет.

Использование энергии поверхностного волнения для зарядных станций беспилотников

Одним из первых в этом направлении в 2002 г. был предложен шведский проект буя с гидравлическим преобразователем энергии поверхностного волнения для электроснабжения подводного гаража (док-станции) подзарядки АНПА [7]. Эта идея была развита в 2011 г. американской компанией «Ocean Power Technologies» (OPT), разработавшей энергетический буй-преобразователь энергии волнения PowerBuoy (APB350) для электроснабжения подводной зарядки АНПА [5, 6]. Конструкция зарядной станции на базе APB350 представлена на рис. 4.

Стабилизированный буй «PowerBuoy» (APB350) действует как постоянно подзаряжаемый источник бесперебойного питания. Он предназначен для работы в океане в районах с широким диапазоном глубин от 20 м до 3000 м. Вертикальные колебания на волнении тороидального поплавка, размещенного на цилиндрическом корпусе стабилизированного буя, с помощью гидравлической системы обеспечивает работу привода высокоскоростного генератора со средней мощностью в 400 Вт, снабжающего электроэнергией накопитель большой емкости подводного гаража (док-станции) зарядки АНПА [8]. Кроме того, этот накопитель обеспечивает питанием бортовое оборудование буя и системы связи с берегом, а также расположенные на дне различные средства океанской техники. Общая длина буя составляет 13,3 м и масса 8,0 т, осадка буя 9,3 м, диаметры корпуса и поплавка буя соответственно 1,0 м и 2,65 м. Энергобуй APB350 обеспечивает среднюю дневную выработку электроэнергии 8,4 кВт-ч, пиковую мощность полезной нагрузки от 3,0 до 7,0 кВт и выходы электроэнергии постоянного тока напряжением 24 В и 300 В. Проект APB350 объединяет передовые запатентованные технологии в области гидродинамики, электроники, преобразования энергии и компьютерных систем управления, что позволило получить долговременный, автономный, надежный источник экологически чистой возобновляемой электроэнергии для различных океанских средств робототехники, датчиков и приборов анализа данных, телекоммуникаций и передачи данных на берег.

Использование волновых зарядных станций для АНПА в нефтегазовом секторе

Нефтяная компания «Eni» (Италия) подписала контракт с компанией «OPT» на многолетнюю установку с конца 2018 г. энергобуя APB350 у итальянского побережья для мониторинга морской среды и инспекции морских объектов с использованием морских беспилотников [9, 10]. При этом по проекту «Eni MaREnergy» технология APB350 используется в качестве автономной зарядной станции для системы связи и дистанционного управления, а также подводной зарядки аккумуляторов АНПА, что обеспечивает их долговременную работу на больших площадях акватории. За полгода выполнения этой программы, к лету 2019 г., волновым буем APB350 было уже выработано более 1,0 МВт-ч электроэнергии. Интересно отметить, что управление всем исследовательским комплексом в Адриатическом море постоянно осуществляется дистанционно из расположенного в США центра в Нью-Джерси [10]. Специалисты отмечают, что успешно развивающийся проект «OPT» с «Eni» демонстрирует возможности использования энергетических и коммуникационных платформ на базе APB350 «PowerBuoy» для широкого спектра операций по разведке и добыче нефти и газа в суровых морских условиях,, включая зарядку подводных беспилотных аппаратов для обеспечения их долговременной автономности, океанологические и метеорологические исследования, мониторинг и инспекцию скважин с помощью АНПА, а также вывод подводного оборудования из эксплуатации (рис. 5).

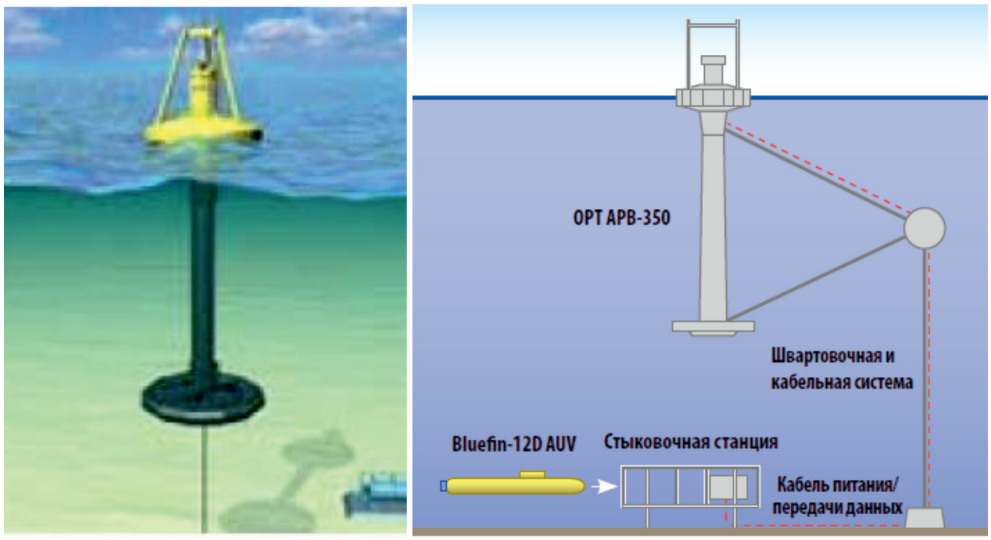

Рис. 4. Конструкция волнового энергетического буя APB350 «PowerBuoy» (слева) и гараж (док-станция) подводной зарядки АНПА от этого буя (справа)

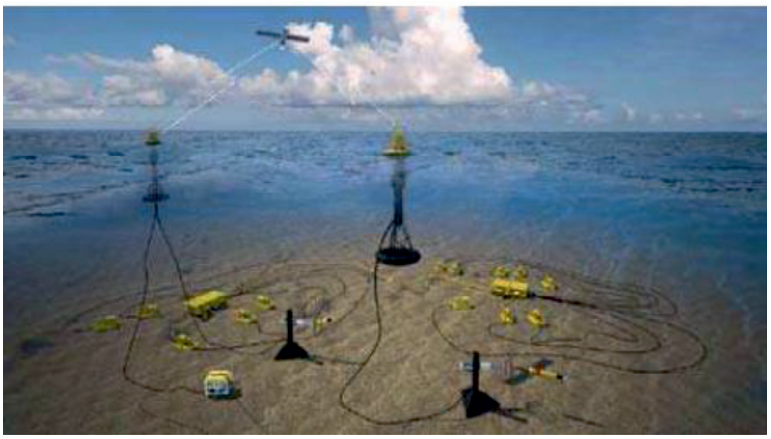

Рис. 5. Стабилизированный буй – преобразователь энергии волнения APB-350 в акватории нефтяной платформы для электроснабжения средств морской робототехники и передачи информации

Аналогичное соглашение компания «OPT» подписала с компаниями «Premier Oil» и «Acteon», управляющими большим количеством морских нефтегазовых месторождений по всему миру, на установку в 2018 г. волновых буев APB350 для работы около нефтяных платформ в центральном и британском секторах Северного моря [11]. Основной целью этих проектов является изучение, при поддержке шотландского Центра нефтегазовых технологий, взаимных перспектив офшорной нефтегазовой отрасли и возобновляемых источников энергии на мировых рынках. Для этого планируется исследовать в натурных условиях системы подводной робототехники и АНПА для мониторинга и обеспечения безопасности подводного оборудования с электропитанием от волновых зарядных станций, в частности выполнять постоянные измерения давления и температуры в скважинах, а также использовать системы сбора данных и связи береговых центров с подводными модулями управления. Всё это потенциально может значительно сократить затраты нефтегазовых компаний на надежный и безопасный вывод подводного оборудования из эксплуатации в конце завершения срока работы скважин.

Китайская зарядная станция для АНПА с волновым МГД преобразователем

Другой перспективный проект автономной зарядной станции для океанской

робототехники разработан рядом институтов Академии наук Китая [6]. Устройство (рис. 6) представляет собой поверхностный стабилизированный буй (1) с демпфером в подводной части (2) и поплавком (3), возвратно-поступательное движение которого на волнении приводит в движение жидкометаллический магнитно-гидродинамический (МГД) преобразователь энергии.

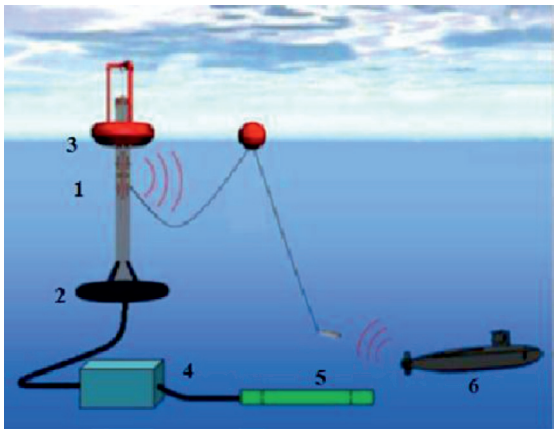

Рис. 6. Стационарная узловая платформа АСОИ ЭО с зарядной станцией на базе точечного МГД преобразователя энергии поверхностного волнения

Вырабатываемая буем электроэнергия поступает по кабелю на установленный на дне мощный литиево-ионный подводный накопитель энергии (4), соединенный кабелем с индукционным блоком (5) бесконтактной подзарядки батарей АНПА (6) и других средств подводной робототехники. Удлиненный цилиндрический корпус буя диаметром 1,0 м, оснащенный в нижней части демпферной пластиной диаметром 6,0 м, обеспечивает его хорошую устойчивость в широком диапазоне параметров волнения. Это позволяет тороидальному поплавку диаметром 4,0 м скользить вверх-вниз по корпусу буя, отслеживая профиль волнения, за счет чего приводится в движение жидкий металл (галинстан – сплав галлия, индия и олова), который, протекая в магнитном поле МГД генератора, обеспечивает производство электроэнергии. Важным преимуществом использования для зарядной станции МГД преобразователя энергии волнения от механико-гидравлического преобразователя APB350 (США) является его практически бесшумная работа, что часто бывает необходимо для проведения гидроакустических исследований в океане.

Прототип МГД преобразователя энергии волнения был разработан в Китае в 2011 г., дальнейшее его усовершенствование позволило получить к 2015 г. при испытаниях в натурных условиях возле острова Чжухае выходную мощность 2,2 кВт. На основе полученных результатов испытаний была разработана подводная зарядная станция для АНПА «Odyssey II», оснащенного бортовой литиево-полимерной батареей, емкостью 1,0 кВт-ч. Для её подзарядки требуется постоянный ток силой 10 А и напряжением 36 В. Максимальная глубина погружения беспилотника этого типа составляет 3000 м, скорость движения до 3,0 узлов, сухой вес 200 кг, длина 2,2 м и диаметр 0,58 м. Бесконтактная индукционная передача электроэнергии имеет ряд преимуществ перед контактным «мокрым» соединением АНПА с гаражом (док-станцией), к которым относятся: отсутствие коррозии разъемов и высоких требований по точности подводной стыковки-расстыковки.

Индукционный блок рассматриваемой зарядной станции способен обеспечить зарядку бортовых аккумуляторов АНПА «Odyssey II» с максимальной мощностью передачи электроэнергии до 1,27 кВт и эффективностью около 85 %. Доработанный проект зарядной станции с МГД генератором, мощностью 4,4 кВт при натурных испытаниях позволил производить одновременно подзарядку трех АНПА, а также обеспечивать электроэнергией приборы океанологического мониторинга окружающей водной среды и спутниковый канал передачи полученных данных. В законченном, рабочем варианте такая зарядная станция при поверхностном волнении высотой 2,4 м и периодом 5,2 с должна обеспечить генерацию около 105,6 кВт-ч и бесконтактную передачу электроэнергии емкостью 57,8 кВт-ч, чего достаточно для зарядки 51 беспилотника типа АНПА «Odyssey II» в течение только одного дня [6].

