Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Уфимский государственный нефтяной технический университет»

при поддержке:
Российской академии естественных наук
Академии наук Республики Башкортостан
Общественной организации
«Профессионалы дистанционного обучения»
Ассоциации образовательных программ
«Электронное образование Республики Башкортостан»
Российского союза научных и инженерных
общественных объединений
Партнерского центра
международного сертификационного холдинга IMQ

Информационные технологии
Проблемы и решения

У ф а
УНПЦ «Издательство УГНТУ»
2 0 2 1

ISSN 2500-2996

Информационные технологии. Проблемы и решения. – Уфа: УНПЦ «Изд-во УГНТУ», 2021, 4(17). 156 с.
Information technology. – Ufa: ERPC «USPTU Publishing House», 2021, 4(17). 156 p.

Учредитель:
ФГБОУ ВО Уфимский государственный нефтяной технический университет

2021, 4(17)
Издается с 2014 г.

Founder:
FSBEU HE Ufa State Petroleum Technological University

2021, 4(17)
Published since 2014

Полнотекстовая версия выпуска размещена в Научной электронной библиотеке elibrary.ru по ссылке:
https://elibrary.ru/title_about.asp?id=61250
Подробности на сайте: http://vtik.net

Отпечатано с готового электронного файла.

Подписано в печать 10.09.2021. Формат 60x80 $^{1}/_{16}$. Гарнитура «Таймс». Усл. печ. л. 9,07. Тираж 800 экз. Заказ 150.
Учебный научно-производственный центр «Издательство Уфимского государственного нефтяного технического университета»
Адрес учебного научно-производственного центра «Издательство Уфимского государственного нефтяного технического университета»: 450064, Российская Федерация, Республика Башкортостан, г. Уфа, ул. Космонавтов, 1.

ОГЛАВЛЕНИЕ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В НАУКЕ, ОБРАЗОВАНИИ И ПРОИЗВОДСТВЕ

Можаев М.А., Абакумцев Р.В. СУЩНОСТЬ ИНТЕРНЕТА ВЕЩЕЙ В ЦИФРОВОМ ПРОИЗВОДСТВЕ……. 4

Чжан Ж., Кинаш Н., Труфанов А. ТОПОЛОГИЧЕСКИЕ ОСОБЕННОСТИ ПРОВИНЦИАЛЬНЫХ ЖЕЛЕЗНОДОРОЖНЫХ СЕТЕЙ КНР……...……. 8

Гумерова К.Р., Тулупова О.П., Ганиева В.Р., Круглов А.А., Еникеев Ф.У. ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ РАСЧЕТА ЗАВИСИМОСТИ ПОДАЧИ ДАВЛЕНИЯ ГАЗА ОТ ВРЕМЕНИ ПРИ СВЕРХПЛАСТИЧЕСКОЙ ФОРМОВКЕ 14

Киреев И.Р., Барахнина В.Б., Шуваева В.Р. ПРОГРАММНЫЙ ПРОДУКТ ДЛЯ ОПРЕДЕЛЕНИЯ ПОКАЗАТЕЛЕЙ ВЗРЫВООПАСНОСТИ РЕЗЕРВУАРА И ВИЗУАЛИЗАЦИИ ПРОЦЕССА РАБОТЫ ТОВАРНОГО ПАРКА……. 21

Ерофеев В.В., Игнатьев А.Г., Олейник Н.И., Шарафиев Р.Г., Кульневич В.Б., Щепеткин В.В. МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ДЛЯ ОЦЕНКИ КОЭФФИЦИЕНТОВ КОНЦЕНТРАЦИИ НАПРЯЖЕНИЙ В СВАРНЫХ ТАВРОВЫХ СОЕДИНЕНИЯХ ……...…… 27

Еникеев Ф.У., Мурзина Г.Р. О РАЦИОНАЛЬНОМ ВЫБОРЕ ФОРМЫ ЗАГОТОВКИ ДЛЯ ПОЛУЧЕНИЯ РАВНОТОЛЩИННЫХ ИЗДЕЛИЙ ТИПА ШАРОБАЛЛОН……. 35

Марьина В.В. ПРИМЕНЕНИЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ РЕШЕНИЯ ЗАДАЧ РАСПОЗНАВАНИЯ РЕЧИ……. 40

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОНОМИКЕ, УПРАВЛЕНИИ И БИЗНЕСЕ

Ткаченко А.Л., Ольшанская О.И., Арышева О.Н. ИСПОЛЬЗОВАНИЕ ПРОГРАММЫ ANYLODGIC ДЛЯ АНАЛИЗА ПОТРЕБИТЕЛЬСКОГО РЫНКА ИГРЫ GENSHIN IMPACT И ПОСТРОЕНИЕ ПРОГНОЗА……... 45

Михайловская И.М., Имаева Л.Р. ТЕХНОЛОГИИ IOT ДЛЯ INDUSTRY 4.0..…… 50

МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ

Носкова Е.Е., Дружинская Е.В. ТЕОРЕТИЧЕСКИЙ ОБЗОР ГЕНЕТИЧЕСКОГО АЛГОРИТМА…… 57

Живодерников А.Ю., Яговитов Д.С., Трофимов А.Ю. ИМИТАЦИОННАЯ МОДЕЛЬ МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ И ИССЛЕДОВАНИЕ НА ЕЕ ОСНОВЕ ПОКАЗАТЕЛЕЙ КАЧЕСТВА ОБСЛУЖИВАНИЯ ТРАФИКА РЕАЛЬНОГО ВРЕМЕНИ…….. 62

СЕТИ И ТЕЛЕКОММУНИКАЦИИ

Ромасевич П.В., Смирнова Е.В. ОБРАЗОВАТЕЛЬНЫЙ ПРОДУКТ D-LINK ДЛЯ ОБУЧЕНИЯ СЕТЕВЫМ ТЕХНОЛОГИЯМ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ НЕФТЕГАЗОВОГО СЕКТОРА ЭКОНОМИКИ…..... 70

СИСТЕМЫ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ И ГИС-ТЕХНОЛОГИИ

Чечет Д.В., Трубаков Е.О. ИССЛЕДОВАНИЕ МЕТОДОВ СКЕЛЕТИЗАЦИИ РАСТРОВЫХ ИЗОБРАЖЕНИЙ ТОПОГРАФИЧЕСКИХ КАРТ…..…… 76

СИСТЕМЫ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Меджидов З.У. ИСПОЛЬЗОВАНИЕ МЕТОДА RAINBOW ДЛЯ РАСКРЫТИЯ ХЕШ-ФУНКЦИЙ MD5……. 82

Давыдова А.О., Кусяпова Д.А., Титух Я.Э., Сенцова А.Ю. ПЕРСОНАЛИЗИРОВАННЫЕ ФИШИНГОВЫЕ АТАКИ..…….... 87

Степанов В.А., Андреев Н.Д. МОДЕЛИРОВАНИЕ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПО НОВОЙ МЕТОДИКЕ ФСТЭК, ИСПОЛЬЗУЯ СРЕДСТВА АВТОМАТИЗАЦИИ……. 95

Сенцова А.Ю., Тимергазин В.Э., Ильясова Р.И. АНТИФРОД-СИСТЕМА КАК ИНСТРУМЕТ ПРЕДОТВРАЩЕНИЯ МОШЕННИЧЕСТВА…… 101

Цветкова И.С., Сенцова А.Ю. ИСПОЛЬЗОВАНИЕ МЕТОДА, ОСНОВАННОГО НА МАРКОВСКИХ МОДЕЛЯХ, ДЛЯ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ…… 107

Ратковский А.А., Муталлапов Р.Н. РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ ОБУЧЕНИЯ И ПОВЫШЕНИЯ НАВЫКОВ ПОЛЬЗОВАТЕЛЕЙ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ……. 113

Джафарова Ш.М. РАЗРАБОТКА МОДЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПРИМЕНЕНИЕМ ПРОДУКЦИОННОЙ МОДЕЛИ……... 118

Корнеев Н.В. БЕЗОПАСНОСТЬ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ КОМПОНЕНТОВ ЭКОСИСТЕМЫ ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО РЫНКА С ЭЛЕМЕНТАМИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА……... 124

СОВРЕМЕННАЯ МЕТОДИКА ПРЕПОДАВАНИЯ ИНФОРМАТИКИ

Бружукова М.А. ОБУЧЕНИЕ РЕШЕНИЮ ЗАДАЧ С ЭКОНОМИЧЕСКИМ СОДЕРЖАНИЕМ В КУРСЕ ИНФОРМАТИКИ ОСНОВНОЙ ШКОЛЫ……. 131

Юрьева М.С. ОБУЧЕНИЕ ПРОГРАММИРОВАНИЮ ЦИКЛОВ В СРЕДЕ ПРОГРАММИРОВАНИЯ КУМИР В ОСНОВНОЙ ШКОЛЕ……... 136

Семтина Е.А., Проценко С.И. ОБУЧЕНИЕ ОСНОВАМ АЛГОРИТМИЗАЦИИ НА БАЗЕ СИСТЕМЫ КУМИР В ОСНОВНОЙ ШКОЛЕ…… 140

Исакова А.И., Левин С.М. ПРЕИМУЩЕСТВА LMS MOODLE В ФОРМИРОВАНИИ ПЕРСОНАЛИЗИРОВАННОЙ СРЕДЫ ЭЛЕКТРОННОГО ОБУЧЕНИЯ СТУДЕНТОВ……... 145

Зиязиева Л.Р. МЕТОДОЛОГИЧЕСКИЕ ПОДХОДЫ ФОРМИРОВАНИЯ ГОТОВНОСТИ СТУДЕНТОВ К САМОСТОЯТЕЛЬНОЙ РАБОТЕ ПОСРЕДСТВОМ БЕНЧМАРКИНГ-ТЕХНОЛОГИИ…… 151

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В НАУКЕ, ОБРАЗОВАНИИ И ПРОИЗВОДСТВЕ

УДК 004.75

СУЩНОСТЬ ИНТЕРНЕТА ВЕЩЕЙ В ЦИФРОВОМ ПРОИЗВОДСТВЕ

THE ESSENCE OF THE INTERNET OF THINGS IN DIGITAL PRODUCTION

Можаев М.А., Абакумцев Р.В.,
Московский государственный технологический университет «СТАНКИН»,
г. Москва, Российская Федерация

M.A. Mozhaev, R.V. Abakumcev,
Moscow state University of technology «STANKIN»,
Moscow, Russian Federation

e-mail: pr0n00gler@yandex.ru

Аннотация. Ежегодно человечество создает огромное количество данных, которых становится все больше. Для того, чтобы эффективно их использовать важно осуществлять качественный анализ. Неполное исследование каких-либо показателей может существенно влиять на общий результат. Полнота информации – это залог ее качественной обработки и использования.

Одной из технологий, которая может позволить автоматизировать процессы работы с данными в рамках цифрового производства является Интернет вещей (IoT). Данная технология позволяет собирать, хранить и проводить анализ информации о различных производственных процессах и событиях, связанных с физическими объектами в режиме реального времени. Это дает возможность выявлять и прогнозировать возникновения различных рисков, контролировать проведение планового и внепланого обслуживания оборудования, учитывая все особенности производственного процесса и общего состояния организации.

В рамках цифрового производства IoT позволит упростить сбор данных с используемого оборудования, имеющейся техники (погрузчики и т.п.). Это необходимо чтобы уменьшить возможные риски от сбоев, а также для более эффективного управления производством. Так IoT платформа влияет на все сферы производства от управления производственными линиями до управления складами.

Abstract. Every year, humanity creates a huge amount of data, which is becoming more and more. In order to use them effectively, it is important to carry out a qualitative analysis. Incomplete research of any indicators can significantly affect the overall result. The completeness of information is the key to its high-quality processing and use.

One of the technologies that can allow you to automate the processes of working with data in the framework of digital production is the Internet of Things (IoT). This technology allows you to collect, store and analyze information about various production processes and events related to physical objects in real time. This makes it possible to identify and predict the occurrence of various risks, monitor the implementation of planned and unscheduled maintenance of equipment, taking into account all the features of the production process and the general state of the organization.

Within the framework of digital production, IoT will simplify the collection of data from used equipment, existing equipment (loaders, etc.). This is necessary to reduce the possible risks from failures, as well as for more efficient production management. So the IoT platform affects all areas of production from the management of production lines to the management of warehouses.

Ключевые слова: интернет вещей, промышленный интернет вещей, прогнозирование, цифровое производство, техническое обслуживание и ремонт, умный склад.

Keywords: Internet of Things, Industrial Internet of Things, predict, digital production, maintenance and repair system, smart warehouse.

В общем случае под Интернетом вещей понимается совокупность разнообразных приборов, датчиков, устройств, объединенных в сеть посредством любых доступных каналов связи, использующих различные протоколы взаимодействия между собой и единственный протокол доступа к глобальной сети. В роли глобальной сети для Интернет-вещей широко применяется сеть Интернет.

Интернет вещей основывается на трех базовых принципах. Во-первых, повсеместно распространенную коммуникационную инфраструктуру, во-вторых, глобальную идентификацию каждого объекта и в-третьих, возможность каждого объекта отправлять и получать данные посредством персональной сети или сети Интернет, к которой он подключен [1].

Также существует понятие промышленного интернета вещей, которое связано с цифровым производством.

Технология промышленного интернета вещей – или же IIoT (Industrial Internet of Things) – активно применяется для реализации корпоративных целей в разных отраслях промышленности.

IIoT-платформа позволяет успешно накапливать данные и совершать их пересылку автоматически без выполнения каких-либо действий вручную. Для оптимизации работы системы предусмотрена возможность удаленно контролировать и управлять процессами.

Промышленный IoT состоит из компьютерной сети и специальных датчиков, которые подключаются к необходимым производственным объектам и устройствам для аккумулирования данных.

Для поддержки принятия решений и управления физическими объектами с учетом заданных требований IIoT оперирует большими объемами данных.

Система проводит непрерывный контроль всех важных показателей, которые напрямую определяют выполнение основных этапов работы.

Выявление проблемных моментов в самые короткие сроки позволяет создать лучшие условия для их эффективного устранения.

Система мониторинга, которая основывается на работе с данными, получаемых от IoT устройств, позволяет визуально отображать процесс выполнения действий. Таким образом человек, который совершает обслуживание установок, может визуально определить состояние выполнения технологических элементов, а также получать предупреждения о возможных и имеющихся сбоях в работе оборудования.

Большое количество информации обрабатывается за очень маленькие временные промежутки, что обеспечивает своевременное получение важных показателей.

Все положительные моменты и возможности платформы помогают большому количеству компаний различных промышленных направлений обеспечивать

эффективную деятельность и выделяться среди конкурентов надежностью и точностью выполнения всех обязательств без рисков и сбоев.

Промышленный интернет вещей обеспечивает:

– полное, эффективное и рациональное использование активов и оборудования фирмы;

– сокращения или полное отсутствие простоев производства;

– существенное уменьшение статей расходов на ремонт оборудования и его обслуживание.

– рост коэффициента полезного действия каждого агрегата и аппарата, что увеличивает объемы производительности.

– расходы на оплату энергии можно существенно сократить, проанализировав показатели процессов и выявив реальные способы экономии [2].

Главная сложность организации связи в задачах IIoT связана с периферийными устройствами, потому что в сеть необходимо интегрировать самые разные их типы, и большая часть из этих устройств является устаревшими (последовательными), которые, вероятно, старше, чем большая часть современных мобильных телефонов или ноутбуков. Что еще больше усложняет ситуацию, так это то, что эти устройства обмениваются данными по разным протоколам.

Данные с разных устройств и разных протоколов должны быть преобразованы и переданы на центральное устройство, которое обеспечивает сбор и обработку информации для выработки дальнейшего прогноза по работе оборудования. Именно здесь устройства внутрисетевого взаимодействия становятся чрезвычайно важными, поскольку они обеспечивают организацию связи.

На рисунке 1 показаны типы последовательных устройств, которые обычно используются в различных промышленных системах.

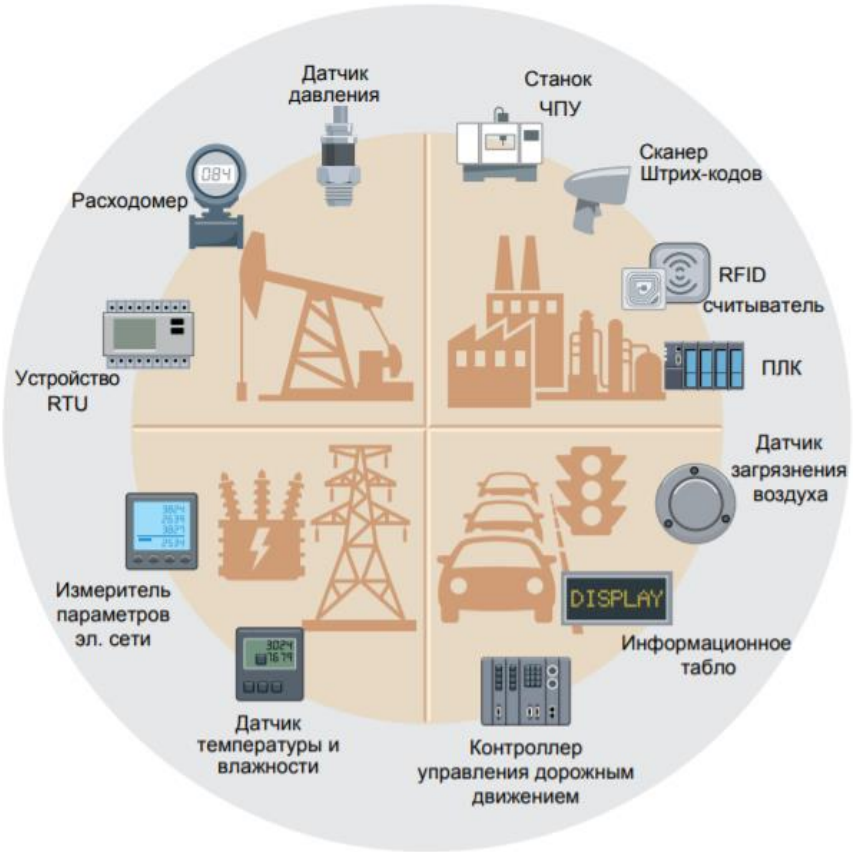

Рисунок 1. Типовые устройства в различных сферах промышленности [3]

Эти последовательные устройства общаются либо по проприетарным протоколам, либо по стандартным протоколам полевой шины, таким как Modbus, PROFIBUS и т.д.

Одним из возможных применений IIoT платформ, является автоматизация процесса технического обслуживания и ремонта (ТОиР). В ее рамках, IIoT платформа позволит вести мониторинг остаточного ресурса используемого оборудования по определенным методикам. В результате менеджмент предприятия обладает актуальной информацией по достижении экстремальных точек, по которым можно своевременно взвесить альтернативы и принять решение: списать оборудование и заменить его новым, или же провести капитально-восстановительный ремонт и продолжить эксплуатацию.

Также технологии Интернета вещей широко применяются в умных складах, чтобы помогать оптимизировать процедуры управления запасами на складе, планирование труда [4].

IoT обеспечивает связь и обмен данными между несколькими объектами, взаимодействующими друг с другом.

К примеру, на склад поступают пакеты с товаром, оснащенные RFID-метками. RFID-сканер сканирует метки и подсчитывает количество пакетов. Затем WMS связывается с роботами, информируя их о местонахождении пакетов и месте на складе, на которое их необходимо доставить. Без Интернета вещей сотруднику склада пришлось бы выполнять каждый шаг этого процесса вручную. Это неизбежно привело бы к ошибкам. Ведь количество информации о каждом продукте огромно.

Склады, использующие IoT, могут быстро реагировать на поступившие заказы, что дает им конкурентное преимущество перед компаниями с традиционным подходом к бизнесу. Например, можно эффективно автоматизировать задачи, чтобы обеспечить приоритет выполнения наиболее важных задач, а не использовать традиционную систему очередности по времени поступления.

Без IoT невозможно представить умную инвентаризацию и контроль за целостностью товаров и других материальных активов.

Также IoT-решения позволяют повысить эффективность работы складского оборудования, начиная от погрузчиков и заканчивая лентами транспортеров: они могут быть оснащены датчиками, чтобы определить оптимальную пропускную способность и скоростной режим [5].

Выводы

Технологии интернета вещей могут играть существенную роль в цифровом производстве. IIoT платформа будет выполнять оперативный анализ всех необходимых данных для поиска самого рационального и правильного способа устранения возникших неполадок в работе оборудования или рисков появления таких проблем.

Литература

1. Интернет вещей: учебное пособие [текст] / А.В. Росляков, С.В. Ваняшин, А.Ю. Гребешков. – Самара: ПГУТИ, 2015. – 200 с.

2. Промышленный интернет вещей (IIoT): что означает, принцип работы [Электронный ресурс] – https://clck.ru/WD4vU, (дата обращения 27.12.2020 г.).

3. Подключение устройств последовательных интерфейсов к инфраструктуре IIoT [Электронный ресурс] – https://clck.ru/WD4x6, (дата обращения 28.12.2020 г.).

4. Гущина П.Ф., Саркисова И.О. Концепция внедрения блокчейна в 1С: ПРЕДПРИЯТИИ 8.3 для экспедиторской компании. // Теория и практика проектного образования. – 2019. – №4(12). – С. 80-81.

5. Какие технологии изменят сферу складской логистики | iot.ru Новости Интернета вещей [Электронный ресурс] – https://clck.ru/WD54H, (дата обращения 31.01.2021 г.)

UDC 004.94: 519.179

TOPOLOGICAL FEATURES OF PROVINCIAL RAILWAY NETWORKS IN PRC

ТОПОЛОГИЧЕСКИЕ ОСОБЕННОСТИ ПРОВИНЦИАЛЬНЫХ ЖЕЛЕЗНОДОРОЖНЫХ СЕТЕЙ КНР

R. Zhang, N. Kinash, A. Trufanov,
FSBEI HPE “Irkutsk National Research Technical University”,
Irkutsk, Russian Federation

Чжан Ж., Кинаш Н., Труфанов А.,
ФГБОУ ВПО «Иркутский национальный исследовательский технический университет»,
г. Иркутск, Российская Федерация

e-mail: 2812841322@qq.com

Abstract. Transportation systems are key factors for any nation economic and social development. Practically all significant countries risen along with their railway widening so that pertinent structures became very sophisticated. Just to understand nature, performance and robustness of complicated structures a fascinating domain- network science-has been designed for the last twenty years. Notably that structural shape of a network defines its robustness (vulnerability) to a spectrum of threats. Being a matter of scholar research network scope is more and more imbedding into industrial practice, even to standardization systems. However, some local issues are left beyond powerful network approaches. In this study we analyzed Chinese provincial railway networks with paying attention to their topological metrics in whole and vulnerabilities in particular. The results demonstrate their practical value to focus on key nodes of the railway networks to provide safety and stability of local transportation systems. Network scope as productive and versatile one to be implemented not only on global level but on local level as well has been discussed.

Аннотация. Транспортные системы являются ключевыми факторами экономического и социального развития любой страны. Практически все значительные страны выросли вместе с расширением своих железных дорог, так что соответствующие структуры стали очень сложными. Чтобы понять природу, производительность и надежность сложных структур, в течение последних двадцати лет была разработана увлекательная предметная область – сетевая наука. Примечательно, что структурная форма сети определяет ее устойчивость (уязвимость) к спектру угроз. Сфера научных исследований сети все больше и больше внедряется в промышленную практику, даже в системы стандартизации. Однако некоторые локальные проблемы остаются за рамками

мощных сетевых подходов. В этом исследовании мы проанализировали провинциальные железнодорожные сети Китая, уделяя внимание их топологическим показателям в целом и уязвимостям в частности. Результаты демонстрируют их практическую ценность для сосредоточения на ключевых узлах железнодорожных сетей для обеспечения безопасности и устойчивости местных транспортных систем. Обсуждались возможности сетевого подхода как продуктивного и универсального, который будет реализован не только на глобальном, но и на местном уровне.

Keywords: provincial railway networks, network science, topological robustness, threats, attacks, failures, metrics.

Ключевые слова: провинциальные железнодорожные сети, сетевая наука, топологическая надежность, угрозы, атаки, сбои, метрики.

Introduction

Transportation systems are key factors for any nation economic and social development. Practically all significant countries risen along with their railway widening so that pertinent structures became very sophisticated. Just to understand nature, performance and robustness of complicated structures a fascinating domain- network science-has been designed for the last twenty years. Actually, network science provides impressive techniques to analyze interacting actors within t huge angled complex systems which put almost unresolved difficulties being considered by traditional methods.

Related works

The topology-based network concept has been applied for modelling diverse transportation systems in their technological and sociological aspects. In this regard a general transportation problem might be unfolded through three networked sheets: physical lines that connects sites (roads, railways), routes supported by vehicle entities, and passenger flows.

As described in [1], transportation networks are often modelled in L-space or in P-space configuration architectures. These architectures consider nodes sets equivalently, e.g., stations and stops, with no difference for all the three sheets mentioned above. Contrary, link sets in the sheets are constructed in different ways. In the L-space architecture, each pair of sequential neighboring nodes along a physical line is connected by a link. Contrary P-space corresponds mainly to route links so that all nodes belonging to the same route are connected by links directly with no regard to real physical distances.

Diverse national railways models were explored in many works (e.g. [2]).

Notably that structural shape of a network defines its robustness (vulnerability) to a spectrum of threats. Being a matter of scholar research network scope is more and more imbedding into industrial practice, even to standardization systems.

Network-based conception is of value not only from the academic point of view but it has attracted practical railway experts as well. Thus, a graph model “UIC RailTopoModel” [3] with four levels that reflect details of real practice was proposed as International Railway Standard (IRS 30100) [6] in 2016.

As being critical infrastructures railways are systems to be contemplated with concern of their safety. It is of value to understand the pertinent vulnerabilities to wide spectrum of threats. However, some local issues are left beyond powerful network approaches. In this study we analyzed Chinese provincial railway networks with paying attention to their topological metrics in whole and vulnerabilities in particular.

Model

As mentioned in [4] information on network topology is crucial to attack the network successfully. However even the information is open and available it is of sense to study how the network can withstand the threats. Experts in safety and security traditionally section threats into intentional and unintentional ones. And consequential events are named as attacks and failures (technological or organizational). Usually while modelling vulnerability of a network a scholar assess to what extent it disintegrates with removal of nodes (or edges). In n quantitative format it means that the number of connected cluster increases and the giant cluster (maximal connected one) reduces with every element removal.

It appeared in the beginning of network science (late 1990- early 2000) that topological properties of complex networks presented for example by diverse technological systems have a key impact on their vulnerability to such principle threats as failures and attacks [5] Series of works demonstrated on synthetic and real networks that scale-free structures (those with power-law connectivity distribution) occurs much more vulnerable to intentional attacks if compare with random networks. In contrast the latter are more sensitive to occasional failures.

Some papers considered removal strategy toward links. General set of threats is numerous enough and might include not deleting elements but blocking them with diverse temporal dependencies.

In the current work we deepen understanding of the vulnerability differences of the provincial railway networks in PRC when exposing those to failures or attacks on nodes. Attacks are modelled in “classic” way: the nodes with highest degree are eliminated first.

Data

Figure 1. Map of railways in Shandong province of PRC

Two neighbor regions are chosen to examine the features of the pertinent railway topologies: Shandong province and Henan province. The maps of the PRC railway system one can find in [6], the one of Shandong railways is portrayed on Figure 1.

Findings

The data presented on maps was processed into Excel format to be further imported into Gephi instrument [7].

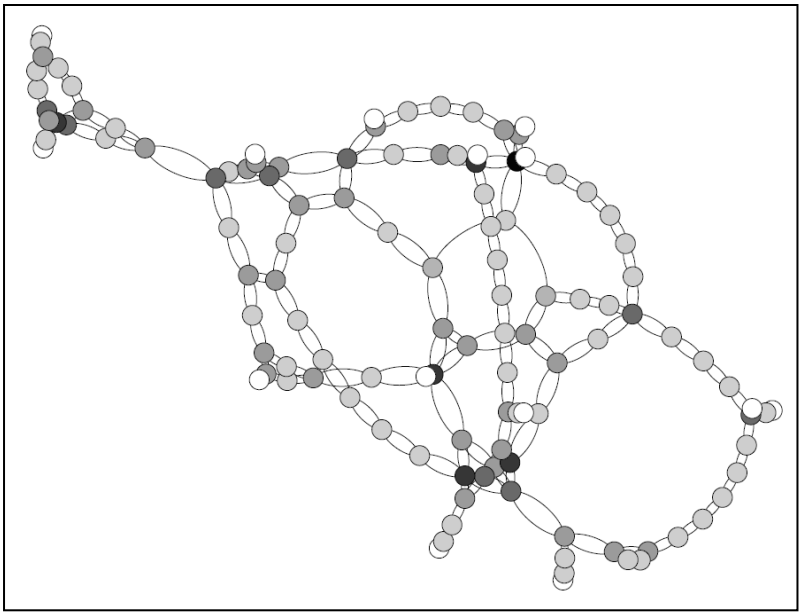

Figure 2. Shandong railway network

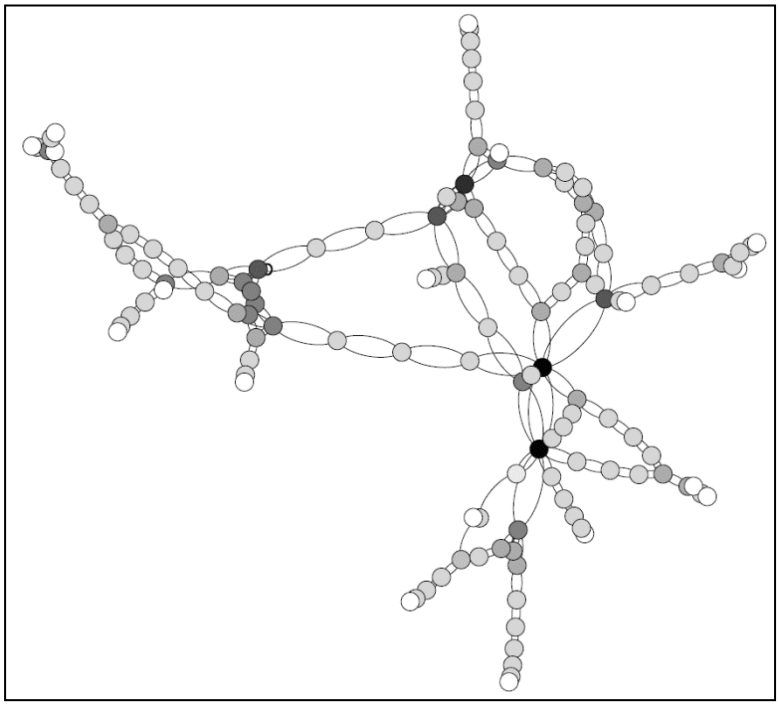

Figure 3. Henan railway network

To layout the corresponding graphs we used “Force Atlas” and ranked the node’s color according to their degree. The network model for railways of Shandong and Henan provinces are shown on Figure 2 and Figure 3 respectively.

Being exposed to diverse threats with consequent attacks or random failures with removal of nodes the network topologies are modified. Attacks break the networks into unconnected clusters: these for ten removed nodes according to descending degree order are shown on Figure 4.

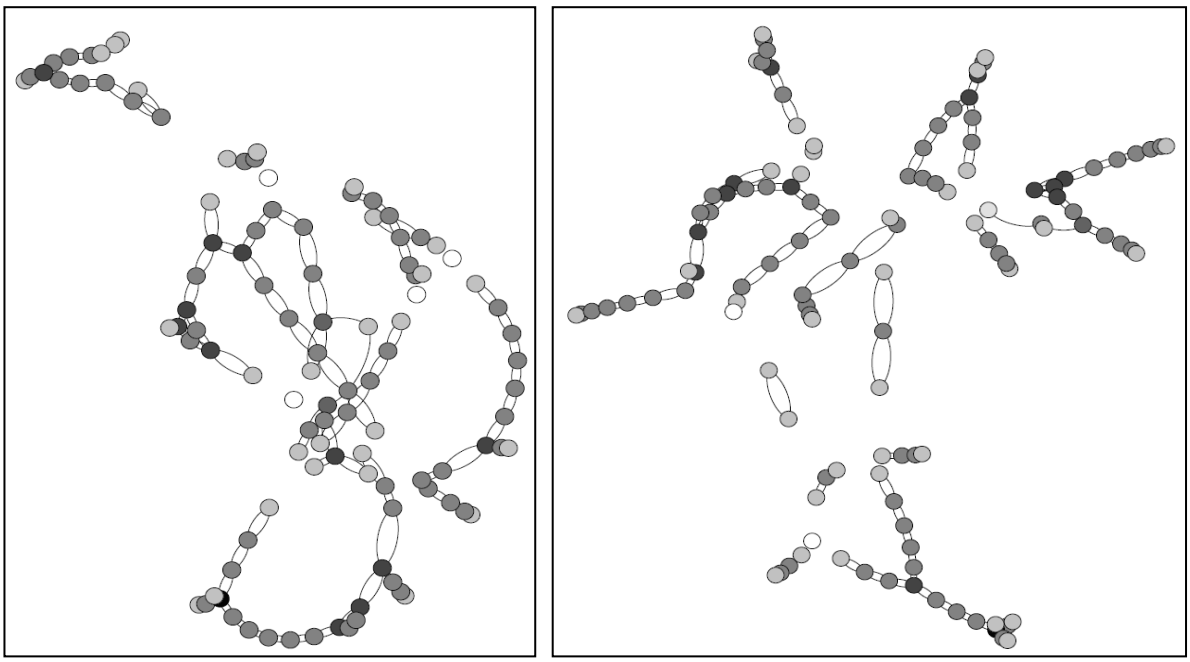

Figure 4. Scattered Shandong (left) and Henan (right) railway networks after being exposed to ten attacks

The calculated values of metrics for the networks exposed to intentional attacks and met with random failures are presented in Table.

Table – Size of giant cluster G and number of connected components NC for the networks exposed to intentional attacks and giant cluster size in networks met random failures

Number, removed nodes	G, attacks, Shandong province	NC, attacks, Shandong province	G, failures, Shandong province	G, attacks, Henan province	NC, attacks Henan province	G, failures, Henan province
0	119	1	119	128	1	128
1	118	1	116	104	3	125
2	114	2	113	83	4	122
3	112	2	110	82	4	120
4	111	3	107.5	48	5	118
5	110	3	105	38	7	116
6	95	4	102.5	37	10	114
7	67	6	100	36	10	112
8	49	8	97.5	28	12	110
9	37	10	95	28	15	108

Discussion

Topological vulnerability in terms of dependences of giant cluster size and number of connected components versus number of removed nodes are displayed on the Figures 5-6 respectively.

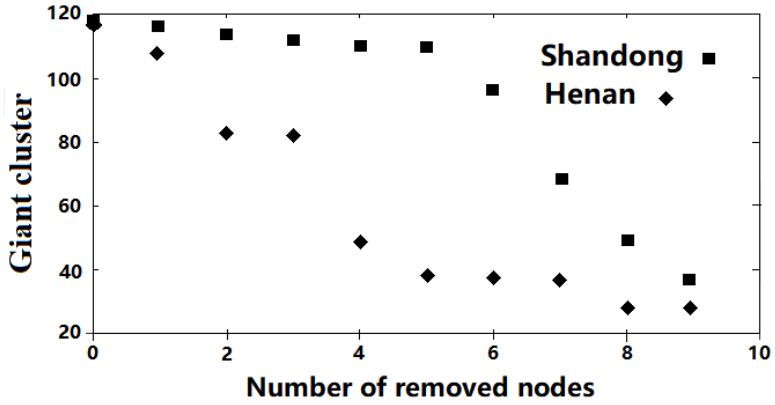

Figure 5. Vulnerabilities of Chinese provincial railway networks exposed to classic attacks

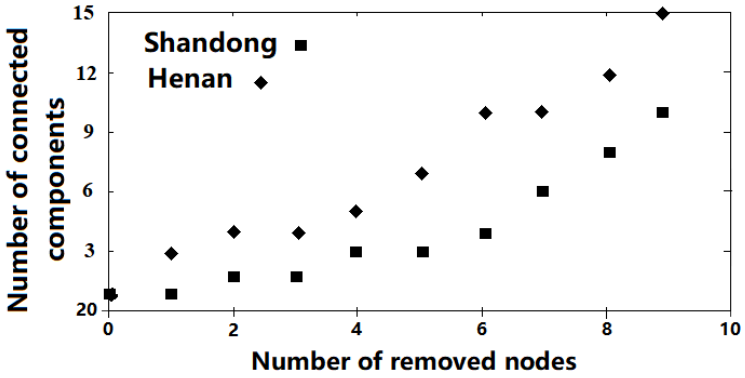

Figure 6. Connected nodes in Chinese provincial railway networks exposed to classic attacks

The modelling we performed showed clearly that Henan railway network is more sensitive to intentional attacks (removed nodes in descending degree order) than that of Shandong province. The structural vulnerability of these two entities to random failures is similar. Thus, to provide safety and stability of transportation system expert should put in focus not only on global level issues but those of local character as well.

Conclusions

The network scope-based study showed that provincial railway critical structures might differ severely in context of their vulnerability to intentional attacks as destroying nodes. Some more investigations are needed to clarify the role of blocked and removed links and cascade effects.

Acknowledgements
The reported study was funded by RFBR and MECSS, project number 20- 57-44002

References

1. Derrible, S., Kennedy, C. 2009. Transportation Research Record: Journal of the Transportation Research Board 21(12) 17-25.

2. Tikhomirov, A., Rossodivita, A., Kinash, N., Trufanov, A., & Berestneva, O., 2017. General topologic environment of the Russian railway network. Journal of Physics: Conference Series, 803, 012165. doi:10.1088/1742-6596/803/1/012165

3. RailTopoModel – Railway Network Description – A conceptual model to describe a railway network, 2015. International Union of Railways. pp 58. URL: https://clck.ru/WDAYr

4. Xiao, S., Xiao, G., 2006. NISp1-06: On Intentional Attacks and Protections in Complex Communication Networks. IEEE Globecom 2006, San Francisco, CA, USA, 2006, P. 1-5. doi:10.1109/glocom.2006.313

5. Guillaume, JL., Latapy, M., Magnien, C., 2005 Comparison of Failures and Attacks on Random and Scale-Free Networks. In: Higashino T. (eds) Principles of Distributed Systems. OPODIS 2004. Lecture Notes in Computer Science, vol 3544. Springer, Berlin, Heidelberg.P.186-196. doi:10.1007/11516798_14

6. 12306 China Railway. URL:https://clck.ru/WDAz8

7. The Open Graph Viz Platform (Release 0.9.2/ 26 September 2017). URL:https://clck.ru/WDBBn

УДК 004.512.2

ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ РАСЧЕТА ЗАВИСИМОСТИ ПОДАЧИ ДАВЛЕНИЯ ГАЗА ОТ ВРЕМЕНИ ПРИ СВЕРХПЛАСТИЧЕСКОЙ ФОРМОВКЕ

SOFTWARE COMPLEX FOR CALCULATING THE DEPENDENCE OF GAS SUPPLY PRESSURE ON TIME IN SUPERPLASTIC FORMING

[1]Гумерова К.Р., [1]Тулупова О.П., [1]Ганиева В.Р., [2]Круглов А.А., [1]Еникеев Ф.У.,
[1]Уфимский государственный нефтяной технический университет,
ул. Космонавтов, 1, г. Уфа, Республика Башкортостан, 450064, Россия
[2]Институт проблем сверхпластичности металлов РАН,
Уфа, Российская Федерация

K.R. Gumerova[1], O.P. Tulupova[1], V.R. Ganieva[1], A.A. Kruglov[2], F.U. Enikeev[1],
[1]Ufa State Petroleum Technological University,
Kosmonavtov Str., 1, Ufa, Republic of Bashkortostan, 450064, Russia
[2]Institute for Metals Superplasticity Problems RAS,
Ufa, Russian Federation

e-mail: kas.kasper90@gmail.com

Аннотация. В данной работе описывается разработка программного комплекса для расчета зависимости подачи давления газа от времени при сверхпластической формовке.

Интерес к процессу сверхпластической формовки в научной сфере и производстве вызван тем, что данный процесс позволяет получить детали сложной формы из труднодеформируемых сплавов, например, на основе железа, титана, магния и т.д.

Поскольку в процессе сверхпластической формовки под воздействием давления газа возможно разрушение формуемой детали, необходимо обеспечить протекание процесса с постоянной скоростью деформации. Для этого следует подавать величину

давления в зависимости от времени формовки. В связи с этим, вычисление зависимости величины подачи давления от времени формовки является актуальной задачей, требующей множественные вычисления.

Отсюда, целью данной работы является расчет зависимости величины давления газа от времени формовки для проведения технологического эксперимента сверхпластической формовки листовой заготовки в цилиндрическую матрицу.

Для автоматизации расчетов был разработан программный комплекс, который реализует вычисления по выбранной методике идентификации материальных констант m, K входящих в стандартную двухконстантную модель сверхпластичности с учетом входного радиуса матрицы и учитывающий начальный участок повышения давления газа.

Для проведения численных расчетов по выбранной методике была построена имитационная модель процесса сверхпластической формовки в программе для имитационного моделирования ANSYS. Проведены сопоставления зависимостей, полученных в результате аналитических и численных расчетов с экспериментальными данными.

Программный комплекс позволяет рассчитывать не только зависимость давления газа от времени формовки, но и прочие временные зависимости, строить графики зависимостей, записывать результаты в текстовые файлы.

Практическая значимость результатов работы состоит в возможности применения данного программного комплекса для учебных целей, лабораторных исследований, например, в Институте проблем сверхпластичности металлов Российской академии наук (сокращенное название ИПСМ РАН) в г. Уфе, а также в условиях промышленного производства.

Abstract. This article describes the development of a software complex for calculating the dependence of gas supply pressure on time in superplastic forming.

Interest in the process of superplastic forming in the scientific field and production is caused by the fact that this process allows you to get parts of complex shapes from hard-to-form alloys, for example, based on iron, titanium, magnesium, etc.

Since the superplastic forming process under the influence of gas pressure may destroy the formed part, it is necessary to ensure that the process proceeds at a constant strain rate. To do this, the pressure value should be applied depending on the forming time. In this regard, calculating the dependence of the pressure supply value on the forming time is an urgent task that requires multiple calculations.

Hence, the purpose of this work is to calculate the dependence of the gas pressure value on the time for conducting a technological experiment of superplastic forming of a sheet billet into a cylindrical die.

Software complex was developed that implements calculations using the selected method to automate calculations.

To perform numerical calculations using the chosen method, a simulation model of the superplastic forming process was constructed in the ANSYS finite element modeling software package. The dependencies obtained as a result of analytical and numerical calculations are compared with experimental data.

The software complex allows you to calculate not only the dependence of gas pressure on the molding time, but also other time dependencies, build dependency graphs, and record the results in text files.

The practical significance of the results is the possibility of using this software complex for educational purposes, laboratory research, for example, at the Institute of superplasticity of

metals of the Russian Academy of Sciences (abbreviated as IPSM RAS) in Ufa, as well as in industrial production.

Ключевые слова: программный комплекс, имитационное моделирование, сверхпластичность, цилиндрическая матрица, степенная модель сверхпластичности, материальные константы, скорость деформации, линейно возрастающее давление, входной радиус, временные зависимости.

Keywords: software complex, simulation modelling, superplasticity, cylindrical die, power model, material constants, strain rate, linearly increasing pressure, entry radius, time dependencies.

Главной функцией программного комплекса является расчет зависимости подачи давления газа от времени. Так же программный комплекс рассчитывает и другие временные зависимости. Для выполнения расчетов были выбраны методика учитывающая влияние давления газа на начальном участке времени [1] и методика учитывающая значение входного радиуса цилиндрической матрицы [2]. Поскольку на практике невозможно моментально установить величину давления газа на необходимую для проведения сверхпластической формовки, некоторый промежуток времени, а именно с начала подачи давления газа до достижения им необходимой величины, давление линейно возрастает. Учитывая этот участок времени и изменение величины давления в течении этого времени, можно достичь более точных результатов в расчетах зависимостей различных величин, характеризующих процесс сверхпластической формовки.

Так как данный программный комплекс нацелен на обработку сложных и трудоемких вычислений, перед самой разработкой, необходимо понимать, в каком именно порядке должны производиться вычисления [3]. Для этого была построена структурно-функциональная модель в CASE-средстве BPwin (рисунок 1).

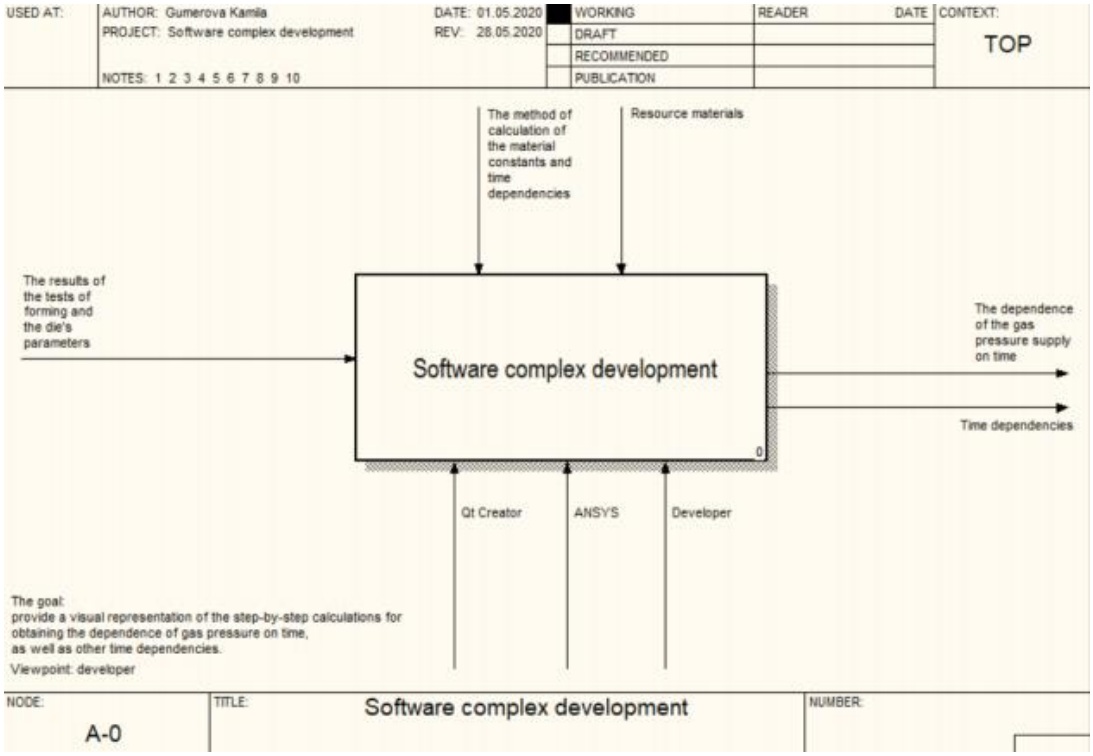

Рисунок 1. Контекстная диаграмма модели

При написании программы была использована среда разработки Qt Creator и язык высокого уровня программирования C++.

Программный комплекс разработан как графический пользовательский интерфейс.

Он состоит из главного окна (рисунок 2), условно поделенного на три «области»:

1. Область ввода входных данных;
2. Область вычисления;
3. Область построения графиков.

Ввод входных данных в программном комплексе может быть осуществлен двумя способами: ручной ввод и считывание с текстового файла.

«Область» для ввода входных данных представляет собой девять полей для ввода данных и соответствующие им текстовые «лэйблы».

Также данная область содержит две кнопки: «Choose file» и «Start calculations».

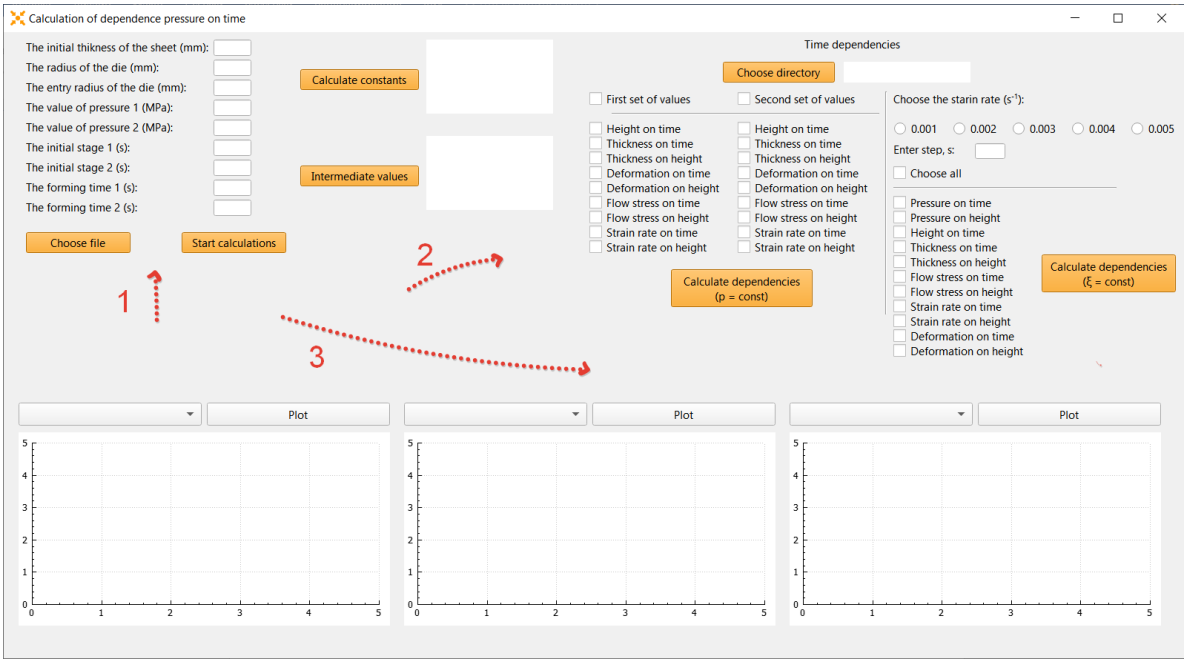

Рисунок 2. Главное окно программного комплекса

Если пользователь хочет ввести значения входных данных вручную, то он вводит в каждое поле соответствующие числа (область ввода данных на рисунке 2) и нажимает на кнопку «Start calculations».

Если у пользователя есть текстовый файл со значениями входных данных, то он нажимает на кнопку «Choose file», выбирает необходимый файл и значения из файла автоматически считываются, записываются в переменные и выводятся в поля ввода для проверки их пользователем на корректность.

После ввода всех данных, пользователю нужно рассчитать значения материальных констант m, K, n и C для дальнейших расчетов [4].

Константы n и C применяются для построения имитационной модели в программе ANSYS [5].

Для вывода результатов вычислений материальных констант необходимо нажать на кнопку «Calculate constants» (рисунок 3).

Далее по нажатию на кнопку «Intermediate values» происходит вычисление промежуточного значения угла между осью симметрии и радиусом сферы (рисунок 3).

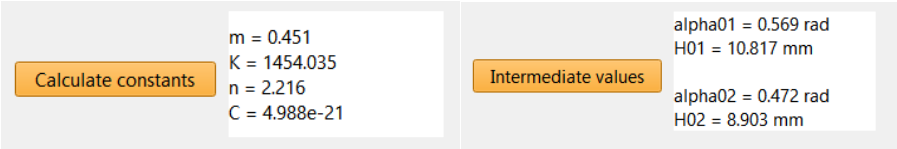

Рисунок 3. Вычисленные материальные константы
и промежуточные значения

Далее необходимо выбрать директорию, куда будут сохраняться все вычисленные результаты.

По нажатию на кнопку «Choose directory» появляется окно, где пользователю предоставляется выбор директории.

Затем пользователю нужно выбрать, какие именно зависимости рассчитать и при каком режиме деформирования: формовка при постоянной подаче давления или формовка при постоянной скорости деформации.

Для выбора той или иной зависимости необходимо отметить соответствующий ей чекбокс. При формовке с постоянной подачей давления доступны девять различных вариантов временных зависимостей (рисунок 4):

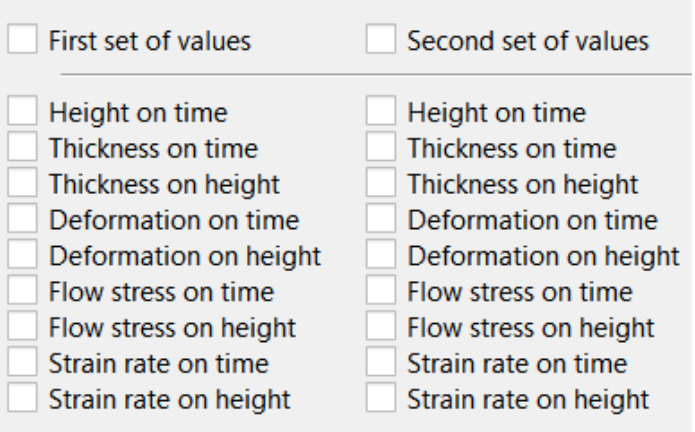

Рисунок 4. Временные зависимости при постоянной подаче давления

При формовке с постоянной скоростью деформации доступны 11 различных вариантов временных зависимостей (рисунок 5):

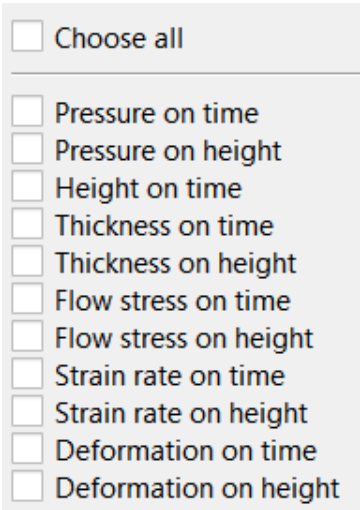

Рисунок 5. Временные зависимости
при постоянной скорости деформации

Для вычисления зависимостей при режиме деформирования с постоянной скоростью деформации нужно выбрать одно из пяти значений скорости деформации, при котором будут рассчитываться остальные значения. Также необходимо ввести шаг расчета, то есть с каким интервалом будет меняться время в зависимостях (рисунок 6).