Использование энергии течений для зарядных станций беспилотников

В 2010 г. сотрудниками Вудс-Холского океанографического института (США) был создан подводный блок «Flip Wing» с турбиной малой мощности, специальный профиль лопаток рабочего колеса которой позволял эффективно использовать кинетическую энергию течений с малыми скоростями потока для обеспечения электроэнергией автономной зарядной станции АНПА [6]. В 2017 г. шотландская компания «EC-OG» завершила натурные испытания в Европейском центре морской энергии (EMEC) автономной зарядной станции «Subsea Power

Hub» (рис. 7), представляющей собой гибридный подводный блок гидротурбины с вертикальной осью (3) и генератор (4) для преобразования энергии океанических течений в электрическую энергию, поступающей во встроенный бортовой литиево-ионный накопитель (2) большой емкости [12]. На энергетическом блоке установлены также аппаратура передачи-приема данных (1) и модуль (5) управления работой скважиной во время подводной добычи нефти и газа, получающей питание от зарядной станции.

Возможность использовать возобновляемую электроэнергию прямо в точке проведения буровых работ позволяет отказаться от многочисленных кабелей и гидравлических шлангов к поверхности или берегу, что значительно снижает капитальные затраты, а также повышает надежность и эффективность офшорных нефтегазовых работ. Подводные блоки «Subsea Power Hub» предназначены для автономного питания различной подводной инфраструктуры и средств робототехники, в том числе и для зарядных станций бортовых батарей АНПА, выполняющих долговременные океанологические исследования.

АСОИ ЭО как средство повышения эффективности океанологических исследований

Кроме обеспечения энергией стационарных узловых платформ АСОИ ЭО, включая автономные зарядные станции АНПА и других средств океанской робототехники для океанологических исследований и офшорной нефтегазовой индустрии, подобные энергетические блоки могут быть широко использованы в различных направлениях морской экономики, таких как обеспечение электроэнергией и холодом центров обработки данных морского базирования, электроснабжения морских рыбных ферм и опреснительных установок, в офшорной ветровой энергетике, а также для снабжения чистой электроэнергией населения островных государств и т.д. Так как чистая энергия вырабатывается непосредственно в точке потребления, это обеспечивает значительное снижение выбросов CO_2 по сравнению с традиционными источниками энергии.

Внедрение системы АСОИ ЭО может также значительно повысить качество научных исследований за счет того, что использующиеся в ней основные элементы и робототехнические средства с энергоснабжением от возобновляемой энергии океана позволяют автоматически и практически без временных ограничений получать непрерывные большие массивы различных данных о биологических, геологических, физических и химических процессах в океане. Кроме того, отсутствие дефицита энергии позволяет обеспечить постоянный обмен данными и управляющей информацией в реальном масштабе времени между элементами АСОИ ЭО и дата-центрами, а также дистанционно изменять программы наблюдений и порядок взаимодействия технических средств непосредственно в исследуемой среде [5]. Получаемые от АСОИ ЭО высококачественные океанологические и метеорологические данные возможно использовать в сложных многофакторных математических моделях и получать гораздо более точные прогнозы погоды или вероятных природных и технологических катастроф, а значит – предотвратить гибель людей и значительный экономический ущерб.

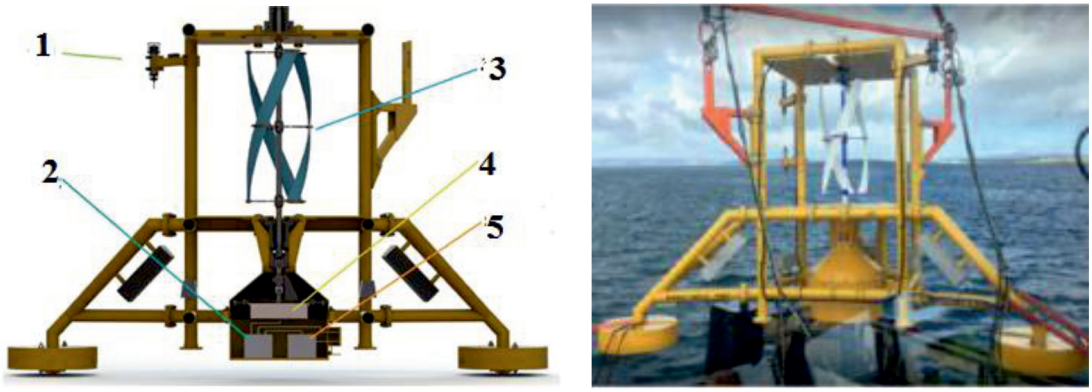

Рис. 7. Подводный преобразователь энергии течений «Subsea Power Hub» с встроенным накопителем зарядной станции для средств робототехники

Заключение

В последние годы многие из 33 океанских научно-исследовательских судов Российской академии наук, Росгидромета и Роснедр пришли в «катастрофическое и кризисное состояние» и они «могут полностью прекратить работу в ближайшие годы» [2]. Выполненные нами оценки показали, что стоимость строительства и эксплуатации океанских беспилотников за 35-летний «жизненный цикл» в десятки сотен раз меньше, чем у НИС [2]. Кроме того, актуальность использования экологически чистой морской робототехники значительно повышается с учетом новых требований к морским судам в области выбросов выхлопных газов дизелей с большим содержанием вредных оксидов азота и серы. Без дорогостоящей модернизации отечественных НИС под новые правила им просто могут запретить выход в море. Единственный эффективный выход из создавшейся в нашей стране ситуации заключается в ускоренном развитии океанских средств робототехники повышенной автономности и широком внедрение систем концепции АСОИ ЭО (Digital Ocean). Для этого необходимо разобраться, какие океанологические программы и по каким научным направлениям возможно выполнять морскими беспилотниками, а какие – пока только с использования НИС [1]. По мере расширения использования робототехники по новым многоцелевым комплексным научным программам суммарная экономия экспедиционных затрат всех ведомств нашей страны, проводящих океанологические исследования и наблюдения, может достигнуть значительного объема. Долговременность и высокая степень автоматизации элементов АСОИ ЭО позволяет в значительной степени отказаться от использования НИС для выполнения многих научных задач в морях и океанах, что также обеспечит значительный экономический эффект в масштабах всех заинтересованных отечественных организаций, за счет существенного снижения экспедиционных расходов, прежде всего на топливо для судов. Широкое внедрение отечественных средств робототехники позволит перейти к новой парадигме океанологических исследований, обеспечивающей автоматическое, непрерывное, не ограниченное по времени и экономически эффективное получение данных о различных процессах, происходящих на границе атмосферы и Мирового океана, а также в его водной толще и на дне.

Работа выполнена в рамках государственного задания ИО РАН (тема № 0149-2019-0011).

Список литературы

1. Горлов А.А. Океанологические исследования поверхностными беспилотниками повышенной автономности // Научное обозрение. Технические науки. 2018. № 5. С. 5–13.

2. Горлов А.А. Морские беспилотники долговременной автономности на базе ВИЭ // Энергия: экономика, техника, экология. 2018. № 4. С. 30–41.

3. The Abyss, Now Live on Your Desktop. Sensors&Systems – 2013. [Электронный ресурс]. URL: https://sensorsandsystems.com/the-abyss-now-live-on-your-desktop (дата обращения: 27.07.2019).

4. From Sea to Space | Robots Explore Extreme Environments. Ocean NetWork Canada – 2014. [Электронный ресурс]. URL: https://www.oceannetworks.ca/sea-space-robots-explore-extreme-environments (дата обращения: 27.07.2019).

5. Горлов А.А. Возобновляемые источники энергии для повышения эффективности исследований Мирового океана // Энергетический вестник Международного центра устойчивого энергетического развития под эгидой ЮНЕСКО. 2014. № 18. С. 14–32.

6. Zhao L.Z. and other. MHD Wave Energy Underwater Recharging Platforms for AUVs. Proceedings of the Twenty-sixth (2016) International Ocean and Polar Engineering Conference.Rhodes. Greece. 2016. P. 400–403 [Электронный ресурс]. URL: https://www.onepetro.org/conference-paper/ISOPE-I-16-342 (дата обращения: 22.07.2019).

7. Hagerman G. Wave energy systems for recharging AUV energy supplies. Proceedings the 2002 Workshop on Autonomous Underwater Vehicles. 2002. P. 75–84. [Электронный ресурс]. URL: https://www.semanticscholar.org/paper/Wave-energy-systems-for-recharging-AUV-energy-Hagerman/ab5bceb43c525e93f3c629bf409d2de88311aae2 (дата обращения: 20.07.2019).

8. Горлов А.А. Энергия ветрового волнения // Энергия: экономика, техника, экология. 2015. № 2. С. 30–40.

9. Eni to use wave-energy device for AUV charging – 2018. [Электронный ресурс]. URL:https://www.offshoreenergytoday.com/eni-to-use-wave-energy-device-for-auv-charging/ (дата обращения: 21.07.2019).

10. OPT Achieves Power Generation Milestone in Adriatic Sea – 2019. [Электронный ресурс]. URL: https://marineenergy.biz/2019/05/14/opt-achieves-power-generation-milestone-in-adriatic-sea/ (дата обращения: 21.07.2019).

11. OPT and Premier Oil ink deal for lead-in PowerBuoy o&g lease – 2018. [Электронный ресурс]. URL:https://marineenergy.biz/2018/06/28/opt-and-premier-oil-ink-deal-for-lead-in-powerbuoy-lease/ (дата обращения: 20.07.2019).

12. Ocean current-powered hybrid fuses with external oil equipment – 2018. [Электронный ресурс]. URL: https://marineenergy.biz/2018/04/10/ocean-current-powered-hybrid-fuses-with-external-oil-equipment/ (дата обращения: 19.07.2019).

СТАТЬЯ

УДК 004.021:004.056.55

АНАЛИЗ СОВРЕМЕННЫХ ПОСТКВАНТОВЫХ АЛГОРИТМОВ ШИФРОВАНИЯ

Буковшин В.А., Чуб П.А., Черкесова Л.В., Короченцев Д.А., Поркшеян В.М.
ГОУ ВПО «Донской государственный технический университет», Ростов-на-Дону, e-mail: chia2002@inbox.ru

В данной статье проводится анализ существующих на данный момент постквантовых алгоритмов шифрования, таких как: криптосистема Мак-Элиса, криптосистема Ниддерайтера, криптосистемы с использованием квантового хэширования, криптосистемы на основе задач на решетках, криптосистемы с обучением на ошибках. В описанных выше постквантовых криптосистемах производится углубленное и пошаговое представление каждого алгоритма, а также приводятся соответствующие структурные блок-схемы генерации ключей, шифрования и расшифровывания алгоритма, также рассматриваются преимущества и недостатки отдельно взятых алгоритмов, предлагаются варианты решения проблемы защиты от криптоатак с использованием квантовых компьютеров. Анализ приведенных постквантовых алгоритмов шифрования содержит: оценку асимптотической сложности алгоритмов, оценку требований к вычислительным ресурсам, необходимым для корректной работы каждого этапа алгоритма, необходимые теоретические сведения из прилегающих областей, достижения которых использовались при создании алгоритмов, преимущества и недостатки каждого алгоритма в отношении применения для защиты информации, общие рекомендации по модификации алгоритмов с целью снижения требований к вычислительным ресурсам и асимптотической сложности алгоритмов, а также оценку криптостойкости систем. Оценка криптостойкости описываемых в данной статье алгоритмов содержит: описание найденных уязвимостей систем, известных на момент написания данной статьи, с подробным описанием возможностей их эксплуатации с целью атаки на информационные системы, анализ защищенности параметров криптосистемы, описание и анализ частей алгоритма, подверженных теоретическому взлому и общие рекомендации для модификации и улучшения защищенности данных частей алгоритма.

Ключевые слова: постквантовые алгоритмы шифрования, криптосистема, алгебраическое кодирование, квантовое хэширование, кубит

ANALYTICAL REVIEW OF EXISTING POST-QUANTUM ENCRYPTION ALGORITHMS

Bukovshin V.A., Chub P.A., Cherkesova L.V., Korochentsev D.A., Porksheyan V.M.
Don State University, Rostov-on-Don, e-mail: chia2002@inbox.ru

This article analyzes the currently existing post-quantum encryption algorithms, such as: McElice cryptosystem, Nidderaiter cryptosystem, quantum hashing cryptosystems, lattice-based cryptosystems, error-learning cryptosystems. In the post-quantum cryptosystems described above, an in-depth and step-by-step representation of each algorithm is performed, as well as the corresponding structural block diagrams of key generation, encryption and decryption of the algorithm are given, the advantages and disadvantages of individual algorithms are also considered, options for solving the problem of protection against crypto attacks with using quantum computers. The analysis of the above post-quantum encryption algorithms contains: an estimate of the asymptotic complexity of the algorithms, an estimate of the requirements for computing resources necessary for the correct operation of each stage of the algorithm, the necessary theoretical information from the adjacent areas, the achievements of which were used to create the algorithms, the advantages and disadvantages of each algorithm with respect to the application to protect information, general recommendations on the modification of algorithms in order to reduce the requirements for computing resources and asympt ical complexity of the algorithms, as well as an assessment of the cryptographic stability of systems. Assessing the cryptographic stability of the algorithms described in this article contains: a description of the found vulnerabilities of the systems known at the time of this writing, with a detailed description of the possibilities of their exploitation with the aim of attacking information systems, an analysis of the security of cryptosystem parameters, a description and analysis of parts of the algorithm that are subject to theoretical hacking and general recommendations for modifying and improving the security of these parts of the algorithm.

Keywords: post-quantum encryption algorithms, cryptosystem, algebraic coding, quantum hashing, qubit

Защищенность информации в современном цифровом мире целиком и полностью основывается на устойчивости современных криптосистем к различным информационным атакам. В то же время, учитывая стремительный рост в исследовании области квантовой криптографии, можно предположить, что появление квантовых компьютеров станет угрозой для современных криптосистем, защищенность которых зависит от сложности некоторых вычислительных задач, таких как факторизация больших простых чисел, дискретное логарифмирование, задачи на решетках и других.

Учитывая вышесказанное, поиск более защищенных постквантовых криптографических систем является актуальным, так как повысит устойчивость информационных систем к атакам с использованием квантовых компьютеров.

Данная работа посвящена анализу современных постквантовых алгоритмов, а также содержит выводы по перспективе их использования для конструирования криптосистем эпохи квантовых компьютеров и возможные варианты модификации данных алгоритмов для повышения криптостойкости или скорости выполнения. Далее в статье будут рассмотрены современные постквантовые криптографические системы, такие как криптосистема Мак-Элиса, криптосистема Ниддерайтера, криптосистемы с использованием квантового хэширования, криптосистемы на основе задач на решетках, криптосистемы с обучением на ошибках.

Криптосистема Мак-Элиса

McEliece – криптосистема с открытыми ключами, основанная на основе теории алгебраического кодирования и разработанная в 1978 г. Робертом Мак-Элисом. Это была первая схема, использующая рандомизацию в процессе шифрования. В целом работу данной криптосистемы можно разбить на три основных алгоритма:

– алгоритм случайной генерации ключа, дающий на выходе открытый и закрытый ключи;

– алгоритм случайного шифрования, дающий на выходе шифротекст;

– детерминированный алгоритм расшифровывания, дающий на выходе исходный открытый текст.

Рассмотрим каждый из алгоритмов более подробно. Алгоритм генерации ключей выполняется в несколько этапов:

– выбирается линейный (n, k)-код C, который исправляет *t* ошибок. Далее для этого кода генерируется оптимальная порождающая матрица G [1, с. 128];

– для более сложного восстановления исходного кода, на шифрующей стороне генерируется случайная невырожденная $k \times k$ матрица S;

– здесь же генерируется случайная $n \times n$ матрица перестановки P;

– происходит вычисление публичной порождающей матрицы G_{pub}:

$$G_{pub} = SGP \qquad (1.1)$$

– в виде открытого ключа представляется пара (G_{pub}, t), а в качестве закрытого – набор (S, G, P);

Блок-схему вышеописанного алгоритма можно увидеть на рис. 1.

Проанализируем более подробно каждый шаг алгоритма. На первом шаге необходимо сгенерировать так называемую оптимальную порождающую матрицу G. Оптимальной назовём матрицу, порождающую код C, который будет иметь максимальную корректирующую способность, то есть максимально возможное количество ошибок канала связи, которые код в состоянии исправить при декодировании [1, с. 128].

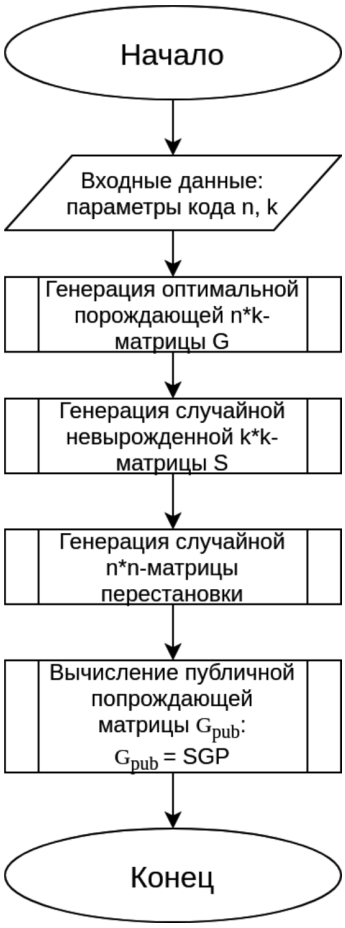

Рис. 1. Блок-схема алгоритма генерации ключей криптосистемы Мак-Элиса

Одним из возможных способов решения поставленной задачи является полный перебор всех возможных добавочных матриц вида $P_{k*(n-k)}$. Для двоичного (n,k)-кода общее число таких матриц составляет $2^{(k*(n-k))}$, а сложность алгоритма приближается к экспоненциальной $O(2^n)$ [1, с. 129]. Данный метод является очень требовательным как к вычислительным, так и к временным ресурсам, с увеличением параметров кода будет существенно увеличиваться вычислительная сложность [1, с. 129].

О некоторых альтернативных способах поиска оптимальной порождающей матрицы можно узнать в следующих работах [1, 2].

Алгоритмы генерации матрицы S и матрицы перестановки P не требовательны к вычислительным ресурсам даже при существенном увеличении параметров кода.

Последний этап алгоритма с вычислением публичной порождающей матрицы G_{pub} представляет больший интерес с точки зрения анализа вычислительной сложности. Сложность вычисления произведения матриц по определению составляет $O(n^3)$ [3, с. 266], однако существуют более эффективные алгоритмы, которые применяются для перемножения больших матриц, такие как алгоритм Штрассена, алгоритм Пана, алгоритм Бини, алгоритм Копперсмита – Винограда и другие [3, с. 279].

Важно отметить, что в рамках данной работы все операции выполняются в GF(q) (поле Галуа).

Для выполнения алгоритма шифрования необходимо следовать следующей последовательности шагов:

– все сообщения m превращается в последовательность символов в поле GF(q) длины k;

– происходит генерация случайного вектора ошибки z, то есть вектора длины n и весом Хэмминга t;

– происходит вычисление шифротекста по формуле и дальнейшая его передача адресату:

$$c^{'} = mG_{pub} + z. \quad (1.2)$$

Блок-схема алгоритма шифрования представлена на рис. 2.

И наконец, алгоритм расшифровывания включает в себя следующие этапы:

– вычисление обратной матрицы P^{-1};

– происходит первый этап декодирования, вычисляется кодовый вектор по формуле

$$\overline{c} = cP^{-1} \quad (1.3)$$

– используется известный для рассматриваемого кода алгоритм декодирования, с целью получения $\overline{m}$ из $\overline{c}$;

– вычисляется исходное сообщение по следующей формуле

$$m = \overline{m}S^{-1}. \quad (1.4)$$

Блок-схема алгоритма расшифровывания представлена на рис. 3.

С точки зрения анализа алгоритмов интерес представляет только операция поиска обратной матрицы, которая может потребовать чуть больше вычислительных ресурсов с увеличением длины кода. Сложность алгоритма поиска обратной матрицы по определению оценивается как $O(n^6)$ [4, с. 407]. Общая сложность будет выражаться некоторой степенной функцией, которая будет зависеть от выбора алгоритмов генерации оптимальной порождающей матрицы, матричного умножения и поиска обратной матрицы.

Рис. 2. Блок-схема алгоритма шифрования сообщения криптосистемы Мак-Элиса

После выполнения алгоритма расшифровывания работа криптосистемы Мак-Элиса завершается. Всё множество дешифрованных слов складывается в единый текст, который в точности совпадает с исходным.

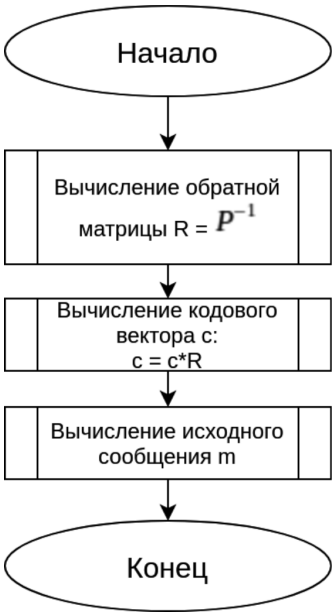

Рис. 3. Блок-схема алгоритма расшифрования сообщения криптосистемы Мак-Элиса

Алгоритм не получил широкого признания, но в то же время является кандидатом для постквантовой криптографии, так как устойчив к атаке при помощи алгоритма Шора. Алгоритм основан на сложности декодирования полных линейных кодов (общая задача декодирования является NP-сложной) и использует двоичные коды Гоппа, которые легко декодируются благодаря алгоритму Петерсона [5, с. 150]. Открытый ключ получается при помощи маскировки выбранного кода как полного линейного.

Существует несколько вариантов криптосистемы, использующих различные типы кодов. Большинство из них оказываются менее защищенными. Отдельного рассмотрения заслуживает вопрос выбора параметров криптосистемы.

До сих пор криптосистема Мак-Элиса с кодами Гоппы не поддается криптоанализу [6, с. 191]. Наиболее известные атаки используют алгоритм декодирования множества данных. В других работах показано, что для квантовых вычислений размер ключа должен быть увеличен на четыре порядка из-за усовершенствования декодирования.

Криптосистема имеет несколько преимуществ, например над RSA. Шифрование и дешифрование проходит быстрее и с ростом длины ключа степень защиты данных возрастает. Долгое время считалось, что криптосистема Мак-Элиса не используется для ЭЦП должным образом. Однако оказалось возможным построить схему для ЭЦП на основе криптосистемы Нидеррайтера (модификация криптосистемы Мак-Элиса).

Прежде всего, рассмотрим криптостойкость рассматриваемой криптосистемы. В различной литературе можно найти множество всех возможных атак.