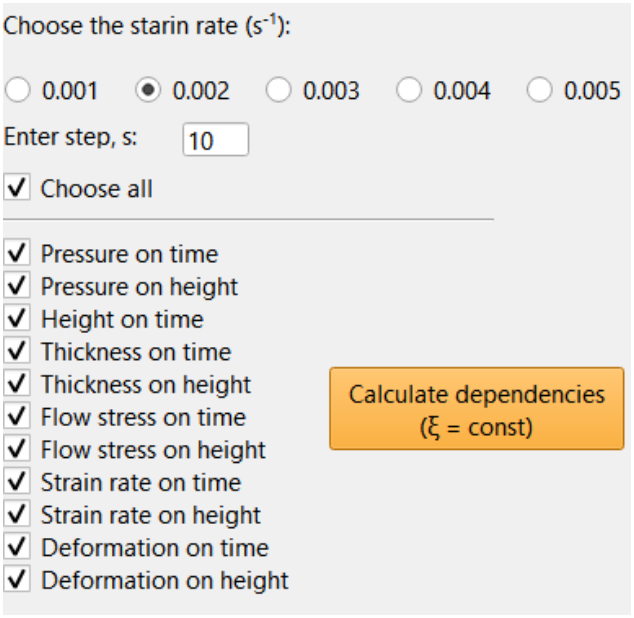

Рисунок 6. Выбор зависимостей при режиме деформирования с постоянной скоростью деформации

После того, как необходимые чекбоксы отмечены, нужно нажать на кнопки «Calculate dependencies (p = const)» и «Calculate dependencies (ξ = const)» для расчета зависимостей. При корректном заполнении всех полей и выбора чекбоксов появляется окно с информационным сообщением о том, что результаты записаны.

Для построения графиков использована библиотека QCustomPlot. После вычислений формируются комбобоксы с названиями вычисленных зависимостей. Пользователь может выбрать любой элемент комбобокса и увидеть соответствующий ему график (рисунки 7-9).

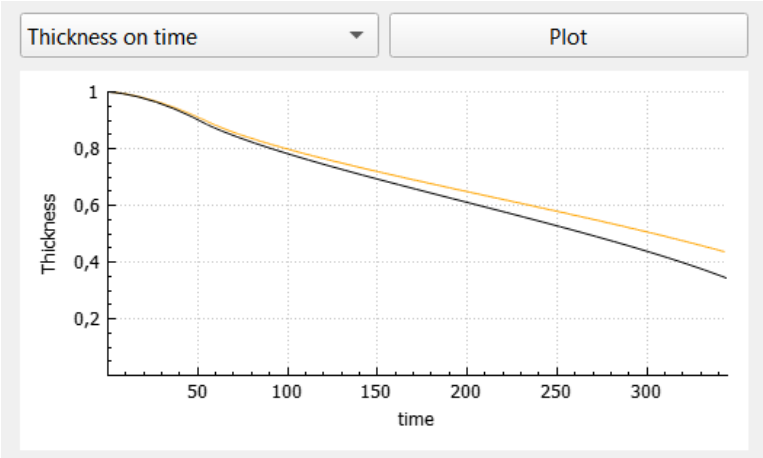

Рисунок 7. График зависимости толщины листа на полюсе купола от времени при постоянной подаче давления

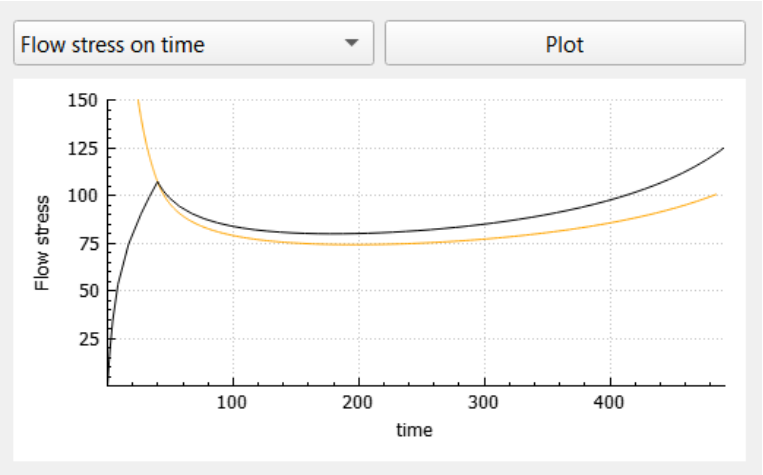

Рисунок 8. График зависимости напряжения течения на полюсе купола от времени при постоянной подаче давления

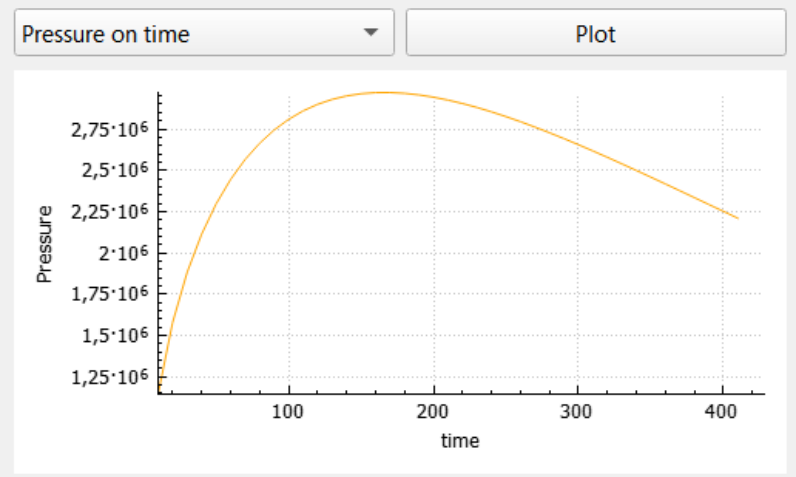

Рисунок 9. График зависимости величины давления от времени при постоянной скорости деформации

Зависимость, рассчитанная программным комплексом, строится оранжевым цветом, зависимость, рассчитанная программой ANSYS, строится черным цветом. На рисунке 9 нет зависимости, построенной черным цветом, так как зависимость величины давления от времени рассчитывается только в программном комплексе.

Результаты имитационного моделирования записываются в текстовые файлы, обрабатываются программным комплексом в таблице и на рисунках 7-9 видна разница между вычислениями программного комплекса и программы ANSYS.

Таблица – Результаты расчета

Давление газа, МПа	Продолжительность формовки, с			Отклонение расчета в ANSYS от расчета в программном комплексе, %	Отклонение расчета в програм-мном комплексе от эксперимен-тальных данных, %	Отклонение расчета в ANSYS от эксперимен-тальных данных, %
	Програм-мный комплекс	ANSYS	Экспери-ментальные данные			
3	360,0	359,6	360,0	0,1	0,0	0,1
2,5	510,0	513,6	510,0	0,7	0,0	0,7

Выводы

Данный программный комплекс, разработанный для расчета временных зависимостей сверхпластической формовки титанового листа в цилиндрическую матрицу с учетом её входного радиуса, учитывает влияние двухэтапной нагрузки инертным газом, что позволяет более точно рассчитать значения выходных данных. Установлено, что учет начального участка подачи давления повышает точность расчетов на 2,5% при давлении 3 МПа и на 1,9% при давлении 2,5 МПа.

Литература

1. Enikeev F.U., Kruglov A.A. An analysis of the superplastic forming of a thin circular diaphragm // Int. J. of Mech. Sci. 1995. Vol. 37. P. 473-483.
2. Tulupova O.P., Ganieva V.R., Kruglov A.A., Enikeev F.U. A new method of identification of constitutive equations according to the results of technological experiments // Letters on materials. 2017. Vol.7, №1. P. 68-71.
3. Данилова Т.В. Учебно-методический комплекс по дисциплине «Проектирование информационных систем». Ростов-на-Дону: НОУ ВПО Институт управления, бизнеса и права, 2014. – С. 137.
4. Backofen W.A., Turner I.R., Avery D.H. Superplasticity in an Al Zn Alloy // Trans. ASM. 1964. Vol. 57. P. 980-990.
5. Vasin R.A., Enikeev F.U., Tokuda M., Safiullin R.V. Mathematical modeling of the superplastic forming of a long rectangular sheet. // Int. J. Non-linear Mechanics. 2003. Vol. 35. P. 799-807.

УДК 004.5

ПРОГРАММНЫЙ ПРОДУКТ ДЛЯ ОПРЕДЕЛЕНИЯ ПОКАЗАТЕЛЕЙ ВЗРЫВООПАСНОСТИ РЕЗЕРВУАРА И ВИЗУАЛИЗАЦИИ ПРОЦЕССА РАБОТЫ ТОВАРНОГО ПАРКА

SOFTWARE FOR DETERMINATION OF TANK EXPLOSION INDICATORS AND VISUALIZATION OF THE PRODUCT PARK OPERATION PROCESS

Киреев И.Р., Барахнина В.Б., Шуваева В.Р.,
Уфимский государственный нефтяной технический университет,
ул. Космонавтов, 1, г. Уфа, Республика Башкортостан, 450064, Россия

I.R. Kireev, V.B. Barakhnina, V.R. Shuvaeva,
Ufa State Petroleum Technological University,
Kosmonavtov Str., 1, Ufa, Republic of Bashkortostan, 450064, Russia

e-mail: verarosental@rambler.ru

Аннотация. На сегодняшний день в России насчитывается парк резервуаров общей ёмкостью около 150 млн. тонн. Из имеющихся на балансе предприятий нефтяной промышленности РФ резервуарных парков 81% находится в состоянии, требующем ремонта и технологического обслуживания различного уровня. Ежегодно увеличивается

количество резервуаров, отработавших свой нормативный срок. Высокий уровень аварийности и производственного травматизма в нефтегазовой отрасли обусловлен низкой эффективностью существующей системы образования и обучения специалистов по промышленной безопасности и охране окружающей среды, а также низким уровнем контроля в сфере охраны труда, защиты окружающей природной среды и ликвидации аварий.

Пути повышения промышленной безопасности товарных парков (диагностика, анализ рисков, мониторинг технического состояния, оценка взрывоопасности резервуаров) наряду с уменьшением потерь углеводородов от испарения и снижением отложений нефти при хранении являются основными направлениями развития резервуаростроения, которое требует современных инновационных решений.

Разработан программный продукт для определения показателей взрывоопасности резервуара и визуализации процесса работы товарного парка, который используется при изучении работы резервуарных парков в процессе обучения. Он предназначен для использования на кафедре «Промышленная безопасность и охрана труда» Уфимского государственного нефтяного технического университета.

Abstract. Today in Russia there is a fleet of tanks with a total capacity of about 150 million tons. Of the tank farms available on the balance sheet of oil industry enterprises of the Russian Federation, 81% are in a state that requires repair and technological maintenance of various levels. The number of reservoirs that have served their standard term is increasing annually. The high level of accidents and industrial injuries in the oil and gas industry is due to the low efficiency of the existing education and training system for industrial safety and environmental protection specialists, as well as a low level of control in the field of labor protection, environmental protection and emergency response.

Ways to improve the industrial safety of commodity parks (diagnostics, risk analysis, monitoring of the technical condition, assessment of the explosiveness of tanks), along with reducing hydrocarbon losses from evaporation and reducing oil deposits during storage, are the main directions for the development of tank construction, which requires modern innovative solutions.

A software product has been developed for determining the indicators of the explosiveness of the tank and visualizing the process of the operation of the commodity park, it is used in the study of the operation of the tank farms in the learning process. It is intended for use at the Department of Industrial Safety and Labor Protection of the Ufa State Petroleum Technical University.

Ключевые слова: промышленная безопасность, резервуар, товарный. парк, программный продукт, показатели взрывоопасности, визуализация.

Keywords: industrial safety, tank, commodity park, software product, explosion hazard indicators, visualization.

Резервуаростроение в РФ связано с историей развития нефтяной промышленности, а именно с ростом объемов добычи и переработки нефти (рисунок 1) [4-8]. В настоящее время разработано множество видов резервуаров, а также систем автоматизации резервуарного парка, защиты резервуаров от коррозии, статического и атмосферного электричества.

Применяются также современные системы пожаротушения, водяного охлаждения, очистки и др.

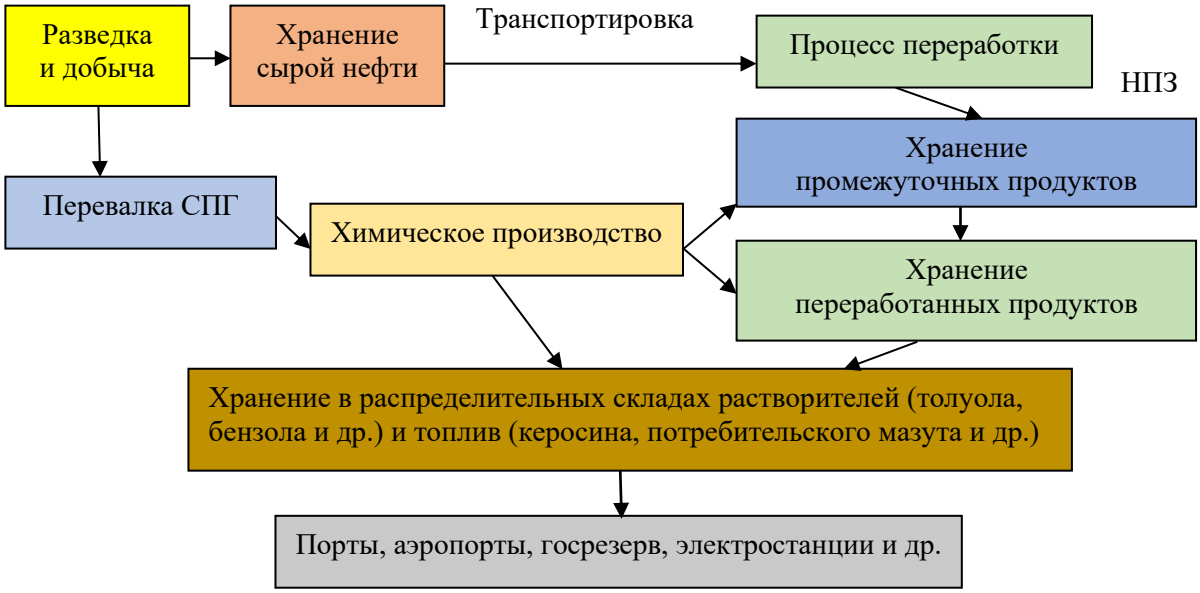

Рисунок 1. Области применения резервуаров в ТЭК

Особое внимание уделяется промышленной безопасности резервуарных парков (группе резервуаров, сосредоточенных в одном месте).

Резервуарные парки, служащие для приема и хранения нефти, прошедшей установку обезвоживания и обессоливания, называются товарными парками [1, 2].

Разработан программный продукт (ПП) для определения показателей взрывоопасности резервуара и визуализации процесса работы товарного парка, используется при изучении работы резервуарных парков в процессе обучения. Он предназначен для использования на кафедре «Промышленная безопасность и охрана труда» УГНТУ [3].

Товарный парк укомплектован следующими резервуарами:

1. вертикальными стальными цилиндрическими.
   – со стационарной крышей (РВС),
   – с понтоном (РВСП),
   – с плавающей крышей (РВСПК);
2. горизонтальными стальными цилиндрическими (РГС).

Они используются для постоянного выполнения технлогических операций, длительного хранения, смещения и отстаивания.

Разработка предоставляет следующие возможности:

– расчет показателей давления и температуры;

– отслеживание уровня вещества в резервуаре [4, 5].

Пользователь должен иметь опыт работы:

– с ОС MS Windows (XP/Vista/7/8/10),

– навык работы с програмным обеспечением,

– иметь основное понимание физических величин.

ПП предназначен для использования в процессе обучения при изучении обучающимися процесса хранения нефти и нефтепродуктов.

Условие применения доступно для всех обучающихся, присутствующих на занятии, в котором применяется ПП. Последний не имеет дистрибутива.

Перед началом работы с ПП на рабочем месте пользователя необходимо выполнить следующие действия:

– скопировать папку программы на компьютер из основного;

– открыть папку;
– найти и запустить исполняемый файлEtESotT.exe.

Ниже приведено описание пользовательских операций для выполнения каждой из задач.

Операция 1: реализация рассчетов.

Основные действия в требуемой последовательности:

1. Открыть окно «Расчеты» нажав кнопку «Расчеты» в главном окне (рисунок 2).
2. В окне «Расчеты» (рисунок 3) заполнить поля с соответсвующими им единицам измерения.

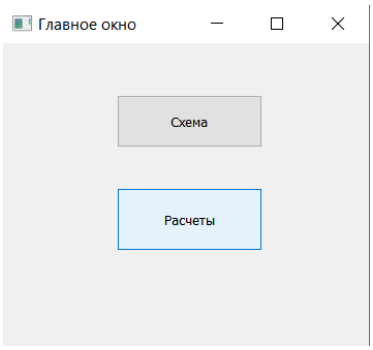

Рисунок 2. Главное окно

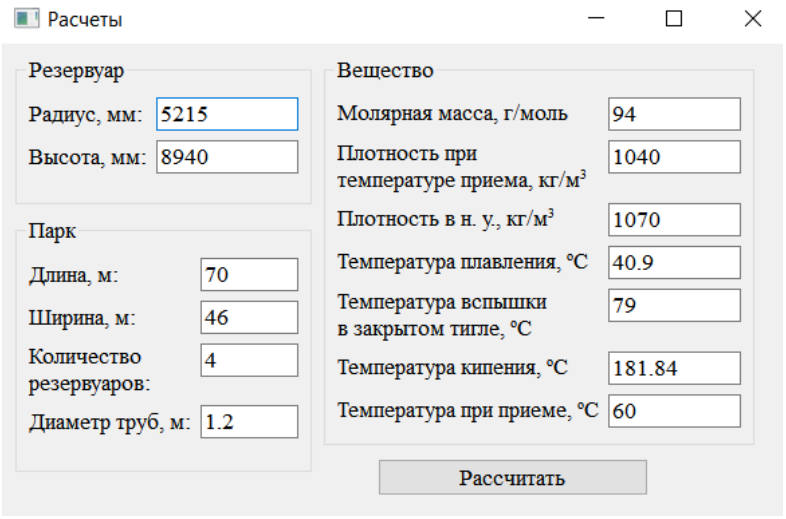

Рисунок 3. Окно «Расчеты»

Для исключения аварийных ситуаций поля заполняют корректными данными:
– радиус (натуральные числа, в миллиметрах);
– высота (натуральные числа, в миллиметрах);
– длина (натуральные числа, в метрах);
– ширина (натуральные числа, в метрах);
– количество резервуаров (натуральные числа, количество штук);
– диаметр труб (положительные рациональные числа, в метрах);
– молярная масса (положительные рациональные числа, в грамм на моль);
– температура при приеме (рациональные числа, в градусах Цельсия);
– температура плавления (рациональные числа, в градусах Цельсия);
– температура вспышки (рациональные числа, в градусах Цельсия);
– температура кипения (рациональные числа, в градусах Цельсия);
– плотность при температуре приема (положительные рациональные числа, в килограмм на кубический метр).

Рациональные числа записывают в виде десятичной дроби и целая часть в данном случае, отделяется точкой, а не запятой.

В этом же окне нажать на кнопку «Рассчитать».

Заключительные действия: закрыть окно.

Операция 2: управление визуализированным процессом.

Основные действия в требуемой последовательности:

1. Открыть окно «Схема» нажав кнопку «Схема» на главном окне (рисунок 4).
2. В окне «Схема» нажать на кнопку «Заполнить». Начинается процесс заполнения резервуаров, который представлен на рисунке 5.

Значение давления растет, исходя из количества вещества.

Процесс заполнения резервуаров заканчивается автоматически при наполнении, или его можно остановить заранее кнопкой «Остановка заполнения».

После этого можно начинать управлять значениями температуры и давления с помощью дисков, которые зависят друг от друга.

3. Измененное значение температуры представлено на рисунке 5. Взрывобезопасность обеспечивается тем, что значения температуры и давления можно изменять только в безопасном диапазоне, поэтому при предельных значениях формируется предупреждающее сообщение (рисунок 6).

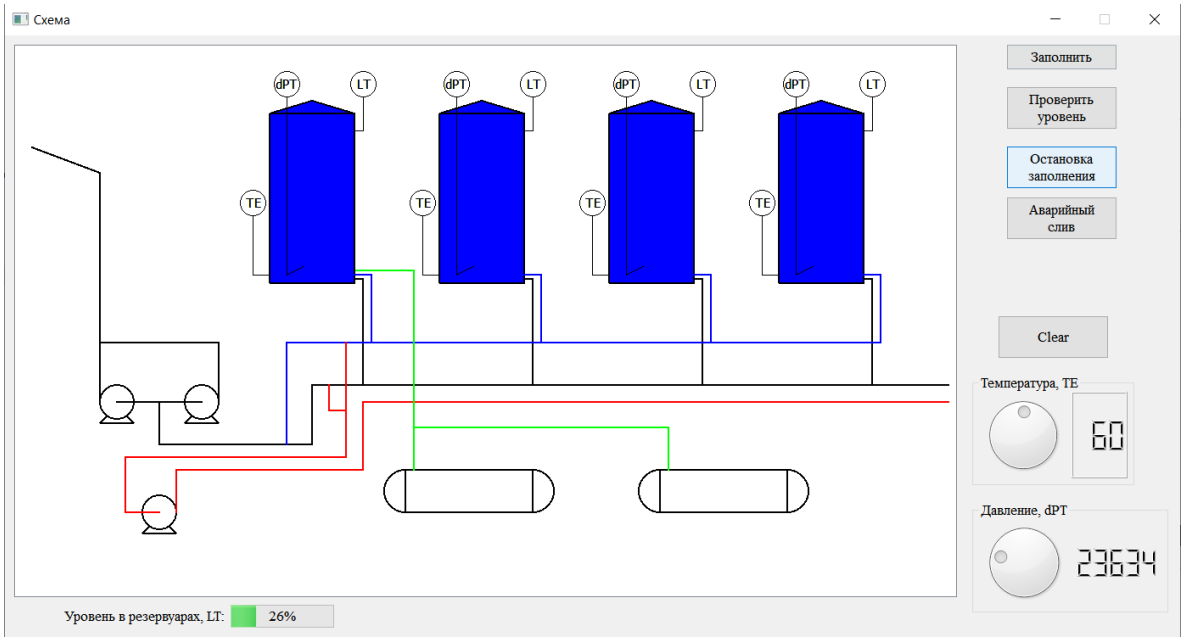

Рисунок 4. Процесс заполнения резервуаров

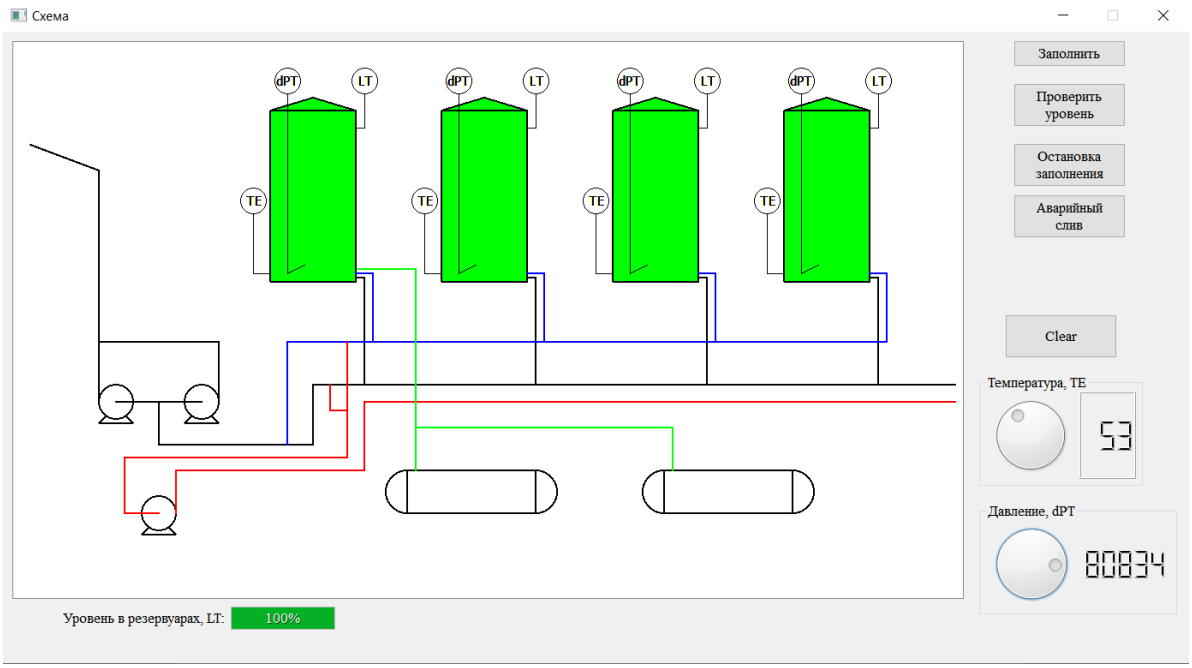

Рисунок 5. Измененное значения температуры

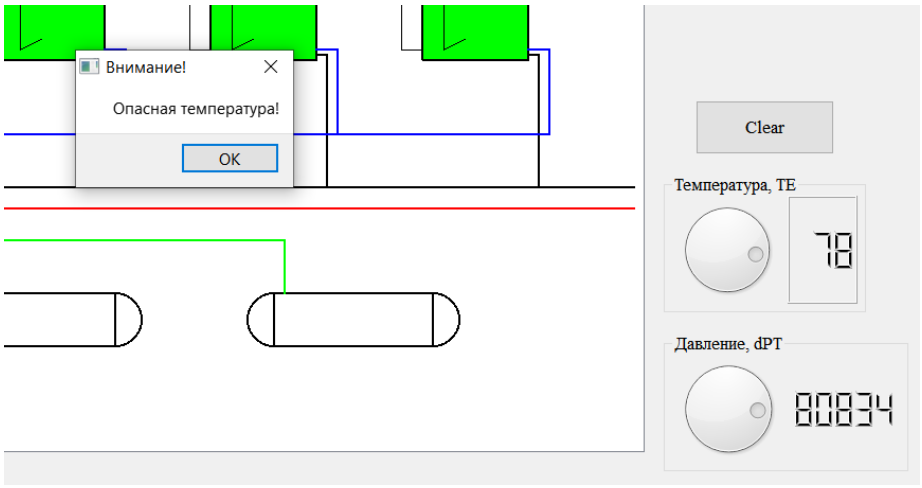

Рисунок 6. Предупреждающее сообщение

4. Кнопка «Проверить уровень» показывает количество вещества в резервуарах, «Аварийный слив» приводит к опустошению резервуаров, а «Clear» переводит окно в исходное положение. Заключительные действия: закрыть текущее и главные окна.

Выводы

Разработанный программный продукт определения показателей взрывоопасности резервуара и визуализации процесса работы товарного парка позволит повысить уровень обучения специалистов по охране труда и промышленной безопасности.

Литература

1. Галиахметова Н.А., Киреев И.Р., Шарафиев Р.Г., Абдрахманов Н.Х., Барахнина В.Б. Мероприятия (условия) по обеспечению взрывобезопасности при перевозке железнодорожными цистернами углеводородных газов. Научный журнал «НоваИнфо», 2019, №100-1. С. 29-31. URL: https://novainfo.ru/article/16483.

2. Киреев И.Р., Бисенгулова Э.М., Барахнина В.Б. Новый способ защиты от коррозии резервуаров для хранения нефти и нефтепродуктов. Тезисы докладов XIV Международной учебно-научно-практической конференции «Трубопроводный транспорт – 2019», Уфа: Издательство УГНТУ, 2019. С. 247-248.

3. Киреев И.Р., Латыпова Г.И., Маковичук К.И., Барахнина В.Б. Мероприятия по защите резервуаров для хранения нефти и нефтепродуктов от коррозии. Сборник материалов Внутривузовской научно-практической конференции «Инновационные технологии в промышленности: образование, наука и производство», 16 декабря 2016 г., Т. 1, г. Стерлитамак, Уфа: Изд-во «Нефтегазовое дело», 2016. С. 225-228.

4. Киреев И.Р., Шарафиев Р.Г., Идрисова К.Р., Филиппова А.Г., Барахнина В.Б. Новая автоматизированная система контроля технологических параметров резервуарного парка. Материалы международной научно-практической конференции «Информационные технологии. Проблемы и решения», Уфа: Изд-во УГНТУ, 2019. С. 44-49.

5. Киреев, И.Р. Теория горения и взрыва / И.Р. Киреев, В.Б. Барахнина, А.А. Гилязов / Учеб. пособие. Уфа: Изд-во УГНТУ, 2008. – 90 с.

6. Латыпова Г.И., Киреев И.Р., Барахнина В.Б. Современные полимерные материалы для защиты стальных резервуаров для хранения нефти и нефтепродуктов от коррозии. Экологический вестник России, №3, 2017. С. 18-22.

7. Сафонов, С. К. Методы расчета показателей пожароопасности газов и жидкостей: учебно-метод. пособие / сост.: С.К. Сафонов. Ульяновск: Изд-во УВАУ ГА, 2005. – 42 с.

8. Тагирова К.Б., Шарафутдинова Г.М., Барахнина В.Б. Байесовская модель риска для сценария разрушения резервуара, оборудованного паровыми клапанами. Материалы II Международной научно-практической конференции «Актуальные проблемы и тенденции развития техносферной безопасности в нефтегазовой отрасли», Уфа: Изд-во УГНТУ, 2019. С. 117-120.

УДК 004.621.791.052:539.013.3:001.891.57

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ДЛЯ ОЦЕНКИ КОЭФФИЦИЕНТОВ КОНЦЕНТРАЦИИ НАПРЯЖЕНИЙ В СВАРНЫХ ТАВРОВЫХ СОЕДИНЕНИЯХ

MATHEMATICAL MODEL FOR ASSESSING STRESS CONCENTRATION FACTORS IN T-SHAPED WELDED JOINTS

[1, 2]Ерофеев В.В., [3]Игнатьев А.Г., [2]Олейник Н.И., [1]Шарафиев Р.Г.,
[2]Кульневич В.Б., [2]Щепеткин В.В.
[1]Уфимский государственный нефтяной технический университет,
ул. Космонавтов, 1, г. Уфа, Республика Башкортостан, 450064, Россия
[2]ФГБОУ ВО Южно-Уральский государственный аграрный университет,
г. Троицк, Российская Федерация,
[3]ФГБОУ ВО Южно-Уральский государственный университет,
г. Челябинск, Российская Федерация

V.V. Erofeev[1, 2], A.G. Ignatiev[3], N.I. Oleinik[2], R.G. Sharafiev[1],
V.B. Kulnevich[2], V.V. Shchepetkin[2],
[1]Ufa State Petroleum Technological University,
Kosmonavtov Str., 1, Ufa, Republic of Bashkortostan, 450064, Russia
[2]FSBEI HE «South Ural State Agrarian University»,
Troitsk, Russian Federation,
[3]FSAEI HE «South Ural State University»,
Chelyabinsk, Russian Federation

e-mail: ervv52@ mail.ru

Аннотация. Представлена математическая модель концентрации напряжений в тавровых сварных соединениях при неполном проплавлении стенки. Эта модель описывает особенности напряженного состояния в окрестности вершины концентратора с позиции механизма и критериев механики разрушения. На основе модели предложен новый расчетный метод оценки концентрации напряжений в тавровых сварных соединениях. В технологии изготовления конструкций предполагается применение неравнокатетных угловых швов. Эта технология обеспечивает снижение эффекта концентрации напряжений в рассматриваемых тавровых соединениях. Предложенные решения могут быть использованы на стадии конструктивно-технологического проектирования, изготовления и ремонта сварных металлоконструкций. Они позволяют

проводить оптимизацию конструктивно-геометрических параметров сварных соединений.

Abstract. A mathematical model for stress concentration in T-shaped welded joints with incomplete wall penetration is presented. This model describes the stress state features in the concentrator vertex vicinity in terms of the fracture mechanic mechanism and criteria. Based on the model, a new computational method for assessing the stress concentration in T-welded joints is proposed. In the manufacturing structures technology, the perform T-welded joints with unequal cathetus dimensions seams is assumed. This technology reduces the effect of stress concentration in the considered T-joints. The proposed solutions can be used at the structural and technological design stage for welded metal structures manufacture and repair. This solutions allow optimization for the structural and geometric parameters of welded joints.

Ключевые слова: металлоконструкции, тавровые сварные соединения, неравнокатетные швы, концентрация напряжений, математическая модель.

Keywords: steel structures, T-welded joints, unequal cathetus dimensions seams, stress concentration, mathematical model.

Основными видами сварных соединений, применяемых для изготовления металлоконструкций, являются нахлесточные и тавровые соединения, выполняемые угловыми швами (до 70% от общего количества). Эффект концентрации напряжений в таких соединениях в наиболее полной мере проявляется в месте перехода от шва к основному металла (рисунок 1, *а*, *б*, точки *A*), а также в случае неполного проплавления вертикальной стенки – в вершине непровара (рисунок 1, *в*, точка *C*).

Для оценки коэффициента концентрации напряжений в месте перехода от шва к основному металла (точках *A*) нахлесточных и тавровых соединений K_{σ}^{A} можно воспользоваться соотношениями, полученными в работе [1]. Для тавровых соединений, выполненных с неполным проплавлением вертикальной стенки, наблюдается непровар *C*-*C* с радиусом ρ^{C} в его вершине (рисунок 1, *в*). Ввиду сложностей математического характера до сих пор отсутствуют расчетные соотношения для определения коэффициентов концентрации напряжений в вершине непровара K_{σ}^{C}, и последние, как правило, определяются экспериментально [2 и др.].

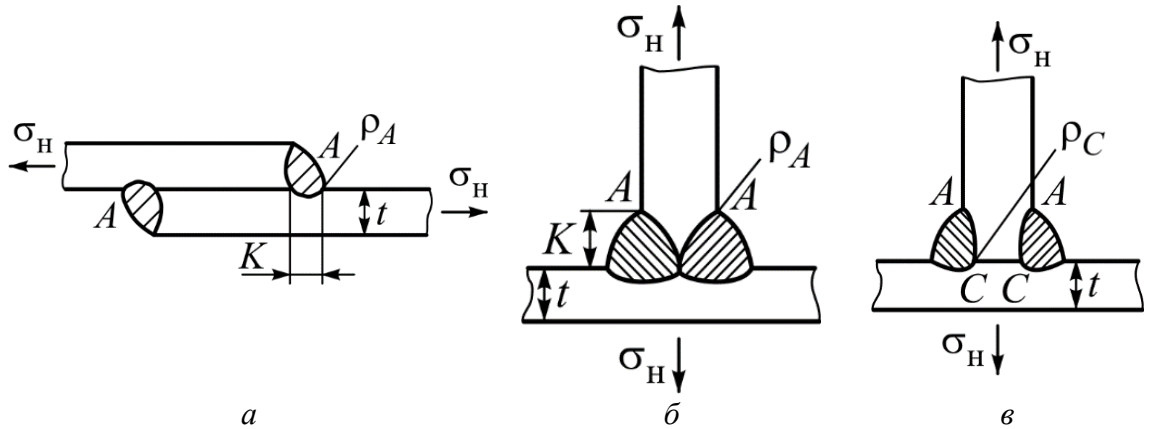

Рисунок 1. Сварные соединения с угловыми швами: *а* – нахлесточное, *б, в* – тавровое с полным проплавлением и непроваром полки

В настоящее время благодаря интенсивному развитию аппарата механики разрушения решен достаточно широкий класс задач для конструкций со сложной геометрической формой и имеющих в своем составе концентраторы типа трещин.

Анализ расчетных соотношений, полученных в работах [3, 4], позволяет предположить, что они могут быть использованы в качестве базовых для определения коэффициентов концентрации напряжений K_σ без дополнительного решения прикладных математических задач.

Остановимся на рассмотрении одного из подходов определения коэффициентов концентрации напряжений K_σ^C в сварных тавровых соединениях, который является основой для создания математической модели для оценки K_σ^C, базирующейся на классической задаче растяжения бесконечной пластины, ослабленной эллиптическим концентратором (рисунок 2, *а*).

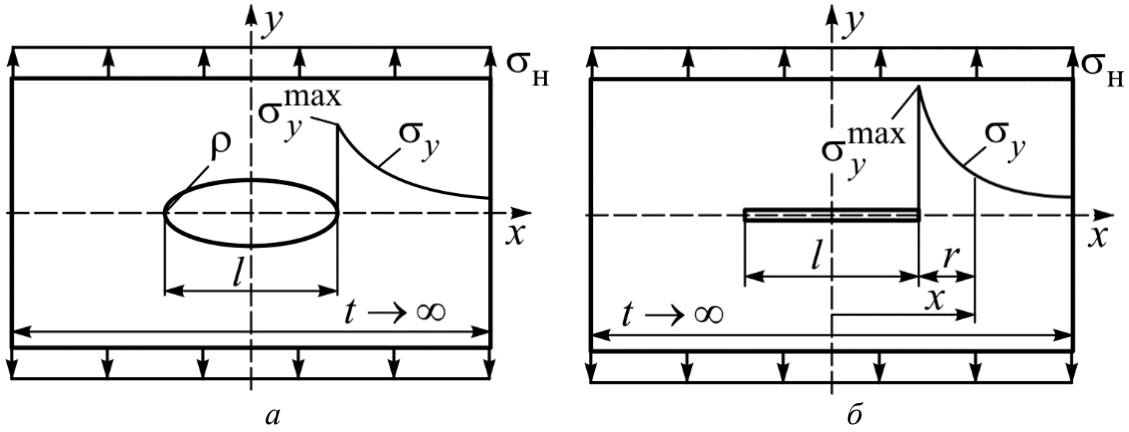

Рисунок 2. Пластина, ослабленная эллиптическим отверстием (*а*)
и модель трещины Вестергаарда в бесконечной пластине (*б*)

Исходя из анализа напряженного состояния данной пластины, выполненного в работе [5], были получены аналитические выражения, описывающие характер распределения главных напряжений $\sigma_y(x)$ по центральному ослабленному сечению пластины (вдоль оси x), на основании которых было предложено следующее соотношение для оценки величины K_σ в окрестности вершины эллипса:

$$K_\sigma = \frac{\sigma_y^{\max}}{\sigma_н} = 1 + 2\sqrt{\frac{l}{2\rho}}, \qquad (1)$$

где l, ρ – горизонтальная ось эллипса и радиус в его вершине.

Нетрудно заметить, что при $\chi = 2\rho/l = 1$ эллипс трансформируется в круг, для которого в условиях растяжения пластины $K_\sigma = 3$, при уменьшении радиуса в вершине эллипса в пределе до $\chi = 2\rho/l \to 0$ эллиптическое отверстие превращается в трещину длиной l и с радиусом в вершине ρ (рисунок 2, *б*).

Позднее в работе [6] была рассмотрена задача об оценке напряжений около острой трещины в виде математического надреза нулевой толщины ($2\rho/l = 0$). В частности, было получено выражение для описания функции распределения напряжений $\sigma_y(x)$ вдоль оси x (см. рисунок 2, *б*):

$$\sigma_y = \frac{\sigma_{\text{н}}\left(\frac{l}{2}+r\right)}{\sqrt{4r}}\left(1-\frac{r}{2l}\right), \qquad (2)$$

где $r = x - l/2$ – расстояние от вершины трещины до рассматриваемой точки на оси *x*.

Приведенное соотношение (2) представлено двумя начальными членами ряда разложения функции напряжений.

Позднее решение (2) было положено в основу математического аппарата при рассмотрении предельно-равновесного состояния тел с трещинами [5, 6 и др.]. При этом ограничивались рассмотрением только первого члена ряда, что справедливо при $r << l$. Последнее привело к существенному упрощению исходного соотношения:

$$\sigma_y = \sigma_{\text{н}}\sqrt{\frac{l}{4r}}, \qquad (3)$$

которое было сведено к классическому виду, используемому в настоящее время при анализе напряженного состояния в окрестности вершины математического надреза нулевой толщины ($2\rho/l = 0$), расположенного в бесконечной пластине, на базе критериев механики разрушения:

$$\sigma_y = \frac{K_{\text{I}}}{\sqrt{2\pi r}}, \qquad (4)$$

где $K_{\text{I}} = \sigma_{\text{н}}\sqrt{\frac{\pi}{2}l}$ – коэффициент интенсивности напряжений [4].

При оценке напряженного и предельно-равновесного состояний тел с трещинами необходим учет многообразия факторов – толщины *t*, ориентации трещины по отношению к вектору растягивающих напряжений $\sigma_{\text{н}}$, конечности радиуса в вершине трещины ρ и т.п.

Для этого в исходное соотношение (4) были введены поправки на величину K_{I}, которые определялись исходя из решения соответствующих задач [3, 4, 7 и др.]:

$$\sigma_y = \frac{K_{\text{I}}}{\sqrt{2\pi r}} \cdot f_t \cdot f_\gamma \cdot f_\rho \ldots, \qquad (5)$$

где f_t – поправка на толщину *t*, f_γ – на ориентацию трещины, f_ρ – на конечность радиуса ρ в вершине трещины и т.п.,

$$f_t = \sqrt{\sec\left(\frac{\pi}{2}\frac{l}{t}\right)}, \qquad (6)$$

$$f_\gamma = \cos^2 \gamma, \tag{7}$$

$$f_\rho = \left[1 - \frac{(\pi - 2)\left(2 - \sqrt{2}\right)}{\pi} \chi - \frac{(\pi - 1)(\pi - 2)\left(2 - \sqrt{2}\right)}{\pi} \chi^2 \right]^{1/4}. \tag{8}$$

Например, используя поправку (8) из соотношения (5) можно получить следующее выражение для определения K_σ для бесконечной пластины, ослабленной концентратором с радиусом вершине ρ:

$$K_\sigma = \sqrt{\frac{l}{4r}} f_\rho. \tag{9}$$

Путем несложных математических преобразований нетрудно показать, что полное соответствие значений K_σ, полученных на основании решений [5] и [6], может быть обеспечено при значениях параметра r_{min}, отвечающих условию

$$r_{min} = \rho \cdot f(\chi), \tag{10}$$

где $$f(\chi) = \frac{1}{2} f_\rho^2 \left(\frac{1}{\sqrt{\chi} + 2} \right)^2. \tag{11}$$

Как показал сравнительный анализ, условие (10) нивелирует погрешность базовых соотношений (3) и (4), возникшую в результате исключения второго члена ряда разложения функции напряжений при рассмотрении концентраторов с конечным радиусом в вершине ρ.

В этом нетрудно убедиться путем сравнения значений напряжений σ_y, полученных из соотношений (2) и (3), при которых максимальные расхождения в результатах не превышают 0 ... 2,5%.

Таким образом, окончательное выражение для определения K_σ в пластине, ослабленной концентратором с радиусом ρ, имеет вид:

$$K_\sigma = 1 + 2\sqrt{\frac{l}{2\rho}} \cdot f_t \cdot f_\gamma. \tag{12}$$

В качестве примера использования данного подхода рассмотрим процедуру определения коэффициента K_σ^C в тавровых соединениях, выполненных неравнокатетными угловыми швами с неполным проплавлением стенки.

В работе [3] на основании рассмотрения предельно-равновесного состояния таврового соединения (рисунок 3) получены расчетные соотношения по определению поправок f_t и f_γ, а также поправки f_λ на смешанный тип нагружения в окрестности вершины концентратора.

В частности, учитывалось изменение направления силового потока вблизи вершины концентратора, характеризующееся углом γ (см. рисунок 3, *а*), связанное с возникновением смешанного типа нагружения, описывающегося двумя коэффициентами интенсивности напряжений K_{I} (нормальный отрыв) и K_{II} (поперечный сдвиг):

$$\gamma = \operatorname{arctg}\lambda. \tag{13}$$

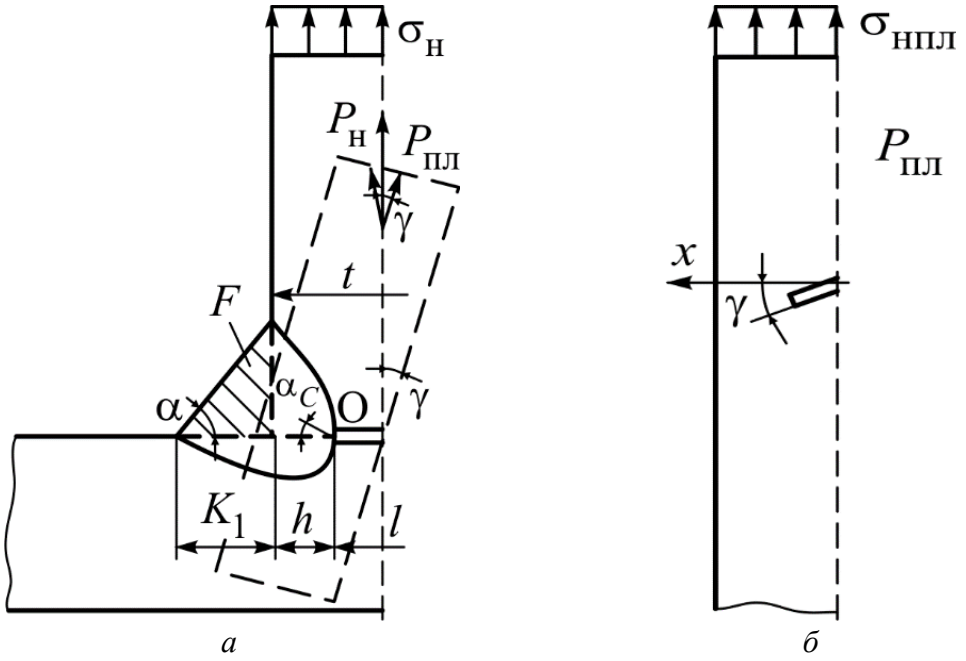

Рисунок 3. Расчетная схема таврового соединения для оценки коэффициента концентрации напряжений K_{σ}^{C}

Также учитывали, что направление старта трещины от вершины непровара (точки *C*) в общем случае не является его продолжением и образует с плоскостью расположения непровара угол α_C, величина которого может быть определена из соотношения (14) по значению параметра $\lambda = K_{\text{II}} / K_{\text{I}}$ [4] или из соотношения (15) по известному углу наклона лобовой грани шва *а* [3]:

$$\alpha_C = 2\operatorname{arctg}\left[\frac{1-\sqrt{1+8\lambda^2}}{4\lambda}\right], \tag{14}$$

$$\alpha_C = \frac{\pi}{4} - \frac{\alpha}{2}. \tag{15}$$

Данный тип нагружения реализуется, например, в пластинах, ослабленных наклонным концентратором.

Используя соотношения (14) и (15), были установлены зависимости $\lambda = \lambda(\alpha)$ и $\gamma = \gamma(\alpha)$, характеризующие изменение параметра λ и направления силового потока в окрестности вершины непровара γ от величины наклона углового шва α:

$$\lambda = \mathrm{tg}\left(\frac{\pi}{8} - \frac{\alpha}{4}\right), \tag{16}$$

$$\gamma = \frac{\pi}{8} - \frac{\alpha}{4}. \tag{17}$$

При выводе основных расчетных соотношений учитывали также зависимость относительного размера концентратора *l*/*t* от относительной глубины проплавления стенки соединения *h*/*t*:

$$\frac{l}{t} = 1 - 2\frac{h}{t}. \tag{18}$$

Таким образом, окончательное выражение для определения коэффициента концентрации K_σ^C имеет вид:

$$K_\sigma^C = \left(1 + 2\sqrt{\frac{1 - 2h/t}{2\rho/t}}\right) \cdot f_t \cdot f_\lambda \cdot f_\gamma, \tag{19}$$

$$f_\lambda = 4\sqrt{2}\lambda^3 \frac{1 + 3\sqrt{1 + 8\lambda^2}}{\left(12\lambda^2 + 1 - \sqrt{1 + 8\lambda^2}\right)^{3/2}}, \tag{20}$$

$$f_\gamma = \cos^2\gamma, \tag{21}$$

$$f_t = \frac{\sqrt{\sec\left[\frac{\pi}{2}\frac{l}{t}\frac{1}{\Phi}\right]}}{\Phi}\left(1 + \lambda^2\right), \tag{22}$$

где $\Phi = 1 + 2\psi\lambda$.

Как было показано в работе [3], для реальных значений параметров тавровых соединений величина λ находится в пределах [0…0,2], произведение поправочных функций $f_\lambda f_\gamma$ находится в интервале значений [1,0…1,015], т.е. практически равно 1,0. Последнее позволяет исключить из полученного соотношения (19) для определения K_σ^C данное произведение поправочных функций.

С учетом несложных преобразований после подстановки соотношений (16) и (18) в выражение (19) имеем:

$$K_{\sigma}^{C}=\left(1+2\sqrt{\frac{1-2\frac{h}{t}}{2\frac{\rho}{t}}}\right)\frac{\sqrt{\sec\left[\frac{\pi}{2}\left(1-2\frac{h}{t}\right)\left(1+2\psi\mathrm{tg}\left(\frac{\pi}{8}-\frac{\alpha}{4}\right)\right)^{-1}\right]}}{1+2\psi\mathrm{tg}\left(\frac{\pi}{8}-\frac{\alpha}{4}\right)}\left(1+tg^{2}\left(\frac{\pi}{8}-\frac{\alpha}{4}\right)\right), \quad (23)$$

Для определения K_{σ}^{C} по соотношению (23) необходимо знать глубину проплавления вертикальной стенки таврового соединения *h* и величину радиуса в вершине непровара ρ. Как было показано в работе [8], глубина проплавления вертикальной стенки таврового соединения *h* зависит от способа дуговой сварки и угла наклона углового шва α:

$$h=K\left[\left(\frac{\beta_{45}}{0,7}-1\right)+\frac{\mathrm{tg}^{2}\alpha-1}{2\sqrt{\mathrm{tg}\alpha}}\right], \quad (24)$$

где $K=K_{1}\sqrt{\mathrm{tg}\alpha}$ при условии обеспечения постоянной площади наплавленного металла *F*.

В соответствии с рекомендациями работы [9] для сварных соединений, выполненных угловыми швами с применением различных способов сварки, следует принимать:

– β_{45} = 0,7 – для ручной дуговой сварки (РДС), многопроходной автоматической (АДС) и механизированной (МДС) сварки;
– β_{45} = 0,8 – для двух- и трехпроходной МДС;
– β_{45} = 0,9 – для однопроходной МДС и двух- и трехпроходной АДС;
– β_{45} = 1,1 – для однопроходной АДС.

Величина ρ^{C} в соответствии с результатами работы [10] может быть определена по параметру шероховатости стыковочных поверхностей R_z и в первом приближении равна $\rho^{C}=R_z$.

Использование соотношения (23) для оценки коэффициента концентрации K_{σ}^{C} в сварных тавровых соединениях возможно лишь при условии, когда не обеспечивается полное проплавление стенки: $h<t/2$. При условии $h=t/2$ (l = 0, λ = 0, Φ = 1) в точке соприкосновения угловых швов $K_{\sigma}^{C}=1$ и очаг концентрации напряжений перемещается в точку перехода от углового шва к основному металлу стенки (в точку *A*), в которой величина K_{σ}^{A} может быть определена по соотношению, приведенному в работе [3].

Литература

1. Турмов Г.П. Определение коэффициентов концентрации напряжений в сварных соединениях // Автоматическая сварка. 1976. №10. С. 14-17.

2. Bakshi O.A., Zaitsev N.L., Shron A.B. Effect of the geometry of fillet welds on stress concentration and stress gradients in tee joints // Сварочное производство. 1982. Т. 8. С. 3-5.

3. Когут Н.С., Шахматов М.В., Ерофеев В.В. Несущая способность сварных соединений. Львов: Свит, 1991. 183 с.

4. Черепанов Г.П. Механика хрупкого разрушения. М.: Наука, 1974. 640 с.