Большинство атак основаны на попытке построить декодер кода, генерируемого публичной матрицей G_{pub}. Такие атаки называют структурными. Если у кого-либо получится узнать G_{pub}, то закрытый ключ G будет довольно быстро раскрыт, что приведет к полному взлому криптосистемы. Злоумышленник в таком случае должен будет сравнить огромное множество эквивалентных кодов. При описании системы было предложено использовать в качестве достаточно криптостойкого (1024,524,50) – код. Таким образом, потребуется перебор более чем 2^{466} различных кодов.

Также имеют место атаки, анализирующие зашифрованный текст. На деле они оказались менее сложными по сравнению со структурными. Многие из них основаны на декодировании множества данных, что также называют парадоксом дней рождения.

Основные недостатки криптосистемы Мак-Элиса:

– размер открытого ключа слишком большой. При использовании кодов Гоппы с параметрами, предложенными Мак-Элисом, открытый ключ составляет 2^{19} бит, что вызывает сложности в реализации;

– зашифрованное сообщение гораздо длиннее исходного;

– криптосистема не может быть использована для аутентификации, потому что схема шифрования не является взаимно-однозначной, а сам алгоритм является асимметричным.

Криптосистема Нидеррайтера

Криптосистема Нидеррайтера – криптосистема с открытыми ключами, основанная на теории алгебраического кодирования, разработанная в 1986 г. Харальдом Нидеррайтером [5, с. 432].

В отличие от криптосистемы Мак-Элиса криптосистема Нидеррайтера включает в себя следующее:

– использование проверочной матрицы кода;

– создание цифровой подписи;

– устойчивость к атакам с использованием алгоритма Шора;

Используемый в криптосистеме Нидеррайтера алгоритм основан на сложности декодирования полных линейных кодов, а также содержит следующее:

– генерацию ключей;

– шифрование исходного сообщения;

– расшифрование зашифрованного сообщения.

Рассмотрим каждый этап алгоритма по отдельности.

Генерация ключей происходит поэтапно:

– выбирается (n, k) – код C над полем Галуа GF(q), который способен исправить t ошибок. Выбранный код, конечно же, должен обладать эффективным алгоритмом декодирования;

– генерируется проверочная матрица H кода C, которая должна иметь размер $(n-k)\times n$;

– случайным образом генерируется невырожденная $(n-k)\times(n-k)$ матрица S над полем GF(q) и матрица перестановки P размера $n\times n$;

– вычисляется публичная проверочная матрица по формуле

$$H_{pub} = SHP. \qquad (1.5)$$

Размерность представленной матрицы составляет $(n-k)\times n$;

– в виде открытого ключа представляется пара (H_{pub}, t), а в качестве закрытого набор (S^{-1}, H, P^{-1}).

Блок-схема генерации ключей в криптосистеме Нидеррайтера представлена на рис. 4.

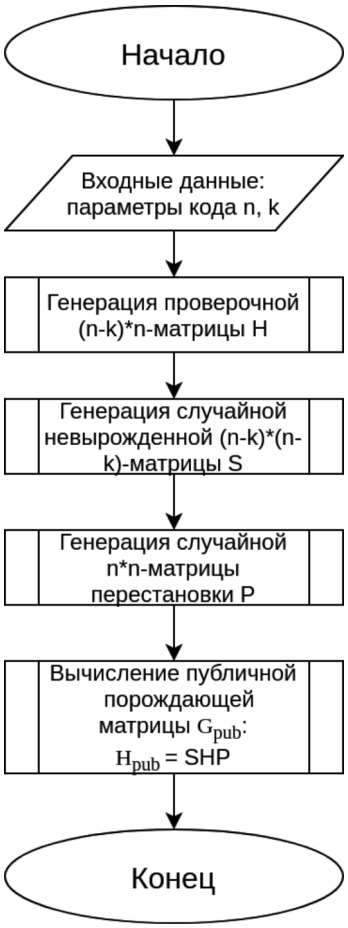

Рис. 4. Блок-схема алгоритма генерации ключей криптосистемы Нидеррайтера

Рассмотрим подробнее алгоритмы декодирования, которые можно применить на первом этапе.

Один из таких алгоритмов состоит в табулировании заранее вычисленных синдромов ошибок. Простейшим декодером такого типа является декодер Меггита, который проверяет синдромы только для тех конфигураций ошибок, которые расположены в старших позициях [7, с. 266]. Если вычисленный синдром находится в ранее сформированной таблице, то зашумлённый вектор исправляется в соответствии с подходящим вектором ошибок [7, с. 344]. Зачастую для реализации первого шага вышеописанного алгоритма применяются циклические коды, поэтому алгоритм декодирования будет реализован через полиномы.

Декодирование на основе решения алгебраических уравнений заключается в той простой идее, что каждой позиции кодового слова ставится в соответствие локатор ошибка. Декодирование состоит в отыскании локаторов, а в случае недвоичных кодов и значений ошибок – в символах, отмеченных локаторами [7, с. 397].

Мажоритарный алгоритм декодирования базируется на системе проверочных равенств. Система последовательно может быть разрешена относительно каждой из независимых переменных, причем в всилу избыточности это можно сделать не единственным способом [7, с. 401].

Алгоритм шифрования сообщения включает в себя выполнение следующих шагов:

– сообщение представляется в виде q-ичной подпоследовательности m длины n и имеющей вес t;

– вычисляется шифротекст по следующей формуле

$$c = mH_{pub}^{T}. \qquad (1.6)$$

Таким образом, шифротекст в криптосистеме Нидеррайтера представляет собой синдром шифруемого вектора ошибки.

Блок-схема алгоритма шифрования в криптосистеме Нидеррайтера представлена на рис. 5.

Рис. 5. Блок-схема алгоритма шифрования в криптосистеме Нидеррайтера

Алгоритм расшифровывания сообщения может быть описан следующим образом:

– нахождение синдрома s по следующей формуле:

$$\hat{s} = \hat{c}(S^{-1})^{T} = \hat{m}P^{T}H^{T}S^{T}(S^{T})^{-1} = \\ = (\hat{m}P^{T})H^{T} = \hat{m}'H^{T}. \qquad (1.7)$$

Здесь $\dot{m}' = m'P^T$, при этом вес $\dot{m}'$ не превосходит вес $\dot{m}'$, это означает, что, используя алгоритм декодирования, можно найти соответствующий текущему синдрому вектор ошибок;

– на этом шаге необходимо по синдрому найти $\dot{m}'$ и декодировать сообщение по следующей формуле:

$$\hat{m} = \hat{m}'(P^T)^{-1} = \hat{m}P^T(P^T)^{-1}. \qquad (1.8)$$

Блок-схема алгоритма шифрования в криптосистеме Нидеррайтера представлена на рис. 6.

Несмотря на то, что данная криптосистема была взломана, некоторые её модификации остаются криптостойкими [5, с. 501].

Преимущества криптосистемы Нидеррайтера:

– в отличие от криптосистемы Мак-Элиса, в криптосистеме Нидеррайтера не используются случайные параметры. Таким образом, результат шифрования одного и того же текста будет одинаковым. Этот факт позволяет использовать именно систему Нидеррайтера, а не Мак-Элиса, для создания электронно-цифровой подписи;

– размер открытого ключа в криптосистеме Нидеррайтера в порядки раз меньше, чем в криптосистеме Мак-Элиса [5, с. 530];

– по сравнению с RSA, скорость шифрования выше приблизительно в 50 раз, а дешифрования – в 100 раз [5, с. 534].

Рис. 6. Блок-схема алгоритма расшифровывания криптосистемы Нидеррайтера

Недостатки криптосистемы Нидеррайтера:

– размер ключей больше, чем в классических криптосистемах с открытым ключом, таких как RSA, Эль-Гамаль и других.

Квантовое хэширование

В отличие от алгоритмов классического хэширования, условно разработанных на однонаправленных функциях, квантовая криптография при построении хэш-функций основывается на принципах квантовой механики и квантовой теории информации, гарантирующих физическую однонаправленность квантовых хэш-функций. Эта особенность является одним из центральных потенциальных преимуществ перед классическими хэш-конструкциями. Для создания квантовых хэш-функций необходимо рассматривать универсальные хэш-семейства, которые являются основой цифровой подписи. Идея универсальных хэш-семейств заключается в обобщении понятия хэширования и хэш-семейств функций на квантовый случай, что означает отображение слов исходного сообщения в квантовые состояния, кубиты.

Кубит – единичный вектор в двумерном гильбертовом комплексном пространстве с таким свойством, что координаты вектора – комплексные числа, а сумма квадратов их амплитуд равняется единице. При таком определении кубит можно представить как вектор в трехмерном пространстве. Это означает, что кодирование сообщений можно проводить с помощью кубитов, для этого в теории квантовой информатики существует понятие квантового хэш-генератора – семейство функций, для каждой из которых можно построить отображения битов исходного сообщения в ансамбль из конкретного числа кубит, а также, скомбинировав их, получить квантовую хэш-функцию.

Сейчас можно говорить о том, что на создание действительно производительного квантового компьютера, который будет превосходить по вычислительной мощности все существующие классические машины, уйдет много времени. На данный момент остро стоит вопрос построения квантовой памяти, а именно, квантовых репитеров или увеличителей сигнала.

Обучение с ошибками

Обучение с ошибками – концепция машинного обучения, суть которой заключается в том, что в простые вычислительные задачи намеренно вносится ошибка, что превращает их решение известными методами в неосуществимую задачу за приемлемое время. Возникновение вышеописанной концепции отслеживается в работах Миклоша Айтаи и Синтии Дворк, которые первыми привели криптосистему на открытых ключах с использованием криптографии на решётках с последующими улучшениями и модификациями.

Диапазон криптографических приложений данной концепции достаточно широк. В качестве примера криптосистемы с использованием обучения с ошибками приведём криптосистему на открытых ключах. Система описывается следующими числами: n – секретный параметр, m – размерность, q – модуль и распределение вероятности случайной величины ε из поля Z_n. Для гарантии безопасности и корректности системы следует выбрать следующие параметры для произвольной константы ε: $q \geq 2$

$$m = (1+\varepsilon)(n+1)*\log q. \qquad (1.9)$$

Работа вышеописанной криптосистемы будет состоять из следующих алгоритмов:

– генерация ключей;

– шифрование сообщения;

– расшифровывание сообщения.

Данные алгоритмы удовлетворяют следующей последовательности шагов:

– секретный ключ описывается следующей формулой:

$$s \in Z_q^n \qquad (1.10)$$

– открытый ключ состоит из

$$(a_i b_i = \frac{\langle a_i, s \rangle}{q} + e_i)_{i=1}^{m} \qquad (1.11)$$

– шифрование бита производится посредством выбора случайного подмножества S из [m] и определением шифра Enc(x) как

$$\left(\sum_{i \in S} a_i, \frac{x}{2} + \sum_{i \in S} b_i \right) \qquad (1.12)$$

– рисшифровывание происходит декодированием пары (a, b) в 0, если $b = a, s / q$ ближе к 0, чем к $\frac{1}{2}$, и 1 в противном случае.

Криптография на решётках

Решёткой называется множество

$$\Delta = \left\{ \sum_{i=1}^{d} x_i b_i \vee x_i \in Z \right\} в R^n, \qquad (1.13)$$

где b_i, i: = 1,…, d, линейно независимы над R.

Постквантовая криптография на решётках основана на неосуществимых как для квантовых, так и для классических компьютеров задачах на решётках, таких как:

– нахождение кратчайшего вектора;

– нахождение идеального кратчайшего вектора;

– нахождение кратчайшего независимого вектора;

– поиск короткого целого решения.

Данные задачи легли в основу некоторых криптографических конструкций, активно используемых на данный момент. К ним относят:

– GGH;

– NTRUSign.

Дадим подробное описание каждому из приведенных выше криптографических конструкций.

GGH – первая подпись, основанная на решетках, которая была представлена на CRYPTO в 1997 г. Голдрихтом и соавторами. Их идея заключалась в использовании решеток, для которых «плохой» базис, чьи вектора длинные и почти параллельные, является открытым, и «хороший» базис, с короткими и почти ортогональными векторами, является закрытым.

По их методу, сообщение необходимо хэшировать в пространство, натянутое на решетку, а подпись для данного хэша в этом пространстве является ближайшим узлом решетки. Схема не появилась с формальным доказательством безопасности, и ее базовый вариант был взломан в 1999 г. Nguyen. В 2006 г. модифицированная версия была снова сломана Nguyen и Regev [8, с. 157].

Опишем пошагово работу рассматриваемой криптографической конструкции:

– генерация ключей, которая состоит из открытого и закрытого ключей. В качестве открытого ключа выступает некоторый базис из решетки L вида

$$B' = UB. \qquad (1.14)$$

Для некоторого M, пространство состоит из вектора $(\varphi_1,..., \varphi_n)$, где $-M < \varphi_i < M$. Закрытый ключ представляет собой базис B решетки L и унимодулярную матрицу U;

– алгоритм шифрования. Задается сообщение $m = (\varphi_1,..., \varphi_n)$, искажение e, открытый ключ B'. Процесс шифрования в векторной форме имеет следующий вид:

$$v = \sum \varphi_i b_i'. \qquad (1.15)$$

Соответственно, в матричной форме имеет вид

$$v = m * B'. \qquad (1.16)$$

Исходя из представленных выше формул, шифротекст имеет следующую структуру:

$$c = v + e = m * B' + e \qquad (1.17)$$

– алгоритм расшифровки. Чтобы получить исходное сообщение, пользователю необходимо по формуле, представленной ниже, вычислить значение

$$c * B^{-1} = m * U + e * B^{-1}. \qquad (1.18)$$

Следовательно, исходя из соображений, часть $e*B^{-1}$ убирается, тем самым формула (1.18) имеет следующую структуру:

$$m = m * U * U^{-1}. \qquad (1.19)$$

NTRUSign – специальная версия GGH, отличающейся меньшим ключом и размером подписи и являющейся более эффективной. С другой стороны, она использует только решетки подмножества множества всех решеток, связанных с некоторыми полиномиальными кольцами. NTRUSign была выдвинута на рассмотрение IEEE-standard P1363.1 [8, с. 249]. Стойкость алгоритма обеспечивается трудностью поиска кратчайшего вектора решётки, которая более стойкая к атакам, реализуемым с помощью квантового компьютера.

Работа криптосистемы включает в себя следующие алгоритмы:

– генерация ключей;

– шифрование сообщения;

– расшифровывание сообщения.

Опишем генерацию ключей.

Для передачи сообщения от Алисы к Бобу необходимы открытый и закрытый ключи. Открытый знают как Боб, так и Алиса, закрытый ключ знает только Боб, который он использует для генерации открытого ключа. Для этого Боб выбирает два «маленьких» полинома f, g из R. «Малость» полиномов подразумевается в том смысле, что он маленький относительно произвольного полинома по модулю q. В произвольном полиноме коэффициенты должны быть примерно равномерно распределены по модулю q, а в малом – они много меньше q. Малость полиномов определяется с помощью чисел df и dg:

– полином f имеет df коэффициентов равных «1» и df-1 коэффициентов равных «–1», а остальные – «0»;

– полином g имеет dg коэффициентов равных «1» и столько же равных «-1», остальные – 0.

Причина, по которой полиномы выбираются именно таким образом, заключается в том, что f, возможно, является обратным, а g – нет (g (1) = 0, а нулевой элемент не имеет обратного).

Следующим шагом станет вычисление Бобом обратных полиномов f_p и f_q. Это можно пронаблюдать из представленных ниже формул:

$$(f * f_q) \equiv 1 \bmod q, \qquad (1.20)$$

$$(f * f_p) \equiv 1 \bmod p. \qquad (1.21)$$

Секретный ключ представляет собой пару (f, f_p), а открытый h имеет следующий вид:

$$h = (pf_q * g) \bmod q. \qquad (1.22)$$

Опишем процесс шифрования сообщения.

Сообщение представляется в виде полинома m с коэффициентами по модулю p. Далее выбирается полином r, определяемый с помощью числа dr следующим образом: количество коэффициентов равных «1» совпадает с теми, которые имеют значение «–1», оставшиеся – 0.

Используя эти полиномы, можно получить зашифрованное сообщение по формуле

$$e = (r * h + m) \bmod q. \qquad (1.23)$$

Рассмотрим процесс расшифровывания поэтапно.

На первом шаге необходимо определить промежуточный полином вида:

$$a = (f * e) \bmod q. \qquad (1.24)$$

Вторым шагом нужно расписать шифротекст, который со всеми возможными и необходимыми преобразованиями имеет вид

$$a = (pr * g + f * m) \bmod q. \qquad (1.25)$$

На третьем шаге вычисляется значение полинома b, исходя из выбранных значений коэффициентов в диапазоне. Расчет производится по следующей формуле:

$$b = (f * m) \bmod p. \qquad (1.26)$$

На заключительном этапе, имея вторую половину секретного ключа и посчитанный полином b, Боб может расшифровать сообщение следующим образом:

$$c = (f_p * b) \bmod p. \qquad (1.27)$$

На данный момент известны следующие атаки на вышеописанную криптосистему:

– полный перебор;

– встреча посередине;

– атака на основе множественной передачи сообщения;

– атака на основе решётки;

– атака на основе подобранного шифротекста.

Опишем параметры криптостойкости рассматриваемой криптосистемы.

Так как на сегодняшний день существуют быстрые алгоритмы поиска обратного полинома, в качестве секретного ключа стоит выбирать следующее значение:

$$f = 1 + pF, \qquad (1.28)$$

где F – малый полином. В таком случае, выбранный ключ включает в себя следующее:

– f всегда имеет обратный элемент по модулю p;

– при расшифровке сообщения не нужно умножать на обратный полином f_p.

Заключение

В качестве итога можно сказать, что на данный момент кандидатов-криптосистем для постквантовой криптографии предоста-

точно. Среди них криптосистемы, основанные на вычислительной сложности, которая будет предположительно достаточно высока и для производительности квантовых компьютеров, и криптосистемы, основанные на неосуществимости решения некоторых математических задач. Также стоит сказать и о том, что в области разработки постквантовых алгоритмов шифрования ведутся активные исследовательские работы, которые уже дают шокирующие результаты в плане повышения сложности криптосистем, к примеру, появление целой теории квантового хэширования. Все это даёт надежду на то, что область информационной безопасности окажется полностью подготовленной к появлению квантовых компьютеров и предоставит возможность обезопасить данные пользователей по всему миру.

Список литературы

1. Bocharova I. Searching for tailbiting codes with large minimum distance. IEEE Transactions on Information Theory. 2015. № 47. P. 335–337.

2. Grassl M. New Binary Codes from a Chain of Cyclic Codes. IEEE Transactions on Information Theory. 2015. № 47. P. 1178–1181.

3. Coppersmith D., Winograd S. Matrix multiplication via arithmetic progressions. Journal of Symbolic Computation. 2017. № 9. P. 251–280.

4. Кормен Т., Лейзерсон Ч., Ривест Р., Штайн К. Алгоритмы: построение и анализ. М: Вильямс, 2013. 700 с.

5. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М: Триумф, 2014. 816 с.

6. Canteaut A., Sendrier N. Cryptanalysis of the Original McEliece Cryptosystem. Advances in Cryptology – ASIACRYPT 2015: International Conference on the Theory and Applications of Cryptology and Information Security. 2015. № 1. P. 187–199.

7. Блейхут Р. Теория и практика кодов, контролирующих ошибки. М: Книга по требованию, 2013. 566 с.

8. Душкин Р.В. Квантовые вычисления и функциональное программирование. М: ДМК Пресс, 2014. 437 с.

СТАТЬЯ

УДК 551.46.09

АНАЛИЗ ИССЛЕДОВАНИЙ ГАЗОВЫХ ГИДРАТОВ НА ОЗЕРЕ БАЙКАЛ И ПРЕДЛОЖЕНИЯ ПО РАЗРАБОТКЕ ГИДРОЛОГО-ГИДРОХИМИЧЕСКИХ КОМПЛЕКСОВ НОВОГО ПОКОЛЕНИЯ

[1]Лискин В.А., [1]Егоров А.В., [1,2]Римский-Корсаков Н.А., [1]Тихонова Н.Ф.

[1]Институт океанологии им. П.П. Ширшова РАН, Москва, e-mail: nrk@ocean.ru;

[2]Московский государственный технический университет им. Н.Э. Баумана, Москва

Настоящая работа посвящена исследованиям и предложениям по созданию глубоководных гидролого-гидрохимических комплексов на базе анализа исследований газогидратных месторождений на озере Байкал. Исследованы способы проведения глубоководных экспериментов и полученные результаты. Проводился подъем со дна озера Байкал на поверхность с помощью глубоководного аппарата отдельных образцов гидрата метана и образцов гидратной пены, помещаемых в специальный контейнер, Отбор гидратных образцов осуществлялся из донных залежей, а подъем проводился в контейнерах, в которых дно отсутствовало, а верхняя часть и стенки непроницаемы (при этом пена формировалась всплывающими от метановых образцов пузырями, которые, в свою очередь, скапливались в верхней части контейнера). На основании проведенных экспериментов выявлена необходимость создания гидролого-гидрохимических комплексов нового поколения, предполагающих применение высокоразрешающих методов непрерывного гидрофизического и акустического зондирования (профилирования) водной толщи и современных методов гидролого-геохимического анализа потоков вещества придонного слоя, что позволит проводить исследования по прогнозу нефтегазоносности и прогнозу других полезных ископаемых морских шельфов. Новые технические средства, ориентированные на ведение поиска и исследований залежей газовых гидратов, могут быть использованы для разнообразных экологических исследований, касающихся влияния захоронений различных отходов, например радиоактивных, на состояние окружающей среды. Практическая значимость предлагаемых разработок связана также с потребностями нефтепоисковых работ и потребностями нефтегазового комплекса. В этом направлении основной задачей является проведение исследований новых нетрадиционных форм углеводородсодержащего сырья – газовых гидратов. Их запасы в осадках Мирового океана могут превышать все традиционные источники нефтегазового потенциала на суше. Предлагаемый к разработкам комплекс технических и методических средств, использующий современные микрокомпьютерные методы обработки и представления получаемых данных непосредственно в процессе измерений, с возможностью коррекции программы проводимых исследований в реальном времени, закладывают основу для развития инновационных способов разведки и добычи подводных газовых гидратов.

Ключевые слова: глубоководные эксперименты, негерметичные контейнеры, геохимический анализ, газовые гидраты, гидрохимические комплексы

ANALYSIS OF RESEARCHES OF GAS HYDRATES ON BAIKAL LAKE AND PROPOSALS FOR THE DEVELOPMENT OF HYDRO-HYDROCHEMICAL COMPLEXES OF A NEW GENERATION

[1]Liskin V.A., [1]Egorov A.V., [1,2]Rimskiy-Korsakov N.A., [1]Tikhonova N.F.