5. Inglis C.E. Trans. Instn. Nav. Archit., LV.1< 219 (1913).

6. Westergaard, H.M.J. appl. Mach., A 49 (June, 1939).

7. Ерофеев В.В., Шахматов М.В., Коваленко В.В. Об особенностях предельно равновесного состояния сварных соединений с дефектами конечного радиуса // Мат-лы XIX науч.-техн. конф. сварщиков Урала. Челябинск: ЦНТИ, 2000. С.102-108.

8. Повышение несущей способности вертикальных стальных резервуаров объектов АПК путем рационального проектирования и изготовления сварных соединений уторных узлов / В.В. Ерофеев [и. др.] // АПК России. 2020. Т. 27. №3.

9. Николаев Г.А., Винокуров В.А, Сварные конструкции. Расчет и проектирование. М.: Высшая школа, 1990. 447 с.

10. Ерофеев В.В., Олейник Н.И., Щепеткин В.В. О влиянии качества подготовки кромок под сварку на трещиностойкость сварных соединений сельскохозяйственных машин // Актуальные вопросы агроинженерных наук в сфере технического сервиса машин, оборудования и безопасности жизнедеятельности: теория и практика: мат-лы национ. науч. конф. Института агроинженерии. Челябинск: Южно-Уральский ГАУ, 2020. С. 92-100.

УДК 004.94

О РАЦИОНАЛЬНОМ ВЫБОРЕ ФОРМЫ ЗАГОТОВКИ ДЛЯ ПОЛУЧЕНИЯ РАВНОТОЛЩИННЫХ ИЗДЕЛИЙ ТИПА ШАРОБАЛЛОН

ABOUT THE RATIONAL CHOICE OF THE PROCESSING FORM FOR OBTAINING CARBAR MATERIALS TYPE SHAROBALLON

Еникеев Ф.У., Мурзина Г.Р.,
Уфимский государственный нефтяной технический университет,
ул. Космонавтов, 1, г. Уфа, Республика Башкортостан, 450064, Россия

F.U. Enikeev, G.R. Murzina,
Ufa State Petroleum Technological University,
Kosmonavtov Str., 1, Ufa, Republic of Bashkortostan, 450064, Russia

e-mail: guzelya_murzina@mail.ru

Аннотация. В работе рассматривается процесс сверхпластической формовки полусферы для получения изделия шаробаллон из титанового сплава ВТ6 (Ti-6Al-4V). Шаробаллон – это сосуд, работающий под высоким давлением. Сосуд изготавливается сваркой двух полусфер, получаемых сверхпластической формовкой. В процессе формовки возникает проблема, как неравномерность толщины полусферы. В данной работе уменьшение разнотолщинности полусферы достигается путем использования предварительной (специальной) формы заготовки. Рассмотрены различные формы заготовки и в ходе математического и компьютерного моделирования выявлено, какую форму более целесообразно использовать: постоянной толщины, заготовку переменной

толщины шарообразной или конической форм. В ходе исследований обнаружено, что при использовании заготовки постоянной толщины происходит значительное утонение в полюсе купола полусферы. Более равномерное распределение толщины было достигнуто при использовании заготовки переменной толщины конической формы. Компьютерное моделирование выполняется в программном комплексе ANSYS 10 ED.

Abstract. The paper considers the process of superplastic forming of a uniform hemisphere to obtain a balloon product from titanium alloy VT6 (Ti-6Al-4V). A balloon is a high pressure vessel. The vessel is made by welding two hemispheres obtained by superplastic forming. In Russia, an import substitution program is underway, which includes a balloon that is used as a vessel for storing gases under pressure in domestic launch vehicles. However, in the molding process, a problem arises as the unevenness of the thickness of the hemisphere. In this work, a decrease in the thickness difference of the hemisphere is achieved by using a preliminary (special) shape of the workpiece. Various forms of the workpiece were considered and in the course of mathematical and computer modeling it was revealed which form is more appropriate to use: constant thickness, a workpiece of variable thickness, spherical or conical. In the course of research, it was found that when using a workpiece of constant thickness, a significant thinning occurs at the pole of the dome of the hemisphere. A more even thickness distribution was achieved using a conical shape of varying thickness. Computer simulation is performed in the ANSYS 10 ED software package.

Ключевые слова: разнотолщинность, сверхпластичность, шаробаллон, полусфера, предварительная заготовка, сферхпластическая формовка, моделирование, профилированная заготовка.

Keywords: different thickness, superplasticity, balloon, hemisphere, pre-harvesting, superplastic forming, modeling, profiled sheet.

Титановые шаробаллоны представляют собой герметичные сферические конструкции высокого давления, обеспечивающие работу пневматических систем жидкостных ракетных двигателей. Шаробаллоны используются в составе космических аппаратов «Союз-М» и «Прогресс-М» [1]. Используются в качестве топливных баков, сосудов для транспортировки газов под давлением.

Изготовление шаробаллонов в России входит в программу импортозамещения.

Сваркой двух полусферических оболочек, по их кромкам, получают шаробаллон. В данной работе используется титановый сплав ВТ6 (Ti-6Al-4V).

При формовке заготовки постоянной толщины появляется разнотолщинность, оказывающая негативное влияние на качество изделия, снижается конструкционная прочность шаробаллонов.

Появление разнотолщинности в полусферических оболочках связано с тем, что при СПФ деформация происходит исключительно за счёт утонения свободной части заготовки, а степень деформации достигает больших значений [2].

Рассмотрим заготовку постоянной толщины (рисунок 1).

Компьютерное моделирование СПФ проводится в программном комплексе ANSYS 10 ED.

Основные геометрические параметры отформованного купола:

– радиус купола R (зависимость R(φ) или R(L));

– распределение толщины по профилю купола s=s(φ) или s=s(L), где L=Rφ;

– связь между начальным и конечным положением точки M: пусть M1 − некоторая произвольная точка на поверхности отформованного купола;

– высота купола H, толщина купола в полюсе sa.

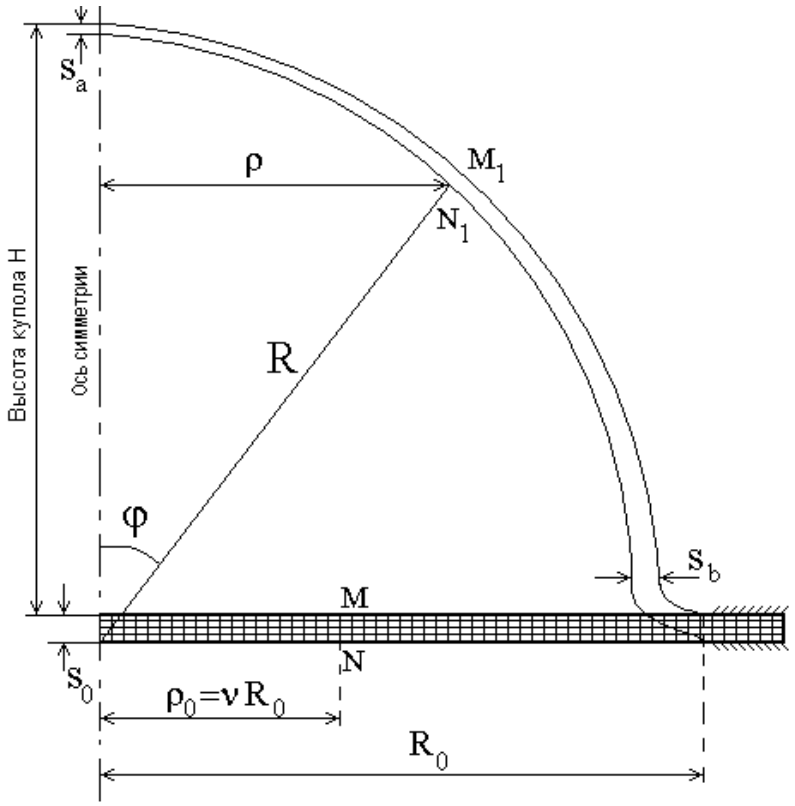

Рисунок 1. Схема деформирования заготовки постоянной толщины

Вывод результатов расчета в ANSYS 10 ED СПФ заготовки постоянной толщины (рисунок 2):

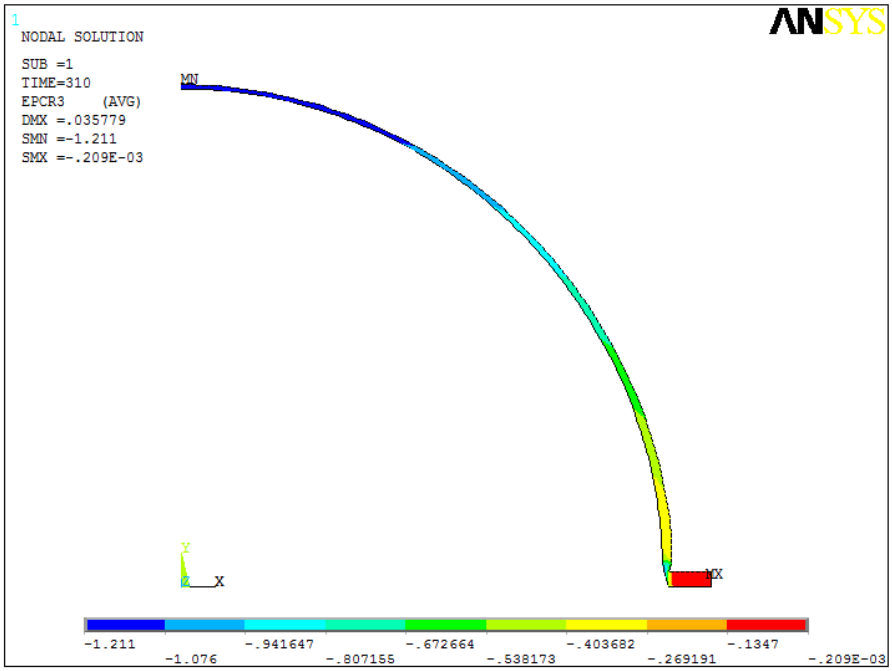

Рисунок **Error! No text of specified style in document.**. Распределение третьей главной деформации полусферы

из заготовки постоянной толщины

Из эпюры видно, что по сечению деформация неоднородная, что является причиной появления разнотолщинности, с минимальной толщиной в полюсе (рисунок 2).

Есть различные способы управления утонением стенок купола [2, 3]. Один из них − формовка заготовки переменной толщины (рисунок 3).

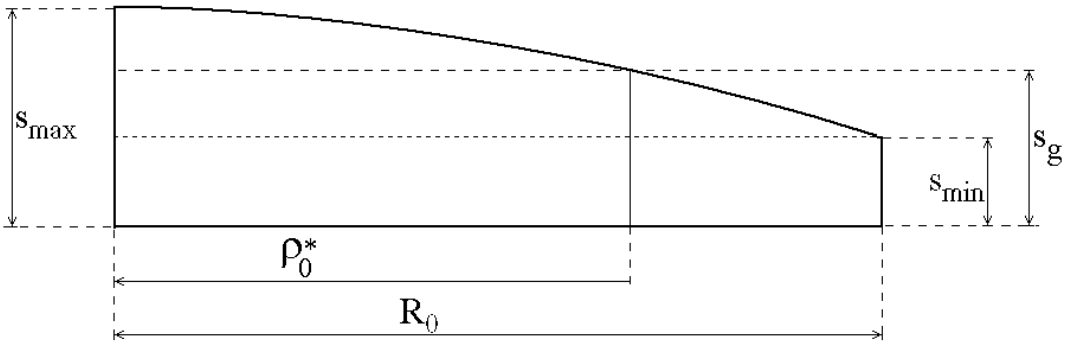

Рисунок 3. Сечение заготовки переменной толщины

На входе заданы три параметра: радиус R_0 и толщина готовой полусферы s_g, а также величина параметра скоростной чувствительности материала m.

На выходе конкретные значения s_{max} и s_{min} (которые определяют значения, вводимые в ANSYS вместе с радиусом R_0).

В ходе работы выявлено, что нерационально использовать заготовку шарообразной формы, т.к. его форма подобна конической.

Рассмотрим схему заготовки переменной толщины конической формы, показанной на рисунке 4 [4]:

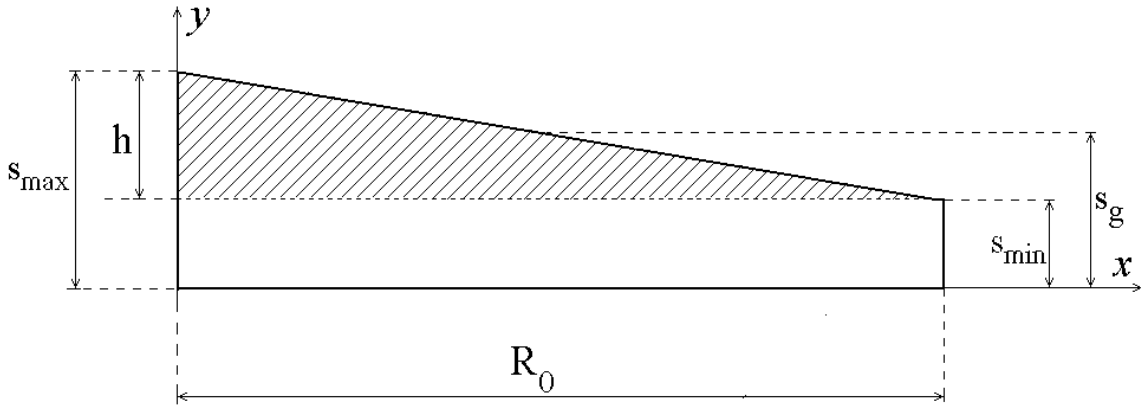

Рисунок 4. Сечение заготовки переменной толщины конической формы

В этом случае объем металла готовой полусферы равен $V_g=\pi R_0^2 s_g$, а объем заготовки V_0 складывается из двух частей: цилиндрической V_1 и конической V_2.

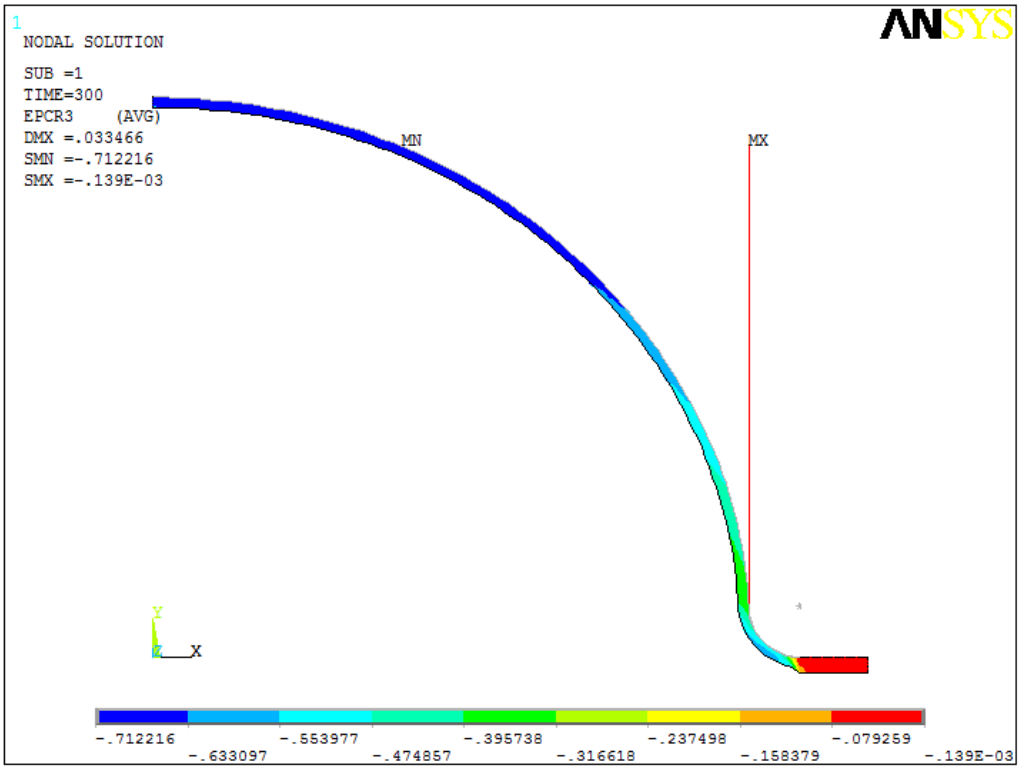

Рисунок 5. Распределение третьей главной деформации

Как видно из рисунка 5, получено довольно однородное распределение толщины по всему объему заготовки.

Выводы

1. При использовании заготовки постоянной толщины происходит значительное утонение в полюсе купола полусферы.
2. Проведено исследование сверхпластической формовки из сплава ВТ6 заготовок постоянной толщины, шарообразной и конической форм. Заготовка конической формы проще в изготовлении и расчете, чем заготовка шарообразной формы.
3. Выбор заготовки конической формы оказывает существенное влияние на уменьшение разнотолщинности формованных полусфер.

Литература

1. Красмаш [Электронный ресурс].– URL: https://clck.ru/WiWnz
2. Круглов А.А., Лутфуллин Р.Я., Еникеев Ф.У. Компьютерное моделирование процесса сверхпластической формовки полусферической оболочки из профилированной заготовки // Информационные технологии. Проблемы и решения. 2019. №3(8). С. 98-102.
3. Нгуен Ч. А. Сверхпластическая формовка листов алюминиевых сплавов с ультрамелким зерном для получения оболочек с рельефом: дис. канд. техн. наук: 05.16.05 / Нгуен Чыонг Ан. – М: МИСиС, 2009. – 142 с.
4. Мурзина Г.Р., Еникеев Ф.У. Моделирование процесса получения полусферы из листовой заготовки переменной толщины // Информационные технологии. Проблемы и решения. 2018. №1. С. 361-364.

УДК 004.934

ПРИМЕНЕНИЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ РЕШЕНИЯ ЗАДАЧ РАСПОЗНАВАНИЯ РЕЧИ

SPEECH RECOGNITION USING ARTIFICIAL NEURAL NETWORKS

Марьина В.В.,
ФГБОУ ВО «Казанский национальный исследовательский технический университет имени А.Н. Туполева»,
г. Казань, Российская Федерация

V.V. Maryina,
FSBEI HE “Kazan National Research Technical University named after A.N. Tupolev”,
Kazan, Russian Federation

e-mail: imciflam@yandex.ru

Аннотация. В данной работе рассмотрен эксперимент, в ходе которого была проанализирована задача распознавания речи при создании голосовых командных интерфейсов, а также возможные методы ее решения с помощью средств глубокого обучения, а именно – искусственных нейронных сетей различных конструкций.

В ходе данной работы были созданы и обучены несколько нейросетевых моделей различных конструкций, проанализированы сильные и слабые стороны каждой отобранной модели, после чего были сделаны соответствующие выводы об их эффективности в различных условиях применительно к задаче распознавания голосовых команд. Основной метрикой, по которой определялась точность результатов, была выбрана точность валидации.

Для обучения моделей были использованы два датасета, каждый из которых содержал приблизительно по тысяче записей голосового воспроизведенния восьми отобранных команд. Первый датасет содержал в себе записи с низким уровнем окружающего шума, второй же датасет содержал записи с повышенным уровнем окружающего шума.

Также было проанализировано влияние фактора шума на результаты работы моделей, и предложены методы для снижения его воздействия. Одним из таких предложенных методов является метод нормализации входящих обучающих данных, позволяющий значительно повысить итоговый процент правильно распознанных голосовых команд. Другим возможным вариантом является применение фильтров Калмана.

Abstract. In this paper, we consider an experiment in which we analyzed the problem of speech recognition when creating voice command interfaces, as well as possible methods for solving it using deep learning tools, namely, artificial neural networks of various designs.

In the course of this work, several neural network models of various designs were created and trained, the strengths and weaknesses of each selected model were analyzed, after which the corresponding conclusions were made about their effectiveness in various conditions

as applied to the task of recognizing voice commands. The main metric by which the accuracy of the results was determined was the accuracy of validation.

For training models, two datasets were used, each of which contained approximately one thousand voice recordings of eight selected teams. The first dataset contained records with a low level of ambient noise, while the second dataset contained records with a high level of ambient noise.

The influence of the noise factor on the results of the models was also analyzed, and methods were proposed to reduce its impact. One of the proposed methods is the method of normalizing incoming training data, which can significantly increase the final percentage of correctly recognized voice commands. Another possible option is to use Kalman filters.

Ключевые слова: распознавание речи, нейронные сети, сверточные нейронные сети, сети с долгой краткосрочной памятью, голосовой интерфейс.

Keywords: speech recognition, neural networks, convolutional neural networks, networks with long short-term memory, voice-user interface.

Голос является основной, распространенной и эффективной формой общения людей. Сегодня речевые технологии обычно доступны для ограниченного, но интересного диапазона задач. Это технологии позволяют машинам правильно и надежно реагировать на человеческие голоса и предоставлять полезные и ценные услуги.

Так как общение с компьютером происходит быстрее с помощью голосовой связи, а не клавиатуры, многие люди предпочитают подобные системы. В общении между людьми преобладает разговорный язык, поэтому естественно, что люди ожидают голосовых интерфейсов для работы с компьютером. Это может быть достигнуто путем разработки системы распознавания голоса: преобразования речи в текст, которая позволяет компьютеру перевести голосовой запрос и соответственно на него отреагировать. Преобразование речи в текст является процессом преобразования акустического сигнала, который захватывается с помощью микрофона, в набор слов. [2]

С тех пор, как на сцену распознавания речи вышло глубинное обучение, количество ошибок в распознавании слов кардинально уменьшилось. Одним из часто применяемых для решения данной задачи приемов являются нейронные сети различных конструкций, задача которых сводится к проведению классификации входного аудиосигнала и вычислению вероятности того, что было произнесено то или иное слово.

Одним из наиболее удобных и инфоемких методов представления аудиосигнала является применение мел-спектрограмм и мел-частотных кепстральных коэффициентов. Мел-частотные кепстральные коэффициенты являются производными мел-спектрограммы, которая была сжата путем применения дискретного косинусного преобразования.

Для получения мел-спектрограммы, исходный сигнал проходит следующие этапы обработки:

1. Деление сигнала на участки. Длина одного участка определяется длиной окна Хэмминга. Конкретная длина окна подбирается экспериментально, зависит от частоты исходного аудиосигнала. Также экспериментально подбирается длина шага, с которым окно Хэмминга накладывается на исходный сигнал.

2. Вычисление быстрого преобразования Фурье для каждого участка. Таким образом совершается преобразование из временной области в частотную область.

3. Генерация мел-шкалы. Берется весь частотный спектр и делится его на несколько (чаще всего – 128) равномерно распределенных частот. Под равномерно

распределенными частотами понимается не расстояние по частотному измерению, а расстояние, которое слышит человеческое ухо.

4. Генерация спектрограммы. Для каждого окна величину сигнала делят на его составляющие, соответствующие частотам в мел-шкале.

Как полученные спектрограммы, так и мел-частотные кепстральные коэффициенты могут быть использованы для распознавания команд с помощью средств машинного обучения, в частности, они могут послужить входными обучающими данными для нейронных сетей.

Так как в ходе решения данной задачи возникает необходимость глубокого анализа существующих во входных данных паттернов, простая конструкция многослойного персептрона показывает недостаточно высокие результаты. Одним из возможных вариантов является применение сверточных нейронных сетей.

В данном эксперименте будет использована VGG16-подобная архитектура. Ее можно будет применить для сверточной нейронной сети, работающей и с одним, и с двумя измерениями – разницей будет лишь формат входящих данных и то, как именно окно фильтрации перемещается по входящего изображению в ходе его обработки сверточным слоем.

Также одним из возможных вариантов является применение рекуррентных нейронных сетей, обладающими долгой краткосрочной памятью.

В данном эксперименте будет использована конструкция, обладающая двунаправленными связями, благодаря которым достигаются более точные результаты вычисления градиентного спуска.

Возможной опцией также является применение сверточно-рекуррентной нейронной сети, которая зачастую производит лучшие результаты, чем сверточные и рекуррентные нейронные сети, однако их производительность заметно ниже, что особенно становится заметно при применении их с датасетами большого размера.

В качестве исходных обучающих данных для данного эксперимента используем Synthetic Speech Commands Dataset [1], включающий в себя тысячи команд, произносимых в условиях отсутствия шума и в условиях наличия шума.

Выберем 8 основных классов команд – а именно, слова «down», «go», «left», «no», «right», «stop», «up», «yes».

Каждый класс представлен приблизительно тысячью коротких аудиозаписей в формате .wav, записанных голосами людей различного пола и возраста.

Каждый класс дополнительно делится пополам по критерию наличия или отсутствия в записях повышенного уровня шума.

Спустя 30 эпох обучения, для аудиозаписей из чистого датасета были получены следующие результаты: точность валидации для одно- и двухмерных сверточных сетей достигает 93.34% и 96,31% соответственно, сверточно-рекуррентная нейронная сеть выдает результат 95,8%, сеть с долгой краткосрочной памятью – 95,18%.

Динамика несколько меняется при обучении нейронных сетей той же конструкции на «шумном» датасете. Тогда точность валидации для одно- и двухмерных сверточных сетей достигает 79.71% и 83.81%, для сверточно-рекуррентной сети – 83.91%, для сети с долгой краткосрочной памятью – 87,6%.

Динамику обучения всех четырех нейронных сетей на обоих датасетах можно наблюдать ниже (рисунок 1).

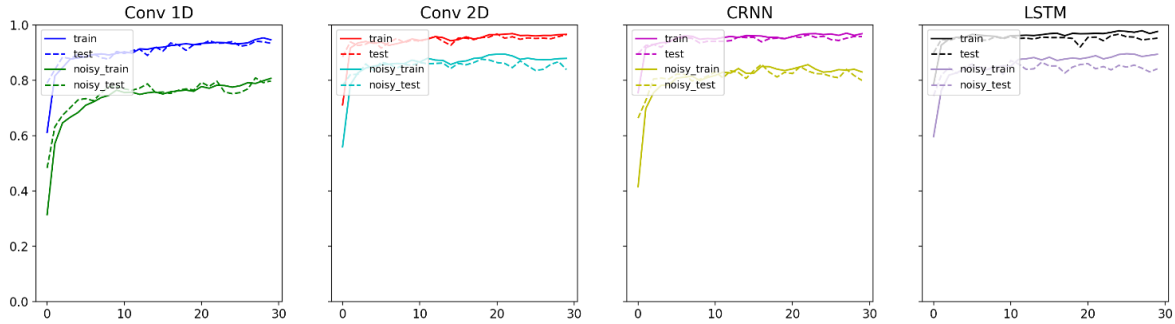

Рисунок 1. Динамика обучения нейронных сетей
на «чистом» и «шумном» датасетах.

Следует отметить, что процент успешного распознавания команды из каждого класса сильно варьируется. Так, глядя на матрицу на рисунке ниже (рисунок 2), легко заметить, что процент заметно снижается в случае похожих друг на друга по звучанию команд, например, «go» и «no», отличающиеся всего на одну букву.

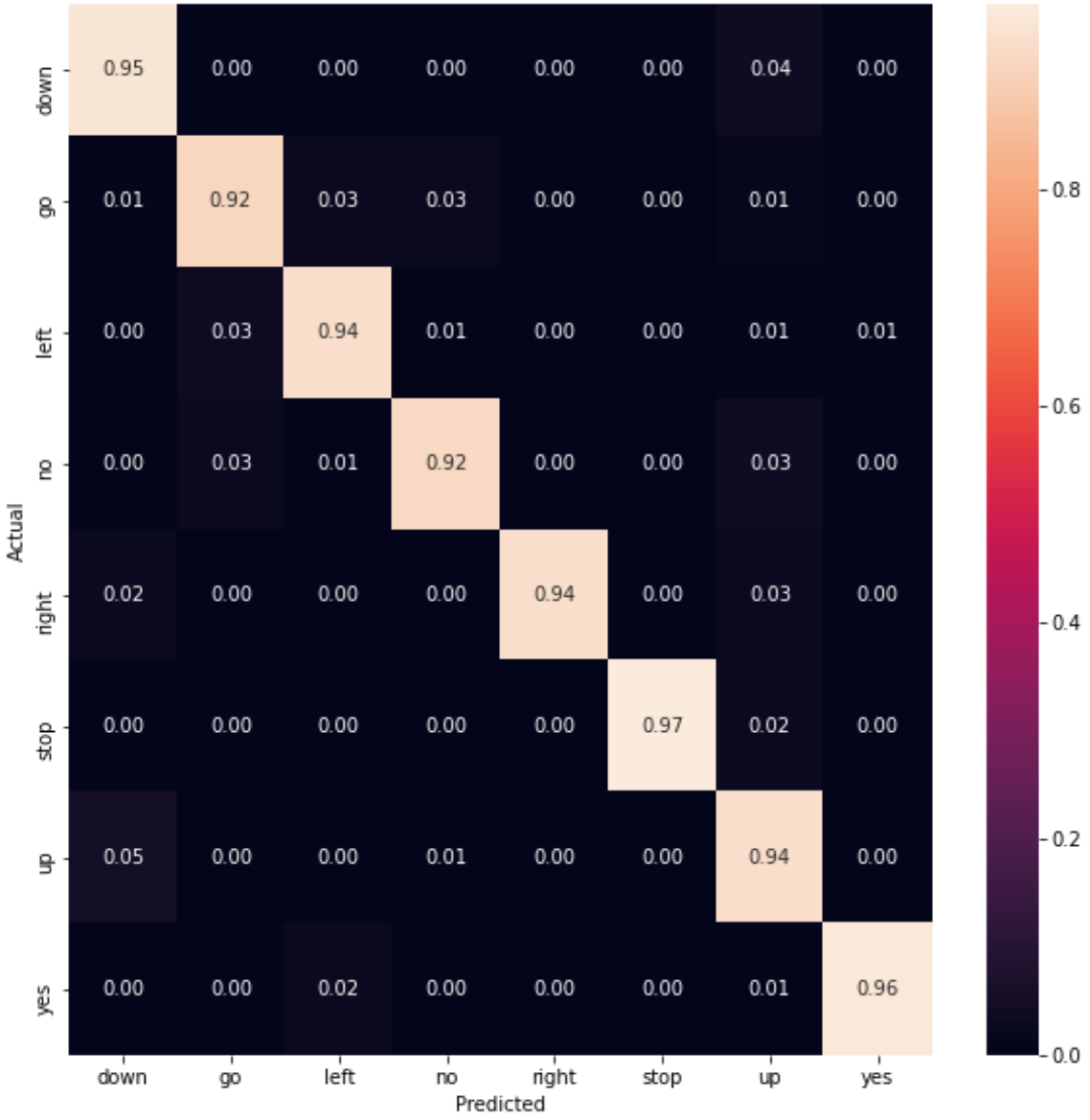

Рисунок 2. Матрица несоответствий.

Также можно видеть, что наиболее распознаваемые команды, как правило, не имеют похожих по звучанию команд в фиксированном наборе.

Для снижения влияния шума на итоговые результаты распознавания существует масса приемов, например, использование нормализации данных или фильтров Калмана. Таким образом, при возникновении необходимости работы с голосовым интерфейсом в условиях повышенного уровня окружающего шума, эти направления являются перспективными для решения задачи.

Выводы

Таким образом, можно сделать вывод, что одним из возможных направлений действий для улучшения точности распознавания команд голосового интерфейса является подбор команд, значительно отличающихся по звучанию.

Что же касается выбора оптимальной конструкции нейронных сетей при решении задач распознавания речи, эксперимент показал, что решение должно приниматься во многом на основе входящих данных и условий, в которых предполагается применять разработанную систему. В среднем же сети с долгой краткосрочной памятью продемонстрировали наиболее высокий результат при решении задачи распознавания команд.

Литература

1. Buchner J. Synthetic Speech Commands: A public dataset for single-word speech recognition // Kaggle. 2017. С. 1.

2. Prerana D. Voice Recognition System: Speech-to-Text // Journal of Applied and Fundamental Sciences. 2015. С. 2395-5562.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭКОНОМИКЕ, УПРАВЛЕНИИ И БИЗНЕСЕ

УДК 004.89

ИСПОЛЬЗОВАНИЕ ПРОГРАММЫ ANYLODGIC ДЛЯ АНАЛИЗА ПОТРЕБИТЕЛЬСКОГО РЫНКА ИГРЫ GENSHIN IMPACT И ПОСТРОЕНИЕ ПРОГНОЗА

USING THE ANYLOGIC PROGRAM TO ANALYZE THE CONSUMER MARKET OF THE GENSHIN IMPACT GAME AND BUILD A FORECAST

Ткаченко А.Л., Ольшанская О.И., Арышева О.Н.,
ФГБУ ВО «Калужский государственный университет им. К.Э. Циолковского»,
г. Калуга, Российская Федерация

A.L. Tkachenko, O.I. Olshanskaya, O.N. Barysheva,
Kaluga State University named after K.E. Tsiolkovski,
Kaluga, Russian Federation

e-mail: TkachenkoAL@tksu.ru

Аннотация. В статье даётся анализ развития потребительского рынка игры Genshin Impact в виде агентной модели и прогноз на будущее. Агентное моделирование – относительно новый метод имитационного моделирования. Поначалу оно являлось преимущественно предметом теоретических дискуссий в академических кругах. Начиная с 2000-х годов разработчики имитационных моделей стали использовать агентное моделирование на практике. Как раз с помощью агентной модели был проведен анализ потребительского игрового рынка для игры Genshin Impact – компьютерной игры в жанре Action-adventure с открытым миром и элементами RPG, разработанная китайской компанией miHoYo Limited. Игра распространяется посредством цифровой дистрибуции по модели free-to-play, но имеет внутриигровой магазин, использующий реальную валюту. Эта игра один из самых больших прорывов 2020 года благодаря безупречному маркетингу. Эта статья будет интересна рекламным агентам, менеджерам по маркетингу и заинтересованным лицам в сфере игр. Разработчиком программного обеспечения является Российская компания, что важно в настоящее время, когда вопрос перехода на отечественные программные продукты стоит особенно остро, ввиду возможный санкций и обеспечения информационной безопасности. Полученные нами результаты, представленные, показывают распространение игры с начала её выхода среди изначально заданных 35млн пользователей. Используя данные взятые из открытого доступа, мы сделали прогноз на будущее развитие игры среди пользователей. В итоге по окончании прогнозного периода мы выяснили, что к 2024 году количество пользователей станет превосходить 35млн и позволит игре расширить свой потребительский рынок.

Abstract. The article provides an analysis of the development of the consumer market of the game Genshin Impact in the form of an agent model and a forecast for the future. Agent-based modeling is a relatively new method of simulation modeling. At first, it was mainly the

subject of theoretical discussions in academic circles. Starting in the 2000s, simulation model developers began to use agent-based modeling in practice. Just with the help of the agent model, an analysis of the consumer gaming market was conducted for the game Genshin Impact – a computer game in the genre of Action-adventure with an open world and RPG elements, developed by the Chinese company miHoYo Limited. The game is distributed through digital distribution on a free-to-play model, but has an in-game store that uses real currency. This game is one of the biggest breakthroughs of 2020 thanks to impeccable marketing. This article will be of interest to advertising agents, marketing managers, and game stakeholders. The software developer is a Russian company, which is important at the present time, when the issue of switching to domestic software products is particularly acute, due to possible sanctions and information security. The results obtained by us, presented, show the distribution of the game since the beginning of its release among the originally set 35 million users. Using data taken from open access, we made a forecast for the future development of the game among users. As a result, at the end of the forecast period, we found out that by 2024, the number of users will exceed 35 million and will allow the game to expand its consumer market.

Ключевые слова: имитационное моделирование, агентная модель, прогноз, потребительский рынок, AnyLogic, Genshin Impact.

Keywords: simulation modeling, agent model, forecast, consumer market, AnyLogic, Genshin Impact.

Для проведения анализа потребительского рынка игровой индустрии, построим агентную модель, которая поможет нам изучить процесс вывода нового продукта на рынок, а в частности компьютерной игры Genshin Impact. Система имитационного моделирования AnyLogic разработана российской компанией и успешно конкурирует с подобными программными продуктами, в том числе Deductor, позволяет бесплатное использование, что немаловажно для студентов и образовательных организаций, что совпадает с мнением авторов [1].

Игра Genshin Impact очень молодая, она буквально появилась полгода назад и уже сумела овладеть огромной массой пользователей.

Genshin Impact – компьютерная игра в жанре Action-adventure с открытым миром и элементами RPG, разработанная китайской компанией miHoYo Limited. Игра распространяется посредством цифровой дистрибуции по модели free-to-play, но имеет внутриигровой магазин, использующий реальную валюту. Эта игра один из самых больших прорывов 2020 года благодаря безупречному маркетингу. Игра распространялась очень стремительно и ещё до официального выхода имела немаленькую базу уже зарегистрированных пользователей. Давайте рассмотрим распространение Genshin Impact среди пользователей за полгода с начала выхода игры. Обратим внимание, что пандемия сыграла большую роль в успехе онлайн-игр, поскольку большинство людей оказались в ловушке у себя дома.

Достоверно неизвестно сколько точно пользователей у этой игры, так как miHoYo не давали официально никаких цифр, и мы решили узнать, как скоро игра превысит точку максимального числа игроков, взятое среди всех возможных предложений и теорий. Так мы пришли к числу в 35 миллионов пользователей на сегодняшний день, которое всё ещё стремительно растёт.

Вот подробная таблица предполагаемых ежемесячных пользователей Genshin Impact. В таблице 1, которая показана ниже, представлено максимальное количество пользователей игры, прирост/убыток, процент прироста/убытка, а также максимальное количество игроков в пике в данный день [2].

Таблица 1 – Данные о количестве игроков с момента выхода игры

Месяц	Среднее количество игроков в месяц	Ежемесячный прирост/убыток	Ежемесячный прирост/убыток, %	Максимальное количество игроков в день
Последние 30 дней	30 901 446	1,351,297	8	5 811 470
30 марта 2021 г.	29 550 149	888 045	12	6 014 429
28 февраля 2021 г.	28 662 104	2,253,132	21	6 200 147
30 января 2021 г.	26 408 972	2 628 429	42	5 462 094
30 декабря 2020 г.	23 780 543	5 201 994	27	4 756 109
30 ноября 2020 г.	18 578 549	-185 709	12	4 334 995
30 октября 2020 г.	18 764 258	2,228,802	13	4 065 589
30 сентября 2020 г.	16 535 456	16 535 455	0	3 380 318

Благодаря AnyLogic мы сможем построить агентную модель распространения игры среди пользователей. Возьмём получившийся у нас потребительский рынок из 35 миллионов пользователей. Так как мы рассматриваем процесс вывода на рынок новой игры, то изначально в неё никто не играет. Люди начнут скачивать её под влиянием рекламы. После этой первоначальной стадии более значительное влияние на распространение игры будет оказывать общение людей друг с другом, рекомендации и положительные отзывы пользователей, побуждающие других на скачивание новой игры.

Люди в нашей модели поначалу не будут пользоваться продуктом, но потенциально могут быть в нем заинтересованы. Для начала мы создадим популяцию агентов, а потом зададим то, как люди приобретают товар под влиянием рекламы, общения, рекомендаций и положительных отзывов.

В нашей модели два типа агентов: Main и Consumer.

Вот так выглядит наша диаграмма агента-потребителя Consumer (рисунок 1):

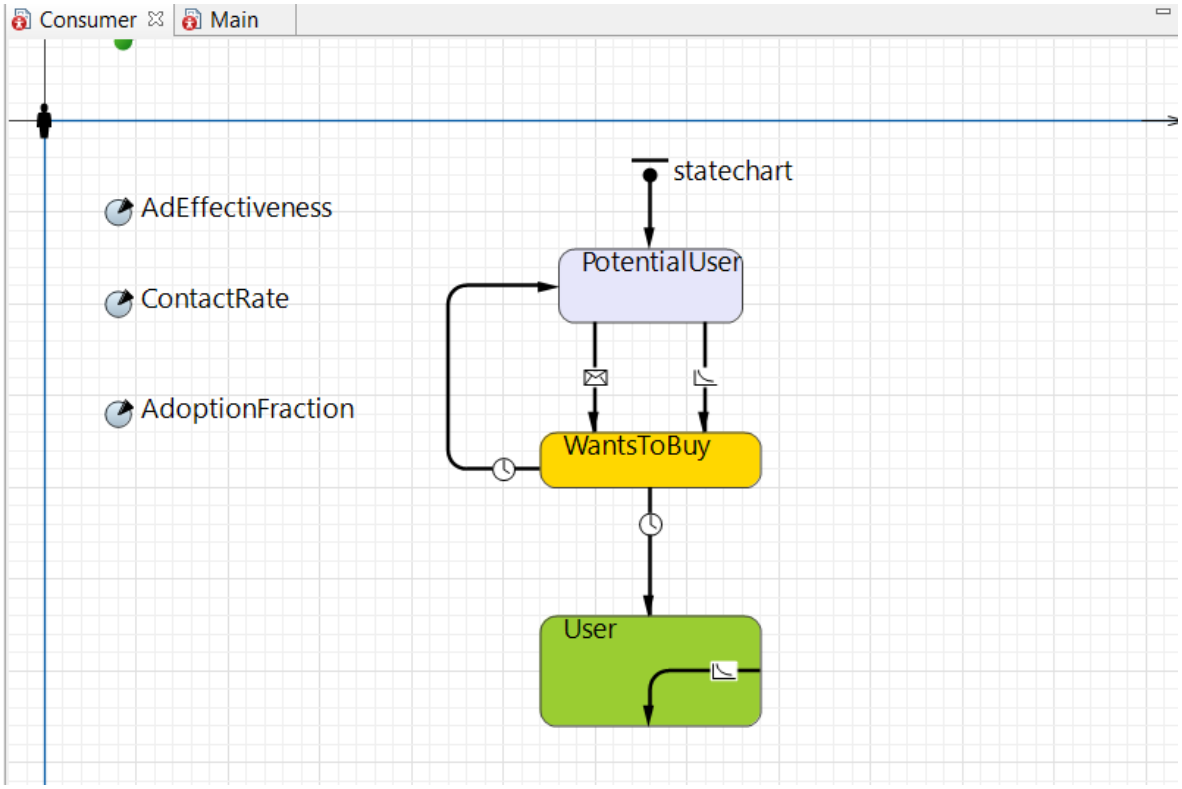

Рисунок 1. Диаграмма агента-потребителя Consumer

А вот так выглядит диаграмма агента Main (рисунок 2) содержащего популяцию агентов, которая называется consumers.

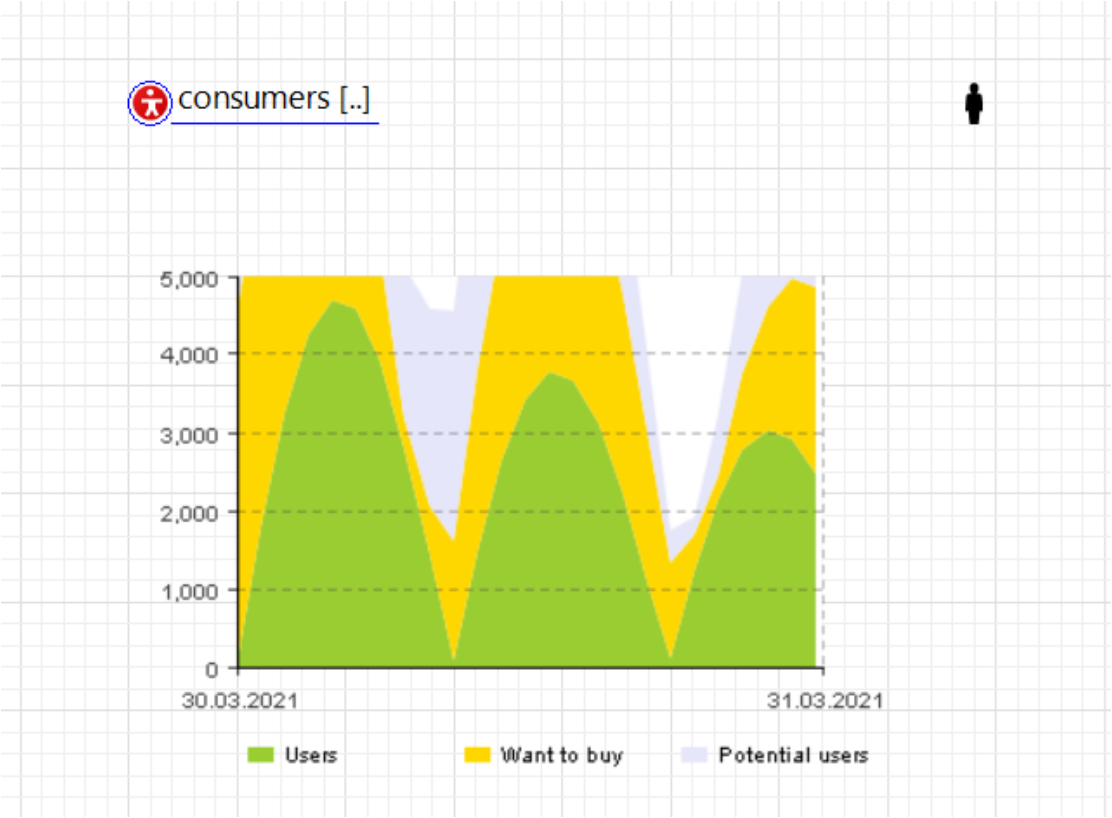

Рисунок 2. Диаграмма агента Main

Благодаря широкой доступности игры она стала набирать так много пользователей.

Она доступна на таких платформах как PS3, PS4, PS5, Xbox, Wii, Nintendo Switch, Windows, Mac, Android и iOS.

Давайте запустим нашу модель и посмотрим на то, как игра распространяется среди пользователей.

Таким образом, мы продемонстрировали, как можно использовать программу AnyLogic для прогноза распространения какого-либо продукта среди агентов [3].

Однако это лишь малая часть функционала данной программы.

В этой программе добавляя разные параметры или изменяя существующие мы могли бы оценить влияние этих изменений на поведение потребителей и состояние рынка [4].

Полученные нами результаты, представленные на рисунках 3 и 4, показывают распространение игры с начала её выхода среди изначально заданных 35 млн. пользователей.

Используя данные взятые из открытого доступа, мы сделали прогноз на будущее развитие игры среди пользователей.

В итоге по окончании прогнозного периода мы выяснили, что к 2024 году количество пользователей станет превосходить 35 млн. и позволит игре расширить свой потребительский рынок.

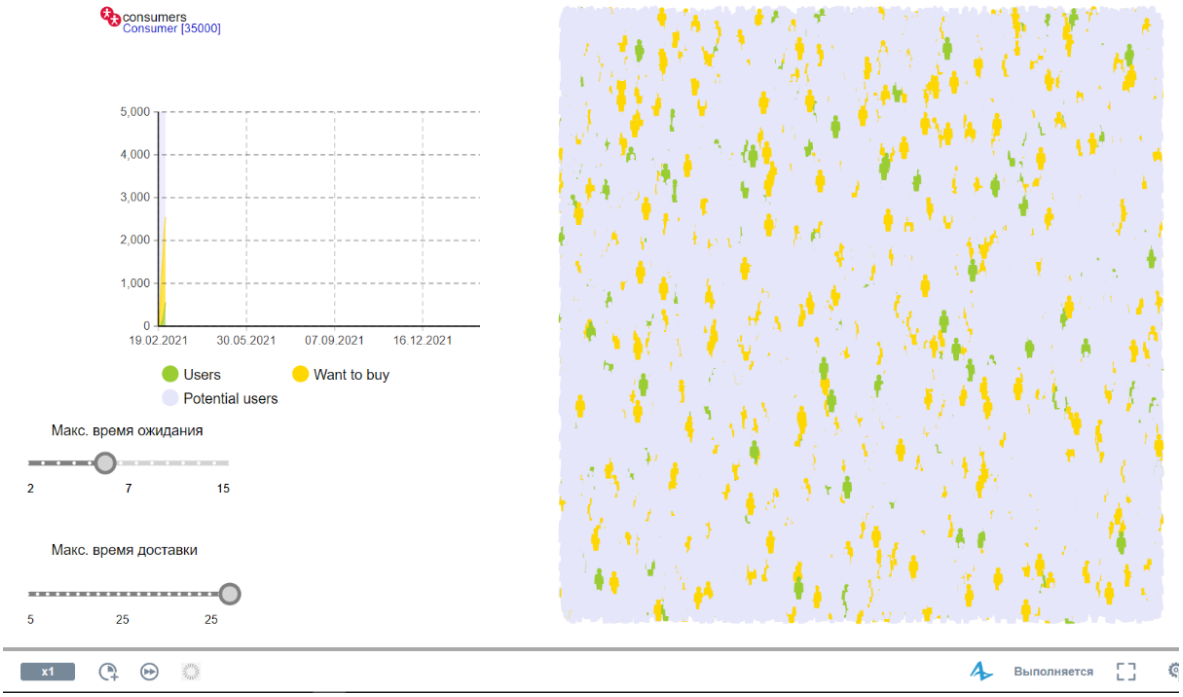

Рисунок 3. Начало распространения игры

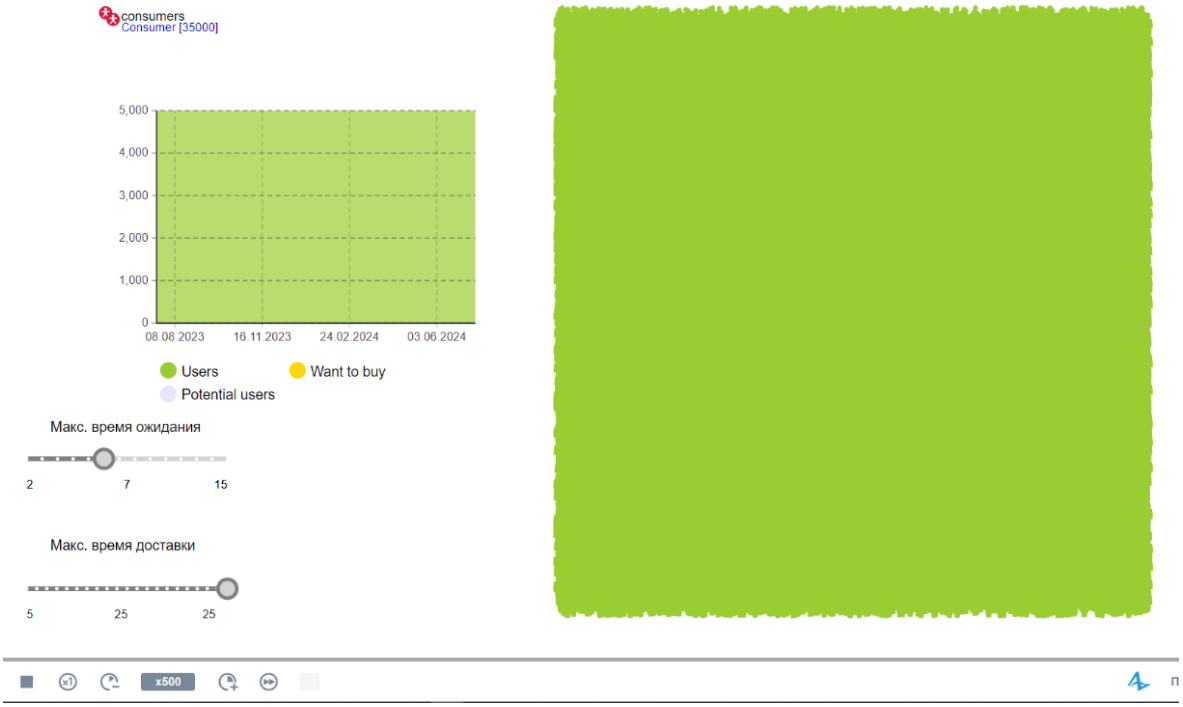

Рисунок 4. Конечная точка распространения игры среди 35 млн.

Выводы

Насколько данный прогноз окажется верным – покажет время, однако считаем, что полученные результаты могут быть полезны рекламным агентам, менеджерам по маркетингу и заинтересованным лицам в сфере игр.

Литература

1. Ткаченко А.Л., Пономарев С.В. Глава 6. Прогноз и перспективы развития страхового рынка в российской федерации // В книге: Состояние и тенденции развития национальной экономики в условиях глобализации. посвящается 100-летию Финансового университета при Правительстве Российской Федерации: монография. Пенза, 2019. С. 236-243.
2. Кондрашова Н.Г., Русу Я.Ю. Применение программных продуктов в сфере управления бизнес-проектами // Modern Economy Success. 2020. №5. С. 94-99.
3. Ткаченко А.Л., Полпудникова О.В. Анализ и моделирование бизнес-информации с помощью унифицированной программной платформы // В сборнике: Математическое моделирование в экономике, управлении, образовании. Материалы Международной научно-практической конференции. Под редакцией Ю.А. Дробышева и И.В. Дробышевой. 2015. С. 292-297.
4. Волкова Т.А., Суслякова О.Н. Страхование информационных рисков (киберстрахование) Инновационная экономика: перспективы развития и совершенствования. 2018. Т.1. №7 (33), С. 117-122.