[1]Shirshov Institute of Oceanology, Russian Academy of Science, Moscow, e-mail: nrk@ocean.ru;

[2]Bauman Moscow State Technical University, Moscow

This paper is devoted to research and proposals for the creation of deep water hydrological and hydrochemical complexes, based on the analysis of research of gas hydrate deposits in Lake Baikal. Methods for conducting deep-sea experiments and the results obtained were investigated. Lift from the bottom of Lake Baikal to the surface was carried out using a deep-sea apparatus of individual samples of methane hydrate and samples of hydration foam placed in a special container. Hydrate samples were taken from bottom deposits, and lifting was carried out in containers in which the bottom was absent and the upper part and walls impenetrable (while the foam was formed by bubbles emerging from methane samples, which, in turn, accumulated in the upper part of the container). Based on the conducted experiments, it was identified the need to create hydrologic and hydrochemical complexes of a new generation, involving the use of high-resolution methods of continuous hydrophysical and acoustic sensing (profiling) of the water column and modern methods of hydrologic-geochemical analysis of the substance of the bottom layer, which will make it possible to conduct studies on the prediction of oil and gas potential and other predictions minerals offshore. New technical tools focused on the search and research of gas hydrate deposits can be used for a variety of environmental studies relating for example to the burial radioactive waste and its environmental impact. The practical significance of the proposed development is related to the needs of oil exploration and the needs of the oil and gas complex. In this direction, the main task is to conduct research on new unconventional forms of hydrocarbon-containing raw materials – gas hydrates. Their reserves in the sediments of the oceans may exceed all traditional sources of oil and gas potential on land. The complex of technical and methodical means offered for development, using modern microcomputer methods for processing and presenting the obtained data directly in the measurement process, with the possibility of correcting the program of conducted research in real time, lays the foundation for the development of innovative methods of exploration and production of underwater gas hydrates.

Keywords: deep-sea experiments, untight containers, geochemical analysis, gas hydrates, hydrochemical complexes

При проведении на оз. Байкал глубоководных исследований (на глубинах порядка 1400 м), с помощью глубоководных обитаемых аппаратов «МИР», была открыта моно-литная достаточно протяженная залежь гидрата метана. Для исследований залежи был применен традиционный подход для геохимических глубоководных исследований,

а именно – отбор образцов на морском дне с последующей доставкой на борт судна. При помещении в специальные контейнеры, описанные ниже, образцы оставались неизмененными и в дальнейшем помещались в подходящую среду, в которой можно было проводить измерения и делать анализы на борту исследовательского судна, или позднее, в стационарной лаборатории. На основании выполненных экспериментальных исследований и анализа процессов обмена химическими компонентам через поверхность раздела вода – осадок оз. Байкал, предлагаются подходы к созданию донных гидролого-гидрохимических комплексов (линейки станций) на базе программно-технических средств нового поколения.

Метановые гидраты на озере Байкал

Проводившиеся на дне оз. Байкал исследования залежей гидратов метана, являющихся перспективным углеводородным сырьем, относятся к разряду уникальных экспериментов и проводились с помощью уникальных исследовательских технических средств – глубоководных обитаемых аппаратов. Эти эксперименты позволяют оценить перспективы и возможности развития глубоководных технических средств для разведки, оценки ресурсов залежей газовых гидратов и, в будущем, возможностей их промышленной добычи (рис. 1).

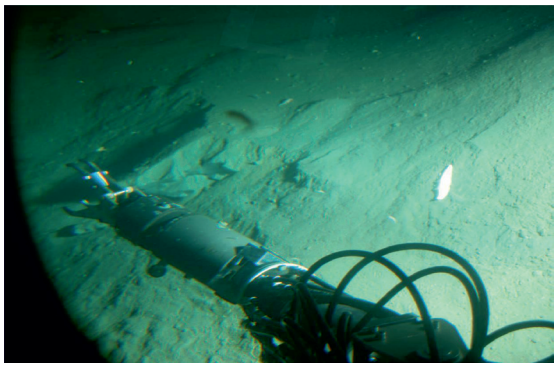

Рис. 1. Наблюдаемые через иллюминатор глубоководного обитаемого аппарата «Мир» монолиты гидрата метана

При проведении научных исследований на борт судна-носителя глубоководного аппарата необходимо было доставлять образцы гидрата метана, которые были обнаружены в предварительных разведочных спусках аппарата и которые манипуляторами аппарата были отломаны от монолитной залежи гидрата метана (рис. 2). Для доставки на поверхность образцов гидрата метана использовались специальные контейнеры. С помощью манипулятора глубоководного аппарата контейнер помещался в местах выхода метановых пузырей со дна озера, а с помощью другого манипулятора заполнялся образцами гидрата метана. После этого контейнер начинали заполнять метановые пузыри, которые при соприкосновении друг с другом не объединялись в один пузырь, а объединялись в твердую гидратную пену, из-за ранее сформировавшейся гидратной оболочки на их поверхности. Контейнер (в стакане контейнера устанавливался термодатчик.), как правило, перед всплытием заполнялся пеной приблизительно наполовину, так что чувствительный элемент термодатчика оказывался внутри гидратной пены. В процессе всплытия происходило расширение газа и, как следствие, происходило вытеснение воды из контейнера. На одном из манипуляторов глубоководного аппарата была установлена видеокамера, которая и регистрировала происходящие внутри контейнера процессы.

Рис. 2. Образец гидрата метана, отломанный от монолита манипулятором глубоководного обитаемого аппарата

Проводившиеся при всплытии измерения параметров внутри контейнеров показали, что в зоне устойчивости гидратов метана и при наличии выделившегося газа в контейнере расширение этого газа способствует значительному охлаждению содержимого контейнера. Как показывают проводившиеся расчеты, оценки и эксперимент, охлаждение возрастает с ростом скорости подъёма контейнера и снижается при уменьшении теплоизоляции контейнера. Таким образом, граница термодинамической устойчивости гидрата метана из-за охлаждения смещается в область меньших давлений, тем самым приближается к условиям поверхности водной среды, что очень важно для доставки на поверхность сохранившихся образцов гидратов метана.

Также объектами изучения являлись, в частности, тепловые эффекты в твёрдой гидратной пене, связанные с её образованием из пузырей метанового газа и ее транспортом. Следует отметить, что на поверхности пузырей происходит образование гидратной оболочки, которая и предотвращает их разрушение при контакте с другими пузырями. Были проведены специальные исследования, связанные с определением, происходит ли в процессе подъема контейнера на поверхность разложение образцов гидрата метана, в случае которого масса газа в контейнере увеличилась бы. Измерения показали сохранение массы газа в контейнере при относительно небольших изменениях температуры, а также свидетельствовали о сохранности гидратных образцов Выполненные экспериментальные исследования показывают, что основой разработки и развития будущих технологий транспорта газовых гидратов с глубоководных месторождений являются возможности управления и регулирования тепловыми процессами при движении на поверхность емкостей с образцами газовых гидратов.

Следует отметить, методы и средства исследований газовых гидратов, изложенные выше, относятся к разряду уникальных. Между тем интенсивно растет интерес к газовым гидратам, которые рассматриваются в качестве перспективного углеводородного сырья. В этой связи следует рассмотреть некоторые подходы и аппаратно-технические средства, для проведения масштабных исследований, разведки, в итоге промышленной добычи газовых гидратов. Подробное содержание описанных выше исследований изложено в [1, 2].

Методы и средства исследований

В настоящее время средства и методы ведения научных наблюдений и исследований в морях, расположенных по окраинам России, особенно это касается регионов с сезонным появлением ледового покрытия, ведет к значительным ограничениям получения экспериментальных данных об объекте исследования. Такую ситуацию предлагается разрешить с помощью разработки современных методик исследований и создания нового поколения технических средств измерений (автономных океанологических станций в виде распределенных сетей и сопутствующего им вспомогательного оборудования). Одним из основных требований является наличие на станциях гидроакустического канала, а также радиоканала для передачи измеренных данных и управления режимом работы станций. Все это позволит проводить долговременный мониторинг исследуемых объектов.

Как упоминалось выше, одним из основных требований является наличие на станциях гидроакустического канала для передачи измеренных данных и управления режимом работы станций. Это связано с тем, что в северных морях высока вероятность неблагоприятных погодных условий, сопровождаемых сильным морским волнением и, как следствие, практически невозможностью уверенной передачи данных измерений через кабель, а также через радиобуй.

Многоцелевые автономные океанологические станции с дистанционным считыванием измеренных данных должны обеспечивать ведение мониторинга океанов и морей, особенно в регионах, где от сезона к сезону проявляется сильное волнение, а также намерзание ледяных корок. Изучение сезонной, синоптической, мезо- и микромасштабной изменчивости водных масс, разработка и использование диагностических и прогностических моделей акваторий морей и океанов с целью активизации хозяйственной деятельности, а именно: ведением разведки, разработки и добычи минеральных ресурсов, сохранением и умножением биоресурсов в комплексе с природоохранной деятельностью, а также развитием инфраструктуры в плане оборонных задач.

Гидролого-гидрохимические комплексы нового поколения предполагают применение высокоразрешающих методов непрерывного гидрофизического и акустического зондирования (профилирования) водной толщи и современных методов геохимического анализа потоков вещества придонного слоя. Необходимо провести модернизацию всех средств измерений, методик пересчета скорости химического обмена через поверхность дна, а также провести совершенствование гидрофизических и гидрохимических измерительных модулей на основе современных микрокомпьютерных технологий. Также выполнить модернизацию алгоритмов микрокомпьютерного управления сетью унифицированных измерительных модулей, а также последовательное совершенствование цифрового гидроакустического канала передачи команд управления и данных измерений. Необходимо провести исследование способов повышения энергетического потенциала автономных комплексов [3–5].

Предложения по разработкам

Предлагается создавать образцы нового поколения автономных донных океа-

нологических станций с использованием гидроакустической телеметрии и энергосберегающих технологий на основе унифицированного ряда измерительных модулей – интеллектуальных датчиков, которые объединяются в единый комплекс.

В многофункциональном комплексе используются отдельные функционально универсальные автономные модули, но назначаемые на выполнение разнородных функций: измерение определенного параметра, выполнение гидроакустической связи, размыкание-замыкание тросовых держателей и т.п. и по командам назначенного управляющего модуля, которым может быть назначен каждый из них. Такие станции могут быть использованы для исследований и прогноза нефтегазоносности и других полезных ископаемых морских шельфов, а также эффективного мониторинга загрязнений акваторий.

Ведущийся мониторинг морей включает в себя изучение целого ряда процессов, таких как массообмен на поверхности раздела «вода – дно», выделение поглощения донными отложениями газов и твердых химических компонентов и многое др. Все эти процессы связаны с формированием месторождений нефти и газа, твердых полезных ископаемых и являются отражением постседиментационных процессов. Необходимо проведение оценок степени антропогенного воздействия на среду.

В этой связи непосредственно на дне следует применять метод донных камер (боксов), позволяющий путем прямых измерений потоков растворенных и газообразных компонентов количественно оценить химический обмен на границе «вода – дно». Боксовые эксперименты, проводимые с помощью донных станций, позволяют решать эту проблему и выполнять расчеты тонких параметров процесса проникновения кислорода в осадок, в частности глубину проникновения, выраженную в миллиметрах и долях миллиметров и отдельные параметры биохимии этого процесса. Данные донных гидрохимических станций являются основой для изучения процессов, ответственных за осадконакопление и биопродуктивность (на начальном этапе фоссилизации органического вещества в осадке, требуется большое количество кислорода, который падает в него через поверхность дна, обедняя придонную воду) акваторий, оценки антропогенного воздействия на среду. Полученные при ведении мониторинга данные позволят применять экономичные схемы численного моделирования процессов, свободные от сложных обратных задач восстановления полей. Все это будет способствовать изучению и прогнозированию процессов синоптической и мезомасштабной изменчивости водных масс, включая положение фронтальных зон, вихрей и линз.

Создание многофункциональных комплексов нового поколения позволит проводить фундаментальные и прикладные исследования, связанные, например, с глобальным циклом углерода, разнообразные экологические исследования, касающиеся захоронений различных загрязняющих компонентов вод (например, радиоактивные загрязнения), так и последующих процессов выхода этих загрязнений из осадка в воду. Разрабатываемое компьютерное моделирование, использование видеокомплексов с применением технологий распознавания образов позволяет эффективно решать вышеперечисленные задачи, а также иные многочисленные задачи прикладных и фундаментальных исследований [6, 7].

Заключение

Практическая значимость предлагаемых методов и технических средств связана, в частности, с потребностями нефтепоисковых работ и нефтегазового комплекса. В этом направлении одной из основных задач являются исследования новых нетрадиционных форм углеводородсодержащего сырья – газовых гидратов. Их запасы в осадках Мирового океана могут превышать все традиционные источники нефтегазового потенциала на суше. Показана необходимость модернизации всех технических средств поиска и исследований газогидратных месторождений, методик пересчета скорости химического обмена через поверхность дна, а также совершенствование многофункциональных гидрофизических и гидрохимических измерительных модулей с применением современных микрокомпьютерных технологий. Предлагаемый к разработкам комплекс технических и методических средств, использующий современные микрокомпьютерные методы обработки и представления получаемых данных непосредственно в процессе измерений, с возможностью коррекции программ проводимых исследований в реальном времени, закладывают основу для развития инновационных способов разведки и добычи подводных газовых гидратов. Эти исследования в перспективе способствуют развитию следующих этапов исследований, а именно, вопросам прокладки трубопроводного транспорта, влияния температурного режима (образование твердой и смешанной за счет примесей, выпадения парафина и т.д.) на процессы транспортировки нефти и газа.

Работа выполнена в рамках государственного задания ИО РАН (тема № 0149-

2019-0011) при поддержке РФФИ (проект № 17-05-41041 «РГО-а», и проект № 18-05-60070 «Арктика»).

Список литературы

1. Егоров А.В., Нигматулин Р.И., Рожков А.Н., Черняев Е.С. Тепловые эффекты при транспортировке глубоководных гидратов метана в негерметичном контейнере Препринт И П Мех РАН. 2012. № 1009. 25 с.

2. Егоров А.В., Рожков А.Н., Сагалевич А.М., Черняев Е.С. Методика исследования глубоководных метановых пузырей в озере Байкал аппаратами «Мир» с помощью ловушек // Современные методы и средства океанологических исследований: материалы XII Международной научно-технической конференции «МСОИ-2011». Т. 1. М., 2011. С. 138–141.

3. Черевко И.В., Розанов А.Г. Лендеры в шведских фьордах для исследования химического обмена на границе вода-дно // Современные методы и средства океанологических исследований: материалы XIII Международной научно-технической конференции «МСОИ-2013». Т. 1. М., 2013. С. 102–104.

4. Torres M.E., Wallmann K., Tréhu A.M., Bohrmann G., Borowski W.S., Tomaru H. Gas hydrate growth, methane transport, and chloride enrichment at the southern summit of Hydrate Ridge, Cascadia margin off Oregon. Earth and Planetary Science Letters. 2004. № 226. P. 225–241.

5. Смирнов Г.В., Аистов Е.А., Оленин А.Л. Многоканальный гидролого-оптико-химический комплекс // Современные методы и средства океанологических исследований: материалы XII Международной научно-технической конференции «МСОИ-2011». Т. 1. М., 2011. С. 104–106.

6. Суконкин С.Я. Технология подводных исследований и поисковых работ, подводные аппараты и роботы // Современные методы и средства океанологических исследований: материалы XII Международной научно-технической конференции «МСОИ-2011». Т. 2. М., 2011. С. 20–21.

7. Вайнерман М.И., Минин М.В., Пономарев Л.О., Эделев О.К. Многофункциональная подводная станция, обеспечивающая выполнение поисковых, научно-исследовательских работ, а также обследование грунтов при работе на глубоководных шельфовых месторождениях // Современные методы и средства океанологических исследований: материалы XII Международной научно-технической конференции «МСОИ-2011». Т. 1. М., 2011. С. 28–30.

СТАТЬЯ

УДК 004.5

АНАЛИЗ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ ДЛЯ ИСПОЛЬЗОВАНИЯ В МУНИЦИПАЛЬНЫХ ОРГАНИЗАЦИЯХ

Назарова О.Б., Мекешкин Е.Т.

Магнитогорский государственный технический университет им. Г.И. Носова, Магнитогорск, e-mail: mekeshkin-1996@mail.ru

В данной статье приведено общее описание муниципальных организаций и обозначено, почему такие организации должны быть защищены системами контроля и управлением доступом. Обозначена проблема систем контроля и управления доступом в муниципальных организациях, которые не в состоянии выполнять максимально желаемый функционал из-за неправильного развертывания таких систем. Как правило, такие системы разрознены, и выполняемые ими функции не взаимодействуют между собой, тем самым не образуя единую, целостную систему обработки данных, для достижения максимального функционала. Таким образом, разрозненность систем контроля и управления доступом образует брешь в безопасности объекта, на котором развёрнуты такие системы, что позволяет посторонним лицам проще проникать на объекты для исполнения корыстных или преступных замыслов. Был произведен краткий обзор таких систем в целом, приведена их классификация и основные компоненты. Рассмотрены популярные системы контроля и управлением доступом, представленные на отечественном рынке, и отечественными разработчиками, даны их основные характеристики, выделены их сильные стороны, специализации, а также рассмотрены на рисунках принципы их работы и основные компоненты. Рассмотренные системы отвечают всем необходимым требованиям, чтобы обеспечить безопасность и необходимый функционал практически на любом муниципальном предприятии, от школы до организации местного самоуправления какого-либо населенного пункта.

Ключевые слова: системы контроля и управления доступом, безопасность, контроль доступа, СКУД, управление доступом, системы контроля, учет рабочего времени

ANALYSIS OF MANAGEMENT SYSTEMS AND CONTROL OF ACCESS FOR USE IN MUNICIPAL ORGANIZATIONS

Nazarova O.B., Mekeshkin E.T.

Magnitogorsk State Technical University G.I. Nosov, Magnitogorsk, e-mail: mekeshkin-1996@mail.ru

This article provides a general description of municipal organizations and outlines why such organizations should be protected by access control and control systems. The problem of access control and management systems in municipal organizations, which are not able to perform the most desirable functionality due to improper deployment of such systems, is identified. As a rule, such systems are scattered, and the functions performed by them do not interact with each other, thus not forming a single, complete data processing system, in order to achieve maximum functionality. Thus, the separation of access control systems creates a breach in the security of the object where such systems are rotated, which makes it easier for unauthorized persons to penetrate objects for the execution of clandestine or criminal plans. A brief review of such systems as a whole was made, their classification and main components were given. Considered popular control systems and access control presented on the domestic market, and domestic developers, given their main characteristics, highlighted their strengths, specialization, as well as in the figures considered the principles of their work and the main components. The considered systems meet all the necessary requirements to ensure the safety and the necessary functionality in almost any municipal enterprise, from the school to the organization of local self-government of any locality.

Keywords: access control and management systems, security, access control, access control, access control, control systems, time tracking

Муниципальные организации тесно связаны с нашей жизнью, так как образуют социальную инфраструктуру современного общества. Школы, поликлиники, расчетно-кассовые центры, организации местного самоуправления связаны со значительным потоком людей, как работающих в этих организациях сотрудников, так и граждан, обратившихся в такие учреждения. В то же время подавляющее большинство муниципальных организаций являются государственными структурами, которые работают с персональными данными граждан, государственными документами и другой конфиденциальной информацией, способной нанести ущерб или вред при ее разглашении.

Таким образом, каждая муниципальная организация должна быть защищена, а значит, должна использовать системы контроля и управления доступом (СКУД), чтобы разграничить права на доступ к данным различных категорий пользователей.

Современные СКУД позволяют решать широкий спектр задач, таких как:

– защита от промышленного шпионажа;

– защита от воровства;

– противодействие саботажу;

– защита от умышленного повреждения или разрушения материальной собственности организации;

– учёт рабочего времени;

– контроль своевременности ухода и прихода сотрудников;

– защита конфиденциальной информации от несанкционированного доступа:

– контроль потока посетителей на объекте;

– контроль въезда и выезда транспорта [1].

Грамотно построенная система управления доступом способна значительно повысить уровень обеспечения безопасности муниципального предприятия, минимизировав риски несанкционированного доступа к конфиденциальной информации.

Зачастую организации, в том числе и муниципальные, сталкиваются с проблемой, при которой уже внедренные системы контроля доступа полностью не выполняют возложенные на них функции или не могут быть адаптированы под новые виды задач.

Цель исследования состоит в анализе современных систем контроля и управления доступом для их эффективного использования в муниципальных организациях. Сравнительный анализ основных характеристик современных СКУД проводится для определения наиболее рациональных вариантов их эксплуатации с учетом максимально возможного функционала и возможностью интеграции с существующими и будущими системами.

Материалы и методы исследования

Основное предназначение любой СКУД – ограничение доступа на режимные объекты и хранилища данных. Кроме того, такого рода системы могут успешно осуществлять функции учета рабочего времени, контроля трудовой дисциплины, сохранности материальных ценностей и др. В целом СКУД является совокупностью программно-технических средств, а также организационно-методических средств, позволяющих решить вышеперечисленные задачи [2].

В качестве преграждающих барьеров, наиболее часто используемых в составе СКУД, можно выделить следующие: турникеты обычные и настенные, турникеты для прохода в коридорах, шлюзовые кабины, автоматические калитки, роторные турникеты, вращающиеся двери, дорожные блокираторы, шлагбаумы, парковочные системы, круглые раздвижные двери, трёхштанговые турникеты, полноростовые турникеты, раздвижные турникеты [3].

Очень важным является вопрос о возможности интеграции СКУД с любой системой безопасности с использованием открытого протокола. Используя входы и выходы в информационных системах при помощи коннекторов, можно получать и изымать данные из систем для их совместного взаимодействия.

Системы контроля и управления доступом как совокупность программных и аппаратных средств подлежат сертификации и стандартизации. Рассмотрим документы, которые регулируют данного рода системы [4].

ГОСТ Р 51241-98 «Средства и системы контроля и управления доступом» устанавливает классификацию и общие технические требования, и испытания, а также подразделяет СКУД по способу управления, по числу контролируемых точек доступа, по функциональным характеристикам, по виду объектов контроля и по виду защищённости системы от несанкционированного доступа извне [5].

Документ Р 78.36.005-99 разделяет все системы контроля и управления доступом на 4 класса:

– СКУД 1 класса – системы малой ёмкости, обладающие ограниченным функционалом. Работают в автономном режиме и осуществляют допуск всех лиц, имеющих идентификатор. Такие системы используют ручное или автоматическое управление исполнительными устройствами, а также световую, звуковую или светозвуковую сигнализацию;

– СКУД 2 класса – это многофункциональные системы. Данные системы могут быть как одноуровневыми, так и многоуровневыми. Могут работать как в автономном, так и сетевом режиме. Поддерживают разбиение посетителей на группы. Имеют функционал, позволяющий предоставлять допуск лицам или группам лиц по дате или временным интервалам. Система способна обеспечивать автоматическую регистрацию событий и автоматическое управление автоматическими устройствами;

– СКУД 3 и 4 класса – в основном сетевые системы контроля и управления доступом. В таких системах используются более сложные идентификаторы и различные уровни сетевого взаимодействия (клиент-сервер, интерфейсы считывателей карт Виганда или магнитных карт, специализированные интерфейсы и т.д.) [6].