УДК 004.738.5

ТЕХНОЛОГИИ IOT ДЛЯ ИНДУСТРИИ 4.0

IOT TECHNOLOGIES FOR INDUSTRY 4.0

Михайловская И.М., Имаева Л.Р.,
Уфимский государственный нефтяной технический университет,
ул. Космонавтов, 1, г. Уфа, Республика Башкортостан, 450064, Россия

I.M. Mikhaylovskaya, L.R. Imaeva,
Ufa State Petroleum Technological University,
Kosmonavtov Str., 1, Ufa, Republic of Bashkortostan, 450064, Russia

e-mail: MessageIM@mail.ru

Аннотация. Технологии IoT позволяют производителям получать больше информации о производственных процессах за счет эффективного использования данных и более тесной интеграции разрозненных систем. А также дают возможность укрепления делового сотрудничества между поставщиками и потребителями, не только благодаря поставке продукции, но и оказанию различных услуг. Интернет вещей может способствовать развитию экономики и бизнеса за счет повышения эффективности и качества производства. По сути, это программа повышения эффективности внутренней деятельности предприятий отрасли, поэтому данные проекты гарантировано будут успешными. Это возможность оптимизации обработки данных в режиме реального времени, реализуемая с помощью Интернета вещей. Достаточно установить в производственной среде необходимые датчики и проанализировать динамику показателей, чтобы сделать действенные выводы. Компания Accenture прогнозирует, что к 2030 году оптимизация производства за счет внедрения Интернета вещей, может привнести в мировую экономику 14,2 триллиона долларов США. Однако это лишь часть преимуществ, которые Интернет вещей может предоставить для промышленности.

Помимо этого, технологии Интернета вещей могут способствовать крупномасштабной трансформации бизнеса, но эту программу реализовать гораздо сложнее.

Abstract. IoT technologies enable manufacturers to gain more insight into manufacturing processes by leveraging data efficiently and tighter integration of disparate systems. They also provide an opportunity to strengthen business cooperation between suppliers and consumers, not only through the supply of products, but also through the provision of various services. The Internet of Things can help boost economies and businesses by improving efficiency and quality of production. In fact, this is a program to improve the efficiency of the internal activities of enterprises in the industry, so these projects are guaranteed to be successful. It is an opportunity to optimize data processing in real time, realized with the help of the Internet of Things. It is enough to install the necessary sensors in the production environment and analyze the dynamics of indicators in order to draw effective conclusions. Accenture predicts that IoT-enabled manufacturing optimization could contribute $ 14.2 trillion to the global economy by 2030. However, these are just a few of the benefits that the Internet of Things can bring to industry. In addition, IoT technologies can drive large-scale business transformation, but the program is much more difficult to implement.

Ключевые слова: Интернет вещей, производство, экономика, бизнес, технологии, бизнес-процессы, датчики, агроботы, умный дом, умный город, здравоохранение, сельское хозяйство, промышленность.

Keywords: IoT, production, economy, business, technologies, business processes, sensors, agrobots, smart home, smart city, healthcare, agriculture, industry.

Интернет вещей (IoT) представляет собой систему взаимосвязанных вычислительных устройств, механических и цифровых машин, объектов, животных или людей, которым присвоены уникальные идентификаторы и обеспечена возможность передавать данные по сети без необходимости взаимодействия человека с человеком или человека с компьютером.

Вещью в IoT может быть человек с сердечным имплантатом, сельскохозяйственное животное с биочипом, автомобиль со встроенными датчиками, или любой другой физический или антропогенный объект, которому может быть назначен IP-адрес и который может передавать данные по сети.

Организации в различных отраслях промышленности все чаще используют Интернет вещей для повышения эффективности работы, лучшего понимания потребностей клиентов, повышения качества обслуживания, улучшения процесса принятия решений и увеличения прибыли в бизнесе.

Мотивацией для развертывания IoT в производственной сфере (промышленного Интернета вещей) является получение прибыли. С одной стороны, это возможность производить продукцию с более низкой себестоимостью и, следовательно, продавать с большей маржой, с другой – ряд дополнительных преимуществ, которые в конечном итоге можно приравнять к сэкономленным средствам. Сюда входит экономия за счет увеличения производительности труда, минимизации потребления энергии, экономии затрат, увеличения срока службы оборудования и времени безотказной работы за счет профилактического обслуживания.

С производством все ясно: за счет развертывания систем IoT, деньги можно и сэкономить, и заработать. Несколько иначе обстоят дела с инвестициями. Обеспечить возврат инвестиций сложно из-за незрелости рынка и отсутствия аналогичных проектов, на основе которых можно было бы делать прогнозы. Для того, чтобы получить четкое

представление об окупаемости инвестиций, необходимо рассчитать прямую финансовую экономию и выгоду. Создание каталога примеров рентабельности инвестиций требует проведения дополнительных исследований.

Интернет вещей предоставляет организациям ряд преимуществ. Некоторые из них зависят от отрасли, другие применимы во многих отраслях (рисунок 1).

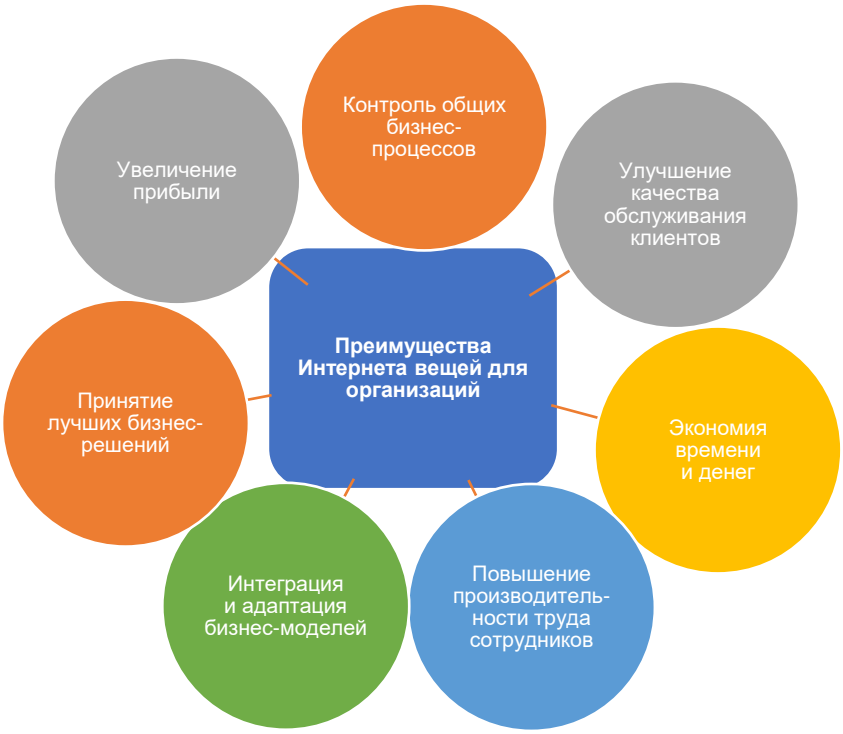

Рисунок 1. Преимущества использования Интернета вещей для организаций

Интернет вещей побуждает компании переосмыслить подходы к своему бизнесу и дает инструменты для улучшения бизнес-стратегий.

Технологии Интернета вещей нашли широкое применение в производственных, транспортных и коммунальных организациях где используются датчики и другие устройства. Однако инновации активно проникают и в другие сферы: сельское хозяйство, здравоохранение, городскую инфраструктуру, автоматизацию дома. Это способствует цифровой трансформации окружающей нас действительности.

Несколько примеров применения технологии Интернета вещей в Индустрии 4.0.

Технологии Интернета вещей могут принести пользу работникам сельского хозяйства и существенно облегчить их работу. Приложения IoT в сельском хозяйстве нацелены на традиционные операции, удовлетворение растущих потребностей и снижение производственных потерь.

Интернет вещей в сельском хозяйстве использует:

– дроны, роботов, удаленные датчики;

– компьютерную визуализацию в сочетании с инструментами машинного обучения;

– аналитические инструменты для мониторинга роста сельскохозяйственных культур, съемки и картирования полей.

Обработанные данные предоставляются специалистам для рационального планирования и управления сельскохозяйственным предприятием.

Сельское хозяйство во всем мире испытывает недостаток рабочей силы. Помочь в решении этой проблемы может робототехника. Последние достижения в области

сенсоров и технологий искусственного интеллекта позволяют создавать агроботов, которые могут заменить людей.

Оснащение машин контроллерами, позволяет управлять ими дистанционно. Так работой тракторов и тяжелого пахотного оборудования можно управлять автоматически, не выходя из дома, через GPS. Интегрированные механизмы обладают высокой точностью и возможностью самонастраиваться на местности, что упрощает выполнение трудоемких задач. Траекторию их движения и ход работ можно легко проверить с помощью смартфона. С развитием машинного обучения, эти механизмы становятся умнее благодаря различным новым функциями, например, автоматическому обнаружению препятствий.

Агроботов можно использовать для прополки: они сравнивают изображения посевов со своей базой данных, пропалывают сорняки и вносят удобрения.

Использование агроботов решает проблему нехватки рабочей силы при сборе урожая. Инновационные механизмы способны осуществлять деликатный процессе сбора фруктов и овощей 24 часа в сутки, 7 дней в неделю. Устройства используют механизм обработки изображений и роботизированные манипуляторы для определения зрелости плодов, которые нужно собирать. Боты подходят для выращивания и сбора урожая в теплицах, даже таких нежных культур, как помидоры и клубника.

Управление этими устройствами осуществляется дистанционно.

Помимо поддержания благоприятных условий для роста, ухода за растениями и сбора созревших плодов, роботы могут выполнять тяжелую ручную работу: поднимать и переносить тяжести на нужное расстояние.

Сельское хозяйство – одна из основных отраслей, использующих дроны. Дроны, оснащенные датчиками и камерами, используются для получения изображений, картографирования и съемки посевов.

Существуют наземные и воздушные дроны – беспилотные летательные аппараты.

Наземные дроны – это боты, которые передвигаются на колесах.

Воздушные дроны – беспилотные летательные аппараты (БПЛА) или беспилотные авиационные системы (БПАС) – летающие роботы.

Дронами можно управлять дистанционно или использовать встроенные программно-управляемые планы, которые координируются датчиками и GPS.

На основе данных с дронов можно сделать выводы о здоровье сельскохозяйственных культур, орошении, опрыскивании, почве, прогнозе урожайности и многом другом.

Датчики, установленные на посевных площадях, позволяют производить дистанционное зондирование. Они контролируют посевы на предмет изменений освещенности, влажности, температуры, формы и размера. Любая аномалия сразу же обнаруживается датчиками. Собранные данные передаются для аналитической обработки и анализа. С их помощью аграрии могут отслеживать состояние посевов и принимать меры на основе полученных сведений. Это позволяет следить за ростом сельскохозяйственных культур, принимать решение о необходимости полива, внесения удобрений и других манипуляциях. Данные, собранные датчиками, позволяют сделать выводы о том, выращивание какой культуры будет более рентабельным в данном регионе.

Для компьютерной визуализации используются сенсорные камеры, установленные в разных концах хозяйства, или дроны, оснащенных камерами.

Видеоряд, полученный с помощью данных устройств, подвергается цифровой обработке с использованием компьютерных алгоритмов. При обработке изображения просматривают с различной спектральной интенсивностью, например, в инфракрасном свете. Сравнивают изображения, полученные за определенный период времени,

отслеживают изменения в динамике, анализируя различные факторы – это помогает принимать стратегические решения.

Одна из самых важных областей экономики – здравоохранение. Его эффективность определяется по таким показателям, как продолжительность и качество жизни. При этом важным остается вопрос снижения затрат на здравоохранение. Проблемы, которые требуют решения:

– создание оборудования для диагностики и проведения медицинских процедур,

– доставка медицинских препаратов и оказание услуг.

Их можно решить, используя технологии Интернета вещей.

Для мониторинга и обработки данных о состоянии здоровья используется робототехника. Диапазон возможностей робототехники будет расширяться и становиться более интеллектуальным, а также позволит обеспечить более высокий уровень ухода за пациентами. Учитывая нехватку квалифицированных специалистов и младшего медицинского персонала, это один из способов качественного выполнения рутинных процессов.

Технология IoT позволяет медицинскому учреждению собирать необходимую информацию, получать аналитические данные о состоянии здоровья пациентов и, при необходимости, использовать другие ресурсы для решения неотложных медицинских проблем. Доставка анализов, расходных материалов или медицинских препаратов достаточно простые манипуляции, которые могут выполнять роботы.

Продолжительность жизни в развитых странах увеличивается. Одна из серьезных проблем, которая возникает в связи с этим – уход за пожилыми людьми. Проживание с уходом за больным – дорогостоящая медицинская услуга. Обеспечение пожилым людям полноценной самостоятельной жизни – актуальная задача для решения которой необходим комплекс мероприятий, который может быть реализован с помощью IoT технологий. В настоящее время этим озабочены многие компании. Они предлагают точечные решения: от носимых устройств, отслеживающих основные показатели жизнедеятельности, до приборов, определяющих состояние окружающей среды и отслеживания движения и активности. Все это области, в которых ключевую роль играют распознавание, общение и ответные действия. Гарантией того, что даже находясь вне стен лечебного учреждения, инвалиды и пожилые люди могут рассчитывать на получение оперативной медицинской помощи, является создание интегрированных интеллектуальных систем, объединяющих все датчики и устройства мониторинга, которыми пользуются пациенты. Задачи IoT – агрегирование данных и их использование для прогнозирования возникновения проблем со здоровьем или рецидивов.

Известно, что окружающая среда в медицинских учреждениях может содержать чрезвычайно токсичные патогены на поверхностях и в воздухе. В больницах и поликлиниках применяются специальные процедуры обеззараживания, чтобы предотвратить размножение и распространение патогенов. В настоящее время ведутся исследования по разработке систем уничтожения патогенов с использованием технологий, отличных от химических реактивов.

Среди новых – технологии, использующие мощные ультрафиолетовые светодиоды. Флуоресцентное ультрафиолетовое излучение существует много лет, но морально устаревшие системы недолговечны, а их эффективность со временем падает. В сочетании с робототехникой и другими технологиями, появляется возможность использовать для уничтожения патогенов ультрафиолетовое излучение с помощью светодиодов. Интернет вещей позволяет встраивать такую систему в инфраструктуру учреждения и автоматизировать процесс очистки.

Также ведется много исследований по быстрому обнаружению патогенов, которые переносятся по воздуху, присутствуют в организме человека или на нем. В этом

также значительную роль играет IoT. Разработка недорогих устройств обнаружения поможет нейтрализовать специфические генные аномалии. Хотя эта технология еще находится на ранних стадиях разработки и пока не готова к массовому использованию, она открывает многообещающие перспективы для раннего выявления и нейтрализации заболеваний. Когда датчики или мобильные устройства смогут быстро обнаруживать патогены, это позволит оперативно принимать меры для изоляции инфицированных и прогнозирования распространения инфекции.

Возможность мониторинга операций, связанных с инфраструктурой населенных пунктов, также является областью, в которой может помочь IoT. Датчики можно использовать, например, для отслеживания состояний или изменений в конструкциях зданий, мостов и других объектов. Это обеспечит экономию затрат и времени, повысит качество работ, обеспечит безбумажный рабочий процесс.

В сфере домашней автоматизации Интернет вещей можно успешно использовать в системе «умный дом» для мониторинга и управления механическими и электрическими системами. В системе «умный город» IoT поможет сократить отходы и потребление энергии.

Некоторые достоинства и недостатки использования Интернета вещей:

1) достоинства:

– возможность доступа к информации из любого места, в любое время, на любом устройстве;

– улучшенная связь между подключенными электронными устройствами;

– передача пакетов данных по подключенной сети, позволяющая сэкономить время и деньги;

– автоматизация задач, помогающая улучшить качество бизнес-услуг и снизить потребность в участии человека.

2) недостатки:

– риск кражи конфиденциальной информации по мере увеличения количества подключенных устройств и обмена информацией между ними;

– предприятиям, возможно, придется иметь дело с огромным количеством, IoT-устройств, сбор данных со всех этих устройств и управление ими будет сложной задачей;

– есть вероятность, что возникновение системной ошибки, может привести к сбою в работе подключенных устройств;

– сложность взаимодействия устройств разных производителей, ввиду отсутствия международного стандарта совместимости для IoT.

Выводы

Промышленный Интернет вещей (IIoT) позволяет:

– объединить в единую сеть датчики, контроллеры и другие устройства;

– обеспечить к ним удаленный доступ;

– осуществлять мониторинг, сбор и анализ данных из различных источников.

IIoT обладает огромным потенциалом и преимуществами для повышения производительности, снижения затрат и повышения эффективности. Данные инновации имеют невысокую стоимостью и могут быть быстро внедрены в производство.

Промышленная автоматизация – это использование автоматических систем управления, таких как промышленные компьютеры, программируемые логические контроллеры (контроллеры ПЛК) или роботы, что снижает потребность в ручном труде при управлении производственными процессами или оборудованием.

Интернет вещей помогает промышленной автоматизации создавать эффективные, доступные и гибкие системы, в соответствии с потребностями клиентов.

Подключение промышленного оборудования к облаку и обмен данными в реальном времени, может существенно повлиять на эффективность производства, время безотказной работы оборудования, а также помогает разрабатывать машины следующего поколения.

Менеджеры и руководители получают детальную информацию о потреблении электроэнергии, информацию об отходах, производительности, грядущих отказах оборудования, соблюдении нормативных требований и многом другом.

Благодаря Интернету вещей можно:

– *регулировать потребление ресурсов:* мониторинг потребления энергии в реальном времени позволяет оптимизировать график производственного процесса, выявить аномалии и возможности для экономии;

– *проводить сравнительный анализ:* сравнение аналогичного оборудования или местоположение предприятий, позволяет выявить системы, не работающие должным образом; обнаружить неэффективные операции и потери энергии;

– *перейти к профилактическому обслуживанию:* если система обнаруживает признаки грядущего отказа оборудования или изменение энергопотребления, производители получают информацию о необходимости проведения профилактического обслуживания. Это позволяет предотвратить капитальный ремонт и длительный простой оборудования;

– *повысить эффективность производства:* технологические и организационные изменения для оптимизация производственных процессов и систем позволяют эффективно использовать энергию и повысить производительность;

– *изменить корпоративную культуру:* владея информацией о потреблении ресурсов, менеджеры могут формировать в своей команде рачительное отношение к ним и развивать навыки осознанного потребления;

– *реализовать принципы социально ориентированного, экологичного производства, используя определенную модель управления,* например, «Шесть сигм»;

Автоматическое агрегирование, сравнительный анализ и аналитика позволяют лицам, принимающим решения, действовать быстро и принимать более обоснованные и ориентированные на прибыль решения.

Если до недавнего времени технологии Интернета вещей казались научной фантастикой, конкурентным преимуществом в производственной экосистеме, то сейчас они постепенно становятся основополагающей производственной необходимостью.

МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ

УДК 004

ТЕОРЕТИЧЕСКИЙ ОБЗОР ГЕНЕТИЧЕСКОГО АЛГОРИТМА

THEORETICAL OVERVIEW OF THE GENETIC ALGORITHM

Носкова Е.Е., Дружинская Е.В.,
Уфимский государственный нефтяной технический университет,
ул. Космонавтов, 1, г. Уфа, Республика Башкортостан, 450064, Россия

E.E. Noskova, E.V. Druzhinskaya,
Ufa State Petroleum Technological University,
Kosmonavtov Str., 1, Ufa, Republic of Bashkortostan, 450064, Russia

e-mail: noskova-79@inbox.ru

Аннотация. В статье представлен теоретический обзор генетического алгоритма. Статья посвящена комплексному исследованию актуальности применения генетических алгоритмов для решения множества современных задач, в различных направлениях, например, настройки и обучения нейронной сети, компьютерных программ, а также, робототехнике.

Определены основные преимущества использования генетических алгоритмов и отмечено, что данные алгоритмы оптимизируют функции, что позволяет решать и сокращать перебор в сложных задачах.

Произведен сбор и анализ научной литературы, проведены систематизация и структурирование сведений о генетическом алгоритме: выделены и описаны основные этапы алгоритма и критерии окончания цикла, даны определения понятий, используемых в генетических алгоритмах, рассмотрены операторы работы с данными алгоритмами, построена обобщённая модель генетического алгоритма в виде блок-схемы.

Проведённое теоретическое исследование позволяет сделать вывод о применимости генетических алгоритмов при оптимизации решения задач на принятие решений.

Abstract. The article presents a theoretical overview of the genetic algorithm. The article is devoted to a comprehensive study of the relevance of the use of genetic algorithms for solving a variety of modern problems, in various areas, for example, the configuration and training of a neural network, computer programs, as well as robotics.

The main advantages of using genetic algorithms are identified and it is noted that these algorithms optimize functions, which allows you to solve and reduce the search in complex problems.

The collection and analysis of scientific literature, systematization and structuring of information about the genetic algorithm are carried out: the main stages of the algorithm and the criteria for the end of the cycle are identified and described, the definitions of the concepts used in genetic algorithms are given, the operators of working with these algorithms are considered, a generalized model of the genetic algorithm in the form of a block diagram is constructed.

The conducted theoretical research allows us to draw a conclusion about the applicability of genetic algorithms in optimizing the solution of decision-making problems.

Ключевые слова: генетические алгоритмы, оператор скрещивания, мутация генетического набора, генетическая выборка, цикл генетического алгоритма.

Keywords: genetic algorithms, crossing operator, genetic set mutation, genetic selection, cycle of a genetic algorithm.

Естественный отбор является основным фактором эволюции.

Суть естественного отбора заключается в том, что в результате действий в популяции увеличивается число наиболее приспособленных особей, так как они имеют больше шансов на выживание и размножение.

Потомки получают лучшие качества от родителей вследствие генетического наследования. Но в природе не всегда побеждает сильнейший из-за нерегулируемых случайностей.

В отличие от природных явлений, программно-реализованные генетические алгоритмы предоставляют возможность принудительного выбора и сохранения лучших экземпляров набора.

Основная идея генетических алгоритмов заключается в том, что, используя принципы «естественного отбора», среди пробных решений выбирается наиболее качественное.

Генетические алгоритмы дают возможность оптимизировать функции дискретных переменных, непрерывные функции, компьютерные программы, а также, принимать решение о стратегии выполнения активности для достижения поставленной цели и сокращать перебор в сложных задачах.

Генетические алгоритмы применяются для настройки и обучения искусственной нейронной сети, задач компоновки, составления расписаний и игровых стратегиях, а также, робототехнике и создание моделей искусственной жизни.

Генетические алгоритмы используют такие понятия как:

– особь – одно решение задачи;

– популяция – несколько решений задач;

– скрещивание – обмен частями хромосом между двумя (может быть и больше) хромосомами в популяции;

– мутация – случайное изменение одной или нескольких позиций в хромосоме.

В начале алгоритма генерируется начальная популяция, которая является набором решений.

В свою очередь, эти решения будут становиться лучше, то есть эволюционировать, что приведет к наилучшему решению, удовлетворяющему условиям задачи.

Критерием окончания цикла в алгоритме может являться заданное количество поколений или схождение популяции до одной особи (рисунок 1).

Схождение популяции происходит в том случае, если все строки находятся в состоянии некоторого экстремума, и практически никак не изменяется.

В этом случае мутация почти никак не изменяет популяцию, а потомки представляют собой копии родителей с переменными участками хромосом. Эти особи склонны вымирать, так как имеют меньшую приспособленность [1, С. 14-15].

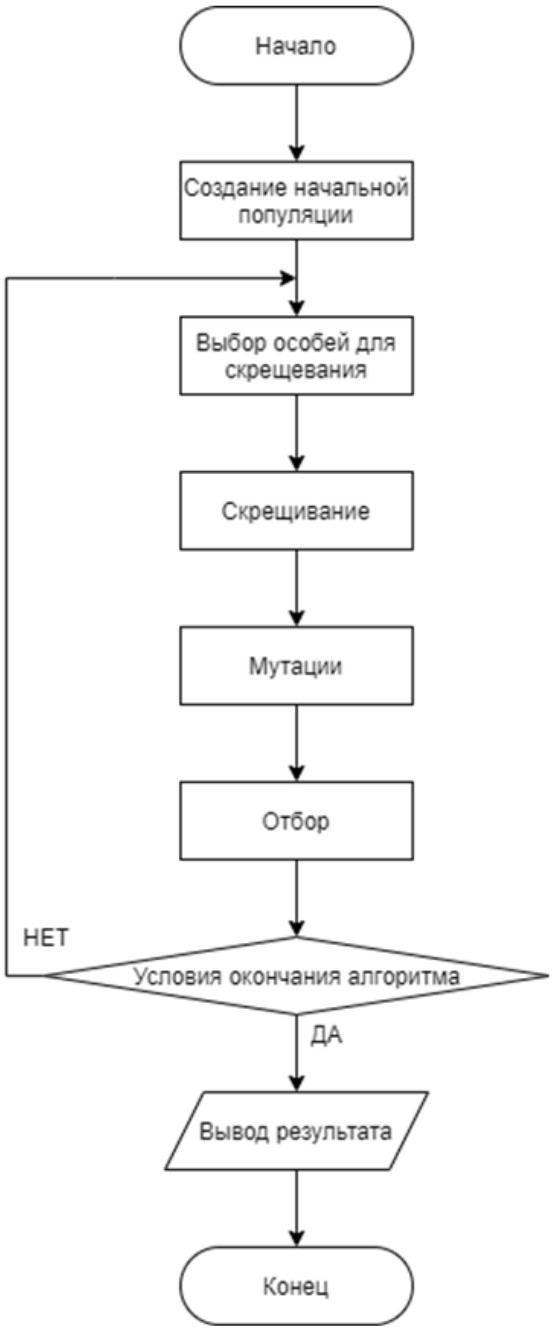

Рисунок 1. Графическая модель алгоритма

Реализация и эффективность генетических алгоритмов зависит от выбора операторов. Основными операторами этих алгоритмов являются мутация, отбор (селекция), скрещивание и выбор родителей (рисунок 2).

Использование чистых или модернизированных операторов приводит к получению генетических алгоритмов, которые пригодны для решения различных типов задач [4]. Рассмотрены наиболее распространённые операторы выбора пары, которые станут родителями:

Панмиксия является самым простым оператором отбора.

В данном операторе каждому члену популяции присваивается число от 1 до N, где N – это количество особей в популяции. При таком выборе некоторые из членов популяции не будут участвовать в процессе размножения, так как будут образовывать

пары сами с собой, а какие-то члены популяции примут участие в размножении несколько раз с различными особями популяции.

С ростом популяции, снижается эффективность алгоритма, поэтому данный алгоритм чувствителен к численности популяции.

Рисунок 2. Операторы генетических алгоритмов

Ингбридинг – метод, при котором оба родителя являются членами одной популяции, и первый родитель выбирается случайным образом, а второй родитель является ближайшим «родственником» к первому [3, С. 19].

При аутбридинге используется понятие схожести особей, в котором брачные пары формируются из максимально далеких по родству особей [1, С. 15].

Оператором скрещивания выступает рекомбинация, которая применяются сразу же после отбора предков для получения нового поколения. Смысл воспроизведения заключается в том, что потомки наследуют генную информацию от обоих родителей.

Следующим этапом после скрещивания выполняется этап мутации. Данный тип операторов необходим для вывода популяции из локального экстремума. Изменение случайно выбранного гена в хромосоме препятствует преждевременной сходимости популяции.

Для задач, использующих вещественные числа необходимо определить величину шага мутации — число, на которое будет изменяться значение гена при мутации.

Для особей, кодированных двоичным кодом, применяется двоичная мутация. Суть этой мутации заключается в том, что происходит случайное инвертирование гена: ноль заменяется единицей и наоборот.

Мутация, использующая понятие плотности, заключается в том, что каждый ген мутируется с заданной вероятностью. Существуют и другие виды мутаций, которые применяются для особи f, которая представляется как последовательность генов f_i : $f = f_1, \ldots, f_k$. Тогда можно использовать такие операторы, как:

1. Присоединение случайного гена из совокупности всевозможных значений генов к концу последовательности: $f \rightarrow f_1, \ldots, f_k, s$.

2. Вставка случайного гена из совокупности всевозможных значений генов в случайно выбранную позицию в последовательности: $f \rightarrow f_1, \ldots, f_{i-1}, s, f_i, \ldots, f_k$.

3. Удаление случайно выбранного гена из последовательности: $f \rightarrow f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_k$.

4. Обмен местами в последовательности двух соседей одного случайно выбранного гена: $f \rightarrow f_1, \ldots, f_{i+1}, s, f_{i-1}, \ldots, f_k$.

На этапе построения выборки из нового поколения применимы несколько типов операторов. Наиболее применимыми являются:

1. Отбор усечением. Для популяции подбирается целевая функция, и рассчитываются её значения для каждой особи набора. При отборе усечением используют популяцию, состоящую как из родителей, так и из особей потомков, отсортированную по возрастанию значений функции пригодности особей. Этот метод не имеет аналогов в естественной эволюции и обычно используется для больших популяций. При этом сначала отбираемые особи упорядочиваются согласно их значениям целевой функции. Затем в качестве родителей выбираются только лучшие особи. Далее, с равной вероятностью, среди них случайным образом выбирают пары, которые производят потомков. Вычисляется доля особей, пригодных для участия в отборе называемая порогом $T \in [0; 1]$, который используется для определения числа индивидов для скрещивания, то есть, определяет долю особей, начиная с самой сильнейшей, или как еще называют приспособленной, из которых будут выбираться лучшие [2]. Особи с высокой пригодностью входят в новую популяцию, причем одна и та же особь может встречаться несколько раз, а некоторые особи, имеющие пригодность выше пороговой, могут не попасть в новую популяцию.

2. Элитарный отбор создает промежуточную популяцию, которая включает в себя не только потомков, но и их родителей. А затем, члены этой популяции оцениваются, чтобы выбрать лучших представителей, которые и войдут в следующее поколение.

3. В отборе вытеснением выбор особи в новое поколение зависит не только от величины ее пригодности, но и от того, есть ли в формируемой популяции особь с аналогичным хромосомным набором. Отбор проводится не только из числа родителей, но и числа потомков. Из всех особей с одинаковой пригодностью и приспособленностью выбираются особи с разными генотипами. Данный алгоритм помогает достичь таких целей, как сохранение лучших найденных решений, обладающих различным генотипом и поддерживание различного генетического разнообразия. Из удаленных особей формируется новая популяция, то есть, популяция, не состоящая из особей, которые группируются около текущего найденного решения методом вытеснения [1, С. 27].

Вновь построенная выборка проверяется на соответствие условию завершения алгоритма и по результатам проверки делается вывод о запуске следующей итерации или прекращении процесса и выводе результата.

Выводы

Применение генетического алгоритма позволяет в условиях неопределённости выполнять подбор наиболее правильного решения с максимальным соблюдением всех ограничений, накладываемых на результат.

Алгоритм является итерационным: каждый цикл обрабатывает одну популяцию, первоначально сгенерированную случайным образом, а на каждом следующем повторении полученную в предыдущей итерации. Всего тело цикла состоит из трёх

этапов, для каждого из которых существуют несколько вариаций операторов. Выбор конкретной деятельности зависит от типа решаемой задачи, характеристик обрабатываемой популяции и ограничений, накладываемых на решение.

Направления дальнейших исследований включают в себя составление программ, использующих данный алгоритм для оптимизации вычислений.

Литература

1. Панченко, Т.В. Генетические алгоритмы [Текст]: учебно методическое пособие / под ред. Ю.Ю. Тарасевича. – Астрахань: Издательский дом «Астраханский университет», 2007. – 87 [3] с.

2. Лекция 3: Модификации генетических алгоритмов [Электронный ресурс]. – URL:https://clck.ru/WJ76c (дата обращения: 08.04.2021).

3. Гладков Л.А., Курейчик В.В., Курейчик В.М. Генетические алгоритмы / под ред. В.М. Курейчика. – 2-е изд. исправл. и доп. – М.: ФИЗМАТЛИТ, 2010. – 368 с.

4. Генетический алгоритм. Просто о сложном [Электронный ресурс]. – URL: https://clck.ru/WJ78W (дата обращения: 04.04.2021).

УДК 004.942

ИМИТАЦИОННАЯ МОДЕЛЬ МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ И ИССЛЕДОВАНИЕ НА ЕЕ ОСНОВЕ ПОКАЗАТЕЛЕЙ КАЧЕСТВА ОБСЛУЖИВАНИЯ ТРАФИКА РЕАЛЬНОГО ВРЕМЕНИ

A SIMULATION MODEL OF A MULTISERVICE COMMUNICATION NETWORK AND STUDY BASED ON IT OF THE QUALITY OF SERVICE INDICATORS FOR REAL-TIME

Живодерников А.Ю., Яговитов Д.С., Трофимов А.Ю.,
ФГКВОУ ВО «Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С.М. Буденного»,
г. Санкт-Петербург, Российская Федерация

A.Yu. Zhivodernikov, D.S. Yagovitov, A.Yu. Trofimov,
FSPMEI HE «Marshal Budyonny Military Signal Academy»,
St. Petersburg, Russian Federation

e-mail: sabir.81@mail.ru

Аннотация. Цель исследования: создание имитационной модели мультисервисной сети для исследования точности оценки показателей качества обслуживания в зависимости от точности оценки показателей качества функционирования мультисервисной сети связи в реальном масштабе времени на основе анализа разнородного трафика и проведения имитационных экспериментов. В разработанной модели мультисервисной сети связи использованы модели генераторов трафика, формирующие пакеты видеоконференцсвязи, пакеты речевого трафика, создающие агрегированные потоки с распределением Парето и экспоненциальным распределением. Также учитываются свойства самоподобия трафика и сочетания длительности *ON/OFF*-периодов. Применены положения теории графов, теории

массового обслуживания, теории вероятности, среда имитационного моделирования *NS*2 (*Network Simulator* – 2). На основе созданной имитационной модели мультисервисной сети связи рассчитываются значения потерь пакетов, задержки, вариации задержки (джиттер) как в информационном направлении связи, так и на каждом участке этого направления. При использовании полученных данных расчета возрастает вероятность уменьшения времени оценки для расчета показателей качества обслуживания разнородного трафика в мультисервисной сети связи в информационном направлении связи, тем самым уменьшая время реакции системы управления на управляющее воздействие.

Abstract. The purpose of the study: to create a simulation model of a multi-service network to study the accuracy of evaluating service quality indicators depending on the accuracy of evaluating the quality indicators of the functioning of a multi-service communication network in real time based on the analysis of heterogeneous traffic and conducting simulation experiments. The developed model of a multiservice communication network uses traffic generator models that form video conferencing packets, speech traffic packets that create aggregated flows with Pareto distribution and exponential distribution. The properties of traffic self-similarity and the combination of the duration of ON/OFF periods are also taken into account. Applied the provisions of graph theory, queuing theory, probability theory, and the NS2 simulation environment (Network Simulator – 2) are applied. Based on the created simulation model of a multiservice communication network, the values of packet loss, delay, and delay variations (jitter) are calculated) both in the information direction of communication, and in each section of this direction. When using the obtained calculation data, the probability of reducing the evaluation time for calculating the quality of service indicators of heterogeneous traffic in a multiservice communication network in the information direction of communication increases, thereby reducing the response time of the control system to the control action.

Ключевые слова: мультисервисная сеть связи, *QoS, NS2,* трафик реального времени.

Keywords: multiservice communication network, QoS, NS2, real-time traffic.

Анализ работ [1-3] показывает, что постоянное развитие сетей связи приводит к ужесточению требований к их параметрам.

Структурные элементы сетей связи имеют различную техническую оснащенность, функционируют с использованием различных сетевых технологий, используют множество протоколов и интерфейсов.

В связи с этим достаточно сложно определить четкие и прозрачные требования к элементам сети связи таким образом, чтобы выполнение данных требований обеспечивало заданное качество предоставляемых услуг пользователям.

В настоящее время, в связи с развитием высокоскоростных сетей связи, растет доля циркулирующего в них мультисервисного трафика (передача данных реального времени, речи, видео) [4].

Благодаря этому повышаются требования к качеству обслуживания *QoS (Quality of service)* трафика реального времени.

Во многих работах [1, 3, 5] было отмечено, что одним из важнейших свойств трафика реального времени является его структурная сложность, которая оказывает существенное влияние на своевременность обслуживания поступающих пакетов в узлах мультисервисной сети связи (МСС).

Для трафика реального времени характерны нестационарные свойства, которые моделируются потоками, имеющих сложную структуру и обладающие свойствами самоподобия.

Свойство самоподобия оказывает влияние на своевременность обработки трафика, циркулирующего в реальных сетях связи.

При этом показателем наличия данного свойства у трафика является коэффициент Херста, принимающий значения в диапазоне $H \in (0,5;1]$[4].

Таким образом, анализ параметров трафика (потери пакетов, задержка пакетов, джиттер) в режиме реального времени является актуальной задачей.

С учетом того, что имитационную модель можно разработать с любой детализацией процесса и явления, а это важная часть при выполнении задачи анализа мультисервисной сети связи, то имитационное моделирование применимо для проведения анализа параметров мультисервисной сети связи.

Для создания имитационной модели был выбран сетевой симулятор *NS*2.

Сетевой симулятор представляет собой программное средство для моделирования и анализа функционирования цифровых сетей с коммутацией пакетов.

Широкие возможности симулятора для исследования корректности и эффективности протоколов различных уровней, а также для моделирования разнородных приложений способствовали его быстрому распространению.

Главные особенностями *NS*2 можно считать:

– открытый код и свободное распространение;

– модульный принцип построения и открытая архитектура;

– возможность модификации ядра программы и гибкая настройка в соответствии с требованиями конкретного пользователя;

– мультиоперационность, на данный момент работоспособны под управлением *Unix*-операционных систем, а также всех версий ОС *Windows*;

– широкий диапазон методов и средств абстрагирования;

– наличие библиотеки сетевых топологий и генераторов трафика.

Иллюстрация этапов моделирования, отображающая процесс моделирования, представлена на рисунке 1.

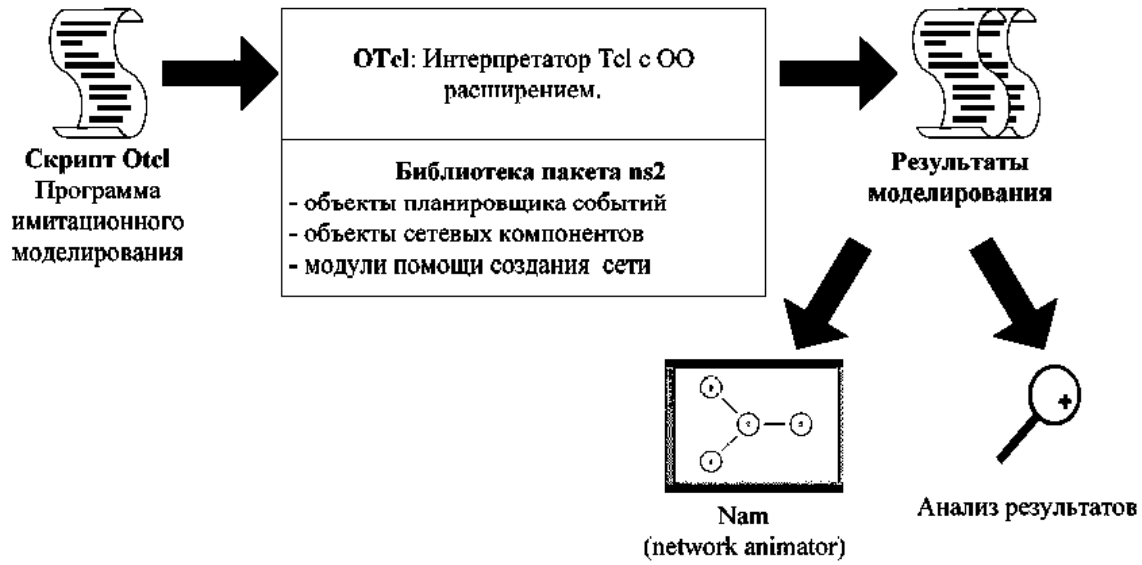

Рисунок 1. Иллюстрация этапов моделирования в *NS2*

Используемая схема моделирования представлена на рисунке 2.

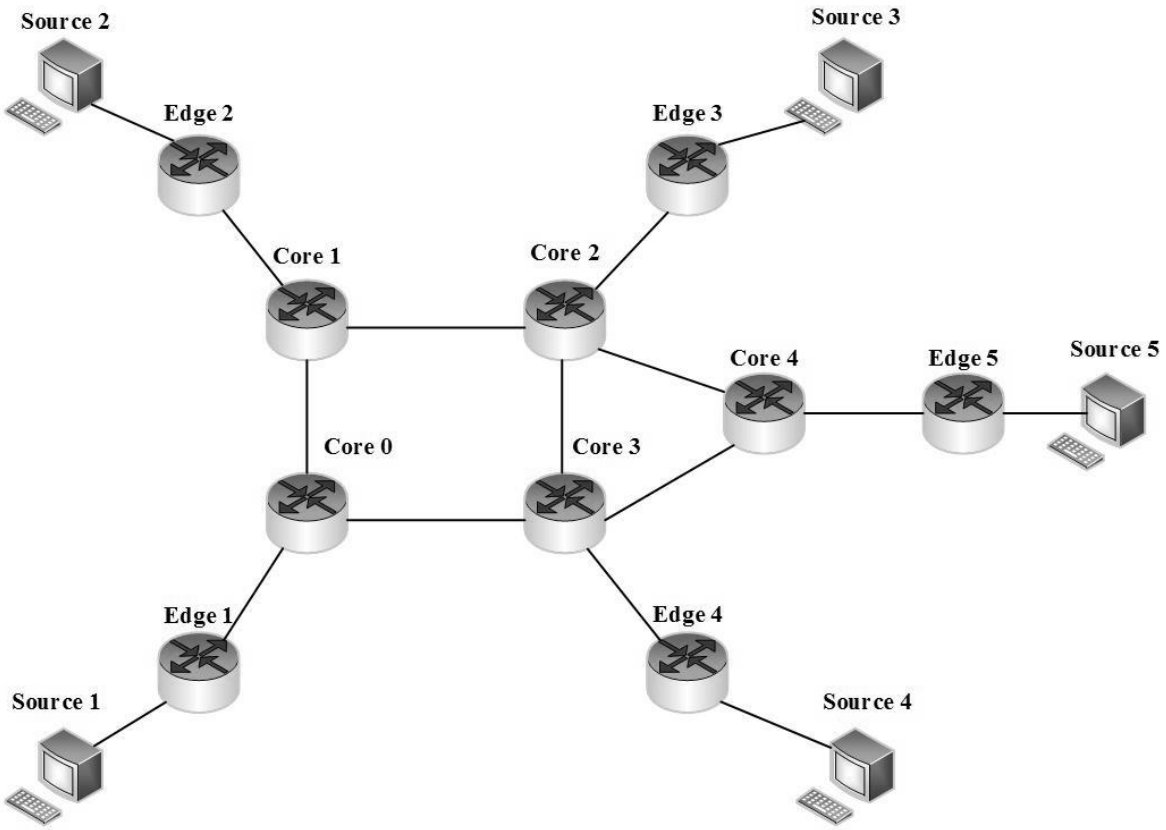

Рисунок 2. Схема моделирования в *NS2*

Схема моделирования построена таким образом, чтобы максимально сымитировать реальную ситуацию в сети.

Источники (*Source*) формируют потоки различных приложений, которые поступают на пограничные маршрутизаторы (*Edge*) узлов доступа, а затем передаются через маршрутизаторы транспортной сети (*Core*).

Исследуемый трафик создается приложениями видеоконференцсвязи (*VKS*) и *IP*-телефонии (*VoIP*).

Каналы связи между маршрутизаторами дуплексные.

В маршрутизаторах реализован алгоритм управления очередью *RED* (*Random Early Detection* – случайного раннего обнаружения).

Потоки передаются между источниками Source, распределенных согласно таблицы 1.

Таблица 1 – Распределение потоков

Source 1		*Source* 2		*Source* 3		*Source* 4		*Source* 5	
Id источника	Приложение	*Id* источника	Приложение	*Id* источника	Приложение	*Id* источника	Приложение	*Id* источника	Приложение
1	*VoIP*	6	*VoIP*	14	*VoIP*	10	*VoIP*	2	*VoIP*
3	*VKS*	7	*VoIP*	15	*VKS*	11	*VKS*	18	*VKS*
4	*VKS*	8	*VKS*	16	*VKS*	12	*VoIP*	19	*VKS*
5	*VoIP*	9	*VKS*	17	*VoIP*	13	*VKS*	20	*VoIP*

Имеется 20 источников, формирующих *IP*-пакеты приложений (см. таблицу 1) с использованием протокола транспортного уровня *UDP*.

Процедура формирования пакетов описывается *ON/OFF*-моделью.

Чередование *ON/OFF*-периодов происходит через случайные промежутки времени со средними интервалами T_1, T_2 для *ON*-периода каждого источника в зависимости от применяемого приложения и T_3 для *OFF*-периода.

Интенсивность поступления пакетов от каждого источника в *ON*-период имеет случайный характер со средними значениями интенсивности λ_1, λ_2.

ON/OFF генератор трафика Парето в симуляторе является приложением, создающим трафик согласно закону распределения Парето.

При постоянном размере пакетов период *ON* и *OFF* также распределены по этому закону.

Такой генератор может быть использован для моделирования агрегированного трафика, который обладает медленно-затухающим распределением.

Используя исходные данные, генератор производит вычисления:

$$interval = \frac{packetsize \cdot 8}{rate}, \quad (1)$$

где *interval* – величина, показывающая какой интервал времени занимает передача пакета (измеряется в секундах);
packetsize – размер одного пакета в битах;
rate – скорость потока в течение периода *ON*.

$$burstlen = \frac{burst\_time}{interval}, \quad (2)$$

где *burstlen* – величина, показывающая среднее количество пакетов в пачке;
burst_time – время периода *ON*.

В каждом цикле проводится расчет двух случайных величин:

– *next_burstlen* – количество пакетов в пачке, для передачи в следующем *ON*-периоде;

– *next_idle_time* – длина следующего *OFF*-периода в секундах.

Затем генератор трафика проводит расчет величины *next_burstlen* по имеющимся значениям *burstlen* и *shape* (характеристический показатель распределения).

Отправка всех *next_burstlen* пакетов и расчет величины *next_idle_time* в соответствии со значениями *idle_time* (время *OFF*-периода) и *shape*.

Далее осуществляется переход в режим ожидания в течении времени *next_idle_time* и возврат к расчету величины *next_burstlen*.

Обозначим плотность вероятности распределения Парето $f(x)$, а математическое ожидание $E(x)$:

$$f(x) = \frac{\alpha b^{\alpha}}{x^{\alpha+1}}, x \geq \mathrm{b}, \quad (3)$$

где α – характеристический показатель распределения;
b – минимальное значение величины *x* (масштабный коэффициент).

$$E(x) = \frac{b\alpha}{\alpha - 1},\ \alpha > 1. \quad (4)$$

В таком случае:

$$burstlen = E(x) = \frac{b_1\alpha}{\alpha - 1}, \quad (5)$$

$$idle\_time = E(y) = \frac{b_2\alpha}{\alpha - 1}. \quad (6)$$

Тогда:

$$b_1 = \frac{burstlen \cdot (\alpha - 1)}{\alpha}, \quad (7)$$

$$b_2 = \frac{idle\_time \cdot (\alpha - 1)}{\alpha} + interval. \quad (8)$$

Исходными данными для моделирования выбраны параметры трафика, указанные в таблице 2.

Таблица 2 – Исходные данные

Параметр	Речь	Видео
Скорость потока, кбит/с	64	384
Закон распределения интенсивности передачи пакетов	Парето	Парето
Количество байт в пакете	306	1458
Интенсивность передачи λ_1, λ_2 пакет/сек	22	86
Длительность *ON*-периода, T_1, T_2, сек	180	120
Длительность *OFF*-периода, T_3, сек	30	30
Характеристический показатель распределения, α	1,5	1,5

Опытным путем было определено, что интервалами времени для формирования значений показателей качества являются интервалы времени длительностью 1 час.

При заданных исходных данных и результатов, полученных в ходе имитационного моделирования, предлагается проводить расчеты показателей качества обслуживания при помощи метода косвенной оценки. Для этого внесем следующие ограничения и допущения:

– представим ветвь графа сети с точки зрения теории систем массового обслуживания в виде модели M/M/1 (по классификации Кендалла-Башарина);

– функция распределения вероятностей распределена по экспоненциальному закону;

Исходя из этого можно рассчитать сумму интенсивностей потоков на ветви по формуле:

$$\Lambda_{вет} = \sum_{i,j}^{k} \lambda_{i,j} \quad , \tag{9}$$

где k – количество потоков на ветви.

Получив значение суммарной $\Lambda_{вет}$, можно найти вероятность потерь на ветви для k потоков:

$$P_{вет} = \frac{(1-\rho_{вет})\rho_{вет}^{w}}{1-\rho_{вет}^{w+1}}, \tag{10}$$

где w – размер очереди в буфере.

В свою очередь функция распределения времени обслуживания определяется по формуле:

$$G_T(t) = p(T_{обсл} < t). \tag{11}$$

Плотность вероятности рассчитываем по формуле:

$$g(t) = \frac{dG(t)}{dt}. \tag{12}$$

В свою очередь, среднюю вероятность своевременной доставки можно рассчитать для всей сети:

$$p_{ф} = \sum_{I}\sum_{R} p_{i,r}\, p_{фi}(r),\ i = \overline{1,I}, \sum_{I}\sum_{R} p_{i,r} = 1, \tag{13}$$

где $p_{фi}(r)$ – вероятность своевременной доставки в i-ом потоке;

$p_{i,r}$ – вероятность попадания сообщения r-приоритета в i-й потоке, определяемая как часть общего трафика, в i-м информационном направлении.

Указанные расчеты можно провести для любой модели ветви, тем самым получая выигрыш во времени оценки для расчета показателей качества обслуживания «из конца в конец». Это в свою очередь уменьшает время реакции системы управления на управляющее воздействие.

Литература

1. Бахарева Н.Ф., Карташевский И.В., Тарасов В.Н. Анализ и расчет непуассоновских моделей трафика в сетях ЭВМ. // Инфокоммуникационные технологии, т. 7, №4, 2009. С. 61-66.

2. Тарасов В.Н., Бахарева Н.Ф., Горелов Г.А. Математическая модель трафика с тяжелохвостным распределением на основе системы массового обслуживания H2/M/1 // Инфокоммуникационные технологии. Т. 12. №3. 2014 С. 36-41.

3. Макаренко С.И. Преднамеренное формирование информационного потока сложной структуры за счет внедрения в систему связи дополнительного имитационного трафика. // Вопросы кибербезопасности. №3 (4), 2014. С. 7-13.

4. Ушанев К.В. Имитационные модели системы массового обслуживания типа Pa/M/1, H2/M/1 и исследование на их основе качества обслуживания трафика со сложной структурой. // Системы управления, связи и безопасности №4, 2015. С 217-251.

5. Карташевский И.В., Буранова М.А. Влияние механизмов управления QoS на показатели качества обслуживания мультимедийного трафика сети Internet // T-comm: телекоммуникации и транспорт. №8, 2013. С. 54-60.

СЕТИ И ТЕЛЕКОММУНИКАЦИИ

УДК 004.7

ОБРАЗОВАТЕЛЬНЫЙ ПРОДУКТ D-LINK ДЛЯ ОБУЧЕНИЯ СЕТЕВЫМ ТЕХНОЛОГИЯМ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ НЕФТЕГАЗОВОГО СЕКТОРА ЭКОНОМИКИ

D-LINK EDUCATION PRODUCT FOR LEARNING NETWORK TECHNOLOGIES IN THE DIGITAL TRANSFORMATION OF THE OIL AND GAS ECONOMY SECTOR

[1]Ромасевич П.В., [2]Смирнова Е.В.,
[1]ФГАОУ «Волгоградский государственный университет»,
г. Волгоград, Российская Федерация
[2]ООО «Д-Линк Трейд»,
г. Москва, Российская Федерация

P.V. Romasevich[1], E.V. Smirnova[2],
[1]FSAEI «Volgograd State University»,
Volgograd, Russian Federation
[2]Ltd. «D-Link Trade»,
Moscow, Russian Federation

e-mail: promasevich@dlink.ru

Аннотация. Цифровизация производственных процессов топливно-энергетического комплекса (ТЭК) предполагает превентивное создание отказоустойчивой инфокоммуникационной инфраструктуры предприятий данного сектора экономики и обучение ИТ-специалистов по её эксплуатации и развитию. Это органично интегрирует ведомственный проект Министерства энергетики «Цифровая энергетика», неотъемлемой частью которой является цифровизация нефтегазового сектора, с направлениями «Информационная инфраструктура» и «Кадры для цифровой экономики» Национальной программы «Цифровая экономика Российской Федерации». В этой связи оригинальный образовательный продукт компании D-Link может быть востребован для подготовки и переподготовки специалистов по сетевым технологиям для создания, эксплуатации и модернизации инфокоммуникационной инфраструктуры предприятий нефтегазовой сферы.

Abstract. Digitalization of the fuel and energy complex (FEC) assumes preventive creation of failsafe infocommunication infrastructure of this economy sector and training of IT specialists in her operation and development. This organically integrates the departmental Energy Ministry project “Digital Energy”, with the areas “Information Infrastructure” and “Personnel for the Digital Economy” of the National Program “Digital Economy of the Russian Federation”. In this regard, the original educational product of D-Link may be required for the training and retraining of specialists in network technologies for the creation, operation and modernization of the information and communication infrastructure of oil and gas enterprises.