На сегодняшний день существует достаточно СКУД от разных производителей, состоящих из различных компонентов, собранных в различные конфигурации в зависимости от предназначения системы и пожеланий клиента. При этом все системы контроля и управления доступом состоят из четырёх основных элементов: идентификатор пользователя, устройство идентификации (считыватели), управляющий контроллер, исполнительные устройства [7,8].

Одним из драйверов роста рынка СКУД специалисты называют распространение новых и перспективных технологий, в числе которых: мобильный доступ, биометрическая идентификация и объединение систем на основе единой программной

платформы. Положительной динамике будет способствовать и интерес рынка к интегрированным решениям, где СКУД часто играет центральную роль как система с наиболее развитой логикой.

Результаты исследования и их обсуждение

На данный момент лидирующими компаниями, предлагающими решения на рынке РФ, являются компании PERCo, Кодос, Bolid и ряд других, представляющих системы PERCo-Web, PERCo-S-20, Кодос-Оптимальный и Орион. Подробные технические данные систем представлены в таблице.

PERCo-Web – инструмент для управления предприятием, предназначенный для усиления дисциплины персонала и безопасности труда. В системе реализованы следующие основные функции: защита от незаконного проникновения, разграничение прав доступа сотрудников и посетителей, верификация прохода сотрудников и посетителей, автоматизация учета рабочего времени, контроль нарушений трудовой дисциплины, а также автоматизация работы бюро пропусков, отдела персонала и бухгалтерии. Система может быть развёрнута в большинстве видов муниципальных организаций, имеет хорошую масштабируемость, а за счет легкой интеграции программного обеспечения и простого монтажа технической части не останавливает работу организации. Надежность и безопасность такой системы доказывают проекты, успешно реализованные в таких организациях, как: Дальневосточный федеральный университет, Владивосток (Система S-20.), Гимназии № 2, Владивосток (Система S-20), СКУД PERCo на проходной Медицинской академии и др.

Система безопасности PERCo-S-20, реализованная для муниципальных учреждений, не только предотвращает проникновение посторонних, но и с помощью системы SMS-сообщений позволяет уведомить службу персонала о времени прибытия сотрудника по месту работы и ухода. В целом же функционал схож с системой PERCo-Web. Отличие заключается в особенности развертывания такой системы в учебных заведениях и возможности пользоваться специализированным программным обеспечением для контроля учеников.

PERCo-S-20 имеет следующие основные функции: защита от проникновения посторонних, SMS-уведомление родителей, SMS-биллинг, верификация. Видеонаблюдение, защита кабинетов и входов на этажи, интеграция PERCo-S-20 «Школа» с «Электронным дневником». Основные компоненты системы PERCo-Web и PERCo-S-20 представлены на рис. 1.

СКУД Кодос также является мощным инструментом с гибкой настройкой, как апаратного, так и программного иструментария системы. Разработчики системы постарались разработать максимально гибкую систему, которую можно модернизировать и интегрировать без существенных потерь и изменений системы. Построение системы можно начинать со СКУД 1 класса и по желанию развить ее до мощной системы безопасности. В целом же функционал СКУД Кодос аналогичен ранее представленным системам, а общая схема работы системы представлена на рис. 2.

СКУД Орион-про, реализуемая компанией Bolid, является мощнейшим средством для построения масштабной системы контроля с неограниченным числом идентификаторов и большим количеством охраняемых зон, что очень важно для больших предприятий для повышения уровня безопасности и осуществления контроля.

Система способна выполнять следующие задачи:

– сбор, обработку, передачу, отображение и регистрацию извещений о состоянии шлейфов охранной, тревожной и пожарной сигнализации;

– контроль и управление доступом (управление преграждающими устройствами типа шлагбаум, турникет, ворота, шлюз, дверь и т.п.);

Характеристики СКУД

Производитель	PERCo	PERCo	Кодос	Bolid
Название системы	PERCo-Web	PERCo-S-20	Кодос-Оптимальный	Орион
Количество работников	100000	10000	3000	Не ограничено
Количество зон охраны	1024	1024	40	16000
Возможность интеграции с БД	+	+	+	+
Возможность интеграции со сторонними сервисами	+	+	+	+
Дополнительные пакеты ПО	+	+	+	+

– видеонаблюдение и видеоконтроль охраняемых объектов;

– управление пожарной автоматикой объекта;

– взаимодействие с инженерными системами зданий;

– модульную структуру, позволяющую оптимально оборудовать как малые, так и очень большие распределенные объекты;

– защищенный протокол обмена по каналу связи между приборами.

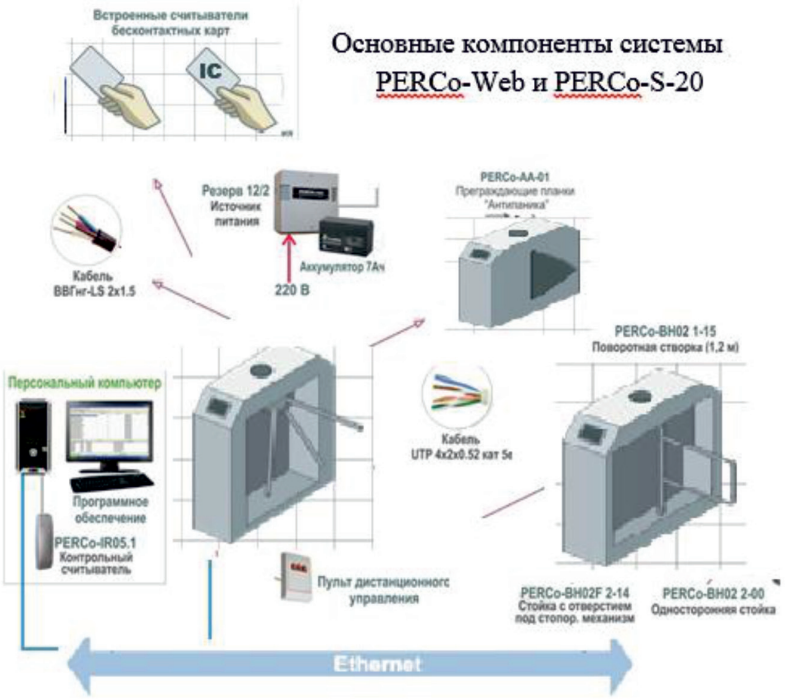

Рис. 1. Основные компоненты системы PERCo-Web и PERCo-S-20

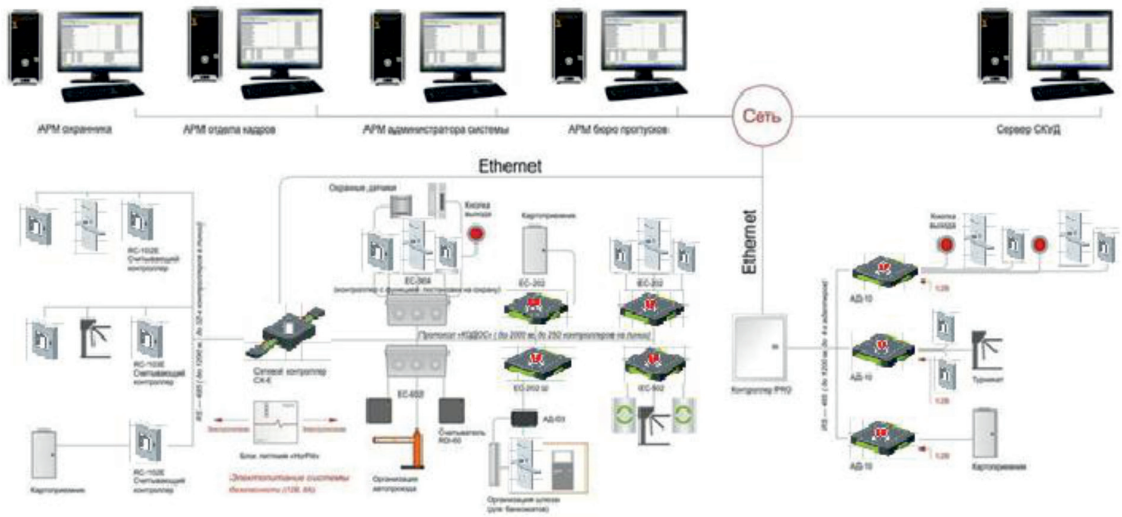

Рис. 2. Схема работы СКУД Кодос

Заключение

Из обзора видно, что существующие СКУД обладают различными возможностями по масштабированию, имеют свои особенности для максимального удовлетворения потребности любой муниципальной организации. «PERCo-Web» и «Bolid Орион» можно использовать практически в любой муниципальной организации с любым масштабом, составом и компоновкой. Системы отлично сбалансированы, имеют широчайший функционал и возможности обработки больших объёмов данных с большим количеством сотрудников, отделов и подразделений, в которых они работают. Системы способны легко интегрироваться в существующие инженерные системы, легко переносить модернизацию, повышая масштаб, функционал и надежность. PERCo-S-20 отлично подходит муниципальным и образовательным организациям за счет специально разработанного программного обеспечения, максимально облегчающего контроль над учениками, учитывая специфику данных учреждений. Имеет специальные возможности для коммуникации с родителями и т.д. Кодос-Оптимальный – мощная и стабильная система, которая также подойдет большинству муниципальных организаций, имеет достаточную мощность обработки и хранения информации, а также весь необходимый функционал, способный по мере необходимости расширяться. Исследовав лишь несколько СКУД, представленных на рынке, видно, что при грамотном подходе к проектированию системы контроля и управлением доступа можно решить множество задач безопасности управлением персоналом.

Рынок таких систем огромен и продолжает расти, с каждым днем появляются все более совершенные системы контроля и управлением доступом, которые проходя сертификацию и реализацию в проектах, также занимают свое место среди таких систем, предлагая все больше функциональных возможностей.

Внедрение СКУД – необходимый этап организации контроля и управления доступом на муниципальном предприятии.

Список литературы

1. Абрамов А.В. Системы контроля доступа. М.: «ОЦ Кудиц образ», 2000. 324 с.

2. Алексеенко В.Н. Современная концепция комплексной защиты. М.: МФИ, 1994. 137 с.

3. Внедрение информационных систем [Электронный ресурс]: учебное наглядное пособие / Скарлыгина Н.В., Михайлец В.Ф.; ФГБОУ ВПО «Магнитогорский государственный технический университет им. Г.И. Носова». Электрон. текстовые дан. Магнитогорск: ФГБОУ ВПО «МГТУ», 2015. Систем. требования: Adobe Acrobat Reader. Режим доступа: http://magtu/ru:8085/marcweb2/Default.asp (дата обращения: 17.07.2019).

4. ГОСТ Р 54831-2011. Системы контроля и управления доступом. Устройства преграждающие управляемые. Общие технические требования. Методы испытаний. М.: Стандартинформ, 2012. 16 с.

5. Масленникова О.Е., Назарова О.Б. Типовой проект внедрения корпоративной информационной системы для строительных организаций // Электротехнические системы и комплексы. 2015. № 2 (27). С. 47–52.

6. ГОСТ Р 51241-2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. М.: Стандартинформ, 2009. 32 с.

7. Волхонский В.В. Системы контроля и управления доступом. СПб.: Университет ИТМО, 2015. 253 с.

8. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. М.: Горячая линия-Телеком, 2010. 273 с.