Ключевые слова: цифровая энергетика, нефтегазовый сектор, цифровая трансформация, цифровая экономика Российской Федерации, кадры для цифровой экономики, образовательный продукт, D-Link.

Keywords: digital energy, oil and gas sector, digital transformation, digital economy of the Russian Federation, personnel for digital economy, educational product, D-Link.

Развитие нефтегазового сектора экономики на современном этапе невозможно без цифровизации всех производственных процессов – от разведки месторождений и добычи сырья, до глубокой переработки и транспортировки потребителю.

Эту цель и соответствующие задачи регламентирует ведомственный проект Министерства энергетики «Цифровая энергетика» до 2024 года [1], который выстраивает траектории цифровой трансформации отрасли в целом, и нефтегазового сектора в частности, в соответствии с Национальной программой «Цифровая экономика Российской Федерации» [2], реализуемой в настоящее время во исполнение указов Президента Российской Федерации Путина В.В. от 09.05.2017 №203 «О стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» [3] и 07.05.2018 № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» [4], в которых определены национальные цели и стратегические задачи развития Российской Федерации на период до 2030 года.

На этой основе крупные игроки нефтегазового рынка разработали и реализуют собственные стратегии цифровой трансформации.

В качестве примера можно упомянуть концепцию цифровой трансформации «Роснефть-2022» ПАО «Роснефть» [5], включающую в себя направления:

– цифровое месторождение,
– цифровой завод,
– цифровая цепочка поставок,
– цифровой трейдинг,
– цифровая АЗС,
– цифровой рабочий.

Цифровизация производственно-логистических процессов предполагает превентивное создание безопасной и отказоустойчивой инфокоммуникационной корпоративной инфраструктуры и обучение специалистов по ее эксплуатации и развитию.

Это органично интегрирует ведомственный проект Минэнерго и корпоративные программы цифровой трансформации с направлениями Национальной программы «Цифровая экономика Российской Федерации» «Кадры для цифровой экономики» и «Информационная инфраструктура», которые должны обеспечить возможность использования стационарного и мобильного широкополосного доступа для работы корпоративных сетевых приложений, а также сегменты сетей NB-IOT и LPWAN для обеспечения работы телеметрической инфраструктуры.

Инфокоммуникационная структура современного предприятия должна способствовать снижению производственных издержек и может состоять из подсистем видеонаблюдения, мониторинга передвижных средств, телеметрической инфраструктуры сбора первичной обработки информации с датчиков производственных площадок, агрегации и обработки «больших» данных в ЦОД и выдачи сводной аналитической информации для принятия решений (рисунок 1, [6]):

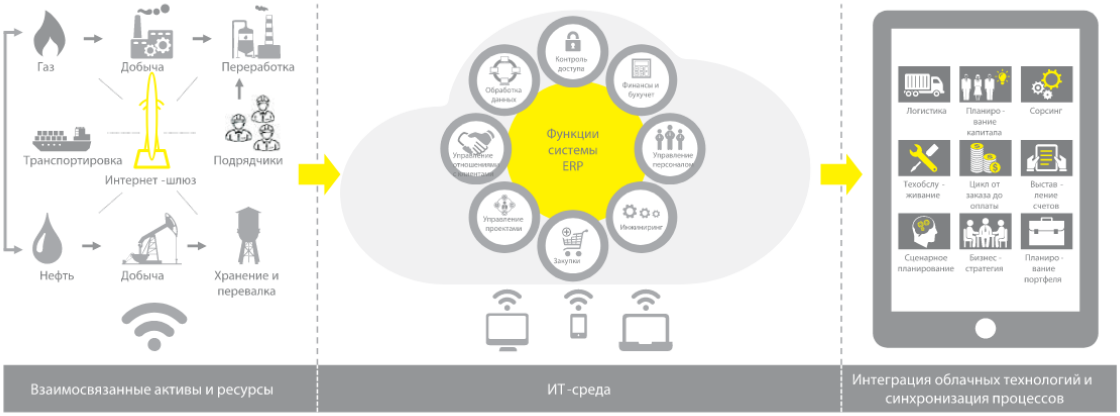

Рисунок 1. Архитектура цифровой трансформации

Основой ИТ-архитектуры предприятия нефтегазового сектора является безопасная и отказоустойчивая телекоммуникационная инфраструктура корпоративной сети с возможностью мобильного доступа к данным по всей его территории.

При этом в современном международном контексте построение и модернизация инфокоммуникационной экосистемы нефтегазового сектора на «неамериканских» продуктах в настоящее время является вопросом безопасности отрасли и страны в целом.

Для создания, эксплуатации и развития безопасной и отказоустойчивой распределенной телекоммуникационной инфраструктуры компаний нефтегазового сектора необходимо наличие ИТ-специалистов с актуальными компетенциями в области сетевых технологий.

По оценкам АПКИТ, в ближайшие годы потребность в ИТ-специалистах различных компетенций составит около 300 тысяч человек ежегодно [7]. Ситуация обостряется также тем, что ИТ-специалистов нужно готовить уже сейчас, поэтому образовательные ресурсы, находящиеся в стадии разработки с последующей апробацией, вряд ли успеют стать востребованными для подготовки кадров в обозримое будущее.

В этой связи комплексный образовательный продукт (рисунок 2) мирового производителя активного сетевого оборудования D-Link [8] который компания развивает более 15 лет, может быть востребован учебными заведениями для подготовки и переподготовки специалистов по сетевым технологиям для предприятий нефтегазовой отрасли.

D-Link основана в 1986 году и является первым производителем активного сетевого оборудования, созданного за пределами США. За двадцать два года работы в России компания накопила солидный методический опыт производственного обучения сетевым технологиям, поставляя оборудование в различные сегменты экономики. Понимание потребностей рынка и практических запросов ИТ-специалистов позволило создать актуальный образовательный продукт обучения сетевым технологиям.

Образовательным продуктом могут бесплатно воспользоваться высшие и средние специальные учебные заведения для подготовки и переподготовки специалистов по сетевым технологиям для предприятий нефтегазовой отрасли.

Для получения и использования образовательного продукта учебному заведению необходимо заключить Соглашение о сотрудничестве с компанией D-Link, выбрав удобную форму взаимодействия – академический партнер и/или авторизованный учебный центр [9], каждая из которых обладает определенным набором возможностей.

В настоящий момент 63 учебных заведения России являются академическими партнерами, а 20 вузов также организовали на своей базе авторизованные учебные центры D-Link.

Рисунок 2. Комплексный образовательный продукт D-Link

В настоящее время образовательный продукт D-Link предлагает восемь обучающих программ:

– «Основы сетевых технологий. Часть 1: Основы передачи и коммутации данных в компьютерных сетях».
– «Основы сетевых технологий. Часть 2: Основы беспроводных сетей Wi-Fi».
– «Основы сетевых технологий. Часть 3: Технологии TCP/IP».
– «Технологии коммутации современных сетей Ethernet».
– «Основы сетевой безопасности. Часть 1: Межсетевые экраны».
– «Основы сетевой безопасности. Часть 2: Технологии туннелирования».
– «Использование Linux при программировании».
– «Введение во встраиваемые системы. Часть 1: Использование Linux и микропроцессорные системы».

Каждая программа обучения включает в себя лекции, презентации к лекциям, методические указания к лабораторным работам, оборудование для учебных классов.

Программы построены таким образом, чтобы их можно было изучать как по отдельности, так и в комплексе. Оборудование для лабораторных классов подобрано с учетом возможности его использования сразу в нескольких программах обучения.

Преподавателям учебных заведений, желающих использовать материалы D-Link, предоставляется техническая и методическая поддержка процесса обучения.

Портал дистанционного обучения может быть использован преподавателями для проведения вебинаров, тестирования и иных учебных мероприятий для студентов.

Программы D-Link доступны для изучения:

– в партнерских учебных заведениях,
– в офисах D-LINK,
– на бесплатном портале дистанционного обучения и сертификации [10].

В настоящее время по четырем программам обучения можно сдать сертификационный экзамен в режиме онлайн. По остальным программам предусмотрен очный экзамен, включающий теоретическую и практическую части. Его можно сдать в любом авторизованном учебном центре D-Link или офисе компании [9].

Помимо перечисленного образовательный продукт включает в себя электронную библиотеку, печатные издания курсов D-Link, каналы в Youtube и Telegram, представительства в социальных сетях Facebook, VK, Instagram.

Печатные издания курсов D-Link, разработанных в сотрудничестве с преподавателями МГТУ им. Н.Э. Баумана и МГУ им. М.В. Ломоносова, имеют гриф УМО для направлений «Информатика и вычислительная техника», «Прикладная математика и информатика» и «Фундаментальная информатика и информационные технологии», и по мнению авторов статьи могут быть использованы в рамках любого направления IT-подготовки, где предусмотрен объем часов по компьютерным сетям.

Уделяя внимание внедрению комплексного образовательного продукта в учебный процесс вузов, вендор оказывает техническую и методическую поддержку учебным заведениям в создании лабораторных классов, обновлению учебных материалов, сертификации преподавателей и т.п. Для этого D-Link проводит цикл вебинаров для профессорско-преподавательского состава учебных заведений, посвященных образовательным ресурсам компании D-Link, которые могут быть полезны для преподавания сетевых технологий в рамках любого направления ИТ-подготовки студентов всех форм обучения:

– учебные курсы и образовательные ресурсы D-Link. Опыт использования на кафедре «Телекоммуникационных систем» Волгоградского государственного университета.
– преподавание сетевых технологий на основе комплекса курсов D-Link «Основы сетевых технологий. Часть 1-3».
– переподготовка и повышение квалификации персонала операторов связи на основе курса «Технологии коммутации современных сетей Ethernet».
– особенности использования комплекса курсов D-Link «Основы сетевых технологий. Часть 1-3» для студентов заочной формы обучения.

Информацию о времени проведения вебинаров можно получить от авторов статьи или в новостной ленте на официальном сайте компании D-Link [12].

Компания D-Link является ведущим мировым производителем сетевого оборудования, предлагающим широкий набор решений для создания локальных сетей Ethernet/Fast Ethernet/Gigabit Ethernet, построения беспроводных сетей и организации широкополосного доступа, передачи изображений и голоса по IP (VoIP). В 2012 году компания открыла в Российской Федерации собственное производство, сертифицированное в соответствии с требованиями ГОСТ Р ИСО 9001-2008 (ISO 9001:2008). В РФ офисы компании D-Link открыты в Москве, Санкт-Петербурге, Екатеринбурге, Калининграде, Кемерово, Краснодаре, Красноярске, Новосибирске, Омске, Перми, Ростове-на-Дону, Рязани, Самаре, Туле, Уфе, Хабаровске и Ярославле. В Брянске, Казани, Тюмени и Челябинске работают региональные представители компании.

Авторизованные учебные центры работают в Москве, Санкт-Петербурге, Екатеринбурге, Ижевске, Кемерово, Магнитогорске, Новосибирске, Омске, Оренбурге, Перми, Ростове-на-Дону, Рязани, Туле и Ярославле.

Литература

1. Ведомственный проект «Цифровая энергетика». Текст: электронный. – URL:https://clck.ru/WKZnR
2. Национальная программа «Цифровая экономика Российской Федерации» утвержденная протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. №7. Текст: электронный. – URL:https://clck.ru/WKZqk
3. Указ Президента Российской Федерации от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // Собрание законодательства РФ. – 15.05.2017 г. – №20 – С. 9079-9080.
4. Указ Президента Российской Федерации от 07.05.2018 г №204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» // Собрание законодательства РФ. – 14.05.2018 г. – №20 – С. 10171-10181.
5. Стратегия Роснефть-2022. – URL: https://clck.ru/VrKwA
6. А. Козловский. С чего начинается путь в цифровую реальность? Текст: электронный. – URL:https://clck.ru/WKa2E
7. «ИТ-кадры для цифровой экономики в России», Текст: электронный. – URL:https://clck.ru/WKa5R
8. Официальный сайт D-Link. – URL:https://www.dlink.ru/ru/education/3/
9. Официальный сайт D-Link. – URL:https://www.dlink.ru/ru/education/5/
10. Официальный сайт D-Link. – URL:https://learn.dlink.ru

СИСТЕМЫ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ И ГИС-ТЕХНОЛОГИИ

УДК 004.62

ИССЛЕДОВАНИЕ МЕТОДОВ СКЕЛЕТИЗАЦИИ РАСТРОВЫХ ИЗОБРАЖЕНИЙ ТОПОГРАФИЧЕСКИХ КАРТ

RESEARCH METHODS OF SKELETIZATION OF RASTER IMAGES OF TOPOGRAPHIC MAPS

Чечет Д.В., Трубаков Е.О.,
ФГБОУ ВО «Брянский государственный технический университет»,
г. Брянск, Российская Федерация

D.V. Chechet, E.O. Trubakov,
FSBEI HE “Bryansk state technological university”,
Bryansk, Russian Federation

e-mail: checkdimon@gmail.com

Аннотация. На данный момент имеется большое количество данных, представленных на твердых носителях. Для их перевода необходимо произвести ряд операций. Одним из таких трудоемких действий является векторизация растровых карт. Скелетизация – это составляющий элемент процесса векторизации растрового изображения. Данный этап векторизации является морфологической операцией и является сложным техническим процессом, в ходе которого преобразуется предварительно бинаризованное изображение в набор линий, преобразуемые в дальнейшем в векторы. В данной статье были рассмотрены наиболее часто реализуемые алгоритмы скелетизации, такие как: алгоритм Zhang-Suen, алгоритм Lee, алгоритм Guo-Hall, алгоритм морфологических преобразований, алгоритм средней оси. Для оценки качества работы алгоритмов скелетизации был выбран набор критериев, таких как: точность, полнота, F-мера (значение, являющееся средневзвешенным между точностью и полнотой), связность контура и скорость выполнения алгоритма. Для проведения эксперимента было выбрано изображение часто встречающегося объекта на растровых картах – река, имеющая сложный набором контуров. В результате проведенного исследования было выявлено, что наиболее точный результат был получен с помощью алгоритма Lee, а самый наихудший, но при этом самый быстрый – с помощью алгоритма средней оси.

Abstract. At the moment, there is a large amount of data presented on hard media. To transfer them, you need to perform a number of operations. One of such time-consuming actions is the vectorization of raster maps. Skeletonization is an integral part of the bitmap vectorization process. This stage of vectorization is a morphological operation and is a complex technical process, during which a preliminary binarized image is converted into a set of lines, which are subsequently converted into vectors. In this article, the most frequently implemented skeletonization algorithms were considered, such as: Zhang-Suen algorithm, Lee algorithm, Guo-Hall algorithm, morphological transformation algorithm, middle axis algorithm. To assess the quality of the skeletonization algorithms, a set of criteria was selected, such as: accuracy,

completeness, F-measure (a value that is weighted average between accuracy and completeness), contour connectivity and algorithm execution speed. For the experiment, we chose an image of a frequently encountered object on raster maps — a river with a complex set of contours. As a result of the study, it was found that the most accurate result was obtained using the Lee algorithm, and the worst, but at the same time the fastest, was obtained using the middle axis algorithm.

Ключевые слова: векторизация, растровые карты, алгоритмы скелетизации, обработка изображений, бинарное изображение, оценка качества.

Keywords: vectorization, raster maps, skeletonization algorithms, image processing, binary image, quality assessment.

В процессе векторизации растровой карты, объекты на изображении необходимо разделить на линейные и полигональные [1].

Для линейных объектов, предварительно бинаризированных, применяется морфологическая задача скелетизации, которая утоньшает линию, удаляя тем самым пиксели, до тех пор, пока это возможно в соответствии с алгоритмом конкретного метода скелетизации.

Согласно данным из работы [2] всего существует около 300 методов скелетизации описанных в 1000 разных научных исследованиях.

Для проведения данного исследования были выбраны наиболее часто реализуемые методы:

1. Алгоритм Zhang-Suen, разработанный в 1984 году [3], который на каждой итерации осуществляет проверку на возможность удаления пикселя с помощью двух шагов в логической маске пикселей размером 3x3.
2. Алгоритм Lee, разработанный в 1994 году [4] для трехмерных объектов, но также подходящий для использования при работе с двумерными. Алгоритм предусматривает удаления пикселя только при соответствии нескольким условиям.
3. Алгоритм Gou-Hall, разработанный в 1989 году [5], каждая итерация которого состоит из двух шагов и проверяет возможность удаления пикселя с помощью логической маске размером, определяемым на каждой конкретной итерации.
4. Алгоритм морфологических преобразований [6] работает по такому же принципу, что и скелетизация: удаление пикселей с помощью операций эрозии и дилатации при условии, что не будет нарушена связность скелета.
5. Алгоритм средней оси, разработанный в 1982 году [7], позволяет удалить лишние пиксели, не нарушая скелета, а также предусматривает возможность хранения информации ширине точки до проведения утоньшения.

Оценка результатов работы методов скелетизации не имеет единого подхода к выбору методик и критериев оценки. При выполнении эксперимента для оценки качества результатов скелетизации была выбрана эмпирическая контролируемая методика оценки [8], которая включает в себя набор критериев:

1. Точность P – отношение количества верно определенных элементов в скелете к общему количеству элементов полученного скелета, найденных в результате действия алгоритма.

$$P = \frac{TP}{S},$$

2. Полнота R – отношение количества верно определенных элементов в скелете к общему количеству элементов эталонного скелета.

$$R = \frac{TP}{B},$$

3. F-мера – среднее взвешенное значение между точностью и полнотой. Чем ближе параметр F-мера к 1, тем выше степень соответствия полученного скелета эталонному.

$$F = \frac{2 * P * R}{P + R},$$

4. Связность контура C – отношение количества концевых точек найденного скелета в результате действия алгоритма к количеству концевых точек эталонного скелета.

$$C = \frac{N_S}{N_B},$$

5. Скорость выполнения – количество секунд, за которое происходит процесс скелетизации предварительно бинаризованного растрового изображения.

Для проведения эксперимента в качестве линейного объекта было использовано изображение формата PNG размером 5103x3712, на котором изображен участок реки, имеющей множество искривлений и ответвлений.

В результате выполнения алгоритмов скелетизации было получено 5 результирующий изображений, которые, для наглядности, были дополнены оригинальным изображением, бинаризованным вариантом и изображением, содержащем идеальный скелет (рисунок 1).

Тестирование проводилось на персональном компьютере со следующими характеристиками: операционная система Windows 10 x64, процессор Intel(R) Core(TM) i7-7700HQ CPU @ 2.80 GHz 2.80 GHz, 16 Гб ОЗУ памяти формата DDR4, видеокарта GeForce GTX 1060.

Результаты исследования представлены в таблице.

Таблица – Значения критериев оценки качества алгоритмов скелетизации

Алгоритм	C	Скорость выполнения, с	P	R	F-мера
Zhang-Suen	1,9334	0,71	0,4643	0,9286	0,6191
Lee	1,4	1,79	0,6191	0,9286	0,743
Guo-Hall	2,3334	27,5	0,3824	0,9286	0,5418
Морфологические преобразования	2,2	15,97	0,4063	0,9286	0,5653
Средней оси	8,0667	0,08	0,1075	0,9286	0,1927

Выводы

По результатам проведенного эксперимента было выяснено, что алгоритм Lee показал себя лучше с точки зрения параметров точность и F-мера и связность, чем алгоритм все остальные алгоритмы.

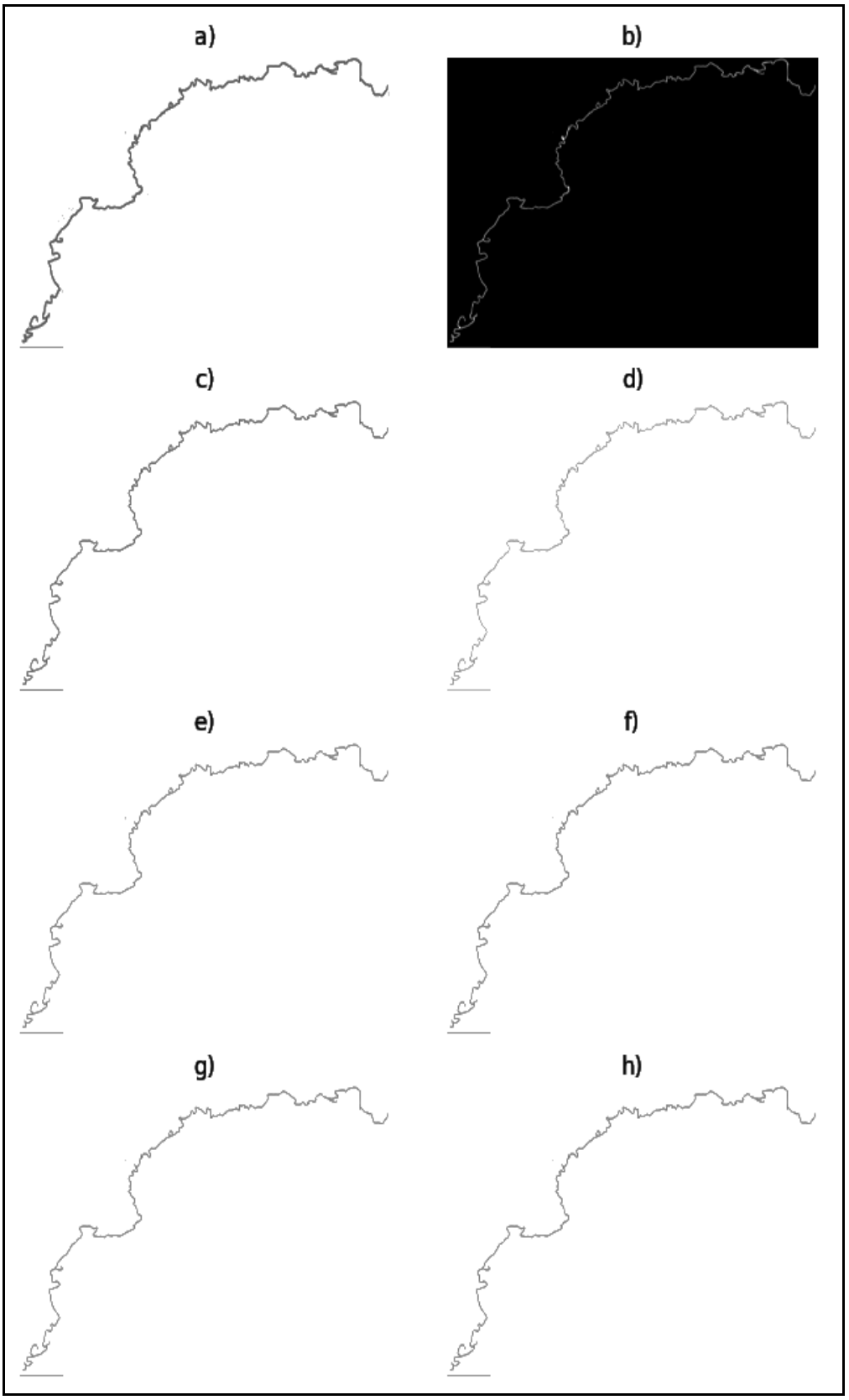

Рисунок 1. Результаты работы алгоритмов скелетизации:
a) исходное изображение; b) бинаризованное изображение; c) эталонный скелет;
d) результат алгоритма средней оси; e) результат алгоритма Zhang-Suen;
f) результат алгоритма Lee; g) результат алгоритма Guo-Hall
h) результат морфологических преобразований

Абсолютно все алгоритмы определили одинаковое количество верных элементов, поэтому значения полноты являются равными.

Стоит заметить, что скорость выполнение алгоритмов не зависит от их точности. Так, например, разница во времени выполнения алгоритма Zhang-Suen и алгоритма морфологических преобразований в 22,5 раза, но алгоритма Zhang-Suen оказался немного точнее. Самый быстрым является алгоритм средней оси, но в то же время он является очень неточным, о чем свидетельствуют самые низкие результаты по всем остальным сравниваемым критериям.

Стоит заметить, что алгоритм Lee, показавший наилучшие результаты, изначально был разработан для трехмерной скелетизации, поэтому использовать его при двумерной скелетизации нужно с осторожностью, а в некоторых случаях лучше использовать алгоритм Zhang-Suen, который уступает в точности, но при этом работает быстрее.

Литература

1. Сташевский, С.Ю. Алгоритм векторизации растровых изображений в общем виде / С.Ю. Сташевский // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2004. – №1 (9). – С. 124-130.

2. Waleed Abu-Ain. Skeletonization Algorithm for Binary Images / Waleed Abu-Ain, Siti Norul Huda Sheikh Abdullah, Bilal Bataineh, Tarik AbuAin // Procedia Technology. – 2013. – том 11, С. 704-709.

3. Zhang, T.Y. A Fast Parallel Algorithm for Thinning Digital Patterns / T.Y. Zhang, C.Y. Suen // Commun. – 1984. – ACM 27, С. 236-239.

4. Lee, T.C. Building skeleton models via 3-D medial surface/axis thinning algorithms / T.C. Lee, R.L. Kashyap, C.N. Chu // Computer Vision, Graphics, and Image Processing. – 1994. – №56(6), С. 462-478.

5. Guo, Z. Parallel Thinning with two Subiteration Algorithms / Z. Guo, R.W. Hall // Communications of the ACM. – 1989. – том 32, №3, С. 359-373.

6. Soille P. Morphological Image Analysis / P. Soille // Springer-Verlag. – Берлин, 1999. – С. 434.

7. Lee. D.T. Medial axis transformation of a planar shape / D.T. Lee // IEEE Trans. Pattern Analysis and Machine Intelligence. – 1982. – PAMI-4, С. 363-369.

8. Кольцов П.П. О количественной оценке эффективности алгоритмов анализа изображений / П.П. Кольцов, С. Осипов, С. Куцаев и др. // Компьютерная оптика. – 2015. – том 39, №4, С. 542-556.

СИСТЕМЫ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 004.056

ИСПОЛЬЗОВАНИЕ МЕТОДА RAINBOW ДЛЯ РАСКРЫТИЯ ХЕШ-ФУНКЦИЙ MD5

USING THE RAINBOW METHOD TO EXPOSE MD5 HASH FUNCTIONS

Меджидов З.У.,
ГАОУ ВО «Дагестанский государственный университет народного хозяйства»,
г. Махачкала, Российская Федерация

Z.U. Medzhidov,
State Autonomous Educational Institution of Higher Education
“Dagestan State University of National Economy”,
Makhachkala, Russian Federation

e-mail: zaur-medzhidov@mail.ru

Аннотация. Hybrid Rainbow – новый сверхмощный метод, комбинирующий гибридную атаку с популярной техникой предвычисления. Сочетая в себе гибкость гибридной атаки, удобство и скорость табличного криптоанализа, он позволяет с легкостью восстанавливать те пароли, которые раньше считали «стойкими» и даже «недоступными для восстановления». Теперь, для любой хеш-функции, единожды посчитав гибридную таблицу по качественному словарю или комбинации словарей, можно за секунды восстанавливать пароли из большого количества символов. Еще в 2003 году, Philippe Oechslin анонсировал новый метод, названный Rainbow Attack (“Making a Faster Cryptanalytic Time-Memory Trade-Off”), который позволил предвычислять прямой перебор паролей. Единожды сгенерировав таблицу для определенного набора символов и определенной длинны пароля (например, 7 латинских символов) и сохранив ее на диск, мы сможем обращаться к таблице сколько угодно раз, и искать пароли для соответствующего набора символов уже не прямым перебором, а, выбирая нужные хеш-значения из таблицы, что на порядки сокращает время атаки. Актуальность рассматриваемой темы определяется тем, что в настоящее время большинство сервисов и приложений используют в своих процессах 128-битный алгоритм хеширования MD5 для обеспечения таких граней информационной безопасности, как целостность и конфиденциальность. Без использования дополнительных параметров, которые применяются при расчете хеш-функции, данные, полученные в результате работы MD5, могут быть скомпрометированы, что может привести к возможности несанкционированного доступа, подмене «подписанного» файла или утечке информации ограниченного доступа.

Abstract. Hybrid Rainbow is a new super-powerful method that combines a hybrid attack with the popular pre-computation technique. Combining the flexibility of a hybrid attack with the convenience and speed of tabular cryptanalysis, it can easily recover passwords that were previously considered “strong” or even “unrecoverable”. Now, for any hash function, having counted the hybrid table once using a quality dictionary or a combination of dictionaries,

you can recover passwords from a large number of characters in seconds. Back in 2003, Philippe Oechslin announced a new method called Rainbow Attack (“Making a Faster Cryptanalytic Time-Memory Trade-Off”), which allowed brute-force password pre-computation. Having once generated a table for a certain set of characters and a certain password length (for example, 7 Latin characters) and saved it to disk, we can access the table as many times as we like, and search for passwords for the corresponding set of characters no longer by brute force, but by choosing the desired hash -values from the table, which reduces the attack time by orders of magnitude. The relevance of the topic under consideration is determined by the fact that currently most services and applications use the 128-bit MD5 hashing algorithm in their processes to ensure such facets of information security as integrity and confidentiality. Without the use of additional parameters that are used in calculating the hash function, the data obtained as a result of MD5 operation can be compromised, which can lead to the possibility of unauthorized access, substitution of a “signed” file, or leakage of restricted information.

Ключевые слова: Rainbow-метод, хеш-функции, перебор паролей, компьютерные атаки, хеширование.

Keywords: Rainbow method, hash functions, brute-force attacks, computer attacks, hashing.

Хешированием называется преобразование массива входных данных произвольной длины в выходную битовую строку фиксированной длины. Зачастую хеш-функции используются для:

– построения ассоциативных массивов;
– поиска дубликатов в наборе данных;
– создания уникальных идентификаторов;
– вычисления контрольных сумм;
– хранения паролей в защищённом виде;
– создания электронной подписи.

MD5 представляет собой 128-битный алгоритм хеширования для проверки целостности и хранения паролей. Принцип действия алгоритма сводится к выполнению пяти последовательных операций:

1. Поток входных данных выравнивается для последующего хеширования.
2. В конец полученного сообщения добавляется 64-битные представления длинны данных. После этого действия длина потока станет кратной 512, а все вычисления будут основываться на потоке массива слов по 512 бит.
3. Происходит инициализация буфера.
4. Циклическое вычисление.
5. Получение результата хеш-функции [1].

Для осуществления «взлома» хеш-функции алгоритма MD5 существует несколько видов атак:

– перебор по словарю;
– brute-force;
– поиск коллизий хеш-функций;
– rainbow-метод.

Использование того или иного метода в конечном итоге приводит к «взлому» хеш-функции и извлечении зашифрованной информации, что может критически отразиться на безопасности защищаемых данных. Рассмотрим принцип «радужного» метода «взлома» хеш-функций и возможные способы защиты алгоритма MD5, которые

позволяют минимизировать потенциальную возможность скомпрометировать защищённые данные.

Rainbow-метод

Основным отличаем Rainbow-метода от методов перебора по словарю и brute-force является время, за которое «радужный» метод создаёт таблицы хеш-функций, с помощью которых происходит «взлом» хеш-функции из выбранного диапазона значений. Использование программного обеспечения Rain-bowCrack, в основу которой положена специализированная таблица отсортированных «хешированных» паролей, даёт возможность быстрого поиска необходимого значения и реализацию обратного хеширования, то есть получения пароля из хеш-функции. Данная программа позволяет расшифровывать не только хеш-функции MD5, но и иные криптографические алгоритмы, такие как:

– LM;
– NTLM;
– SHA1;
– MYSQLSHA1;
– ORACLE-SYSTEM;

и др.

Структура программы RainbowCrack состоит из трёх основных частей:

– подпрограмма генерации «радужных» таблиц (rtgen);
– подпрограмма сортировки «радужных» таблиц (rtsort);
– подпрограммы поиска «радужных» таблиц (rcrack).

2. Для начала подбора хеш-функций необходимо сгенерировать «радужную» таблицу командой rtgen. Данной команде определяется ряд параметров:

– алгоритм хеширования;
– длину открытых текстов в «радужной» таблице;
– длину «радужной» цепи;
– число «радужных» цепей.

На втором этапе работы RainbowCrack необходимо обработать сгенерированные таблицы с помощью команды rtsort. Результатом операции являются отсортированные «радужные» таблицы, хранящееся в оперативной памяти компьютера.

На финальном этапе работы программа RainbowCrack командой rcrack находит необходимую радужную таблицу и произвести дешифровку пароля. В результате реализация «взлома» хеш-функции может быть проведена за относительно небольшой промежуток времени при использовании малых вычислительных мощностей (в процессе функционирования RainbowCrack требуется всего лишь 2 Mb оперативной памяти).

Стоит также отметить недостатки RainbowCrack. Общий размер сгенерированных «радужных» таблиц может превышать 900 Gb, а в самих таблицах могут быть либо прописные, либо строчные символы, что усложняет процесс подбора хеш-функции [2].

Способ защиты от Rainbow-метода

Одним из способов защиты от Rainbow-метода, а также методов перебора хеш-функции является использование криптографической «соли». «Соль» – набор случайных символов, которые дописываются к блокам шифруемой информации, что позволяет многократно усложнить процесс расшифровки информации.

Предположим, что нам необходимо вычислить хеш-функцию пользователя с идентификатором user1 и паролем usergo.

Алгоритм MD5 воспримет данные как запись user1usergo и рассчитает хеш-функцию – ca8881d70b2dc12c16204c782de1c5d. Учитывая, что рассмотренная

комбинация является «словарной», программа RainbowCrack «взломает» такую хеш-функцию за несколько минут.

Добавление «соли» 5hr8Uh32Hr приведет к следующей хеш-функции – e8ed0e735eb76ca4aeb0ca82891f1b06. Так как «соль» представляет собой набор случайных символов, использование Rainbow-метода и методов перебора становится невозможным.

Знание принципов работы протоколов аутентификации и методов разгадывания паролей полезно. Теперь необходимо принять меры для защиты сети. Выполнив 10 рекомендаций, приведенных в данной статье, можно надежно защитить компьютеры от атак со взломом пароля. Рекомендации расположены в порядке убывания важности.

1. Отключение хеша пароля LM. Большинство программ взлома паролей работает исключительно с хешем паролей LM. Блокировать хранение хешей пароля LM можно с помощью трех методов.

Использовать пароли длиной не менее 15 символов. Если длина пароля более 14 символов, система не может генерировать хеш паролей LM.

Отключить хранение хеша паролей LM в масштабах всей системы с использованием Group Policy или Local Security Policy. Следует перейти в раздел Computer Configuration\ Windows Settings\Security Settings\ Local Policies, выбрать Security Options и дважды щелкнуть на пункте Network Security: Do not store LAN Manager hash value on next password change. Щелкните на кнопке Enabled, а затем на кнопке OK. Или же можно отредактировать реестр. Следует открыть редактор реестра (например, Regedt32.exe) и перейти в раздел HKEY_LOCAL_MACHINE\SYTEM\ CurrentControlSet\Control\Lsa. В меню Edit нужно выбрать пункт Add Key и ввести с клавиатуры NoLMHash. Затем необходимо нажать клавишу Enter, выйти из редактора реестра и перезапустить компьютер. Для активизации параметра требуется изменить пароль.

Вставить в пароль специальный символ Unicode. Определенные символы Unicode блокируют генерацию хеша пароля LM.

2. Применение длинных, сложных паролей. Пароли должны иметь длину не менее 15 символов и по крайней мере некоторые элементы сложности. По умолчанию в компьютерах с Windows XP и более новыми операционными системами активизированы сложные пароли (вопрос о том, насколько высок уровень сложности паролей Microsoft, остается открытым). При использовании пароля длиной более 14 символов создание кэша паролей LM блокируется, и большинство инструментов разгадывания паролей, в том числе большинство расчетных таблиц, оказываются бесполезными. А для разгадывания сложного пароля неэффективными будут большинство таблиц, которые не позволяют раскрыть сложные хеши паролей NT за приемлемый период времени. Ситуация может измениться по мере совершенствования методов взлома паролей [3].

3. Отключение аутентификации LAN Manager и NTLM. Большинство анализаторов паролей успешно действуют только против процедур аутентификации LAN Manager и NTLM. После исчерпывающего тестирования, позволяющего убедиться, что такая мера не нарушит производственную среду, следует запретить использование протоколов аутентификации LAN Manager и NTLM. Сделать это можно с помощью редактора реестра или объекта Group Policy Object (GPO). Необходимо перейти к Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options \Network Security: LAN Manager Authentication level и активизировать режим Send NTLMv2 response only/refuse LM&NTLM.

4. Блокировка учетных записей. Блокировка учетных записей остановит или по крайней мере существенно замедлит большинство атак с разгадыванием пароля. Рекомендуется установить блокировки со следующими параметрами [4].

Порог блокировки учетной записи следует установить таким образом, чтобы число неудачных попыток ввода пароля не превышало пяти.

Сбрасывать счетчик блокировки (параметр Reset account lockout counter after) через 1 минуту (минимальное возможное значение).

Установить длительность блокировки (параметр Account lockout duration) равным 1 минуте.

Опасения вызывает компьютерный «червь», вызывающий отказы в обслуживании (DoS), но если «червь» разгадывает пароли, используя имена входа всех пользователей, то лучше блокировать даже законных пользователей, пока «червь» не будет остановлен. После того как угроза «червя» будет устранена, все учетные записи пользователей активизируются в течение 60 секунд.

5. Принудительная замена паролей с разумной частотой. Из Group Policy или Local Security Policy следует перейти в Computer Configuration\Windows Settings\Security Settings\Local Policies\Password Policy и присвоить параметру Maximum password age значение, превышающее 90 дней. Затратив достаточно времени, можно раскрыть любой пароль с помощью любой программы разгадывания, взлома или расчетной таблицы. Но если пароль сложен и имеет длину не менее 15 символов, то для его взлома большинству хакеров потребуется более 90 дней. Подойдет любой интервал смены пароля, но не следует менять пароли слишком часто, чтобы пользователи не начали записывать свои пароли на бумаге.

6. Защита процесса загрузки. Для защиты от физической атаки следует использовать параметры BIOS, запретив загрузку с любого устройства, кроме первичного жесткого диска, а затем защитить BIOS с помощью пароля. Этот прием предотвратит (или, по крайней мере, задержит) локальные, физические атаки с разгадыванием пароля, в том числе сброс паролей и извлечение хешей паролей.

7. Переименование учетных записей с широкими полномочиями. Полезно переименовать учетные записи с широкими полномочиями, такие как Administrator, присвоив им имена, отличные от выбираемых по умолчанию. Смена хорошо известных имен учетных записей с большими полномочиями — эффективная защита от многих программ автоматизированного отгадывания паролей [5].

8. Дополнительная защита учетных записей с широкими полномочиями. Пароли учетных записей с наибольшими полномочиями должны быть самыми длинными и сложными на предприятии, с минимальным интервалом изменения.

9. Активизация предупредительных сообщений на экране регистрации. Активизация предупредительных сообщений на экране регистрации предотвращает многие попытки разгадывания паролей методом грубой силы, поскольку такие автоматизированные программы, как TSGrinder, не ожидают предупредительного сообщения. Активизировать экранные предупреждения можно с помощью Group Policy, переместившись по консольному дереву в Computer Configuration\Windows Settings\ Security Settings\Local Policies\ Security Options и дважды щелкнув на Interactive logon: Message text for users attempting to log on (и связанной с ней функции Interactive logon: Message title for users attempting to log on).

10. Регулярный аудит паролей. И наконец, следует регулярно проводить проверки, пытаясь взломать пароли своей организации с использованием некоторых инструментов, перечисленных во врезке «Типы атак на пароль». Сделать это нужно раньше взломщиков. Результаты можно использовать в качестве теста соответствия, чтобы помочь конечным пользователям, не соблюдающим правил, исправить свои ошибки.

Выводы

На основе проведенного анализа следует, что алгоритм хеширования MD5 подвержен риску взлома, что может привести к компрометации информации ограниченного пользования. Данный риск связан как с особенностью самого алгоритма, так и с активно развивающимися средствами «взлома» криптоалгоритмов. Для существующего риска в данной статье был предложен метод, который повышает уровень надежности MD5, что позволяет в дальнейшем использовать его в различных сервисах, в том числе по защите данных авторизации пользователей. Однако, для обеспечения более высокой надежности шифрования рекомендуется использовать иные алгоритмы хеширования, например, SHA2 или MD9.

Литература

1. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. М.: Горячая линия – Телеком, 2019. 338 с.

2. Меджидов З.У. Анализ тенденций развития средств обеспечения межсетевой защиты // В сборнике: Материалы конференций ГНИИ «НАЦРАЗВИТИЕ». Февраль 2017. Сборник избранных статей. Выпускающий редактор Ю.Ф. Эльзессер; Ответственный за выпуск Л.А. Павлов. 2017. С. 104-106.

3. Меджидов З.У., Гасанова З.А. Проблемы обработки персональных данных в интернете // В сборнике: Теоретические и прикладные вопросы комплексной безопасности. Материалы III Международной научно-практической конференции. 2020. С. 152-155.

4. Угрозы безопасности сетевых информационных систем. Удаленные воздействия на сетевые информационные системы, их классификация [Электронный ресурс]. URL: https://clck.ru/XnYPq

5. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. М.: Издательский центр «Академия», 2005. 256 с.

УДК 004.056.5

ПЕРСОНАЛИЗИРОВАННЫЕ ФИШИНГОВЫЕ АТАКИ

SPEAR PHISHING ATTACK

Давыдова А.О., Кусяпова Д.А., Титух Я.Э., Сенцова А.Ю.,
ФГБОУ ВО «Уфимский государственный авиационный технический университет»,
г. Уфа, Российская Федерация

A.O. Davydova, D.A. Kusyapova, Y.E. Titukh, A.Y. Sentsova,
FSBEI HE «Ufa state aviation technical university»,
Ufa, Russian Federation

e-mail: kusyapovadilara@gmail.ru

Аннотация. Атаки, начальным этапом которых являются действия злоумышленника, использующие методы социальной инженерии, на данный момент являются одним из самых распространенных видов атак. При использовании социальной

инженерии злоумышленник стремится получить конфиденциальную информацию и доступ в различные интересующие сегменты предприятия при помощи психологического воздействия и манипуляций на пользователей. Чтобы успешно провести атаку с помощью социальной инженерии, необходимо войти в доверие к «жертве», что успешно осуществляется с помощью целевого (персонализированного) фишинга. По причине относительной легкости осуществления сегодня наблюдается стремительный рост использования целевых фишинговых атак как на домашние персональные компьютеры, так и на компьютеры сотрудников крупных компаний. Целевые фишинговые атаки тщательно продумываются для воздействия на определенный тип людей, и научить пользователей их различать практически невозможно. В данной статье раскрываются понятие и методы целевого фишинга, а также решения и способы защиты от данного вида атак. Кроме того, эта обзорная статья представляет собой попытку научить пользователей распознавать целевые фишинговые электронные письма. В статье также приводятся примеры атак с использованием целевого фишинга.

Abstract. Attacks the initial stage of which is the actions of an attacker who uses social engineering methods, are currently one of the most common types of attacks. While using social engineering an attacker tries to obtain confidential information and access to various segments of interest of the enterprise through psychological influence and manipulation. To carry out a social engineering attack successfully it is necessary to gain the trust of the victim, this is successfully accomplished by using spear-phishing. Due to the relatively simple implementation of attacks today there is a rapid increase in the use of spear-phishing attacks both on home personal computers and on computers of employees of large companies. Phishing attacks are carefully designed to target a specific type of people and it is almost impossible to teach users to recognize them. This article reveals the concept and methods of spear-phishing as well as solutions and methods of protection against this type of attacks. In addition, this review article is an attempt to educate users how to recognize phishing emails. The article also provides examples of spear-phishing attacks.

Ключевые слова: фишинг, социальная инженерия, целевой фишинг, персонализированный фишинг, атака.

Keywords: phishing, social engineering, spear phishing, personalized phishing, attack.

Одним из самых уязвимых компонентов любой системы защиты информации являются исполнители, которые используют технику защиты информации, а также сотрудники компании, которые могут, зачастую, пренебрегать правилами политики безопасности. Эксплуатируя эту уязвимость системы защиты информации и корпоративной информационной системы в целом, с помощью методов социальной инженерии, злоумышленник может получить пользовательскую информацию для дальнейших мошеннических действий. Наиболее популярный на сегодняшний день метод социальной инженерии – целевой (персонализированный) фишинг.

Самое распространенное определение фишинга – это письма на электронную почту, похожие на сообщения от существующих, легальных организаций. Данные сообщения обычно несут не ознакомительный характер, а принуждают, подталкивают пользователя к какому-либо действию, например, подтверждение своей учетной записи. Такие письма рассылаются большому количеству пользователей и, обычно, не содержат в себе какой-либо детальной информации об атакуемом. Целевой фишинг является более сложной модификацией фишинговых атак и, прежде чем осуществить такую атаку,

злоумышленник должен выяснить как можно больше личной информации о жертве, поэтому целевой или персонализированный фишинг требует тщательной подготовки и немалых физических и материальных затрат от злоумышленника. Но вероятность проведения успешной атаки на основе целевого фишинга в разы увеличивается, по сравнению с обычным нецелевым фишингом. Согласно отчету Verizon о кибербезопасности, злоумышленник, отправивший 10 персонализированных фишинговых писем, имеет 90-процентную вероятность того, что один человек попадется в ловушку [1].

По данным компании Group-IB, ежедневно жертвами финансового фишинга в России становятся около 1000 клиентов различных банков, что в три раза превышает ежедневное количество жертв от вредоносных программ, а около 10–15 % посетителей финансовых фишинговых сайтов вводят на них свои данные [2]. Кроме того, любая фишинговая атака может являться первым этапом жизненного цикла атаки, которая приведёт к еще более серьезным последствиям, в том числе денежному ущербу и деструктивным воздействиям на информационную систему. Поэтому, темы, связанные с социальной инженерией и, особенно с персонализированным фишингом, являются особо актуальными.

Одним из последних примеров атаки с использованием целевого фишинга являются письма, которые приходили пользователям, якобы от портала «Госуслуги». Письмо было похоже на подлинное сообщение портала «Госуслуги» и содержало следующие элементы: логотипы в начале и конце письма, похожий шрифт и гиперссылки голубого цвета. В самом письме содержались сведения о том, что в отношении его получателя вынесено постановление о начислении социальных компенсаций. Для их оформления предлагалось перейти в личный кабинет и обратиться к ведущему юристу, а для идентификации в личном кабинете необходимо указать номер СНИЛС. После перехода по ссылке в браузере открывалось окно, в котором пользователь должен был указать номер своей банковской карты, на которую должны поступить выплаты [3].

Благодаря тому, что злоумышленники обращаются к атакуемому по имени и знают точный адрес получателя, увеличивается степень доверия к вредоносному письму и вероятность того, что атака будет успешной, повышается в несколько раз.

Ситуация усугубляется тем, что на данный момент не существует средств защиты информации, которые были бы способны гарантированно детектировать и предотвращать атаки, начинающиеся с целевого фишинга, в котором злоумышленники используют человеческий фактор как уязвимость системы, и только технических (программных) средств защиты в этом случае недостаточно. Статья направлена на анализ методов целевого фишинга и существующих мер защиты от внедрения вредоносного программного обеспечения (ПО) в корпоративную среду данным путем. Также приводятся рекомендации по комплексности защиты от целевого фишинга.

Особенности целевого фишинга

Классический фишинг – это массовая рассылка писем с идентичным содержанием. Целевой фишинг (англ. spear-phishing), в отличие от классического, направлен на конкретную цель, а значит является намного опаснее. Качественно составленное письмо для целевого фишинга очень трудно отличить от легитимного письма.

Кроме того, целевой фишинг предполагает тщательную подготовку и большие затраты ресурсов, таких как время и денежные средства. Но вероятность проведения такой атаки во много раз успешнее, чем атака с помощью обычного фишинга, следовательно, данная атака окупит все затраты на ее проведение.

Структура целевой фишинговой атаки состоит из нескольких этапов (рисунок 1). Первым этапом, как и в любых других видах атак, является планирование. На данном этапе проводится разведка и анализ уязвимостей. Следующим этапом выступает подготовка, на котором злоумышленники выясняют нужные адреса электронной почты: покупают списки на других теневых ресурсах и получают конкретный список для рассылки писем по действующим адресам либо путем внедрения вредоносного ПО, которое собирает адреса. Затем регистрируется домен и создается фальшивый веб-сайт, с правдоподобным видом, на который будут перенаправляться жертвы и на этом же этапе происходит составление фишинговых писем.

После этого мошенники реализуют атаку: отправляют письма и внедряют вредоносное ПО. Далее производится сбор информации, злоумышленники получают учетные данные или другие сведения о банковских счетах жертв, с помощью которых крадут данные и (или) денежные средства, они используют информацию в своих целях и шантажируют пользователей. Заключающим этапом структуры целевой фишинговой атаки является сокрытие присутствия злоумышленника в системе. Этот этап направлен на маскирование злоумышленника и, в отдельных случаях, на внедрение вредоносного ПО, который позволит скрыть метаданные злоумышленника и повлиять на системные журналы и журналы безопасности, которые могли зафиксировать те или иные действия злоумышленника в системе.

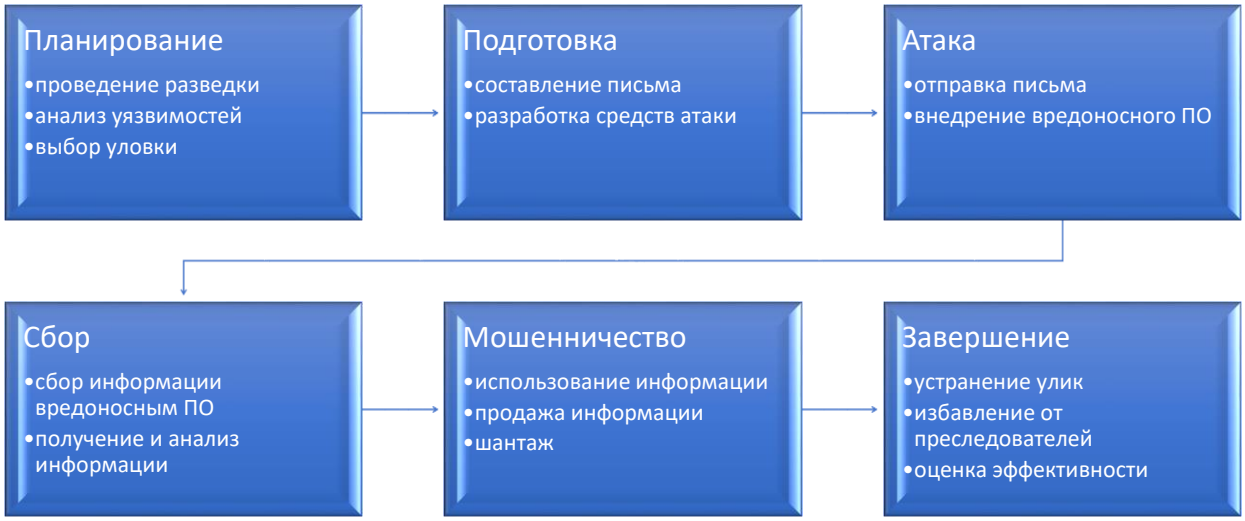

Рисунок 1. Структура целевой фишинговой атаки

В зависимости от атакующего воздействия можно выделить несколько видов фишинговых писем:

1. Письмо, содержащее ссылку.

В таком мошенническом письме содержится ссылка, по которой должен перейти атакуемый. Атакуемый должен перейти на определенный веб-ресурс, где, используя уязвимости самого сайта или браузера пользователя, мошенники попытаются внедрить вредоносное ПО. Для проведения таких действий злоумышленниками специально создаются фишинговые сайты, время жизни которых невелико. Чаще всего они являются точными копиями известных сайтов, повторяя их дизайн, структуру и функциональность. При переходе по ссылке пользователь становится жертвой

различных видов XSS-атак. Суть данных атак заключается в выполнении скрипта в браузере и последующем его взаимодействии с сервером злоумышленника. Эти операции позволяют получить доступ к данным браузера и дают возможность применять к нему эксплойты, а также получать cookie, данные авторизации или, например, выполнять HTTP-запросы от имени пользователя [4]. Сегодня злоумышленники даже рекламируют свои ресурсы в социальных сетях и поисковых системах и выводят в топы ссылки на свои фишинговые сайты.

2. Письмо с вредоносным вложением.

В качестве вложения в фишинговое письмо злоумышленник может поместить имитацию отчета коллеги за предыдущий месяц, задание от руководителя или сообщение от банка, приславшего пользователю иск за неуплату по кредиту. Вложения бывают в форматах *.doc или *.pdf. Файлы формата *.pdf часто содержат объекты JavaScript. Поэтому для злоумышленника достаточно просто создать некоторый скрипт, который использовал бы одну из уязвимостей движка от Adobe [5]. В документах Microsoft Office вредоносное ПО может загружаться при помощи макросов, которые содержит файл. При открытии документа исполнение макроса позволяет установить соединение с сервером злоумышленника и начать загрузку. Для защиты от данного вида писем в рамках политики безопасности в организациях необходимо отключать поддержку макросов. Но, если пользователь не соблюдает политику безопасности, то при использовании социальной инженерии, злоумышленник может заставить его отключить защиту от макросов [5], [6]. На данный момент большинство способов эксплуатации уязвимостей пакета прикладных программ Microsoft Office не требуют использования макросов. Например, используя самую популярную уязвимость 2017 года CVE-2017-0199 [7], при открытии вложенного *.rtf файла можно подгрузить HTA приложение, поддерживающее исполнение сценариев, со стороннего сервиса и запустить его. Помимо рассмотренных случаев существует множество других офисных продуктов и форматов, с которыми они работают. Но принцип атаки один и тот же – запустить скрытый сценарий, который позволит загрузить ПО злоумышленника на атакуемый компьютер. Самыми популярными инструментами для создания вредоносных вложений, отправляемых в фишинговых письмах, стали Microsoft Word Intruder (MWI) и Offensive Ware Multi Exploit Builder (OMEB) [2].

В недавней фишинговой кампании группа 74 (также известная как Sofact, APT28, Fancy Bear) нацелилась на профессионалов в области кибербезопасности. Было написано электронное письмо, якобы связанное с конференцией Cyber Conflict U. S. conference и мероприятиями, организованными United States Military Academy Army Cyber Institute, NATO Cooperative Cyber Military Academy и NATO Cooperative Cyber Defence Centre of Excellence. Хотя CyCon – это настоящая конференция, вложение являлось документом, содержащим вредоносный макрос Visual Basic для приложений (VBA), который загружал и запускал вредоносное программное обеспечение, называемое Seduploader [8]. Хотя атакуемыми были специалисты по безопасности, которые имеют обширные знания в области инструментария злоумышленников, атака была проведена успешно и, злоумышленником удалось получить личные данные большого количества специалистов по безопасности.

Еще одним ярким примером фишинговой атаки является атака Energetic Bear, которая включает в себя рассылку фишинговых писем с вредоносным содержимым. Основными целями этой атаки являются предприятия топливно-энергетического комплекса и другие промышленные предприятия. Проведение такой атаки помогает злоумышленнику провести сканирование скомпрометированных систем на наличие уязвимостей.

Из всех возможных вариантов получения несанкционированного доступа к учётной записи с помощью целевого фишинга самым эффективным на сегодняшний день является использование фишинг-движков, также называемых фейками [9]. Основан этот метод на веб-программировании и социальной инженерии. Движки выполняют три основные функции:

1. Имитация интерфейса по заданной ситуации, связанной с операциями пользователя.
2. Копирование и обработка незаконно полученных учетных данных пользователя.
3. Возврат пользователя на соответствующую ситуации страницу официального сервиса.

Движок состоит из элементов скопированного Интернет-ресурса, и программ скриптов, написанных злоумышленником. Собранный и готовый к работе движок злоумышленник размещает на сервере и присваивает ему подготовленное доменное имя.

В случае использования фишинга как инструмента комбинированный атаки фишинговое письмо может содержать вредоносный файл, например, бэкдор, открывающий доступ злоумышленнику к операционной системе компьютера пользователя и его сетевому окружению.

В ходе подготовки к целенаправленной фишинговой атаке осуществляется изучение круга общения атакуемого, его интересов, сфера деятельности. Кроме этого, злоумышленникам необходимо понимать, каким программным обеспечением и устройствами пользуются атакуемый. В зависимости от используемых методов авторизации, просмотра писем необходимо подготовить интерфейс фишинг-движка. Также для злоумышленника важно знать, в какие периоды времени пользователь осуществляет обработку почты. Кроме того, злоумышленником собирается информация об используемых провайдерах и местах, где осуществляется подключение к сети «Интернет». Эти сведения необходимы для подготовки персонализированного фишинг-движка, а также планирования дальнейших действий злоумышленника.

Существующие меры защиты

1. Организационные меры.

Обучение и осведомленность сотрудников компании являются основным фактором снижения риска целевого фишинга. Чтобы защититься от целевого фишинга, необходимо, в первую очередь, ввести определенные организационные меры, и обучить сотрудников распознаванию таких мошеннических писем.

Первое, на что стоит обратить внимание– это письма, в которых содержится просьба или указание ввести какие-либо данные, путем перехода по ссылке или каким-либо иным способом. Никакая служба не должна спрашивать данные пользователя, поскольку они и так уже есть в их системе.

Второй момент, который должен насторожить пользователя– указание в письме угрозы о блокировки учетной записи, если не последовать инструкции. Это пример манипуляции со стороны злоумышленников.

Конечно же, при получении письма на электронную почту стоит обратить внимание на адрес отправителя. В нем могут быть небольшие отличия от официального электронного адреса службы, например, одна лишняя буква, знак или замена буквы на цифру. В примере, приведенном раннее в этой статье, где недавно был произведен направленный фишинг с помощью письма, присланного от портала «Госуслуги», о том, что письмо мошенническое, ясно говорил адрес отправителя – info@mybusinessplan.ru. Но, тем не менее, даже, несмотря на такой явный признак фишингового письма, многие атакуемые переходили по ссылкам, указываемым в этих письмах.

Однако, при совпадении адреса отправителя с официальным адресом не является стопроцентным доказательством того, что письмо не является фишинговым. Злоумышленники могут манипулировать отображением ссылки в адресной строке с помощью технологии «спуфинг» (англ. Spoofing – обман, мистификация). Злоумышленники также могут подделывать, даже SSL-сертификат – цифровое удостоверение сайта, которое подтверждает, что обмен данными между сайтом и браузером идет по защищенному каналу. Таким образом, использовать только организационные меры для защиты от целевых фишинговых атак нельзя.

2. Программно-аппаратные меры

Помимо организационных мер, которые, безусловно, помогут снизить риск атак целевого фишинга, существуют различные программные решения для обнаружения и пресечения направленного фишинга.

Фильтрация нежелательных писем – основной этап защиты в борьбе с фишингом. Распространенные системы фильтрации спама:

1. Анализ IP-адреса сервера отправителя, направленный на установление репутации IP отправителя, путем его поиска в «черных списках», защита эффективна лишь против массового фишинга.
2. Анализ тела письма, производит поиск словосочетаний, применяемых при фишинговых атаках.
3. SPF/DKIM-анализ. Широкое применение проверки электронной почты с помощью взаимодополняющих методов проверки подлинности писем и выявления почтовых сообщений от злоумышленников, таких как: SPF (Sender Policy Framework– вид проверки подлинности, помогает идентифицировать авторизованные почтовые серверы для конкретного домена) и DKIM (DomainKeys Identified Mail – криптографический способ проверки подлинности, позволяет проверить и определить авторизацию электронного письма, полученного из данного домена) обеспечит эффективное противодействие целевому фишингу. Дополнительную защиту для писем, может также обеспечить очистка HTML, в случаях, когда с помощью SPF и DKIM не удается проверить подлинность сообщения. При использовании очистки HTML возможен просмотр скрытого, потенциально опасного содержимого, так как переход по URL-адресам невозможен и ссылки преобразуются в текст.
4. Анализ заголовков пакетов, заключающийся в работе межсетевого экрана, осуществляющего контроль и фильтрацию сетевого трафика.
5. Анализ загружаемого или работающего ПО, посредством антивирусных решений, с использованием таких методов, как: сигнатурный и эвристический анализы, песочница.

Еще одним методом для борьбы с целевым фишингом может выступить выявление фактов неавторизованного доступа к компьютеру и выявления вредоносного ПО с помощью системы обнаружения вторжений (IDS), а также система предотвращения вторжений (IPS). Первая система осуществляет поиск злонамеренных файлов сигнатурным анализом, при котором эксплуатация уязвимостей нулевого дня останется незамеченной. IPS же проводит ответные действия на нарушение, чем в большей степени полезна для обеспечения безопасности.

Также могут использоваться комплексные решения, к примеру, UTM-системы, включающие в себя сразу вышеперечисленные решения: межсетевой экран, фильтр URL, антивирусное решение, спам-фильтры, IDS/IPS. Их применение упрощает настройки и обучение персонала, а также снижает затраты на защиту.

Одно из комплексных решений представляет компания Cisco – комплексное средство защиты IronPort, которое направлено, именно на борьбу с целевым фишингом. Данное средство защиты обеспечивает защиту от целевого фишинга путем мониторинга

писем и веб-трафика, и технологии проверки подлинности сообщений. Эффективно выявлять и блокировать целенаправленные фишинговые атаки, средству защиты IronPort, позволяет сеть SenderBase, где выполняется постоянный мониторинг более чем 30% мирового почтового трафика и веб-трафика.

Обладая информацией об IP-адресах, SenderBase отслеживает необходимые параметры, (объем письма при отправке и объем трафика с веб-сайта, уровни жалоб, параметры учета в «ловушках спама», разрешение имен DNS, страна происхождения и наличие в черном списке, когда было зарегистрировано доменное имя и др.) используя которые, в дальнейшем, определяет показатель репутации и уровень угрозы письма. Присвоив URL-адресу показатели репутации, посредством фильтра веб-репутации IronPort Web Reputation Filters, устройства IronPort вправе разрешить пометить или заблокировать письма от отправителей [10].

Использование таких комплексных решений позволит во много раз снизить вероятность проведения успешной целевой фишинговой атаки.

Выводы

Знание специалистами основ и тактик применения социальной инженерии, и в частности, механизмов фишинговых атак, способно существенно усовершенствовать систему защиты информации на предприятии в силу того, что почти все атаки начинаются с этапа разведки. Понимание основных принципов социальной инженерии должно учитываться при проектировании системы защиты информации, разработки регламентов информационной безопасности, политики безопасности и, несомненно, поможет при расследовании уже произошедших инцидентов информационной безопасности.

По причине того, что специализированные средства защиты информации, способные обнаружить фишинговые письма, сейчас мало используются на предприятиях, а нормативные правовые акты, которые регламентировали бы сферу социальной инженерии и фишинга практически отсутствуют в нашей стране, проблемы, поднятые в данной статье актуальны и требуют дальнейшего изучения.

Литература

1. Verizone. 2020 Data Breach Investigations Report [Электронный ресурс] URL: https://clck.ru/XnZCw (дата обращения: 27.03.2021).
2. High-Tech Crime Trends 2017 [Электронный ресурс] URL: https://clck.ru/XnZFJ (дата обращения: 27.03.2021).
3. Мошенники придумали новую схему обмана россиян под видом выплат с «Госуслуг» [Электронный ресурс] URL: https://clck.ru/XnZJu (дата обращения: 02.04.2021).
4. Защита внешнего информационного периметра организации от целевого фишинга [Электронный ресурс] URL: https://clck.ru/XnZRW (дата обращения: 07.04.2021).
5. Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing [Электронный ресурс] URL: https://clck.ru/XnZVE (дата обращения: 08.04.2021).
6. Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks [Электронный ресурс] URL: https://clck.ru/XnZY7 (дата обращения: 08.04.2021).

7. National vulnerability Database [Электронный ресурс] URL: https://clck.ru/XnZcK (дата обращения: 12.04.2021).
8. Типы фишинговых атак и способы их выявления [Электронный ресурс] URL: https://clck.ru/SUPUR (дата обращения: 05.04.2021).
9. Cisco. Целевой фишинг [Электронный ресурс] URL: https://clck.ru/XnZmL (дата обращения: 02.04.2021).
10. Масалков, А.С. Особенности киберпреступлений: инструменты нападения и защиты информации. – М.: ДМК Пресс, 2018. – 226 с.

УДК 004.49

МОДЕЛИРОВАНИЕ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПО НОВОЙ МЕТОДИКЕ ФСТЭК, ИСПОЛЬЗУЯ СРЕДСТВА АВТОМАТИЗАЦИИ

MODELING INFORMATION SECURITY THREATS USING THE NEW FSTEC METHODOLOGY USING AUTOMATION TOOLS

Степанов В.А., Андреев Н.Д.,
ФГБОУ ВО «Уфимский государственный технический авиационный университет»,
г. Уфа, Российская Федерация

V.A. Stepanov, N.D. Andreev,
FSBEI HE “Ufa state technical aviation university”,
Ufa, Russian Federation

e-mail: v.stepanov1999@yandex.ru

Аннотация. Статья посвящена моделированию угроз безопасности информации используя актуальные средства автоматизации в соответствии с новой методикой ФСТЭК «Методика оценки угроз безопасности информации» от 05 февраля 2021 года. В данной работе проводится эксперимент с целью выяснить, возможно ли моделирование угроз безопасности информации используя в качестве исходных данных, информацию, которую нам предлагает матрица ATT&CK для предприятий от MITRE, если того не запрещает «Методика оценки угроз безопасности информации». В материале рассматриваются 5 этапов оценки угроз безопасности информации, то есть определение возможных негативных последствий от реализации угроз, возможных объектов воздействия угроз, источников угроз, способов реализации угроз и актуальных угроз безопасности информации. Второй исследуемой частью работы является актуальный вопрос, который в настоящее время задают большинство специалистов в области обеспечения информационной безопасности: «Каким образом связать ключевые пункты методики оценки угроз безопасности информации с матрицей ATT&CK для предприятий от MITRE». Третьей ключевой задачей работы является решение проблемы описания возможных сценариев реализации угроз и определение актуальных угроз безопасности информации. С использованием методики оценки угроз безопасности информации выполнено моделирование угроз для государственной информационной системы. Выполнен анализ существующих развитых устойчивых угроз или APT группировок, также выполнен анализ инструментов в виде вредоносного программного

обеспечения или программно-аппаратных средств, и решены проблемы описания сценариев реализации угроз безопасности информации и определения актуальных угроз безопасности информации с помощью средств автоматизации. На основании полученных результатов сценариев реализации угроз и актуальных угроз безопасности информации была выявлена одинаковая закономерность в последовательности действий APT группировок, атаки которых в основном направлены на информационные системы государственных учреждений.

Abstract. The article is devoted to modeling threats to information security using the latest automation tools in accordance with the new FSTEC methodology “Methodology for assessing threats to information security” dated February 05, 2021. In this work, an experiment is carried out to find out whether it is possible to model information security threats using as initial data the information that the ATT&CK matrix for enterprises from MITRE offers us, if it is not prohibited by the Methodology for assessing information security threats. The material examines 5 stages of assessing threats to information security, that is, the determination of possible negative consequences from the implementation of threats, possible objects of influence of threats, sources of threats, ways of implementing threats and actual threats to information security. The second part of the study under study is a topical question that is currently being asked by most information security experts: “How to connect the key points of the information security threat assessment methodology with the ATT&CK matrix for enterprises from MITRE”. The third key task of the work is to solve the problem of describing possible scenarios for the implementation of threats and identifying actual threats to information security. Using the methodology for assessing threats to information security, the modeling of threats to the state information system has been carried out. The analysis of existing developed persistent threats or APT groups was carried out, the analysis of tools in the form of malicious software or software and hardware was carried out, and the problems of describing scenarios for the implementation of information security threats and identifying actual threats to information security using automation tools were solved. Based on the results of the scenarios for the implementation of threats and actual threats to information security, the same pattern was revealed in the sequence of actions of APT groups, whose attacks are mainly aimed at information systems of state institutions.

Ключевые слова: моделирование угроз, средства автоматизации, матрица ATT&CK для предприятий, государственная информационная система, сценарии реализации угроз, ATT&CK Navigator, актуальные угрозы.

Keywords: threat modeling, automation tools, ATT&CK matrix for enterprises, government information system, threat scenarios, ATT&CK Navigator, current threats

Для моделирования угроз безопасности информации была выбрана государственная информационная автоматизированная система «Менеджмент» (далее ГАИС «Менеджмент»). Для выбранной информационной системы были определены необходимые исходные данные, то есть наименование информационной системы, её назначение, состав обрабатываемой информации, полное описание систем и сетей и их основные характеристики как объектов защиты. Приведена примерная архитектура информационной системы, которая иллюстрирует состав и архитектуру, интерфейсы с помощью которых взаимодействуют компоненты системы и сети, группы пользователей, а также другие поясняющие материалы, необходимые для моделирования угроз.

В соответствии с Методическим документом «Методика оценки угроз безопасности информации», утвержденным ФСТЭК России 05.02.2021 г. (далее – Методика), для оператора государственной информационной системы определили перечень возможных рисков [1]. Затем экспертным методом определили актуальные для нашей информационной системы негативные последствия от реализации угроз безопасности информации. Данные для проведения опроса были взяты из приложения 4 к настоящей Методике [1]. По решению обладателя информации и оператора информационной системы экспертная группа сформирована в составе специалистов дирекции защиты информации из 3 человек. В ходе работы экспертной группы проводился опрос ее членов для определения возможных негативных последствий в случае реализации угроз безопасности информации. Оценка проводилась в 2 раунда. Опрос экспертов проходил следующим образом:

– сначала каждый член экспертной группы проводил оценку возможности негативных последствий по числовой шкале от «1» до «10»;

– в каждом из раундов после оценки негативного последствия каждым участником экспертной группы отбрасывались минимальные и максимальные оценки;

– затем определялось среднее значение сначала по итогу первого раунда, а затем по итогу второго раунда;

– после этого вычислялось итоговое среднее значение из средних значений первого и второго раундов.

Негативные последствия считались актуальными, если итоговое среднее значение по первому и второму раунду равнялось 7 или было больше 7.

Исходя из этого получили таблицу, в первой колонке которой содержится перечень возможных рисков, а во второй колонке возможные негативные последствия, соответствующие им.

Далее перешли к определению объектов воздействия и видов воздействия на них, потому что состав объектов воздействия и их интерфейсов формирует границы оценки угроз и разработки модели угроз безопасности информации.

Группы информационных ресурсов и компонентов информационной системы, которые могут являться объектами воздействия, определили на основе предполагаемой нами архитектуры и условий функционирования систем и сетей, определенных на основе изучения и анализа исходных данных, приведенных в части описания систем и сетей и их характеристик как объектов защиты.

Предполагаемые виды воздействия на объекты воздействия определили нестандартным образом, мы взяли предложенную организацией MITRE тактику «Воздействие», далее выбрали необходимые техники, содержащиеся в данной тактике для объектов нашей информационной системы, то есть предполагаемые виды воздействия на объекты информационной системы, потому что один из аспектов нашей работы заключается в том, чтобы проверить опытно-экспериментальным путем, возможно ли построить модель угроз, если в качестве исходных данных по возможности оперировать только данными, которые приведены в матрице ATT&CK для предприятий от MITRE, так как матрица ATT&CK признается специалистами с области информационной безопасности как одной из лучшей и использование данных, содержащиеся в матрице является хорошим тоном во всем мире [8].

После того как мы определили объекты воздействия и виды воздействия на них, мы построили таблицу, строки которой содержать вектора. В 1-ом столбце указывали негативное последствие, во 2-ом столбце определили объект воздействия для выбранного негативного последствия, которое определили пунктом выше, а в 3-ем столбце выбирали виды воздействия для конкретных объектов воздействия. Далее таким

же образом определяем объект воздействия и вид воздействия для каждого следующего негативного последствия.

Оценка источников угроз безопасности информации осуществляется в несколько этапов. Для оценки источников угроз в качестве исходных данных привлекается приложения 6 и 8 к настоящей Методике, также информация, которую мы получили пунктами выше в ходе процесса моделирования угроз [1].

Первым этапом оценки источников угроз является выявление актуальных возможных целей потенциальных нарушителей применительно к ГАИС, оценка осуществляется экспертным методом экспертной группой, состав которой приведен и описан ранее в данной статье. В ходе работы экспертной группы проводился опрос ее участников, чтобы выявить актуальные возможные цели реализации угроз безопасности информации потенциальными нарушителями. Методология данного опроса и её этапы аналогичны опросу, который проводился при определение актуальных негативных последствий от реализации угроз безопасности информации для нашей информационной системы

После оценки актуальных возможных целей потенциальных нарушителей были сопоставлены нарушители, их возможные цели реализации угроз безопасности информации и возможные негативные последствия, и виды рисков от их реализации. Сопоставления осуществлялось следующим образом:

– сначала выбирался конкретный вид нарушителя;
– затем исходя из его возможных, и для нашей информационной системы, актуальных целей реализации угроз безопасности информации определялось вид нанесения ущерба, то есть физическому лицу, юридическому лицу или государству в различных его аспектах;
– если соответствие было обнаружено, то мы для конкретного типа нанесения ущерба определяли актуальные цели реализации угроз;
– далее если были определены актуальные цели реализации угроз для конкретного типа нанесения ущерба, выбирали соответствующие виды риска(ущерба) для них в совокупности;
– и таким образом повторяли для каждого нарушителя из 13-ти возможных в соответствии с настоящей Методикой [1].

В итоге получилась таблица, которая содержит виды нарушителей, для них возможные цели реализации угроз безопасности информации, включающие виды нанесения ущерба, и соответствие целей видам риска (ущерба) и возможным негативным последствиям.

Следующим пунктом в определении источников угроз безопасности информации является определения актуальных нарушителей при реализации угроз безопасности информации и соответствующие им возможности для ГАИС «Менеджмент». Для начала выбирался вид риска(ущерба) для этого типа риска определялось соответствующее ему одно возможное негативное последствие, в соответствии с таблицей видов рисков (ущерба) и типовые негативные последствия от реализации угроз безопасности информации, это есть 1-ый и 2-ой столбец таблицы. Далее из таблицы оценки целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации, то есть из таблицы, которую получили в предыдущем пункте, для негативных последствий выбираем все виды актуальных нарушителей, это будет 3-ой столбец данной таблицы. Затем для в соответствии с приложением 6 настоящей Методики определили категорию нарушителя для уже выбранного актуального нарушителя, это есть 4-ый столбец таблицы [1]. После этого в соответствии с приложением 8 настоящей методики определили уровень возможности актуального нарушителя. Повторим данную процедуру для каждого

негативного последствия получаем таблицу определения актуальных нарушителей при реализации угроз безопасности информации и соответствующие им возможности для нашей информационной системы [1].

На следующем этапе моделирования угроз определяли способы реализации угроз безопасности информации. Исходными данными для данного этапа моделирования угроз являлись негативные последствия от реализации угроз, объекты воздействия угроз и соответствующие им виды воздействия, виды и категории актуальных нарушителей, которые могут реализовывать угрозы безопасности информации, то есть данные полученные раннее в ходе моделирования угроз безопасности информации. В качестве основных способов реализации угроз были выбраны способы реализации представленные в главе 5, статье 2 настоящей Методики и в описании применяемых к нашей информационной системе техник принадлежащие разделу тактики «Воздействие» [1].

Способы реализации (возникновения) угроз безопасности определяются применительно к объектам воздействия, которые определенны в таблице определения объектов воздействия и видов воздействия на них.

Так как ГАИС «Менеджмент» находится на этапе создания, то определение интерфейсов объектов воздействия, которые могут использоваться в случае реализации угроз, проводится на основе предполагаемой нами архитектуры и условий функционирования ГАИС «Менеджмент».

Определения актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей происходит следующим образом. Из таблицы, содержащую актуальных нарушителей при реализации угроз безопасности информации и соответствующие им уровни возможностей, которую мы определили на предыдущем этапе брали конкретный актуальный вид нарушителя и для него определенную этапом выше категорию нарушителя, далее определяли объект воздействия, на который воздействует нарушитель, для объекта воздействия определяли доступные для нарушителя интерфейсы, а уже для интерфейсов выбирали способы их реализации.

Таким образом у нас получилась таблица актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности для ГАИС «Менеджмент».

Крайним этапом оценки угроз безопасности информации является актуальные угрозы безопасности информации.

На основе анализа исходных данных определили возможные для ГАИС угрозы безопасности информации, к которым относятся осуществляемые нарушителем воздействия на ГАИС, в результате которых возможно нарушение безопасности информации и (или) нарушение или прекращение функционирования ГАИС. Далее построили таблицу, отображающую перечень возможных угроз безопасности информации для соответствующих способов их реализации и уровней возможностей нарушителей.

Затем переходим к описанию возможных сценариев реализации угроз безопасности. Описание возможных сценариев реализации угроз сделать вручную практически не представляется возможным. Данный момент вызывал большое недоумение, массу вопросов и замечаний у специалистов в области защиты информации. Люди были озадачены решением этой непростой задачи. Но выход из этого положения есть. Для этого будем использовать средства автоматизации для данного процесса.

Для использования средства автоматизации ATT&CK Navigator нам потребовались исходные данные, то есть хакерские APT группировки, по-другому развитые устойчивые атаки, атакующие информационные системы государственных

учреждений, также потребовались вредоносные программные обеспечения и программно-аппаратные средства, используемые ими в процессе реализации атак [9].

Для выявления хакерских APT группировок использовали инструментарий TARGET CYBERATTACKS LOGBOOK [10]. Данный инструментарий помогает пользователям понять корреляцию и взаимосвязь между основными целевыми атаками, также показывает дополнительную информацию о некоторых из самых печально известных кибератак в истории, чтобы пользователи веб-приложения могли защитить себя от будущих подобных атак. Также TARGET CYBERATTACKS LOGBOOK позволяет изучить географию заражения, способы распространения вредоносных программ и другие особенности каждой атаки. Инфекции отображаются визуально в виде кораблей, причем размер каждого судна указывает размер и продолжительность отдельных кампаний. Кроме того, пользователи могут фильтровать атаки по категориям, чтобы изолировать информацию о конкретных угрозах и шаблонах атак [10].

В TARGET CYBERATTACKS LOGBOOK настроили конфигурацию согласно нашей информационной системы, фильтр включает следующие разделы: ТОП целевых стран, назначение/наименование атаки, страна происхождения APT группировки, целевые платформы, способы распространения атак, цель атаки и их количество, тип воздействия, первый известный пример атаки и год обнаружения APT группировки. В итоге определили APT группировки и средства, которые они используются по при атаках на государственные информационные системы [10].

Далее перешли в ATT&CK Navigator и настроили параметр «multi-select» [9]. В открывшемся окне, в разделе «threats group» выбрали хакерские APT группировки, которые выдал TARGET CYBERATTACKS LOGBOOK по нашему запросу [10]. Затем в открывшемся окне, в разделе «software» выбрали вредоносные программные обеспечения и программно-аппаратные средства. В разделе «mitigations» выбираем принятые меры защиты дня нашей информационной системы. Чтобы увидеть актуальные сценарии реализации угроз выбираем параметр «background color», в открывшемся окне выбираем цвет. В итоге получаем граф, который содержит описание сценариев реализации угроз, наименование столбцов графа есть тактики, под каждой из 10 тактик представлены соответствующие им техники. Техники, подсвеченные выбранным нами цветом, являются актуальными для информационной системы.

Определение актуальности угроз безопасности информации осуществляется экспертным методом экспертной группой, состав которой приведен и описан ранее в данной статье. В ходе работы экспертной группы проводится опрос ее участников, чтобы выявить актуальные сценарии реализации угрозы безопасности информации. Методология данного опроса и её этапы аналогичны опросу, который проводился при определение актуальных негативных последствий от реализации угроз безопасности информации для нашей информационной системы [1].

Выводы

Насколько хорошей бы не была матрица, при использовании только матрицы ATT&CK от MITRE невозможно достичь эффективного, максимально возможного результата при моделировании угроз безопасности информации [8].

Оценка угроз безопасности информации не может быть построена только на одной матрице, потому что, используя только её не получается затронуть все важные аспекты моделирования угроз, что мы и продемонстрировали. Поэтому рекомендуется рассматривать все исходные данные, по каждому пункту при моделировании угроз по методике, в зависимости от преследуемых целей при оценке угроз безопасности информации. APT группировки, атаки которых в основном направлены на

информационные системы государственных учреждений используют примерно одинаковые сценарии реализации угроз безопасности информации.

Литература

1. Методический документ «Методика моделирования угроз безопасности информации» ФСТЭК России 5 февраля 2021 г.
2. Закон РФ от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Закон РФ от 27.07.2006 г. №152-ФЗ «О персональных данных».
4. Приказ ФСТЭК России от 11 февраля 2013 г. №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
5. Приказ ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
6. Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
7. Постановление Правительства Российской Федерации от 24 октября 2011 г. №861 «О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций)».
8. https://attack.mitre.org/matrices/enterprise/
9. https://mitre-attack.github.io/attack-navigator/
10. https://apt.securelist.com/

УДК 004.056

АНТИФРОД-СИСТЕМА КАК ИНСТРУМЕТ ПРЕДОТВРАЩЕНИЯ МОШЕННИЧЕСТВА

ANTI-FRAUD SYSTEM AS A FRAUD PREVENTION TOOL

Сенцова А.Ю., Тимергазин В.Э., Ильясова Р.И.,
ФГБОУ ВО «Уфимский государственный авиационный технический университет»,
г. Уфа, Российская Федерация

A.Yu. Sentsova, V.E. Timergazin, R.I. Ilyasova,
FSBEI HE “Ufa state aviation technical university”,
Ufa, Russian Federation

e-mail: regiliasova@mail.ru

Аннотация. В статье рассматривается необходимость применения в банковских организациях антифрод-систем, в частности приводится статистика Банка России по мошенническим действиям за период 2019-2020 годов, приводится правовая основа

развития систем противодействия фроду в России, рассматривается единый концепт работы антифрод-систем, классифицируются мошеннические действия, а также приводятся виды систем фрод-мониторинга. Также уделяется внимание классификаторам, по которым можно выявить мошеннические действия в банковской сфере. Актуальность темы не вызывает сомнений в силу того, что почти все банки РФ используют антифрод-системы для противодействия мошенничеству и краже конфиденциальной информации, и данная сфера сейчас активно развивается. Однако, расширение функционала антифрод-систем и увеличение количества методик, применяемых в таких системах, приводит и к усовершенствованию мошеннических схем, используемых злоумышленниками, а банки и регуляторы в последние годы объединяются друг с другом, создавая все новые рекомендации по работе с антифрод-системами и стараются создавать самообучаемые системы, которые способны принимать решение на основе анализа BigData. Таким образом, постоянное совершенствование антифрод-систем является обязательным условием для повышения уровня защищенности банковских систем.

Abstract. The article is about the necessity of using anti-fraud systems in banking organizations, in particular it tells about the statistics of the Bank of Russia on fraudulent activities in the period of 2019-2020, the legal basis of anti-fraud system development in Russia, the unified concept of anti-fraud systems, also fraudulent activities are being classified and the types of fraud monitoring systems are given. The article focuses on classifiers that can be used to identify fraudulent activities in banking sector. The relevance of the topic is beyond doubt since almost all banks in the Russian Federation use anti-fraud systems to counter fraud and theft of confidential information and this area is actively developing nowadays. However, expanding the anti-fraud systems functionality and increasing the number of methods used in such systems also lead to the improvement of fraudulent schemes used by attackers. In the recent years banks and controllers have been uniting, to create new recommendations for working with anti-fraud systems and create self-learning systems that are able to make decisions based on BigData analysis. Thus, continuous improvement of anti-fraud systems is a required condition for improving the level of banking system security.

Ключевые слова: антифрод-система, банки, банковские системы, дистанционное банковское обслуживание, мошенничество, транзакция, фрод-мониторинг.

Keywords: anti-fraud system, banks, banking systems, remote banking, fraud, transaction, fraud monitoring.

Проблемы безопасности информации в автоматизированных банковских системах и в системах дистанционного банковского обслуживания особо актуальны на сегодняшний день. Это связано с увеличивающейся популярностью новых платежных технологий и развития платежных инструментов, но помимо преимуществ, эти тенденции приводят и к мошеннической активности в банковской сфере. Кроме того, расширение функционала антифрод-систем и увеличение количества методик, применяемых в таких системах, приводит и к усовершенствованию мошеннических схем, используемых злоумышленниками. В свою очередь, банки и регуляторы в сфере банковского обслуживания объединяются с целью создания рекомендации по работе с антифрод-системами и стараются создавать самообучаемые системы, которые способны принимать решение на основе анализа BigData. Таким образом, постоянное

совершенствование антифрод-систем является обязательным условием для повышения уровня защищенности банковских систем.

Наиболее подвержены мошенничеству операции с банковскими картами, так как они непосредственно взаимодействует с системами дистанционного банковского обслуживания [1]. По данным Банка России, только за период 2019 года объем операций осуществленных без согласия клиентов посредством мошенничества через банкоматы, терминалы и импринтеры в России составил около 268 млн рублей, через оплату товаров и услуг в интернете составил 1272 млн рублей, через системы дистанционного банковского обслуживания (ДБО) физических лиц и юридических лиц составил 1156 млн рублей. Суммарный объём мошеннических операций составил около 2,7 млрд рублей, когда общий объём операций с использованием электронного кошелька составил 47,1 трлн рублей [2].

В целях предотвращения мошеннических действий, а также противодействия хищений конфиденциальной информации клиентов в финансовой сфере (в частности онлайн-банкинге) прибегают к антифрод-системам. Эти системы занимаются оценкой вероятности того, что совершенная транзакция была осуществлена мошенниками, а не держателем карты.

В простом случае система фрод-мониторинга реализуется путем ограничения суммы платежа. То есть, если платеж больше установленной суммы, это вызывает подозрение и может быть принят за мошенничество. Поэтому необходимо проводить дополнительные проверки для подтверждения данного платежа. [3].

Новые схемы мошеннических действий появляются ежедневно, но и разработчики антифрод-систем также не стоят на месте. Они постоянно совершенствуют и работают над тем, чтобы их программное обеспечение (ПО) подстраивалась под новые условия и своевременно выявляла новые подозрительные операции.

Развитие антифрод-систем в России

Развитие антифрод-систем в России происходило поэтапно. Основным толчком в развитие мониторинговых систем стали зафиксированные инциденты.

Массовые атаки на системы дистанционного банковского обслуживания в 2011-12 гг. Сначала атаке подверглись юридические лица, затем физические. Именно эти случаи, работа банковского трояна «Lurk» и других в 2014-15 гг. помогли найти антифрод-решения.

Законодательно необходимость использования антифрод-систем появилась с принятием Федерального закона от 27.06.2018 № 167-ФЗ «О внесении изменений в отдельные законодательные акты РФ в части противодействия хищению денежных средств», в котором регулируются отношения, возникающие в кредитно-финансовом секторе. Но в то же время выяснялось, что финансовые организации при реализации антифрод-решений теряли больше средств, чем составляли потери из-за мошеннических схем.

Ситуация изменилась, когда в этом же году Сбербанк рассказал о сохранении 32 млрд. рублей благодаря антифрод-системам. Также выяснилось, что большинство мошеннических действий реализуются посредством социальной инженерии и так называемыми «самопереводами». Примерно в 86% случаев клиент сам, под влиянием мошенника, переводит средства на чужой счет.

Сейчас принят ряд законодательных актов, регулирующих работу антифрода и развитие информационной безопасности в банковском секторе, например, №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма» [4].

Виды антифрод-систем

Большинство антифрод-систем работают по единому концепту, состоящему из 5 основных модулей: [5]:

1) отслеживание действий клиента;
2) автоматизированная проверка транзакций (при помощи любых методов: от эвристических до машинного обучения);
3) оценка мошеннического риска;
4) управление пользователями при помощи специально-разработанных интерфейсов;
5) хранение базы данных о действиях клиента.

Если система обнаруживает подозрительные действия пользователя, то она незамедлительно останавливает транзакцию и уведомляет о проблеме оператора, который на основании опыта, базы данных и прочих факторов принимает решения о дальнейшей судьбе транзакции.

Для того чтобы понять принцип работы антифрод-систем необходимо провести классификацию мошеннических действий, направленных на системы дистанционного банковского обслуживания, а также на автоматизированную банковскую систему. Выделяют 4 группы мошеннических операций [6]:

1-я группа – контрактное мошенничество (подделка платежных документов, присвоение чужих счетов, использование чужих документов и др.);

2-я группа – хакерское мошенничество (внесение в электронные сети искажающих или «стирающих» информацию программ);

3-я группа – техническое мошенничество (намеренно неотраженные в отчетности операции);

4-я группа – процедурное мошенничество (проведение неразрешенных типов операций (повлекшие за собой денежные убытки).

Выделяют транзакционный, сессионный и комбинированные антифрод-системы.

Транзакционный антифрод занимается обработкой данных внутрибанковских систем, в особенности в дистанционном банковском обслуживании. Основной задачей данного типа антифрод-систем является выявление тех транзакции, которые не соответствуют обычным операциям клиентов (выявление отклонений от типичного поведения пользователей) и анализ платежей по «черным спискам». Обычно транзакционный антифрод уже при разработке внедрен в дистанционное банковское обслуживание.

Ещё одной задачей транзакционного антифрода является корреляция событий, которые казались незаконными аналитикам через систему сбора и обработки информации, а также анализ существующих мошеннических систем и работа с подозрительными операции и/или информирование о них клиентов.

Транзакционный антифрод анализирует платежные операции и неплатежные активности клиента. Платёжные операции фиксируются через различные каналы обслуживания, такие как интернет-банк, мобильный банк, оплата картами в магазинах и в сети «Интернет», обслуживание в дополнительных офисах банка, операции в банкоматах и другие.

Другие активности клиента, анализируемые транзакционным антифрондом, это неуспешные попытки входа в ДБО, фиксация перемещений пользователя по страницам личного кабинета, изменение информации о себе в кабинете, дата, время и геолокация проведения платёжных операций. На основе этих данных формируется некий стандарт поведение клиента, его типовой профиль и затем фиксируются отклонения от этого стандарта.

Сессионный антифрод, на основе собранных обезличенных данных о пользователе, устройстве, о его окружении помогает фиксировать данные во время пользовательских сессиях и выявлять создание мошеннических сессий. Информация о денежных транзакциях, такие как сумма операций, реквизиты - не собираются.

Совместную работу транзакционного и сессионного антифрода называют комбинированной. Эта связка помогает комплексно подходить к защите средств клиентов и оптимизировать работу с любыми мошенническими действиями, в том числе, с использованием социальной инженерии [7].

Машинное обучение

Распознавание пользователя по различным параметрам производится посредством машинного обучения. При этом антифрод-сервисы в работе с мошенническими действиями используют соответствие информации о клиенте банка, стандартным шаблонам поведения добропорядочных покупателей.

Одним из примеров использования средства машинного обучения является составление шаблонов поведения пользователя на основе алгоритмов кластеризации, фиксируя сумму операций и покупок. Аномалиями будут считаться операции с одной суммой в разные места, переводы маленьких сумм на разные счета.

Благодаря алгоритмам машинного обучения антифрод-система может отслеживать и выявлять подозрительные кейсы, быстро менять параметры фильтров. Средства системы машинного обучения позволяют оптимизировать принятие решений, отклоняют аномальные операции. [8].

Система машинного обучения является гибкой, может подстраиваться в новые расширенные правила.

Недостаток технологии машинного обучения заключается в том, что любое отклонение от шаблонов фиксируется как аномалия. Например, клиент решил провести операцию на нехарактерную сумму, и это будет считаться аномалией.

Для создания и использования системы фрод-мониторинга на основе машинного обучения необходимо определить специальные индикаторы для того, чтобы система могла определять является ли данная операция мошеннической или является легитимной [1].

При выборе критериев для построения модели предотвращения мошеннических действий предлагается использование следующих индикаторов [9]:

1) Динамика осуществления транзакций по счету независимо от установленных лимитов.
2) Параметры геолокации:
   a) транзакция по счёту инициализирована из стран с высоким уровнем мошеннических действий;
   b) осуществление транзакций в другую страну;
   c) транзакции по счёту инициализируются из разных стран за короткий промежуток времени;
3) Параметры размера суммы:
   a) осуществление транзакций на большие суммы денег в тех категориях, где обычно транзакции осуществляются на меньшие суммы (например, продовольственные товары);
   b) оформление транзакции на крупную сумму методом ручного ввода данных;
4) Определение сговора торговых центров с мошенниками:
   a) осуществление серии транзакций из одного магазина за короткий промежуток времени;

b) большое количество возвратов покупки.

5) Зачисления на счет:
   a) серия одинаковых или близких по сумме зачислений на счет;
   b) возврат средств (при возврате товара), покупки которого ранее не осуществлялось.

Антифрод-система, при обработке операций, должна принимать одно из следующих решений:

– пропустить транзакцию без дополнительной проверки;
– отправить транзакцию на дополнительную проверку специалисту антифрод мониторинга;
– прекратить транзакцию без формирования инцидента;
– прекратить транзакцию, заблокировать операции по счету клиента и сформировать инцидент.

Мошеннические операции могут возникать и со стороны работников банковской сферы. Для определения вышеупомянутых действий, со стороны сотрудников возможно использование следующих индикаторов [1]:

– мониторинг досрочного закрытия депозитных счетов и вкладов клиентов;
– отмена ошибочных операций по приходу и расходу в течение одного операционного дня;
– совершение операций по счетам клиентов, длительное время не использующих денежные средства;
– совершение операций по счетам клиентов, попадающих в зону повышенного риска (несовершеннолетние лица, пенсионеры, лица, получающие социальные пособия и пр.);
– массовая выдача кредитных карт, оформление вкладов за короткий промежуток времени на большие суммы

Выводы

Антифрод-системы – это специальное программное обеспечение, способное противостоять кибератакам, злоумышленникам и иного рода мошенничеству в банковских и платежных системах. Благодаря антифрод-системам оперативно выявляются подозрительные транзакции и предотвращается потеря денежных средств клиентов. Однако фрод-мониторинг пока что имеет ряд досадных недостатков: вероятность ошибочной блокировки платежей и переводов, невозможность противостоять человеческому фактору. Если антифрод-система будет часто отклонять платежи и переводы клиентов банка из-за того, что они кажутся подозрительными, то организация начнет терять клиентов, недовольных ограничениями в распоряжении собственными финансами.

Банковское мошенничество останется довольно актуальной проблемой еще очень долго, но внедрение банками антифрод-систем может колоссально снизить количество мошеннических действий. Сегодня существует большое разнообразие антифрод-систем от различных производителей: Featurespace, FICO Application Fraud Manager, FraudWall (компания Фродекс) и другие.

Литература

1. Разина, О.М., Костерина Т.М., «Инновационные инструменты фрод-мониторинга в практике внутреннего аудита банка», 2015.

2. Банк России, «Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств», 2020 [Электронный ресурс]. – Режим доступа: https://clck.ru/Xnb5A

3. Левашов М.В., Овчинников П.В., «Эффективность классификаторов для выявления фрода в финансовых транзакциях», 2019.

4. Д. Слободенюк, «Антифрод в российских реалиях», 2020 [Электронный ресурс]. – Режим доступа: https://clck.ru/Xnb74

5. Кудряшова О.А., Ильина А.В. «Аналитическая система антифрод как комплекс мер для оценки риска финансовых транзакций» // Актуальные вопросы экономической теории: развитие и применение в практике российских преобразований: материалы VII междунар. науч.-практ. конф. Уфа: УГАТУ, 2018. С. 193-196.

6. Ушанов А.Е. «Внедрение процессных инноваций в банке как ответ на новые вызовы» // Российское предпринимательство. 2018/ №4. С. 1135-1142.

7. Itweek, 2020 [Электронный ресурс]. – Режим доступа: https://clck.ru/Xnb9C

8. А. Вичугова, «Умный антифрод: как Big Data и Machine Learning защищают ваши деньги», 2020 [Электронный ресурс]. – Режим доступа: https://clck.ru/XnbAu

9. Логачев В.Г., Карякин Ю.Е., Игнатьева А.М., Любякина Е.А. «Проблема выбора критериев для построения математической модели процесса предотвращения несанкционированных переводов денежных средств в системах дистанционного банковского обслуживания».

УДК 004.056

ИСПОЛЬЗОВАНИЕ МЕТОДА, ОСНОВАННОГО НА МАРКОВСКИХ МОДЕЛЯХ, ДЛЯ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

USING THE METHOD BASED ON MARKOV MODELS TO ASSESS INFORMATION SECURITY RISKS

Цветкова И.С., Сенцова А.Ю.,
ФГБОУ ВО «Уфимский государственный авиационный технический университет»,
г. Уфа, Российская Федерация

I.S. Tsvetkova, A.U. Sentsova,
Ufa State Aviation Technical University,
Ufa, Russian Federation

e-mail: in.tsvetckowa@yandex.ru

Аннотация. В настоящее время деятельность любой организации становится всё более зависимой от информационных технологий. С усилением важности роли информационных систем в бизнес-процессах возрастает необходимость обеспечения информационной безопасности информационных систем, даже если в системе не используется информация ограниченного доступа, так как к негативным последствиям могут привести утрата целостности и доступности информации. В статье выделены два подхода к обеспечению информационной безопасности, проанализированы действующие нормативные акты Российской Федерации, регламентирующие процесс

оценки рисков нарушения информационной безопасности, и некоторые наиболее распространённые методики оценки риска. Определены недостатки методик качественной и количественной оценок риска. В качестве решения некоторых недостатков в статье предлагается использование метода, основанного на марковских моделях, который применяется для оценки рисков физической безопасности. Определены входные данные, приведено описание математического аппарата метода. Формализовав сбор входных данных, метод оценки риска можно реализовать в виде программного обеспечения и автоматизировать процесс оценки. Метод позволит учитывать в оценке риска жизненный цикл атаки на информационную систему, этапы которого также упомянуты в тексте данной статьи.

Abstract. Currently, the activities of any organization is becoming more and more dependent on information technology. With the increasing importance of the role of information systems in business processes, the need to ensure information security of information systems increases, even if the system does not use restricted information, since the loss of the integrity and availability of information can lead to negative consequences. The article highlights two approaches to ensuring information security, analyzes the current regulatory acts of the Russian Federation governing the process of assessing the risks of information security breaches, and some of the most common risk assessment methods. The drawbacks of the methods of qualitative and quantitative risk assessment have been identified. As a solution to some of the shortcomings, the article proposes the use of a method based on Markov models, which is used to assess physical security risks. The input data are determined, the description of the mathematical apparatus of the method is given. By formalizing the collection of input data, the risk assessment method can be implemented in software and the assessment process can be automated. The method will make it possible to take into account in the risk assessment the life cycle of an attack on an information system, the stages of which are also mentioned in the text of this article.

Ключевые слова: информационная безопасность, риски информационной безопасности, управление рисками, оценка рисков, марковские модели, жизненный цикл атаки.

Keywords: information security, information security risk, risk management, risk assessment, Markov models, life cycle of an attack.

В настоящее время деятельность любой организации становится всё более зависимой от информационных технологий. Информационные системы участвуют в процессе решения самых разных задач: от автоматизации торговли до автоматизированного управления технологическими процессами. Соответственно, с усилением важности роли информационных систем в бизнес-процессах возрастает необходимость обеспечения информационной безопасности (ИБ) информационных систем, даже если в системе не используется информация ограниченного доступа, так как к негативным последствиям могут привести утрата целостности и доступности информации.

В обеспечении информационной безопасности можно выделить два подхода [1]:

1. Обеспечение базового уровня ИБ.
2. Оценка и управление рисками ИБ.

При обеспечении базового уровня ИБ информационная система проверяется на защищённость от основных угроз информационной безопасности и на соответствие требованиям стандартов и других документов. Второй подход – оценка и управление

рисками – содержит в себе большее количество задач: анализ всех возможных угроз и вероятности их реализации, оценка ценности активов и возможного ущерба в случае инцидента ИБ и, наконец, определение уровня риска, а также его снижение до заданного приемлемого уровня.

Разные источники приводят разные понятия того, что представляет собой риск нарушения информационной безопасности, однако многие сходятся, что это некое событие, которое при возникновении отличается нежелательными – возможно, разрушительными – последствиями.

Основой российской нормативной базы, регламентирующей оценку рисков, является ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

Также вопросы управления рисками регулируют стандарты:

1. ГОСТ Р ИСО 31000-2019. «Менеджмент риска. Принципы и руководство»;
2. ГОСТ Р ИСО/МЭК 13335-1-2006. «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий»;
3. ГОСТ Р ИСО/МЭК 27002-2012. «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»;
4. РС БР ИББС-2.2-2009. «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности».

ГОСТ Р ИСО 31000-2019 [2] регламентирует основные принципы и содержит практическое руководство относительно процесса менеджмента любого вида рисков на предприятии, однако в нём не учитывается специфика области информационной безопасности, а также нет подробных рекомендаций относительно процесса оценки риска.

Один из первых стандартов Российской федерации, регламентирующий управление рисками ИБ – ГОСТ Р ИСО/МЭК 13335-1-2006 [3] – лишь предписывает осуществление выбора и применения защитных мер на основании определенной методологии управления рисками. Конкретной методологии менеджмента риска документ не предлагает.

В ГОСТ Р ИСО/МЭК 27002-2012 [4] уже формируется концепция ИБ и появляются некоторые требования к оценке риска: она должна быть количественной и нести регулярный характер, чтобы учитывать любые изменения, которые могли бы повлиять на результаты оценки.

В отличие от перечисленных выше стандартов, которые рассматривают оценку риска ИБ лишь поверхностно и, таким образом, имеют низкую практическую ценность, ГОСТ Р ИСО/МЭК 27005-2010 [5] содержит рекомендации для практического применения. Документ рекомендует использовать качественную оценку для получения общих сведений об уровне риска, а для более детального рассмотрения риска переходить к количественной: установке численных значений риска в соответствие качественным по заранее определенной шкале. Однако формирование количественных шкал стандартом не регламентируется, что делает его хорошей основой для разработки собственной методики оценки риска ИБ.

Высокую практическую ценность имеет РС БР ИББС-2.2-2009 [6], так как в этом документе приведен структурированный и подробный алгоритм оценки риска ИБ как качественных, так и в количественных значениях в денежной форме (в том числе, шаблоны для документирования каждого этапа процесса оценки и шкала соответствия

качественных значений количественным). Но данный стандарт применим только в банковской сфере, так как в качестве информационных активов в основном рассматривает информацию обеспечения банковских технологических операций, а также регламентирует ущерб от реализации угрозы только в денежном выражении, не рассматривая социальные, репутационные и другие риски ИБ.

Таким образом, на сегодняшний день не существует единой методики анализа информационных рисков, которая была бы закреплена в нормативных документах. Каждая организация самостоятельно подбирает метод оценки риска исходя, например, из возможностей и инструментов, которыми она располагает.

Все существующие на сегодняшний день методики оценки риска нарушения ИБ принято делить на:

1) методики, использующие качественную оценку;

2) методики, оценивающие риск в количественном выражении, т.е. через числовое значение [1].

К первому виду методов можно отнести CRAMM, OCTAVE, MSAT, FRAP и другие. Они выражают уровень риска по определённой шкале. Например, «высокий», «средний», «низкий». Как недостатки таких методов оценки можно выделить следующее:

– сбор входных данных здесь основывается на экспертных оценках с использованием опросных карт, интервьюирования, метода «мозгового штурма» и т.д.;

– невозможно оценить ущерб в более конкретных значениях. Например, в денежном эквиваленте причинённого инцидентом ущерба.

Методы, относящиеся ко второму виду – ГРИФ, RiskWatch и т.п. – вычисляют уровень риска в численном выражении причинённого ущерба определённому активу в случае реализации конкретной угрозы. Также эти методы позволяют посчитать экономическую выгоду от принятия конкретного набора контрмер. Недостаток методов количественной оценки в том, что в качестве входных данных от организации требуется статистика реальных инцидентов информационной безопасности, а также ущерба, который повлекла реализация той или иной угрозы.

Методический документ, регламентирующий методику оценки угроз, который утверждён ФСТЭК в этом году, требует, чтобы оценка рисков нарушения информационной безопасности на объектах критической информационной инфраструктуры (КИИ) велась с учётом этапов жизненного цикла атаки, чего не имеет ни один из уже упомянутых в данной статье методов оценки.

В качестве решения в статье предлагается использование метода, основанного на марковских моделях, который ранее применялся только для оценки рисков физической безопасности [7].

Входные данные, которые требуется определить во время анализа рисков, — это время, затрачиваемое злоумышленником на реализацию каждого этапа атаки, а также величина ущерба, который понесёт организация в случае реализации определённой угрозы над конкретным активом.

В качестве этапов жизненного цикла атаки приняты:

1) Внешняя разведка (социальная инженерия, фишинг и т.п.);
2) Сканирование системы (сканирование портов: выявление компьютеров, подключенных к интернету, выявление запущенных служб);
3) Нахождение точки входа и повышение привилегий (вертикальное и горизонтальное повышение привилегий);
4) Эксфильтрация (кража данных, их искажение, уничтожение);
5) Осуществление деструктивных воздействий на систему;

6) Обфускация (скрытие следов атаки и присутствия злоумышленника в системе).

Марковские модели для каждой угрозы представляются в виде графа (рисунок 1), описывающего изменения состояния информационной системы в результате действий злоумышленника во время атаки на цель h_k и действий системы защиты, где d_0 – состояние системы при отсутствии атак; $d_1 \ldots d_m$ – промежуточные состояния между d_0 и h_k, которые соответствуют завершению злоумышленником определённого этапа атаки; $t_1 \ldots t_m$ – время, затрачиваемое на реализацию каждого этапа атаки; t_0 – время обнаружения действий злоумышленника средствами защиты.

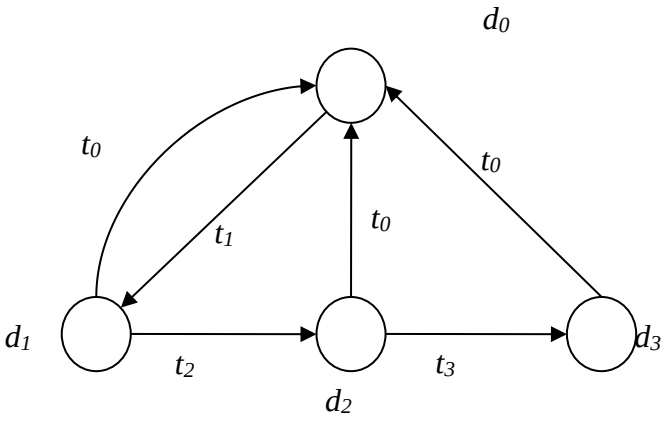

Рисунок 1. Марковская модель,
описывающая изменения состояния информационной системы

Чтобы получить марковскую модель в дискретном времени, нужно единичные элементы матрицы смежности графа заменить переходными вероятностями:

$$p_{ij} = \lambda_{ij} \cdot \Delta t,$$

где Δt — период времени, в течение которого может быть совершено не более одного перехода в рамках данного этапа атаки,
λ_{ij} — интенсивность перехода, из i-того в j-тое состояние или интенсивность действий реагирования на злоумышленника.

Величина λ_i определяется по формуле:

$$\lambda_i = \frac{1}{t_i},$$

где t_i — среднее время выполнения i-го действия, которое зависит от времени, необходимого на проведение этапа атаки, а также от времени обнаружения злоумышленника.

Вероятность нахождения системы в j-ом состоянии после n интервалов времени рассчитывается по формуле:

$$P_j(n) = M_0 \cdot P^n \cdot D_j, \qquad (1)$$

где $M_0 = [P_1(0)\ P_2(0)\ \dots\ P_N(0)]$ – вектор-строка вероятностей начального состояния системы,
P – матрица переходных вероятностей,
$D_j = [0\ 0\ \dots 1\ \dots 0]^T_{N\times 1}$ – вектор-столбец индикатора анализируемого состояния: единица стоит в позиции, соответствующей порядковому номеру состояния.

По формуле 2 рассчитываются вероятности нахождения системы в j-ом состоянии, где P_i – финальная вероятность нахождения системы в состоянии i, λ_i – интенсивность перехода из состояния i в j.

$$\begin{cases} \sum_{i=1}^{n} \lambda_{ij} \cdot P_i(t) \cdot P_j(t) \cdot \sum_{z=1}^{m} \lambda_{iz} = 0 \\ \sum_{i=1}^{N} P_i(t) = 1 \end{cases}, \qquad (2)$$

При этом первое уравнение записывается для каждого состояния j, в которое система может перейти из множества состояний I в состояния Z.

После того, как найдены финальные вероятности, можно переходить к вычислению значений рисков по формуле 3, где C_k — это значение ущерба в случае перехода системы в это состояние.

$$C_\Sigma = \sum_k P_k \cdot C_k \qquad (3)$$

Выводы

Метод оценки рисков, основанный на марковских моделях, можно применять не только для оценки физической, но и информационной безопасности. Поскольку у метода имеется математический аппарат, формализовав сбор входных данных, его можно реализовать в виде программного обеспечения и автоматизировать процесс оценки рисков ИБ. Метод позволит учитывать в оценке рисков жизненный цикл атаки на информационную систему, и таким образом, выполнить требования действующих нормативных правовых документов, а также разрешить проблему субъективности экспертной оценки, которая присутствует в большинстве используемых методов.

Литература

1. Баранова Е.К. Методики анализа и оценки рисков информационной безопасности // Образовательные ресурсы и технологии. 2015. №1(9). С. 73–79.
2. ГОСТ Р ИСО 31000-2019. Менеджмент риска. Принципы и руководство. – Москва: Стандартинформ, 2020.
3. ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. – Москва: Стандартинформ, 2007.
4. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. – Москва: Стандартинформ, 2014.
5. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – Москва: Стандартинформ, 2011.
6. РС БР ИББС-2.2-2009. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков

нарушения информационной безопасности. – Вестник Банка России. 2009. №71.

7. Машкина И.В., Степанова Е.С., Вишнякова Т.О. Анализ рисков объектов информатизации: учебное пособие /И. В. Машкина, Е. С. Степанова, Т. О. Вишнякова – Уфа: УГАТУ, 2011. – 112 с.

УДК 004.414

РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ ОБУЧЕНИЯ И ПОВЫШЕНИЯ НАВЫКОВ ПОЛЬЗОВАТЕЛЕЙ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

DEVELOPMENT OF AN INFORMATION SYSTEM FOR TRAINING AND IMPROVING THE SKILLS OF USERS IN THE FIELD OF CYBERSECURITY

Ратковский А.А., Муталлапов Р.Н.,
Уфимский государственный нефтяной технический университет,
филиал в г. Салават, ул. Губкина, 22б, г. Салават, Республика Башкортостан,
г. Салават, Российская Федерация

A.A. Ratkovsky, R.N. Mutallapov,
Ufa State Petroleum Technological University, Branch in the Salavat,
Gubkin Str., 22b, Salavat, Republic of Bashkortostan,
Salavat, Russian Federation

e-mail: alexwells.corp@gmail.com

Аннотация. Вопросы минимизации рисков утечки информации на предприятии по вине внутреннего пользователя из-за плохой осведомленности в области кибербезопасности являются в современных условиях жизни для компаний наиболее актуальными, т.к. утечка информации влечет за собой раскрытие корпоративной информации и документов, утечку личных данных сотрудников, а также финансовые и репутационные потери. Качество подготовки профессионалов – специалистов с высшим образованием, осведомленных и имеющих навыки в области защиты и кибербезопасности, является одним из приоритетных направлений. В данной статье приведены данные и графики относительно утечек информации на предприятиях по вине внутреннего пользователя за период от 2004 года по 2019 год. Рассмотрен стандарт проведения аудита по направлению кибербезопасности на территории компании или предприятия для минимизации рисков утечки информации. Выявлены причины возникновения проблемы и рассмотрены возможные варианты решения для сохранения репутационного статуса компании или предприятия, а также минимизация рисков финансовых потерь в случае утечки. Кроме того, были отмечены цель разработки и преимущества разработки информационной системы обучения пользователей в области кибербезопасноти.

Abstract. The issues of minimizing the risks of information leakage at the enterprise due to the fault of the internal user due to poor awareness in the field of cybersecurity are the most relevant for companies in modern conditions of life, since information leakage entails the disclosure of corporate information and documents, the leakage of personal data of employees,

as well as financial and reputational losses. The quality of training of professionals-specialists with higher education, knowledgeable and with skills in the field of security and cybersecurity, is one of the priorities. This article provides data and graphs on information leaks at enterprises caused by an internal user for the period from 2004 to 2019. The standard of conducting an audit in the direction of cybersecurity on the territory of a company or enterprise to minimize the risks of information leakage is considered. The causes of the problem are identified and possible solutions for saving are considered

Ключевые слова: утечка информации, минимизация рисков, обучение сотрудников, кибербезопасность, разработка, информационная система**.**

Keywords: information leakage, risk minimization, employee training, cybersecurity, development, information system.

В 2019 году Экспертно-аналитический центр InfoWatch по всему миру зафиксировал 1348 утечек, случившиеся по вине или по неосторожности внутренних нарушителей.

На графике заметно, что очевидного тренда, описывающего динамику утечек указанного типа (внутренних утечек), на горизонте 2004-2019 гг. не наблюдается (рисунок 1) [1].

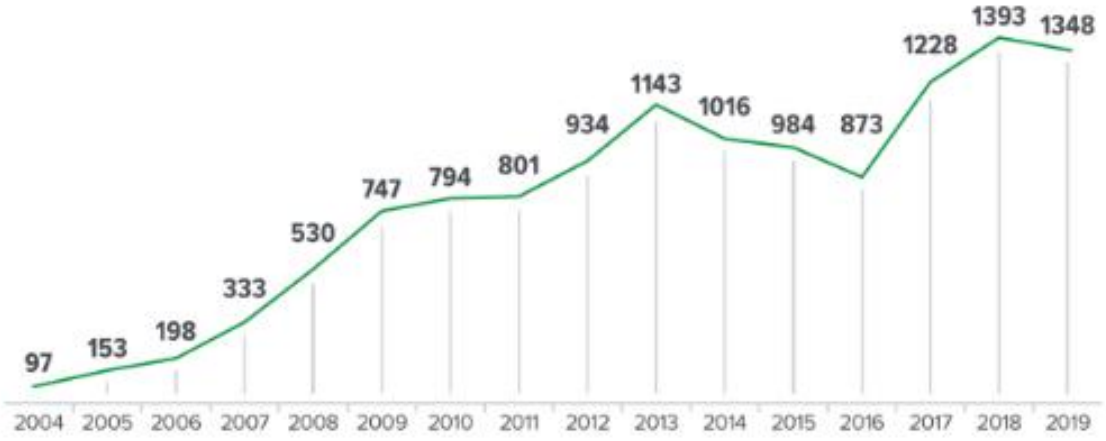

Рисунок 1. Число внутренних утечек информации, 2004-2019 гг.

Так рост числа внутренних утечек, отмечавшийся в 2017-2018 годах, в 2019 году сменился небольшим снижением (на 3,3%).

Более показательно снижение доли внутренних утечек от общего числа утечек – как видно на диаграмме, если в 2018 году этот показатель составлял 61,6%, то в 2019 году доля внутренних утечек составила 53,7%.

При этом уже четыре года подряд доля внутренних утечек от общего числа утечек остается в диапазоне 53-61%, т.е. все эти годы более половины всех утечек, зафиксированных в мире, происходят не по причине воздействия внешних хакеров, а из-за ошибок или умышленных действий сотрудников (в широком смысле, включая руководство) владельцев и операторов информации (рисунок 2).

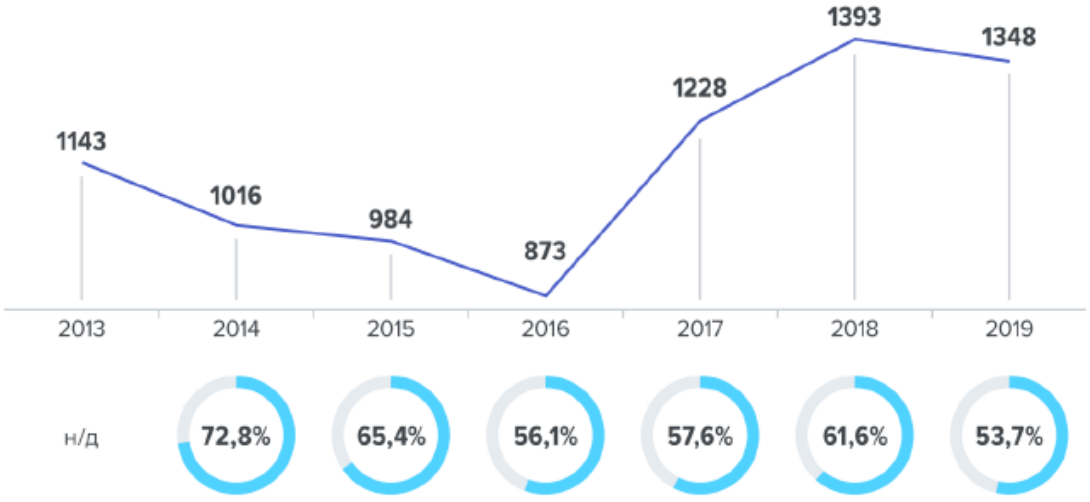

Рисунок 2. Число внутренних утечек информации
и доля утечек этого типа от общего числа утечек, 2013-2019 гг.

Совокупный объем данных, скомпрометированных в результате внутренних утечек, в 2019 году составил 9,87 млрд. записей. Впервые за все время наблюдений объем записей, скомпрометированных в результате внутренних утечек, превысил аналогичный показатель для утечек внешних (в 2019 году в результате внешних утечек скомпрометировано 4,7 млрд записей).

В динамике также видно, что первый заметный пик объема скомпрометированных данных применительно к внутренним утечкам наблюдался в 2017 году – тогда объем скомпрометированных записей вырос почти в 10 раз. Пик 2019 года динамически более скромный – по сравнению с данными 2018 года объем скомпрометированных записей вырос «всего лишь» в 3,6 раза (рисунок 3).

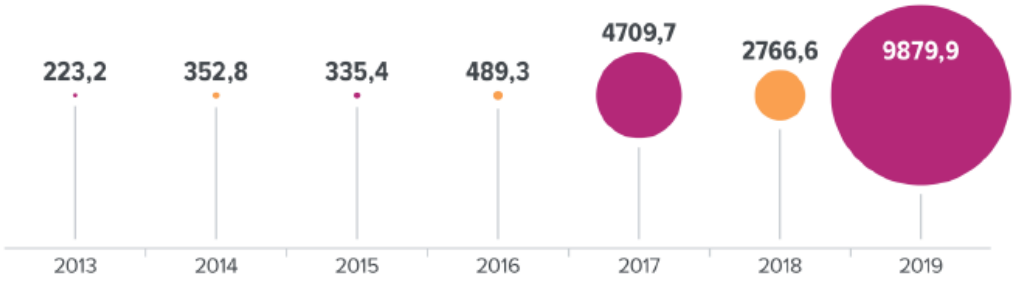

Рисунок 3. Объем данных, скомпрометированных в результате «внутренних» утечек,
млн. записей, 2013-2019 гг.

Естественно такие утечки несут за собой большие финансовые и репутационные потери компании. На текущий момент исследование показало, что в России около 80% утечек персональной и корпоративной информации приходится именно на сотрудников компании в связи с их неосведомленностью в области защиты и кибербезопасности [2].

Чаще всего такие проблемы связаны из-за неосведомленности внутреннего пользователя и информационные системы для обучения и повышения навыков в области кибербезопасности признаны бороться с данной проблемой.

Стоит отметить, что кибербезопасность является одним из разделов информационной безопасности, а согласно требованиям ГОСТ Р ИСО/МЭК 27007-2014,

для обеспечения информационной безопасности требуется регулярно проводить аудит информационных систем [3].

Для минимизации риска человеческого фактора необходимо регулярно проводить обучение сотрудников предприятия, которое в последующем будет мотивировать сотрудников помнить о кибербезопасности в повседневной работе.

Применение типовых информационных систем для данной процедуры невозможно, по причине специфичности проведения обучения. Следовательно, разработка новой информационной системы под данную процедуру, позволит получить возможности типовых информационных систем для обучения, а также внести в нее возможности оценки и практического закрепления знаний.

Из всего этого выходит новая цель – повышение навыков сотрудников в области кибербезопасности и достижение максимальной минимизации рисков утечки информации на предприятии по вине внутреннего пользователя при помощи информационной системы.

Новая информационная система (ИС) позволит снизить организационные риски при планировании и проведении обучения.

Система в автоматическом режиме будет отслеживать успеваемость сотрудников, а также проверять выполненные ими работы и сравнивать их на соответствие реальным данным в базе данных.

Внедрение такой ИС в корпоративную среду компании позволит снизить затраты на отправление сотрудников на обучение или в командировку на определенное место проведения. К тому же, ее возможности позволяют выполнить интеграцию с большим списком корпоративных информационных систем, которые используются внутри компании.

Структура ИС представлена на рисунке 4.

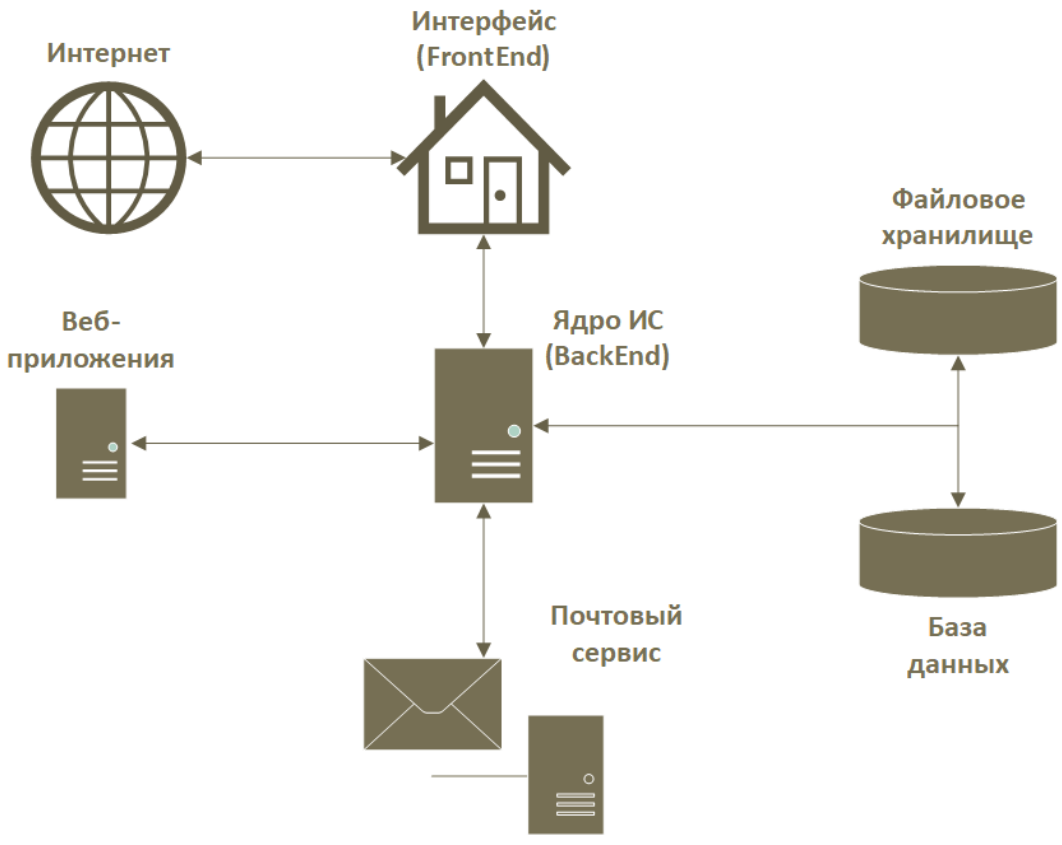

Рисунок 4. Структура информационной системы

Особенностью ИС является симуляция фишинговой атаки с целью проверки усвоенного материала. Также кроме запланированной симуляции можно сгенерировать собственную на определенных пользователей или же на массовую рассылку и настроить ее согласно своим предпочтениям для более точного и детального анализа усвоенного материала.

Для более качественного обучения материал предоставляется сотрудникам на основе их должности и уже имеющихся навыков и знаний в области кибербезопасности.

Разграничение доступа в систему представлена на рисунке 5.

Рисунок 5. Разграничения доступа в систему

Выводы

Постоянно организовываются аудиты или же курсы повышения квалификации сотрудников, на которых рассматриваются вопросы кибербезопасности. Применение информационной системы в их обучении – процесс, открывающий возможности развития компаний в заявленной сфере, при этом минимизируя возможный риск утечки информации в связи с осведомленностью сотрудников в области защиты и кибербезопасности.

Литература

1. Отчет по утечкам информации [Электронный ресурс]. – URL: https://www.infowatch.ru/analytics (дата обращения: 17.04.2021).

2. Пасад, П. «Mastering Modern Web Penetration Testing» [Текст] / П. Пасад. – Livery Place: Packt Publishing Ltd, 2016. – 269 с.

3. ГОСТ Р ИСО/МЭК 27007-2014. Руководства по аудиту систем менеджмента информационной безопасности [Электронный ресурс]. – URL: https://docs.cntd.ru/document/1200112881 (дата обращения: 18.04.2021).

УДК 004.942

РАЗРАБОТКА МОДЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПРИМЕНЕНИЕМ ПРОДУКЦИОННОЙ МОДЕЛИ

DEVELOPMENT OF INFORMATION SECURITY MODEL WITH APPLICATION OF PRODUCTION MODEL

Джафарова Ш.М.,
Сумгаитский государственный университет,
г. Сумгаит, Республика Азербайджан

Sh.M. Jafarova,
Sumgayit State University,
Sumqayit, Republic of Azerbaijan

e-mail: salala.cafarova@mail.ru

Аннотация. В представление знаний продукционные модели можно считать наиболее распространенными. Достоинства систем, основанных на продукционных моделях, заключаются в простоте представления знаний и организации логического вывода. В продукционной базе знаний основным преимуществом является простота анализа, которая является дополнением и модификацией определенных продукционных правил.

Продукционные модели знаний по своей сути близки к логической речи, что позволяет организовать процедуры для логического вывода данных. С другой стороны, если мы сравним продукционные модели знаний с логическими моделями, то первые отражают знания быстрее, что является неоспоримым преимуществом. Поэтому продукционные модели знаний являются одним из основных средств представления знаний в системах искусственного интеллекта.

Каждое из правил, обеспечивающих базу знаний продукционной системы состоит из условной и заключительной части.

Условная часть состоит из одного или нескольких фактов в сочетании с сопряжением.

Заключительная часть содержит факты, необходимые для заполнения рабочей памяти (если условная часть правила верна).

Существует два способа внедрения продукционных систем: прямой и обратный.

Прямой результат называется направлением данных или направлением вниз. В таких системах поиск переходит от исходных данных (фактов) к результатам. То есть проверяются условия *A*, состоящие из известных фактов, и активируются продукты, для которых *A* соответствует действительности.

Нечеткие продукционные правила представлены в виде структурных элементов правилами нечетких продуктов.

Разработана модель управления информационной безопасностью.

На основе правил нечетких продуктов модель управления информационной безопасностью в облачных технологиях анализируются как технология обработки, атак, хранения и защиты информации.

Abstract. In knowledge representation, production models can be considered the most common. The advantages of systems based on production models lie in the simplicity of

representing knowledge and organizing inference. In the production knowledge base, the main advantage is the simplicity of analysis, which is an addition and modification of certain production rules.

Production knowledge models are inherently close to logical speech, which allows organizing procedures for logical inference of data. On the other hand, if we compare the production models of knowledge with logical models, the former reflect knowledge faster, which is an indisputable advantage. Therefore, production models of knowledge are one of the main means of representing knowledge in artificial intelligence systems.

Each of the rules providing the knowledge base of the production system consists of a conditional and a final part.

A conditional part consists of one or more facts combined with a conjugation.

The final part contains the facts necessary to fill the working memory (if the conditional part of the rule is correct).

There are two ways to implement product systems: direct and reverse.

The direct result is called data direction or downward direction. In such systems, the search moves from the original data (facts) to the results. That is, conditions A, consisting of known facts, are checked, and products for which A corresponds to reality are activated.

Fuzzy production rules are represented as structural elements by the rules of fuzzy products.

An information security management model has been developed.

Based on the rules of fuzzy products, the information security management model in cloud technologies is analyzed as a technology for processing, attacking, storing and protecting information.

Ключевые слова: правила, модель, облачная технология, безопасность, продукционная система, нечеткие продукции.

Keywords: rules, model, cloud technology, security, production system, fuzzy products.

Концепция облачных технологий предусматривает создание и использование инфраструктуры компьютерных технологий и программного обеспечения в прямой сетевой среде. Благодаря этой технологии пользовательские данные хранятся и обрабатываются в облачных системах, и в то же время с помощью браузеров запускаются программы обработки и просматриваются результаты.

Инфраструктура системы облачных технологий предусматривает создание центров обработки и хранения данных с широким использованием кластеризации и виртуализации компьютерных вычислений и ресурсов памяти [1-4].

В настоящее время облачные технологии широко используются с большими вычислительными ресурсами и ресурсами памяти, необходимыми для решения сложных задач. В этом случае пользователям, работающим в разных организациях или предприятиях, выгоднее использовать высокоскоростные каналы связи и услуги облачной системы. Передача данных таким образом создает основу для их слабой защиты. Потому такая информация обрабатывается вне ее владельцев. В настоящее время проблема уровня безопасности облачных сервисов очень высока, и с этой точки зрения продукционная моделирования и исследование информационной безопасности в облачных технологиях является одним из ключевых вопросов.

Облачные технологии обычно позволяют создавать и использовать программное обеспечение компьютерных технологий в прямой сетевой среде. С помощью этой технологии пользовательские данные хранятся и обрабатываются в облачных системах

и организуют работу программ обработки и просмотра результатов через определенные браузеры. В последнее время инфраструктура системы облачных технологий широко используется при кластеризации и виртуализации вычислительных ресурсов и ресурсов памяти компьютеров. Это обеспечивает создание центров обработки и хранения данных.

В настоящее время во всем мире проводятся интенсивные исследования по эффективному использованию вычислительных ресурсов и ресурсов памяти с помощью облачных технологий. Эффективное использование больших информационных ресурсов, работающих в неопределенной среде на основе этой технологии, среди пользователей сети и моделирования их безопасности является актуальным.

В настоящее время наиболее часто используемыми сервисами в облачной системе являются:

– программное обеспечение как услуга (SaaS – Software-as-a-Service). Этот сервис считается новым шагом в развитии информационных технологий облачных вычислений. Первоначально эта служба применялась только в случае удаления резервных копий. Опыт, накопленный в этой области, заложил основу для использования сетей VPN (виртуальных частных сетей).

– инфраструктура как услуга (IaaS – Infrastructure as a Service). Здесь осуществляется процесс создания инфраструктуры. Уровень IaaS позволяет внедрить услугу аренды инфраструктуры (вычислительные ресурсы и память). Для решения проблем на этом уровне создается компьютерная инфраструктура.

– платформа как услуга (PaaS – Platform as a Service). Сервис PaaS – это виртуальная платформа, которая позволяет пользователям использовать операционные системы, специальные программные приложения (Apache, MySQL и т.д.) и базы данных, расположенные на виртуальных серверах. Здесь клиент также не управляет и не проверяет структуру облака как сеть, сервер. Он контролирует функциональное программное обеспечение, которое здесь установлено [7, 9].

Компьютерные теоретики утверждают, что будущее Интернета лежит в этой технологии. Ожидается, что в будущем жесткие диски будут заменены онлайн-облаками, а функциональные приложения будут полностью использоваться через онлайн-сеть без какой-либо инфраструктуры. Однако применение информационных технологий таким образом, конечно, не исключает, что многие компании, обеспечивающие обмен информацией в обществе, столкнутся с юридическими проблемами. Потому что замена всех системных приложений открытой инфраструктурой увеличивает риск нежелательного доступа к личной информации.

Форма открытого распространения данных в облачных технологиях показывает, что многие фирмы и компании, обменивающиеся информацией, столкнутся с проблемами безопасности. Потому что в этом случае, когда система работает с открытой инфраструктурой, возникает опасность нежелательного доступа к личной информации [5, 8].

Передача данных в таком виде приводит к их слабой защите. Иногда, поскольку информация обрабатывается за пределами владельцев компьютеров, их безопасность не обеспечивается.

Продукционная модель, предназначенная для управления информационной безопасностью в облачных технологиях, реализуется в несколько этапов.

На которых анализируются как технология обработки, так и хранение, и защита данных.

Модель управления информационной безопасностью, разработанная в облачной технологии (рисунок 1), разработана в соответствии с нечеткими правилами производства:

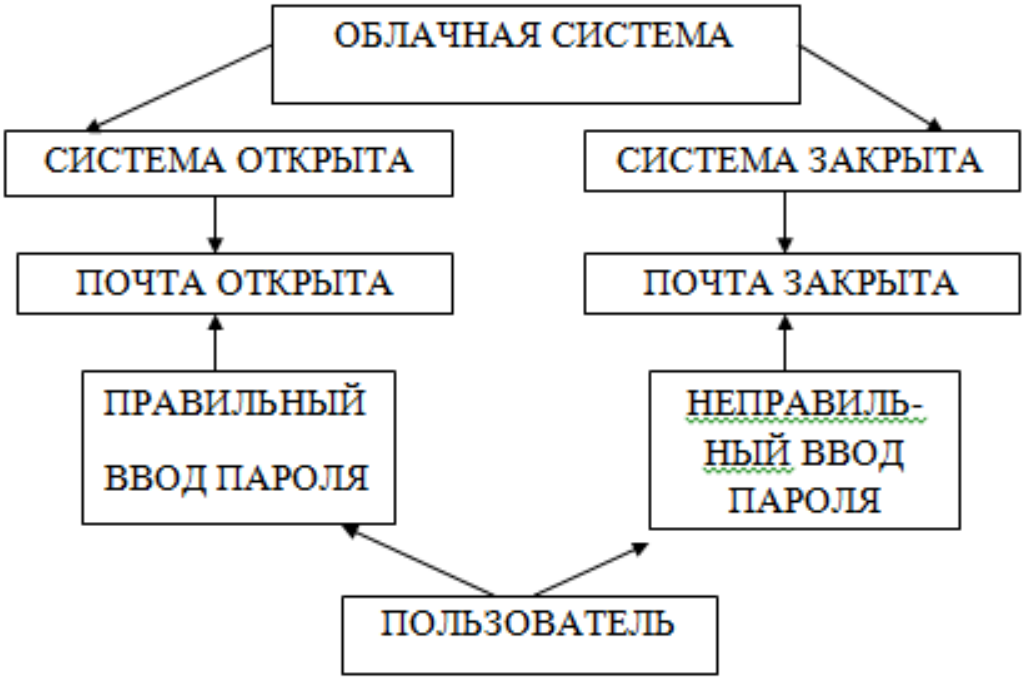

Рисунок 1. Модель управления информационной безопасностью

(СО) – система открывается,
(ПО) – почта открывается,
(СЗ) – система закрывается,
(ПЗ) – почта закрыта,
(ПП) – пароль введен правильно,
(НП) – неверный ввод пароля [6].

Особенностью нечетких моделей является то, что они должны обеспечивать гибкую стратегию обработки разнородных динамических взаимодействующих процессов, которые представляют данные и знания в существенно нечетком пространстве состояний объектов анализа.

Динамические взаимодействующие процессы описываются числовыми и лингвистическими переменными.

В связи с этим:

– нечеткие модели ориентированы на моделирование элементов системы на уровне лингвистических термов (нечетких множеств);

– характеристики системы описываются в лингвистическом формате;

– представление и обработка данных – в условиях неопределенности.

Нечеткие модели базируются на правилах. Эти правили являются наглядным и эффективным средством представления взаимодействующих динамических процессов. Они отображаются данные и знание в виде *«ЕСЛИ … ТО»*.

Здесь «*ЕСЛИ»* – называется посылкой, а «*ТО*» выводом или действием.
В общем виде продукция выражается в следующем виде [10]:

$$(i): W; P; A \Rightarrow B, S, F, N$$

где i – имя продукции;

W – характеризует сферу применения продукций;
$A \Rightarrow B$ – ядра и важная составляющая продукций;
P – определяет условие применимости ядра продукции;
S – метод определения количественных значений степени точности результата ядра;
F – коэффициент точности нечетких продуктов;
n – определяет постусловие продукции.

В реальных конструкциях ядра составляющая *A* характеризуется сложной структурой, включающей также некоторые предикаты, логические операции типа *NOT, AND, OR* и их производные.

Рассмотрим структуру правила продукции в четком представлении знаний:

$$ЕСЛИ \quad A_1 \quad и \quad A_2 \quad и \ldots и \quad A_n \quad ТО \quad B \qquad (1)$$

Такая запись означает, что «если все условия от A_1 до A_n являются истиной, то *B* также истина» или же «когда все условия от A_1 до A_n становятся истиной, то следует выполнить действие *B*».

Выражение (1) на языке булевой логики имеет вид:

$$B = TRUE \,/\, (A_1 \ and \ A_2 \ and \ \ldots \ and \ A_n) = TRUE \qquad (2)$$

Аналогично (1), (2) можно показать справедливость соответствующих решений для правил продукций и содержащих операции *НЕ, ИЛИ* и их производные.

Выражения (1) и (2) в нечетком представлении определяется следующим образом:

$$IF \ \overline{A_1} \ \ is \ \ \mu_{\overline{A_1}}(k) \ \ and \ \ \overline{A_2} \ \ is \ \mu_{\overline{A_2}}(k) \ \ and \ \ldots \ and \ \ \overline{A_n} \ \ is \ \mu_{\overline{A_n}}(k)$$
$$THEN \ \ B \ \ \ is \ \ \mu_{\overline{B}}(k).$$

$$\overline{B} = TRUE \,|\, [\,(\,\overline{A_1} \ \ and \ \ \overline{A_2} \ \ and \ \ldots \ and \ \overline{A_n}\,) = TRUE\,]$$
$$and \ [\ \mu_{\overline{A_1}}(k_1) \geq \mu_{\overline{A_1}}(k_1)^*\ ] \ \ and \ \ [\ \mu_{\overline{A_2}}(k_1) \ \geq \ \mu_{\overline{A_2}}(k_1)^*\ ] \ \ and$$
$$\ldots \ and \ [\ \mu_{\overline{A_n}}(k_1) \ \geq \ \mu_{\overline{A_n}}(k_1)^*\ ] \ and \ [\,\mu_{\overline{B}}(k_1) \ \geq \ \mu_{\overline{B}}(k_1)^*\ ],$$

где $\mu_{\overline{A_1}}(k_1)^*, \mu_{\overline{A_2}}(k_1)^*, \ldots, \mu_{\overline{A_n}}(k_1)^*, \mu_{\overline{B}}(k_1)^*$ – допустимое значение соответствующих функций принадлежностей.

Модель управления информационной безопасностью в виде продукции была разработана в соответствии с нечеткими правилами продукции:

ЕСЛИ система открыта (СО) ***И*** почта, подключенная к системе, открыта (ПО), ***ТО*** надо вводить пароль. ***ЕСЛИ*** пароль был введен правильно (ПП), ***ТО*** система будет готова к использованию.

ЕСЛИ система была открыта (ПО) ***И*** почта, подключенная к системе, была

закрыта (ПЗ), ***ТО*** пароль не вводится.

ЕСЛИ система была открыта (СО) ***И*** почта, подключенная к системе, была открыта (ПО), ***ТО*** пароль вводится. ***ЕСЛИ*** пароль был введен неправильно (НП), ***ТО*** система не будет готова к использованию.

ЕСЛИ система была закрыта (СЗ) ***И*** почта, подключенная к системе, была открыта (ПО), ***ТО*** система не будет готова к использованию.

В состав продукционной системы входит база правил, глобальная база данных и интерпретатор правил.

База правил – это область памяти, которая содержит базу знаний.

Совокупность знаний, представляется в форме правил вида « *ЕСЛИ … ТО* ».

Базы данных у различных систем имеют различную форму. Но все они могут быть описаны как группа данных содержащих имя данных и значение атрибутов.

Выводы

Продукционная система включает в себя интерпретатор правил. Этот интерпретатор представляет механизм влияния, и он является неотъемлемой частью системы, использующей базу правил и базу данных, которая формирует результат.

Литература

1. Alguliyev R.M., Alekperov R.K. Cloud Computing: Modern State, Problems and Prospects // Telecommunications and Radio Engineering, 2013, vol.72, no. 3, pp. 255-266.
2. Aliyev A.A., Samadov R.B. Developing an algorithm and a scheme for integration of multiple merchants to e-commerce solution in cloud computing // «International Journal of Computer Science and Information Security», USA, 2016, Vol. 14, №11, P. 7-11.
3. B. Furht, A. Escalante (eds.), Handbook of Cloud Computing, Springer.
4. Mell P., Grance T. The NIST definition of cloud computing, 2010, https://clck.ru/XwcoX
5. Баранова Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. – М.: Риор, 2017. – 400 с.
6. Бодянский Е.В., Кучеренко Е.И., Михалев А.И. Нейро-фаззи сети Петри в задачах моделирования сложных систем. Монография (научное издание). Днепропетровск: Системное технология, 2005, 311 с.
7. Введение в облачные вычисления, https://clck.ru/XwcuZ
8. Каретников А.В. Безопасность облачных вычислений. Проблемы и перспективы / А.В. Каретников, Д.П. Зегжда // Журнал «Проблемы информационной безопасности. Компьютерные системы». – СПб.: Изд-во Политехи, ун-та, 2011. №4. С. 7-17.
9. Клементьев И.П., Устинов В.А. Введение в облачные вычисления. Екатеринбург: УрГУ, 2009. 233с.
10. Мустафаев В.А. Анализ нечетких продукционных моделей динамических взаимодействующих процессов. // Вестник компьютерных и информационных технологий, №5, Москва, 2012, с. 25-30.

УДК 004.89

БЕЗОПАСНОСТЬ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ КОМПОНЕНТОВ ЭКОСИСТЕМЫ ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО РЫНКА С ЭЛЕМЕНТАМИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

SECURITY CRITICAL INFORMATION INFRASTRUCTURE OF FUEL AND ENERGY COMPLEX ECOSYSTEM COMPONENTS WITH ARTIFICIAL INTELLIGENCE ELEMENTS

Корнеев Н.В.,
РГУ нефти и газа (НИУ) имени И.М. Губкина
Финансовый университет при Правительстве Российской Федерации
ФГБУ «Всероссийский научно-исследовательский институт
по проблемам гражданской обороны и чрезвычайных ситуаций МЧС России»
(Федеральный центр науки и высоких технологий)
г. Москва, Российская Федерация

N.V. Korneev,
Gubkin Russian State University of Oil and Gas
Financial University under the Government of the Russian Federation
All-Russian Scientific Research Institute
of Civil Defence and Emergencies Ministry of Russia
(Federal Science and High Technology Center)

Moscow, Russian Federation

e-mail: niccyper@mail.ru

Аннотация. Раскрыты перспективы развития систем управления безопасностью топливно-энергетического комплекса (ТЭК) с учетом цифровой трансформации. Впервые дано определение и разработана обобщенная структура интеллектуальной системы управления комплексной безопасностью ТЭК, с учетом развития отечественной концепции системы человек-машина. Интеллектуальная система управления комплексной безопасностью ТЭК, как класс управляющих человеко-машинных систем обеспечением всех составляющих безопасности ТЭК с элементами искусственного интеллекта или искусственным интеллектом. Приведены примеры реализации указанного подхода практически во всех областях деятельности, в том числе для ТЭК, как отдельные компоненты системы управления комплексной безопасностью: физической, экономической, пожарной, информационной, безопасности интеллектуальной собственности, техногенной, экологической безопасности, энергетической безопасности, психологической, безопасности от терроризма. Определены основные элементы интеллектуальной системы управления комплексной безопасностью ТЭК: ядро, подсистемы и компоненты и приведены математические зависимости, реализующие функции управления. Она представлена совокупностью подсистем S_n обеспечения всех составляющих безопасности ТЭК: физической (S_1), экономической (S_2), пожарной (S_3), информационной (S_4), психологической (S_5), безопасности интеллектуальной собственности (S_6), техногенной (S_7), безопасности от

терроризма (S_8), экологической безопасности (S_9), энергетической безопасности (S_{10}), в том числе новых составляющих (S_n), и их компонентов.

Abstract. Taking into account the digital transformation, the prospects for the development of security management system fuel and energy complex (FEC) are revealed. For the first time a definition of intelligent complex security management system FEC is given, also, its generalized structure is developed, considering the development of the Russian human-machine concept. Its main elements are defined: a core, subsystems and components and mathematical dependencies implementing management functions are given.

Ключевые слова: интеллектуальная система управления комплексной безопасностью, цифровая трансформация, Индустрия 5.0, Общество 5.0, искусственный интеллект, концепции системы человек-машина, ядро, подсистемы, компоненты, математические зависимости, функции управления

Keywords: intelligent complex security management system, digital transformation, Industry 5.0, Society 5.0, artificial intelligence, human-machine concept, core, subsystems, components, mathematical dependencies, management functions

Бурное развитие информационных технологий привело к цифровой трансформации [1]. Цифровую трансформацию можно рассматривать как процесс интеграции инновационных технологий и бизнес-процессов. В условиях цифровой экономики это потребовало изменить технологии, культуру, операции и принципы создания новых продуктов и услуг. Будущую Индустрию 5.0 сегодня можно определить, как лучшие группы, практики и инструменты цифровой трансформации для Общества 5.0. Определенным толком к развитию Индустрии 5.0 можно считать Национальную стратегию развития искусственного интеллекта на период до 2030 года (Указ Президента РФ от 10.10.2019 г. №490).

Искусственный интеллект [2, 3] – это динамическая система, способная без участия человека: строить полнофункциональные модели, отображающие сложные явления мира вокруг и самого себя в этом мире; анализировать адекватность (соответствие) различных вариантов моделей с целью отбора из них наиболее точных или оптимальных; формировать на основе выбранных моделей вариантные прогнозы ожидаемых последствий.

Все указанное выше открывает новые перспективы в развитии систем обработки информации. Принципиально изменяется структура систем обработки информации, основой которых теперь являются распределенные информационно-вычислительные сети, подключенные к глобальным сетям передачи данных, конвергентные, гиперконвергентные, нейроморфные и квантовые вычислительные системы. В тоже время ужесточаются требования регуляторов, особенно в части комплексной безопасности объектов: физической, экономической, пожарной, информационной, психологической, безопасности интеллектуальной собственности, техногенной, безопасности от терроризма, экологической безопасности, энергетической безопасности.

Понятие объекта мы рассматриваем в его более широком понятии [3]. Объект управления – это любое явление окружающего мира (или сам субъект), которое рассматривается с точки зрения создания некоторого целенаправленного движения. Естественно назвать конечное состояние объекта желаемым, то есть таким, в котором мы заинтересованы и которое определяет цель управления как перевод объекта в желаемое состояние, а сам акт перевода – процессом управления, или просто управлением.

В этом случае ТЭК как объект может включать нефтяную, газовую, угольную и торфяную отрасли, электроэнергетику и теплоснабжение, что в полной мере соответствует Доктрине энергетической безопасности РФ, а в случае рассмотрения комплексной безопасности объекта расширить ее применение для решения задач национальной безопасности.

На основе изложенного становится очевидным суть комплексной безопасности – обеспечение всех составляющих безопасности объекта: физической, экономической, пожарной, информационной, психологической, безопасности интеллектуальной собственности, техногенной, безопасности от терроризма, экологической безопасности, энергетической безопасности в том числе новых составляющих.

В этом случае понятие комплексной безопасности является более гибким и самоорганизующимся под цифровую трансформацию объекта, а теория управления не меняет фундаментальных принципов, что дает возможность строить соответствующую систему управления объектом Индустрии 5.0 в том числе с элементами искусственного интеллекта для Общества 5.0.

Новая концепция заключается не в противопоставлении (замене) человека – ЭВМ, а во взаимно дополнении их. Описанный подход подробно изложен в книге автора [3] как новый класс «систем с элементами искусственного интеллекта». Таким образом, Интеллектуальная система управления комплексной безопасностью ТЭК – это класс управляющих человеко-машинных систем обеспечением всех составляющих безопасности ТЭК с элементами искусственного интеллекта или искусственным интеллектом [2].

В настоящее время наблюдается реализация указанного подхода [2, 3, 4] практически во всех областях деятельности. Для ТЭК разрабатываются отдельные компоненты системы управления комплексной безопасностью, например физической [5, 6], экономической [7, 8, 9], пожарной [4, 10, 11], информационной [12, 13, 14, 15, 16], отдельные решения по безопасности интеллектуальной собственности, предлагают компании «СёрчИнформ» и «InfoWatch», техногенной [17, 18, 19, 20, 21, 22, 23, 24], экологической безопасности [25, 26, 27], энергетической безопасности [7, 28, 29, 30], решения по психологической, безопасности от терроризма [2, 4, 31, 32, 33] практически отсутствуют.

Легко заметить, что по большинству подсистем и компонентов – отечественных решений нет, а в целом отечественная интеллектуальная система управления комплексной безопасностью ТЭК отсутствует. Обобщенная структура интеллектуальной системы управления комплексной безопасностью ТЭК, с учетом развития отечественной концепции системы человек-машина, как сложной информационно-энергетической системы представлена на рисунке 1 [2].

Она представлена совокупностью подсистем S_n обеспечения всех составляющих безопасности ТЭК:

– физической (S_1),
– экономической (S_2),
– пожарной (S_3),
– информационной (S_4),
– психологической (S_5),
– безопасности интеллектуальной собственности (S_6),
– техногенной (S_7),
– безопасности от терроризма (S_8),
– экологической безопасности (S_9),
– энергетической безопасности (S_{10}),

– в том числе новых составляющих (S_n), и их компонентов S_{1p}, S_{2e}, S_{3f}, S_{4s}, S_{5h}, S_{6l}, S_{7t}, S_{8r}, S_{9v}, S_{10g}, S_{nk}.

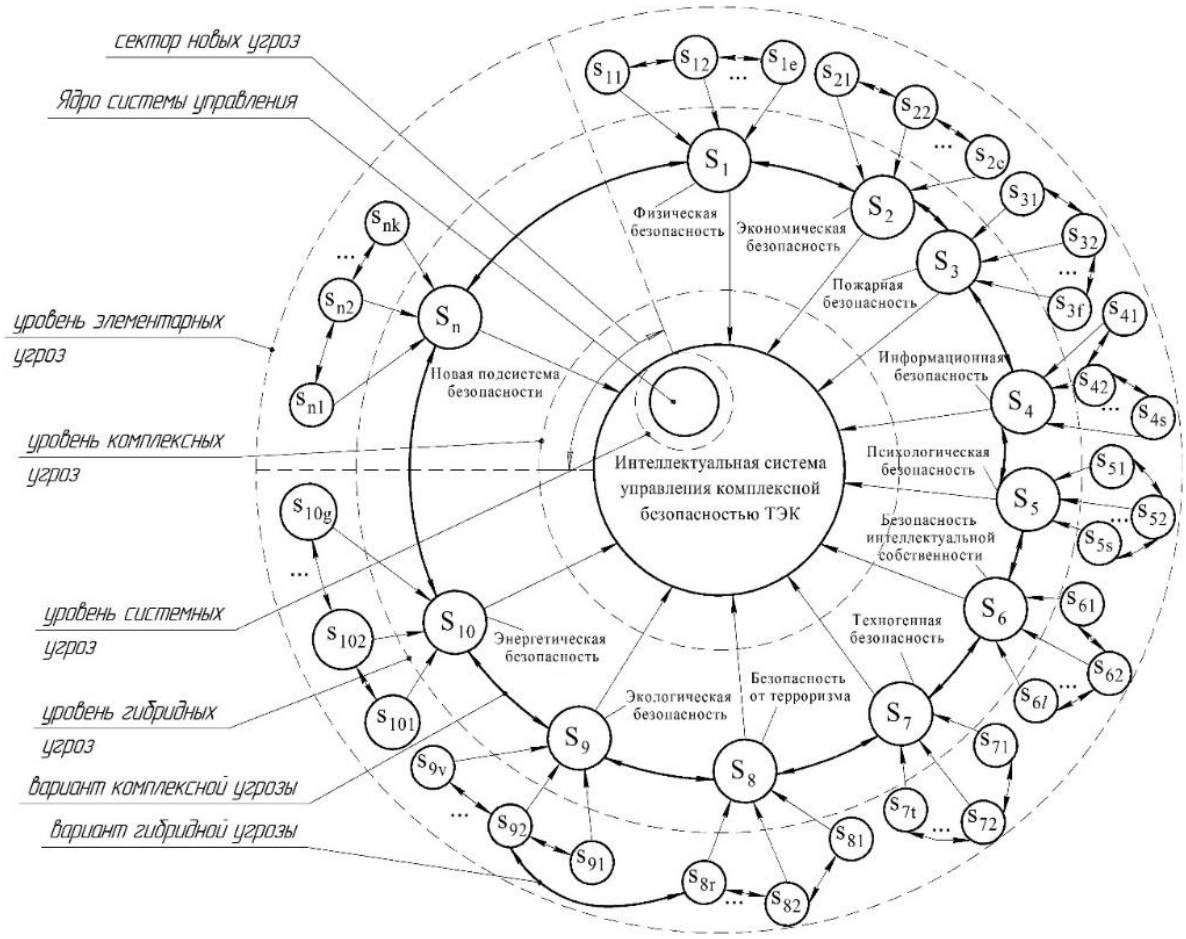

Рисунок 1. Обобщенная структура интеллектуальной системы управления комплексной безопасностью ТЭК [2]

В общем случае количество компонентов в каждой подсистеме различно. Ядро, подсистемы и компоненты – это представление защищаемой системы на уровне управления угрозами безопасности в виде блочно-функциональной схемы системы с элементами искусственного интеллекта [2] отличающихся друг от друга степенью детализации элементов. Для подсистем и компонентов учитываются особенности соответствующей составляющей безопасности ТЭК. Следует отметить, что в случае рассмотрения схемы ядра системы, в качестве оператора интеллектуальной системы управления комплексной безопасностью ТЭК может выступать Президент РФ, а система управления рассматривается, как элемент стратегического планирования в сфере обеспечения национальной безопасности РФ.

Выводы

Достаточно важным и тоже время сложным в решении оказывается вопрос взаимовлияния отдельных подсистем и компонентов друг на друга. На рисунке 1 связи характеризующие такое влияние выделены жирной линией. Такое взаимовлияние связано с взаимным отображением моделей отдельных подсистем и компонентов друг на друга. Один из возможных способов учета этого влияния связан с понятиями гибридная угроза, комплексная угроза, системная угроза [2]. В работе [34] рассмотрена

практическая проблематика комплексных угроз и особенности их формирования и реализации, на основе чего предложены подходы к обеспечению защищенности, что наиболее эффективно может проявляться в наличии средств и методов выявления самого факта наличия комплексной угрозы и определения списка возможных целей комплексной угрозы. Реализация данных механизмов может быть достигнута, используя аналитику больших данных, интегрируемых из различных источников, например, на уровне объекта – предприятия ТЭК. В системной угрозе рассмотрению уже подлежат наборы комплексных угроз, выделенные на основании изложенного выше понятия объекта и решаемой задачи безопасности для подсистемы, и объединенные, например, в кластер.

Литература

1. Patel K., McCarthy M.P. Digital transformation: the essentials of e-Business leadership. New York, McGraw-Hill, 2000. P. 144.

2. Korneev N. V. Intelligent complex security management system FEC for the industry 5.0. В сборнике: IOP Conference Series: Materials Science and Engineering. Сер. “Advanced Problems of Electrotechnology” 2020. С. 012016.

3. Корнеев Н.В., Кустарев Ю.С., Морговский Ю.Я. Теория автоматического управления с практикумом: учебное пособие для вузов (УМО)/Москва, 2008. Сер. Высшее профессиональное образование.

4. Korneev N.V. A Neurograph as a Model to Support Control over the Comprehensive Objects Safety for BIM Technologies. В сборнике: IOP Conference Series: Earth and Environmental Science. Current Problems and Solutions. 2019. С. 012021.

5. Garcia M.L. Design and Evaluation of Physical Protection Systems. Boston, Butterworth-Heinemann, 2007. P. 351.

6. Fennelly L.J. CTPED and Traditional Security Countermeasures: 150 Things You Should Know. Boca Raton, Taylor&Francis, 2018. P. 462.

7. Cao J., Wang Y., Zhu C., Zhang Y., Guo C., Cao Y. CIM-based information model for power grid enterprise asset management and its application //Automation of Electric Power Systems. 36:2. 2012. pp. 77-81.

8. Yu Y.X., Luan W.P. Smart grid and its implementations, Zhongguo Dianji Gongcheng Xuebao//Proceedings of the Chinese Society of Electrical Engineering. 29:34. 2009. pp. 1-8.

9. Корнеев Н.В., Осипов И.В. Алгоритмические и программные принципы построения и разработки системы расширяемых шаблонов для контроля и оптимизации торговых систем на основе облачной сети распределенных вычислений. Ученые записки Российского государственного социального университета. 2012. 3(103). С. 163-169.

10. Danilov A.I., Mel’kov S.A., N.V. Solov’eva, et al, Experience of Interaction between the EMERCOM of Russia and Roshydromet to Provide the Safety of Population and Territories in the Russian Arctic, Russ. Meteorol. Hydrol. 44:4. 2019. pp. 300-304.

11. McNay J., Puisa R., Vassalos D. Analysis of effectiveness of fire safety in machinery spaces. Fire Safety Journal. 108. 2019. P. 102859.

12. Markov A. S., Barabanov A., Tsirlov V. Periodic Monitoring and Recovery of Resources in Information Systems, in: A. Kostogryzov (Eds.), Probabilistic Modeling in System Engineering. IntechOpen. London. 2018. chapter 10.

13. Корнеев Н.В. Алгоритмические и программные методы и средства оценки альтернативных проектов защиты системы обработки информации предприятия на основе многокритериального анализа: монография / ФГБОУ ВПО Поволжский государственный университет сервиса. Москва, 2013.

14. Корнеев Н.В., Меркулов В.Д. Rонцепция интеллектуального обнаружения угроз в вертикально интегрированных иерархиях центров безопасности. Информационные технологии. Проблемы и решения. 2020. 2(11). С. 134-139.

15. Корнеев Н.В., Меркулов В.Д. Методология построения комплексных систем безопасности в интегрированных структурах ТЭК. Информационные технологии. Проблемы и решения. 2020. 3(12). С. 142-149.

16. Корнеев Н.В., Корнеева Ю.В. Аудит системы менеджмента информационной безопасности. Стандарты и качество. 2014. 7. С. 60-64.

17. Oliveira L.E.S., Alvares A.J. Development of a System for Monitoring and Teleoperation of a CNC Machine through the Internet. Procedia CIRP. 53. 2016. pp. 198-205.

18. Wei L., Chuipin K., Qiang N., Jingguo J., Xionghui Z. A method of NC machine tools intelligent monitoring system in smart factories. Robotics and Computer-Integrated Manufacturing. 61. 2020. P. 101842.

19. Корнеев Н.В. Аналитическая и статистическая оптимизация уровня дисбаланса гибких систем турбоагрегатов. Машиностроитель. 2007. 12. С. 25-28.

20. Корнеев Н.В. Концепция разработки и создания интеллектуальных человекомашинных систем управления на транспорте. Машиностроитель. 2009. 12. С. 37-40.

21. Корнеев Н.В., Кустарев Ю.С. Управление дисбалансом высокоскоростных роторных систем: учеб. пособие для студентов, обучающихся по специальности «Автомобиле-и тракторостроение» / Н.В. Корнеев, Ю.С. Кустарев; Федеральное агентство по образованию, Московский гос. технический ун-т «МАМИ». Москва, 2006.

22. Корнеев Н.В. Многокритериальная параметрическая оптимизация динамических характеристик роторных систем турбоагрегатов. Наука – производству. 2006. 6. С. 44-46.

23. Корнеев Н.В. Методология прогнозирования начального дисбаланса турбоагрегатов в условиях сборки. Техника машиностроения. 2006. 3(59). С. 72-74.

24. Korneev N.V., Yanitskiy A.I. A model of a combined electric drive for a dynamic advertising structure. Russian Electrical Engineering. 2019. Т. 90. № 10. С. 696-701.

25. Perez-Valdes G.A., Nørstebø V.S., Ellingsen M.-B., Teräs J., Werner A.T. Bioeconomic Clusters–Background, Emergence, Localization and Modelling. Sustainability. 11:17. 2019. P. 4611.

26. Корнеев Н.В., Смоленская Н.М. Модель средней скорости распространения фронта пламени природного газа с добавками водорода для одноцилиндровой установки УИТ-85, имитирующей режимы холостого хода. Естественные и технические науки. 2014. 9-10(77). С. 167-171.

27. Smolenskaya N.M., Korneev N.V. Modelling of the combustion velocity in UIT-85 on sustainable alternative gas fuel. В сборнике: IOP Conference Series: Earth and Environmental Science. All-Russian Research-to-Practice Conference “Ecology and Safety in the Technosphere”. 2017. С. 012016.

28. Vieira A.C., Houmb S.H., Insua D.R. A graphical adversarial risk analysis model for oil and gas drilling cybersecurity. Electronic Proceedings in Theoretical Computer Science. EPTCS 148. 2014. pp. 78-93.

29. Корнеев Н.В. Методология прогнозирования дисбаланса деталей и узлов турбоагрегатов. Машиностроитель. 2006. 7. С. 19-21.

30. Korneev N.V. Forecasting of a vibration level of nonrigid rotary tables of compressor units from an out-of-balance with allowance for of series of the random mechanical, gaseous dynamic and operation factors. В сборнике: EURO-ECO HANNOVER 2009. Programm Abstracts. 2009. С. 45-47.

31. Young C. The Science and Technology of Counterterrorism: Measuring Physical

and Electronic Security Risk. Elsevier. New York. 2014. P. 492.

32. Корнеев Н.В., Колесникова Ю.В. О построении модели действий нарушителя антитеррористической защиты объектов с использованием динамического программирования. Технологии техносферной безопасности. 2013. 5(51). С. 23.

33. Корнеев Н.В., Колесникова Ю.В. Динамическое моделирование антитеррористической защиты объектов. Программная инженерия и информационная безопасность. 2013. 3. С. 36-44.

34. Korneev N., Merkulov V. Intellectual analysis and basic modeling of complex threats. В сборнике: CEUR Workshop Proceedings. Selected Papers of the X Anniversary International Scientific and Technical Conference on Secure Information Technologies (BIT 2019). 2019. С. 23-28.

СОВРЕМЕННАЯ МЕТОДИКА ПРЕПОДАВАНИЯ ИНФОРМАТИКИ

УДК 004.021

ОБУЧЕНИЕ РЕШЕНИЮ ЗАДАЧ С ЭКОНОМИЧЕСКИМ СОДЕРЖАНИЕМ В КУРСЕ ИНФОРМАТИКИ ОСНОВНОЙ ШКОЛЫ

TEACHING PROBLEM SOLVING WITH ECONOMIC CONTENT IN THE COURSE OF BASIC SCHOOL COMPUTER SCIENCE

Бружукова М.А.,
ФГБОУ ВО «Мордовский государственный педагогический университет имени М.Е. Евсевьева»
г. Саранск, Российская Федерация

M.A. Bruzhukova,
FSBEI HPE “Mordovia State Pedagogical University named after M.E. Evsevyov”
Saransk, Russian Federation

Аннотация. В настоящее время актуальной проблемой экономической грамотности является ее необходимость современному человеку и возможности ее формирования в школьном курсе информатики, ведь в современном мире она имеет огромное значение. Однако многие до сих пор не понимают, что это такое. Поэтому на сегодняшний день перед школой стоит задача подготовить гражданина, способного интегрироваться в современное общество и чьей целью является улучшение этого общества; человека, способного сотрудничать с людьми с разными подходами к управлению, способного реализовать право на свободный выбор взглядов и убеждений. Ведь именно обладание экономической грамотностью помогает человеку добиться финансового благополучия и способности сохранить его на протяжении всей жизни. При наличие подобных знаний гражданину в будущем это принесет доход. Обучающимся будет легко влиться в данную сферу, так как они начнут знакомиться с этим еще в школе. Большинство своего времени молодое поколение использует компьютеры или смартфоны, поэтому для них не составит большого труда научиться с их помощью планировать свой бюджет, оплачивать ЖКХ, совершать покупки, откладывать на «черный день».

Abstract. At the present time the urgent problem of economic literacy is its necessity for a modern person and possibilities of its formation in a school course of computer science, because in the modern world it has great importance. However, many people still do not understand what it is. Therefore, today the school is faced with the task of preparing a citizen who is able to integrate into modern society and whose goal is to improve this society; a person who is able to cooperate with people with different approaches to management, who is able to exercise the right to freely choose their views and beliefs. After all, it is the possession of economic literacy that helps a person achieve financial well-being and the ability to maintain it throughout life. If a citizen has such knowledge, it will bring income in the future. It will be easy for students to get into this field because they will begin to learn about it while they are still in school. Most of the time, the younger generation uses computers or smartphones, so it

will not be difficult for them to learn how to use them to plan their budget, pay for housing and communal services, make purchases, save for a “rainy day”.

Ключевые слова: экономическая грамотность, финансовая грамотность, экономика, финансы, расходы, доходы, информатика.

Keywords: economic literacy, financial literacy, economics, finance, expenses, income, informatics.

Становление рыночной экономики в нашей стране, снижение потребности в неквалифицированных рабочих, возрастающие требования работодателей к профессиональным качествам специалистов, требования общества к наличию у индивидуума экономических знаний и навыков их применения на практике актуализируют вопрос о повышении экономической и финансовой грамотности населения.

Экономическая грамотность становится одним из основных критериев развития конкурентоспособной личности и успешной адаптации обучаемого в современной социально-экономической ситуации. Запросы государства к подготовке компетентных специалистов перекликаются с требованиями общества к воспитанию делового, конкурентоспособного человека, имеющего развитое экономическое мышление и подготовленного к жизни в условиях рыночной экономики. Изложенные обстоятельства определяют актуальность вопросов, связанных с повышением экономической грамотности школьников и делают проблему усиления прикладной направленности, то есть связи содержания и методики обучения информатики с ее применением для решения практических задач, одним из важнейших направлений модернизации информатико-математического образования в школе.

Рассмотрим несколько определений понятия «финансовая грамотность» в различных источниках.

Г.В Белехова: финансовая грамотность – органичное сочетание знаний, информированности, практических умений, индивидуального отношения и конкретного поведения отдельного человека или домохозяйства при принятии решений относительно денежных средств и других финансовых ресурсов в целях достижения собственного экономического благополучия [1].

М.А. Овчинников: финансовая грамотность – способность потребителей финансовых услуг использовать имеющуюся информацию в процессе принятия решений: при осуществлении специальных расчетов, оценке рисков, сопоставлении сравнительных преимуществ и недостатков той или иной финансовой услуги [5].

О.Е. Кузина: финансовая грамотность – это знания и навыки в области финансов, которые должны применяться в повседневной жизни и приносить положительные финансовые результаты [4].

Финансовая грамотность включает способность вести учет всех поступлений и расходов, умение распоряжаться денежными ресурсами, планировать будущее, делать выбор финансовых инструментов, создавать сбережения, чтобы обеспечить будущее и быть готовыми к нежелательным ситуациям, включая потерю работы.

Финансовая грамотность – совокупность знаний о финансовых рынках, особенностях их функционирования и регулирования, профессиональных участниках и предлагаемых финансовых инструментах, продуктах и услугах, умение их использовать с полным осознанием последствий своих действий и готовностью принять на себя ответственность за принимаемые решения.

Выше представленные трактовки понятий финансовой грамотности, можно условно разделить на типы:

1) финансовая грамотность как определенная форма знаний;

2) финансовая грамотность как способность или навык применить это знание;

3) финансовая грамотность как знание;

4) финансовая грамотность как правильное финансовое поведение;

5) финансовая грамотность как финансовый опыт;

6) финансовая грамотность как навык.

Проще говоря, финансовую грамотность можно определить, как способность человека решать возникающие финансовые вопросы в реальной жизни и умение распоряжаться имеющимися денежными средствами.

Рассмотрим теперь определения экономической грамотности.

В словаре Н.Е. Яценко «Толковый словарь обществоведческих терминов» экономическая грамотность трактуется как «уровень экономических знаний, умений и навыков, а также личностных качеств человека, позволяющих ему сознательно участвовать в хозяйственной деятельности общества» [6].

В словаре С.М. Вишняковой «Ключевые понятия, термины, актуальная лексика» содержится следующее определение данного понятия «Экономическая грамотность – это готовность к участию в экономической деятельности, состоящая в знаниях теоретических основ хозяйственной деятельности, понимания природы экономических связей и отношений, в умении анализировать конкретные экономические ситуации» [4].

Обобщая приведённые определения, под термином «экономическая грамотность» в нашем исследовании понимается спектр понятий, информации и знаний из экономической области, а также обладание навыками решения практических задач, главным образом в потребительской сфере.

Таким образом, несмотря на разницу понятий «экономика» и «финансы», (экономика – это хозяйственная деятельность общества, а также совокупность отношений, складывающихся в системе производства, распределения, обмена и потребления; финансы – это как совокупность экономических отношений, возникающих в процессе формирования, распределения и использования централизованных и децентрализованных фондов денежных средств) в изученной нами научной литературе термины «экономическая грамотность» и «финансовая грамотность» подразумевают знания и навыки, позволяющие человеку решать различные жизненные задачи, связанные с деньгами, их распределением и использованием.

Формирование нового экономического мышления – одна из важных задач школы. Создание необходимой для общества образовательной системы возможно при организации подходящего образовательного пространства в школе.

Внедрение в школы «финансовой грамотности» как отдельного предмета столкнулось с рядом проблем, например, с нежеланием учителей и родителей не просто преподавать, но и осознавать необходимость учить ребенка обращению с деньгами. Многие считают, что внедрение финансовой грамотности ухудшит знания других предметов и сделает ребенка меркантильным. Но важно помнить, что дети XXI века – это будущие участники финансового рынка, вкладчики, налогоплательщики. Финансовая грамотность так или иначе внедряется в обиход ребенка еще с раннего возраста: расходы и доходы семьи, походы в магазин, рекламы, использование банковских карт или мобильных – все это напрямую связано с реальностью, в которой живет современный человек. Поэтому уроки финансовой грамотности очень важны и как нельзя актуальны в современных российских условиях. Дети уже с довольно раннего возраста переходят в категорию потребителей. Умение пользоваться деньгами для них

уже крайне важно, так как именно детский мозг больше всего подвержен влиянию рекламы, которая практически везде им встречается.

Формирование понятий «финансовая грамотность», «экономическая грамотность» с точки зрения практической направленности опирается на школьный курс информатики. Учебные материалы и задания подобраны в соответствии с возрастными особенностями детей и включают задачи, практические задания, мини-исследования и проекты. В процессе выполнения заданий такого плана формируются умения и навыки работы учащихся с текстами, таблицами, схемами, а также поиска, анализа и представления информации и публичных выступлений.

Задачи, решаемые в курсе информатики основной школы, содержательно относятся к следующим темам из области финансовой грамотности:

– расходы (выявление и устранение излишних расходов; сравнение вариантов расходов);

– доходы (планирование и учет личных и семейных доходов);

– семейный бюджет (ведение личного и семейного бюджета);

– расчеты и платежи (наличные расчеты; расчеты с помощью банковских карт).

Рассмотрим некоторые примеры таких задач.

Рассмотрим задачу из школьного учебника информатики 11 класса авторов Л.Л. Босовой, А.Ю. Босовой по теме: «Встроенные функции и их использование. Финансовые функции» [3].

Пусть ставка кредита в некотором банке составляет 18% годовых. Клиент хочет взять кредит на сумму 100 000 руб. и может выплачивать банку по 4 000 руб. ежемесячно. Нужно определить, за сколько периодов клиент сможет погасить этот кредит.

Обязательные аргументы функции:

Ставка – годовая ставка в процентах, разделенная на количество периодов платежей за год (в нашем примере это 18%/12);

Плт – сумма, которую клиент ежемесячно должен возвращать банку (в нашем примере это – 4 000, т.к. эти деньги отдаются);

Пс – Размер кредита (в нашем примере это 100 000).

Формула для вычисления количества периодов выплат для погашения взятого кредита будет иметь вид: = КПЕР(18%/12; – 4 000; 100 000) (рисунок 1).

Получаем приблизительно 32 периода (месяца), т.е. более 2,5 лет.

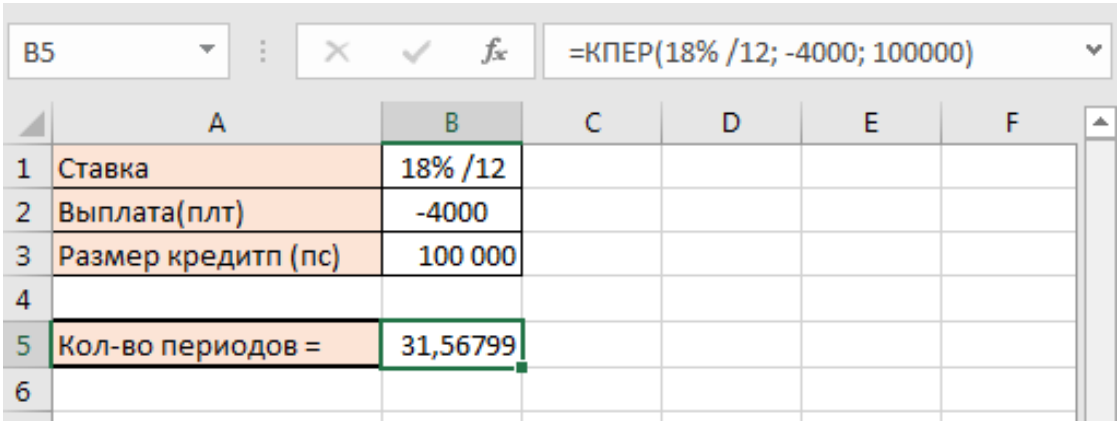

Рисунок 1. Формула для вычисления количества периодов

Следующий рассматриваемый пример задачи был представлен в рамках Международного конкурса педагогического мастерства «Учительская онлайн лаборатория Рыбаков фонда» по направлению «Создание онлайн уроков» (рисунок 2).

Подобные задачи разработаны для элективного курса «Основы финансовой грамотности на уроках информатики».

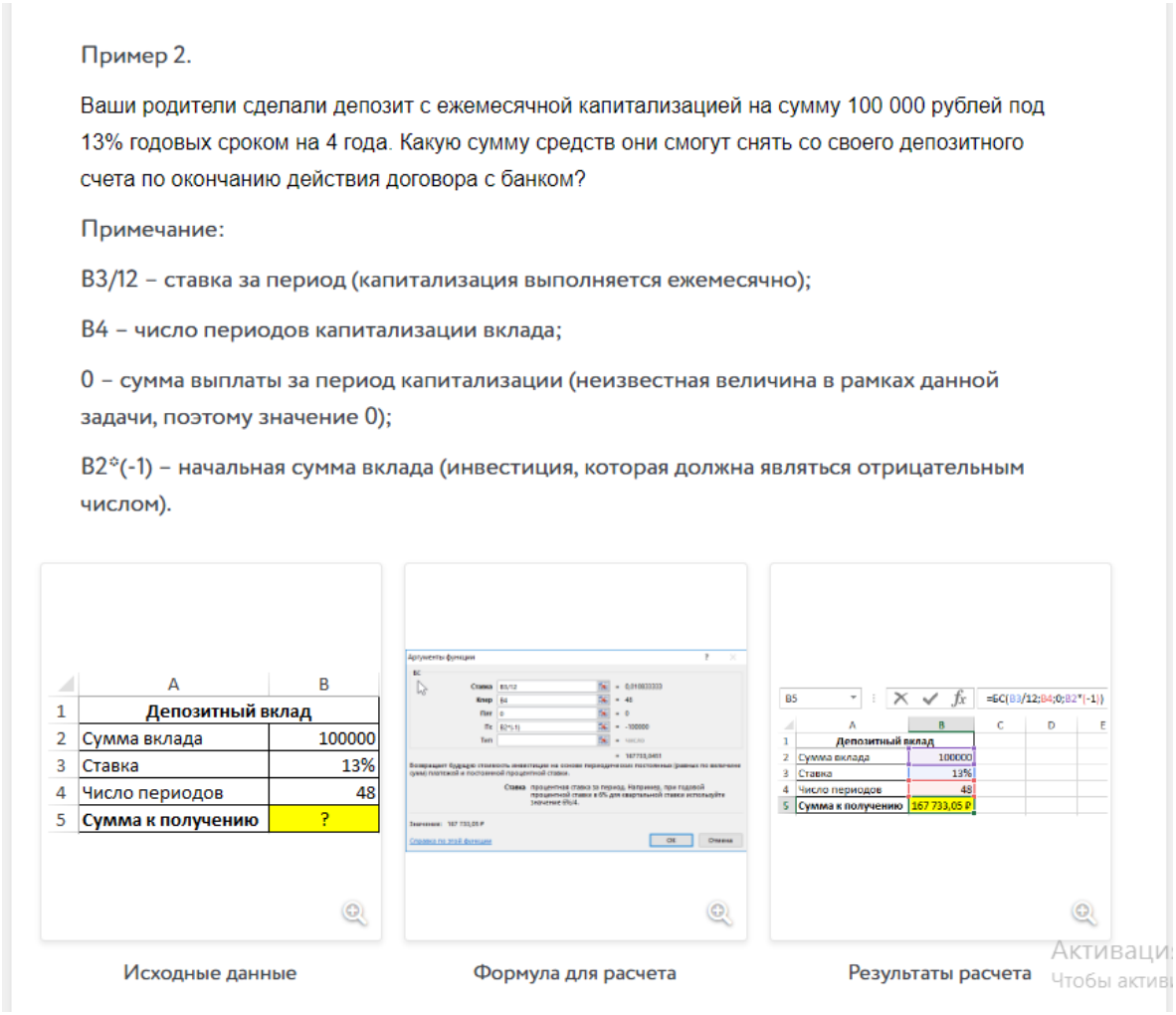

Рисунок 2. Задача с экономическим содержанием

Выводы

Умение решать задачи, формирующие финансовую и экономическую грамотность обучающихся, может быть использовано ими в будущем для выполнения настоящих взрослых задач. Это способствует повышению интереса к изучению информатики и формированию информационной культуры обучающихся.

Литература

1. Белехова Г.В. К вопросу о финансовой грамотности населения // Проблемы развития территории: научный журнал. 2014. С. 53-66.
2. Босова Л. Л., Босова А. Ю. Информатика. 11 класс. Программа для основной школы. Москва: Бином. Лаборатория знаний. 2015. 376 с.
3. Вишнякова С.М. Профессиональное образование: Словарь. Ключевые понятия, термины, актуальная лексика // Министерство общего и профессионального образования РФ. Управление среднего профессионального образования, Научно-методический центр среднего профессионального образования. М.: 1999. 535 с.

4. Кузина О. Финансовая грамотность и финансовая компетентность: определение, методики измерения и результаты анализа в России // Вопросы экономики. 2015. №8. С. 129-148.
5. Овчинников М.А. Обзор международной практики реализации стратегий и программ в области финансовой грамотности. М.: Наука. 2008. 215 с.
6. Яценко Н.Е. Толковый словарь обществоведческих терминов. – СПб: Лань. 1999. 524 с.

УДК 004.021

ОБУЧЕНИЕ ПРОГРАММИРОВАНИЮ ЦИКЛОВ В СРЕДЕ ПРОГРАММИРОВАНИЯ КУМИР В ОСНОВНОЙ ШКОЛЕ

TEACHING PROGRAMMING CYCLES IN THE PROGRAMMING ENVIRONMENT OF THE IDOL IN THE PRIMARY SCHOOL

Юрьева М.С.,
ФГБОУ ВО «Мордовский государственный педагогический университет им. М.Е. Евсевьева»,
г. Саранск, Российская Федерация

M.S. Yurjeva,
Mordovia State Pedagogical University named after M.E. Evseviev,
Saransk, Russian Federation

e-mail: mishel.yurjeva@yandex.ru

Аннотация. Обучение учащихся программированию циклических алгоритмов на языке КуМир является базисом при дальнейшем решении задач на циклы в разных системах программирования. Циклическим алгоритмом называют многократно повторяющийся участок программы. Также циклом может называться любая многократно исполняемая последовательность инструкций, организованная любым способом (например, с помощью условного перехода). Зачастую, при решении алгоритмических задач возникает необходимость в многократном написании одних и тех же действий. Для более простой записи таких алгоритмов используют циклические конструкции, которые содержатся в любом языке программирования и являются важным компонентом программирования. Программисты, в основном, пишут такие программы, которые будут использованы не единожды, а многократно. Циклические алгоритмы многократно встречаются в курсе информатики в разделах «Основы алгоритмизации», «Начала программирования», «Алгоритмизация и программирование». Решение задач на циклы играют значительную роль в формировании у обучающихся отдельных учебных действий, а также в развитии учеников в целом. Таким образом, исследование методических особенностей циклических конструкций остается актуальным, особенно в процессе подготовки специалиста-информатика с помощью базового языка программирования КуМир, который содержит возможности для организации разных видов циклических алгоритмов.

Abstract. Teaching students to program cyclic algorithms in the IDOL language is the basis for further solving problems on cycles in different programming systems. A cyclic

algorithm is a repeatedly repeated section of a program. Also, a loop can be called any repeatedly executed sequence of instructions, organized in any way (for example, using a conditional jump). Often, when solving algorithmic problems, there is a need to repeatedly write the same actions. For easier writing of such algorithms, cyclic constructs are used, which are contained in any programming language and are an important component of programming. Programmers, in general, write such programs that will be used not once, but repeatedly. Cyclic algorithms are repeatedly found in the course of computer science in the sections “Fundamentals of algorithmization”, “Beginnings of programming”, “Algorithmization and programming”. Solving problems in cycles plays a significant role in the formation of individual learning activities in students, as well as in the development of students as a whole. Thus, the study of the methodological features of cyclic constructions remains relevant, especially in the process of training a computer scientist with the help of the basic programming language IDOL, which contains opportunities for organizing different types of cyclic algorithms.

Ключевые слова: методика обучения информатике, программирование, циклические алгоритмы, циклы, языки программирования.

Keywords: methods of teaching computer science, programming, cyclic algorithms, cycles, programming languages.

При обучении учащихся составлению циклических алгоритмов в языке программирования КуМир необходимо опираться на выполнение следующих задач обучения:

– развитие у учащихся умений выстраивать гипотезу и сопоставлять ее с полученным результатом;

– развитие логического мышления учащихся;

– развитие творческих способностей обучающихся;

– развитие у учащихся навыков поиска разных способов решения задач путем составления разных видов циклических алгоритмов для решения одной и той же задачи;

– развитие умения применять знания, полученные на уроках других предметов;

– развитие умения четко и последовательно излагать свои мысли;

– развитие умения отстаивать собственную точку зрения.

Для повышения эффективности обучения программированию циклических алгоритмов необходимо грамотно сочетать используемые технические средства обучения с применением следующих методов:

– проблемный,

– частично-поисковый,

– поисковый,

– программированный,

– репродуктивный [1].

Для овладения учащимися умений организации циклических алгоритмов необходимо отработать с ними следующие действия [2]:

1. Объявление в программе переменной цикла и задание её начального значения перед циклом. Для этого необходимо вместе с учащимися несколько раз прочитать условие задачи и определить, какая величина имеет диапазон или значение какой величины меняется в условии задачи. Данная величина и есть переменная цикла.

2. Составление условия изменения переменной перед каждым следующим выполнением цикла. Для того чтобы определить условие продолжения цикла,

необходимо вместе с учащимися изучить условие задачи и выявить, какое значение должна достигнуть переменная цикла для того, чтобы задача была решена.

3. Организация проверки условия, согласно которому цикл будет либо повторяться, либо заканчиваться. Данную проверку необходимо прописать в программе, опираясь на ранее выявленное условие выхода из цикла.

4. Составление операторов тела цикла, то есть действий, которые будут выполняться при каждом проходе цикла. Для того чтобы составить тело цикла, необходимо в условии задачи найти действия, которые будут неизменны при любом значении меняющейся переменной.

Рассмотрим практическую реализацию каждого из перечисленных действий на примере следующей задачи.

Задача. Вывести квадраты чисел от 10 до 5.

1. Для того чтобы объявить в программе переменную цикла и задать её начальное значение перед циклом, необходимо выявить с учащимися из условия задачи ту переменную, значение которой меняется. Для этого можно задать учащимся следующие наводящие вопросы:

– Что нужно найти в задаче?
(Квадраты чисел от 10 до 5).

– Есть ли в данной задаче переменная, которая будет менять свое значение?
(Да, число, квадрат которого мы будем выводить, меняет свое значение с каждым прохождением цикла).

– Известен ли диапазон значений данной переменной?
(Да, переменная меняет значения от 10 до 5).

– Каким будет начальное значение переменной? Десять или пять?
(Начальное значение переменной равно 10).

– Каким будет конечное значение переменной?
(Конечное значение переменной – пять).

– Каков шаг изменения переменной? Почему?
(Так как переменная меняется от большего значения к меньшему, то шаг будет отрицательным, то есть равен –1).

2. Для того чтобы составить условие изменения переменной перед каждым следующим выполнением цикла, необходимо вместе с учащимися определиться с видом составляемого цикла, и в зависимости от синтаксиса выбранного вида цикла записать условие. Для этого можно задать учащимся следующие наводящие вопросы:

– Какие границы диапазона изменения переменной нам известны?
(Известны обе границы диапазона – верхняя и нижняя).

– Какой вид цикла целесообразно использовать, если известны обе границы диапазона изменения переменной?
(Цикл «Для»).

– Какой синтаксис имеет цикл «Для»?

нц *для i от a до b*
тело цикла
кц

– Опираясь на синтаксис цикла «Для», запишите условие изменения переменной для данной задачи. *(нц для i от 10 до 5 шаг –1).*

3. Прежде чем организовать проверку условия, согласно которому цикл будет либо повторяться, либо заканчиваться, нужно вместе с учащимися выявить необходимость данной проверки при выбранном виде цикла с помощью наводящих вопросов:

– При каком условии цикл будет выполняться повторно?
(Если значение переменной i принадлежит диапазону [10; 5]).

– Нужно ли организовать дополнительную проверку истинности данного условия при выбранном виде цикла?
(Нет, так как диапазон изменения переменной уже задан).

4. Для того, чтобы составить операторы тела цикла, которые будут выполняться при каждом проходе цикла, необходимо задать учащимся следующие наводящие вопросы:

– Какое действие выполняется в задаче независимо от значения переменной *i*?
(Вычисляется и выводится квадрат числа).

– Какой оператор следует прописать в теле цикла?
(Возведение переменной i в квадрат, то есть умножение саму на себя, а также вывод значения переменной i).

В результате выполнения учащимися каждого из четырех перечисленных действий по составлению циклического алгоритма, получили листинг программы решения задачи:

```
алг
нач
    цел i,n
    нц для i от 10 до 5 шаг -1
        n:=i*i
        вывод n, нс
    кц
кон
```

Выводы

На основании вышеизложенного, можно отметить, что среда программирования КуМир является базисом для знакомства учащихся с алгоритмическим языком и началами программирования.

Его достоинством является возможность составления программ на русском языке, что способствует более простому усвоению программирования учащимися.

С помощью различных циклических конструкций можно решить огромный спектр задач, при этом в несколько раз сократив длину программы, что значительно помогает упростить решение больших по объёму задач.

Таким образом, обучение учащихся программированию циклических алгоритмов на языке КуМир имеет большую значимость при дальнейшем изучении более сложных языков программирования и построении сложных программ.

Литература

1. Кузнецов, А.С. Общая методика обучения информатике: учебное пособие / А.С. Кузнецов, Т.Б. Захарова, А.С. Захаров. – М.: Прометей, 2016. – Ч. 1. – 300 с. – ISBN 978-5-9907452-1-6. – Текст: электронный.

2. Семакин, И.Г. Основы алгоритмизации и программирования. Практикум: учеб. пособие для студ. учреждений сред. проф. Образования / И.Г. Семакин, А.П. Шестаков. – М.: Издательский центр «Академия», 2015. – 144 с. – ISBN 978-5-7695-9537-0. – Текст: непосредственный.

УДК 004.021

ОБУЧЕНИЕ ОСНОВАМ АЛГОРИТМИЗАЦИИ НА БАЗЕ СИСТЕМЫ КУМИР В ОСНОВНОЙ ШКОЛЕ

TEACHING THE BASICS OF ALGORITHMIZATION BASED ON THE IDOL SYSTEM IN PRIMARY SCHOOL

Семтина Е.А., Проценко С.И.,
ФГБОУ ВО «Мордовский государственный педагогический университет им. М.Е. Евсевьева»,
г. Саранск, Российская Федерация

E.A. Semtina, S.I Procenko,
FSBEI HE “Mordovia State Pedagogical University named after M.E. Evseviev”,
Saransk, Russian Federation

e-mail: katyusha.semtina@mail.ru

Аннотация. Изучение курса информатики предоставляет учащимся возможность приобрести специальные знания и умения, ведь без них сложно стать успешным и востребованным в дальнейшей профессиональной деятельности. Рассмотрение алгоритмизации в школьном курсе информатики может иметь такие аспекты: развивающий аспект, то есть развитие алгоритмического мышления школьников; программистский аспект, то есть уже формирование навыков составления учебных программ. Несомненно, любовь к программированию у школьников нужно прививать с простых и понятных программ, чтобы процесс обучения был привлекательным, захватывающим и несложным. Такой программой принято считать систему КуМир. Предназначение КуМира есть содействие обучению учащихся основам

программирования на разных уровнях образования: начальном, среднем и высшем. Для того, чтобы составить программу на компьютере, необходимо начать с построения алгоритма, из чего следует, что первостепенным качеством для настоящего программиста является совершенствование и развитие алгоритмического мышления. Рассмотрение данной темы необходимо для: мотивации учащихся к изучению школьного курса информатики; воспитания алгоритмического и аналитического мышления школьников; подготовки учащихся к более легкому вхождению в программирование в старшей школе; подготовки к программированию на языках более высокого уровня и сдачи экзамена по выбору в форме ОГЭ или ЕГЭ. В данной статье будем рассматривать методику обучения основ алгоритмизации в системе КуМир.

Abstract. Studying the course of computer science provides students with the opportunity to acquire special knowledge and skills, because without them it is difficult to become successful and in demand in further professional activities. Consideration of algorithmization in a school course in computer science can have the following aspects: the developing aspect, that is, the development of algorithmic thinking of students; the programming aspect, that is, the formation of skills in the preparation of curricula. Undoubtedly, the love of programming among schoolchildren should be instilled with simple and understandable programs, so that the learning process is attractive, exciting and simple. Such a program is considered to be the IDOL system. The purpose of the IDOL is to help teach students the basics of programming at different levels of education: primary, secondary and higher. In order to create a program on a computer, you need to start with building an algorithm, which means that the primary quality for a real programmer is the improvement and development of algorithmic thinking. Consideration of this topic is necessary for: motivating students to study a school course of computer science; educating algorithmic and analytical thinking of schoolchildren; preparing students for easier entry into programming in high school; preparing for programming in higher-level languages and passing an elective exam in the form of the OGE or USE. In this article, we will consider the methodology for teaching the basics of algorithmization in the IDOL system.

Ключевые слова: алгоритм, алгоритмизация, программирование, КуМир, учащийся, учитель.

Keywords: algorithm, algorithmization, programming, idol, student, teacher.

Приступая к изучению в школе основ алгоритмизации рекомендуется следовать методической последовательности введения теоретических понятий для того, чтобы гарантировать плавный переход между ними. При этом необходимо учитывать усвоение учащимися предыдущей темы для перехода к новой.

Изучение алгоритмизации в школе на уроках информатики в основном подразделяется на два этапа: изучение раздела алгоритмизации, далее программирования. Чаще всего учебные программы ограничиваются изучением алгоритмизации, что, на наш взгляд, не совсем верно [2].

Основной базой для дальнейшего успешного усвоения программирования считается изучение алгоритмизации, что способствует развитию у школьников алгоритмического мышления.

Педагогу необходимо уделить особое внимание изучению раздела алгоритмизации с учащимися, так как она считается важной частью всего курса информатики в школе.

Система программирования, главной целью которой считается поддержка программирования в средней и высшей школах, называется КуМир (Комплект Учебных МИРов).

Описание последовательности действий, выполнение которых приводит к решению задачи за определенное число шагов, называется алгоритмом.

Алгоритм – это основная структурная единица языка КуМир.

Программа на языке КуМир считается простейшей и содержит несколько последовательных алгоритмов.

Всякая неветвящаяся последовательность действий – вступление, которое может находится перед первым алгоритмом. К примеру, это могут быть различные комментарии, в которых рассказывается ход выполнения программы.

В системе КуМир применяется школьный алгоритмический язык с русской лексикой и встроенными исполнителями: Робот, Чертёжник, Черепаха, Водолей и Кузнечик [1].

Для улучшения процесса усвоения программирования в КуМире, при осуществлении программы в пошаговом режиме, на полях выводятся результаты операций присваивания и значения логических выражений.

Данная программная среда дает возможность обрести практические навыки построения и выполнения основных алгоритмических конструкций, используемых в других языках высокого уровня.

Рассмотрим, как можно решить задачу в системе КуМир поэтапно.

Итак, условие задачи таково: «Необходимо найти площадь круглого зеркала, используемого в телескопе. Радиус зеркала равен 100 см».

Для того, чтобы решить задачу на компьютере, рекомендуется выполнить несколько этапов, разберем их по порядку [3].

Этап 1. Постановка задачи.

Из данного условия задачи известно, что зеркало имеет круглую форму. Значит, для того, чтобы найти его площадь, понадобится найти площадь круга, при этом в условии есть данные радиуса.

Этап 2. Разработка математической модели.

Для нахождения площади круга нужно вспомнить формулу:

$$S = \pi R^2,$$

где $\pi = 3{,}141595.$

Этап 3. Разработка алгоритма.

Блок-схема такой программы представлена на рисунке 1.

Также в алгоритмах используются переменные (таблица 1).

Таблица 1. Переменные

Имя	Тип	Смысловое значение
R	Вещественная	Радиус круга (зеркала)
PI	Вещественная	Число π
S	Вещественная	Площадь круга (зеркала)

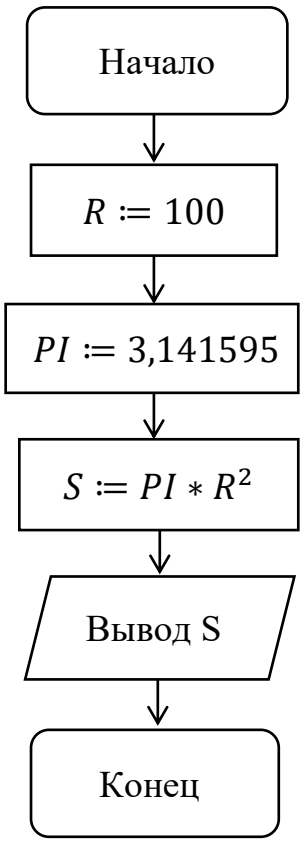

Рисунок 1. Блок-схема

Этап 4. Программирование.

На основе предыдущего этапа можно приступать к написанию программы в системе КуМир.

```
алг Вычисление площади зеркала телескопа
нач
. цел R
. вещ PI, S
. R:=100
. PI:=3.141595
. S:=PI*R**2
. вывод нс, "Площадь зеркала S=", S
кон
```

Этап 5. Тестирование и отладка.

После запуска программы появится результат исполнения (рисунок 2). В том случае, когда появится ошибка, необходимо ее исправить.

```
1  алг Вычисление площади зеркала телескопа
2  нач
3   . цел R
4   . вещ PI, S
5   . R:=100
6   . PI:=3.141595
7   . S:=PI*R**2
8   . вывод нс, "Площадь зеркала S=", S
9  кон
```

```
>> 18:26:00 - Новая программа - Начало выполнения
Площадь зеркала S=31415.95
>> 18:26:01 - Новая программа - Выполнение завершено
```

Рисунок 2. Результат выполнения

Этап 6. Анализ результатов.

После того, как все ошибки были справлены, получаем правильную программу. Ошибки, которые могли возникнуть, вероятно, относятся к синтаксическим или логическим. Для решения данной задачи, применялась линейная структура.

Выводы

На основании вышеизложенного, можно сделать выводы, что система программирования КуМир является доступной для знакомства и усвоения базовых знаний в области алгоритмизации и программирования.

Она представлена на русском языке, что значительно упрощает использование. Простой интерфейс и наглядность выполнения программного кода позволяют быстро разобраться в нем.

Используя исполнителей системы КуМир можно решить массу разнообразных задач.

Таким образом, среда программирования КуМир даёт багаж знаний, необходимый для дальнейшего изучения других языков программирования более сложного уровня.

Литература

1. Васильева, А.М. Элективный курс «Основы алгоритмизации в системе КуМир» для учащихся 8 класса/А.М. Васильева, Л.М. Коколова. – Текст: электронный// Образование и наука в современных условиях. – 2016. – №1. – С. 76-77. – URL: https://elibrary.ru/item.asp?id=25730466. – Дата публикации: 10.02.2016.

2. Гарипов, М.А. Изучение основ алгоритмизации и программирования в школьном курсе информатики/М.А. Гарипов. – Текст: электронный//Информационные технологии в науке, управлении, социальной сфере и медицине. – 2015. – С. 626-627. – URL: https://elibrary.ru/item.asp?id=24281931. – Дата публикации: 22.05.2015.

3. Чапурных, А.А. Использование графических исполнителей среды программирования КуМир для обучения основам алгоритмизации и программирования/ А.А. Чапурных. – Текст: электронный//Педагогическое мастерство. – 2019. – №1. – С. 21-26. – URL: https://www.elibrary.ru/item.asp?id=37046234. – Дата публикации: 05.03.2019.

УДК 004:621.396

ПРЕИМУЩЕСТВА LMS MOODLE В ФОРМИРОВАНИИ ПЕРСОНАЛИЗИРОВАННОЙ СРЕДЫ ЭЛЕКТРОННОГО ОБУЧЕНИЯ СТУДЕНТОВ

LMS MOODLE ADVANTAGES IN A FORMING OF A PERSONALIZED STUDENTS ELECTRONIC LEARNING ENVIRONMENT

Исакова А.И., Левин С.М.,
ФГБОУ ВО «Томский государственный университет систем управления и радиоэлектроники»,
г. Томск, Российская Федерация

A.I. Isakova, S.M. Levin,
Tomsk State University of Control Systems and Radioelectronics,
Tomsk, Russian Federation

e-mail: iai2@yandex.ru

Аннотация. В работе приведены основные возможности популярной платформы управления обучением Moodle, которая стала активно использоваться для обеспечения образовательного процесса в дистанционной форме в период пандемии COVID-19. На примере контента дисциплины «Информационные системы и технологии» для студентов направления подготовки «Прикладная информатика» Томского государственного университета систем управления и радиоэлектроники, в данной работе показаны преимущества использования отдельных компонентов современной образовательной технологии Moodle для формирования персонализированной среды электронного обучения студентов. В статье приведены примеры элементов, позволяющих эффективно организовывать образовательный процесс вуза: зачисление участников на курс, проверка работ студентов и настройка времени выполнения заданий, статистика оценивания заданий в целом всех участников и т.д. В качестве элементов курса в работе приводятся: База данных; Wiki; Глоссарий; Задание; Лекция, Семинар, Тест, Форум, Чат и некоторые другие. В Moodle допускается интеграция таких популярных вебинар-сервисов, как BigBlueButton, Zoom, Jitsi, OpenMeetings, WebEx Meeting, Via-Virtual Classroom. Наиболее удобным, по мнению авторов, является BigBlueButton, который обеспечивает автоматическую публикацию записей конференций на странице курса.

Abstract. The paper presents the main capabilities of the popular learning management platform Moodle, which has become actively used to provide the educational process in a distance form during the COVID-19 pandemic. Based on the example of the content of the discipline “Information Systems and Technologies” for students of the direction of training “Applied Informatics” of the Tomsk State University of Control Systems and Radioelectronics, this paper shows the advantages of using individual components of modern educational technology Moodle for the formation of a personalized e-learning environment for students. The article provides examples of elements that make it possible to effectively organize the university's educational process: enrolling participants in the course, checking students' work and setting the time for completing assignments, statistics on evaluating assignments in general for all participants, etc. As elements of the course, the work includes Database; Wiki; Glossary;

The task; Lecture, Seminar, Test, Forum, Chat and some others. Moodle allows the integration of popular webinar services such as BigBlueButton, Zoom, Jitsi, OpenMeetings, WebEx Meeting, Via-Virtual Classroom. According to the authors, the most convenient is BigBlueButton, which provides automatic publication of conference records on the course page.

Ключевые слова: дистанционное обучение; СДО Moodle; образовательные технологии.

Keywords: distance learning; LMS Moodle; educational technologies.

С весны 2020 года самые передовые информационные технологии активно начали использоваться при реализации образовательного процесса в дистанционной форме, ставшей обязательной в большинстве стран мира в период пандемии COVID-19 [1]. На сегодня Moodle (Modular Object-Oriented Dynamic Learning Environment) – одна из самых популярных платформ электронного обучения [2]. Компоненты этой системы обеспечивают широкими возможностями преподавателя вуза в части организации учебного процесса и контроля за его реализацией.

На примере контента дисциплины «Информационные системы и технологии» для студентов направления подготовки «Прикладная информатика» Томского государственного университета систем управления и радиоэлектроники, в данной работе показаны преимущества использования отдельных компонентов системы управления обучением (Learning Management System – LMS) Moodle (рисунок 1).

Moodle создана как обучающая платформа для формирования персонализированной среды обучения [3].

По состоянию на март 2021 года сборки Moodle поддерживают большинство популярных операционных систем – Windows, MacOS, Linux/Unix [4].

Потребительский функционал реализуется через веб-приложение, что исключает зависимость системы дистанционного обучения (СДО) от операционной системы, установленной на устройстве клиента.

Развёртывание Moodle можно осуществить на собственном производственном сервере или воспользоваться услугами стороннего хостинга.

На рынке также представлены услуги облачного размещения платформы [5].

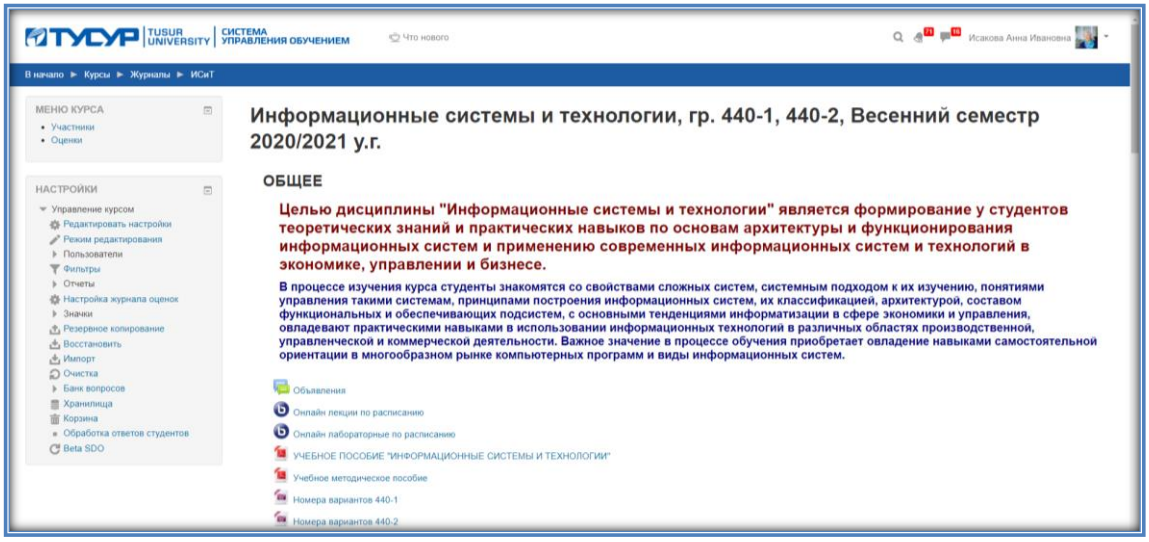

Рисунок 1. Фрагмент контента журнала дисциплины «Информационные системы и технологии» для групп

В Moodle допускается интеграция таких популярных вебинар-сервисов, как BigBlueButton, Zoom, Jitsi, OpenMeetings, WebEx Meeting, Via-Virtual Classroom.

Наиболее удобным, по мнению авторов, является BigBlueButton, используемый, в частности, на платформе СДО Томского государственного университета систем управления и радиоэлектроники (ТУСУР). Помимо того, что BigBlueButton – свободное ПО, по окончании видеоконференций ссылки на записи автоматически размещаются на соответствующей странице личного кабинета, что избавляет администраторов курсов от излишнего ручного труда (рисунок 2).

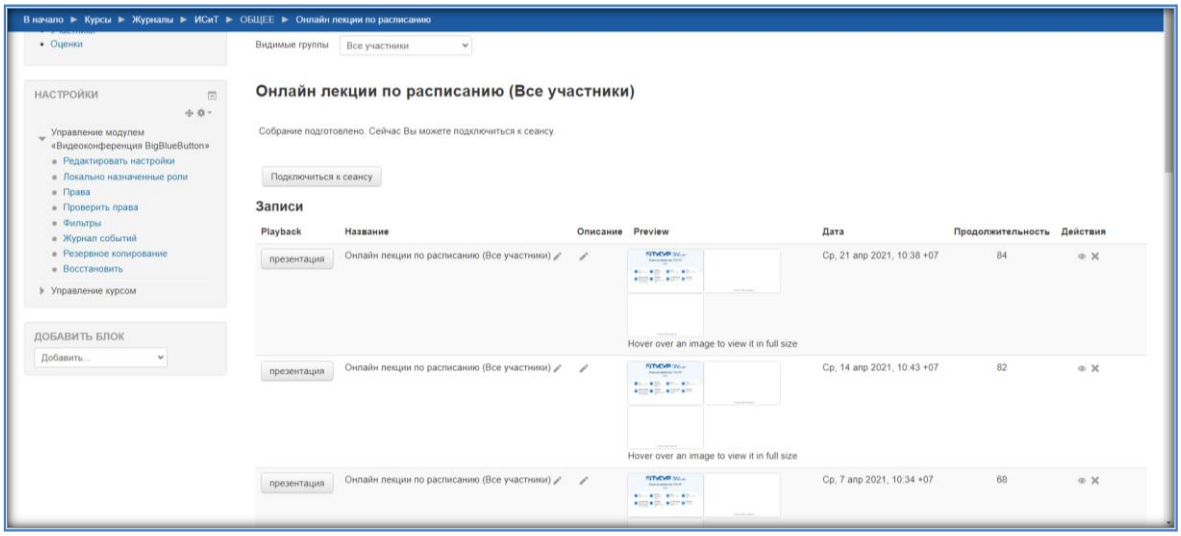

Рисунок 2. Фрагмент ссылок онлайн лекций в BigBlueButton, доступных участникам образовательного процесса по данной дисциплине

Масштабируемость и расширяемость Moodle не ограничена. Согласно документации данного программного обеспечения (ПО), Moodle можно масштабировать от нескольких студентов до миллионов пользователей [6].

Moodle содержит достаточно широкий спектр предустановленных инструментов, позволяющих эффективно организовывать учебный процесс и осуществлять контроль знаний студентов – значимая составляющая при дистанционном обучении [7].

В качестве элементов курса рассматриваются [5]: H5P (пакет HTMP5); База данных; Wiki; Глоссарий; Задание; Лекция.

Помимо указанных выше, в состав элементов курса входят семинар, тест, форум, чат, а также некоторые другие (рисунок 3).

Moodle предоставляет возможность обращения к сторонним системам обучения через СДО, используя Learning Tools Interoperability (LTI – спецификация образовательных технологий, разработанная IMS Global Learning Consortium) [8].

Система также допускает применение пакетов SCORM – созданных по определённому стандарту учебных курсов [9]. Он поддерживается большинством современных СДО и даёт возможность переноса курса с одной СДО на другую, использование курсов сторонних разработчиков либо сохранение своих при смене используемой платформы.

Преподаватель курса имеет возможность зачислять студентов вуза (выбирая группы или объединяя их в подгруппы) и других преподавателей на свой курс, назначать им соответствующие роли.

Доступ к СДО в любом удобном для пользователя месте обеспечивается также приложениями для смартфонов на базе iOS и Android, обладающими минимально необходимым набором функций.

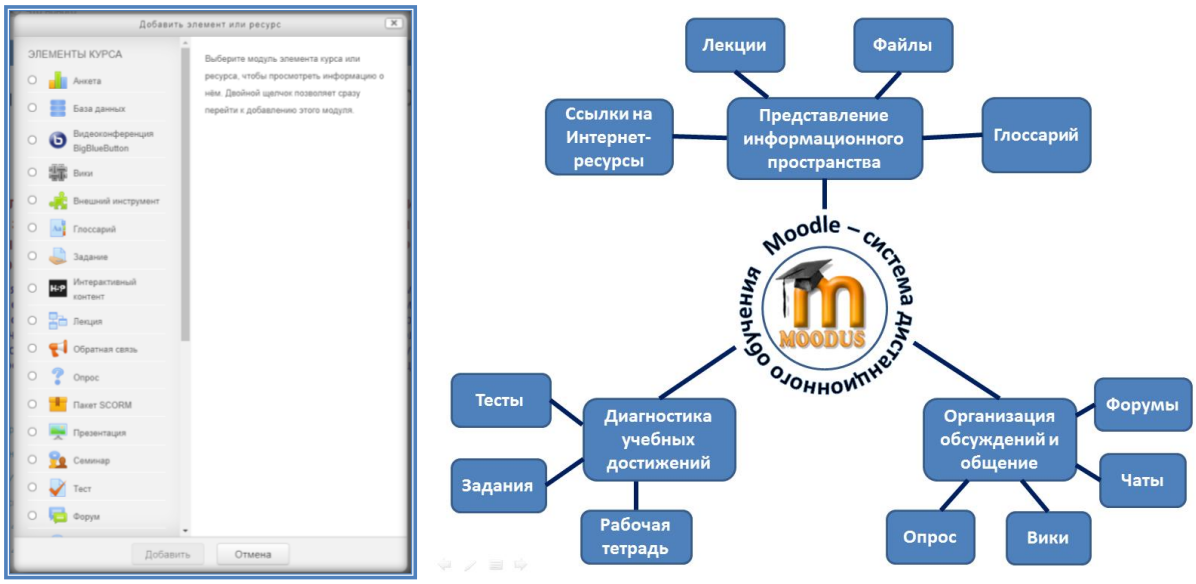

Рисунок 3. Элементы, позволяющие эффективно организовывать учебный процесс в вузе

Описание ценовой политики весьма краткое – платформа бесплатна. Распространяется в рамках Открытого лицензионного соглашения свободного программного обеспечения (GNU – General Public License) и имеет, как уже говорилось выше, открытый исходный код.

Каждый разрабатываемый курс имеет определенную структуру, состоящую из нескольких учебных модулей, посвященных отдельной теме. Элементами модулей могут быть лекции, практические занятие, лабораторные работы, тесты, контрольные работы и др.

По результатам выполнения студентами заданий, преподаватель выставляет оценки (шкалу оценивания также определяется преподавателем) и имеет возможность оставить комментарий к работе в специально отведенном поле. Эта информация сохраняется и сообщается студенту путём отправки уведомления по электронной почте.

Вся информация о проверке задания заносится в журнал (рисунок 4), который также можно настраивать – определять даты начала и окончания сроков сдачи определенных заданий и тестирования; ограничивать период, в пределах которого студентам разрешается выполнить задание и загрузить его в специально отведенную для этого папку (рисунок 5).

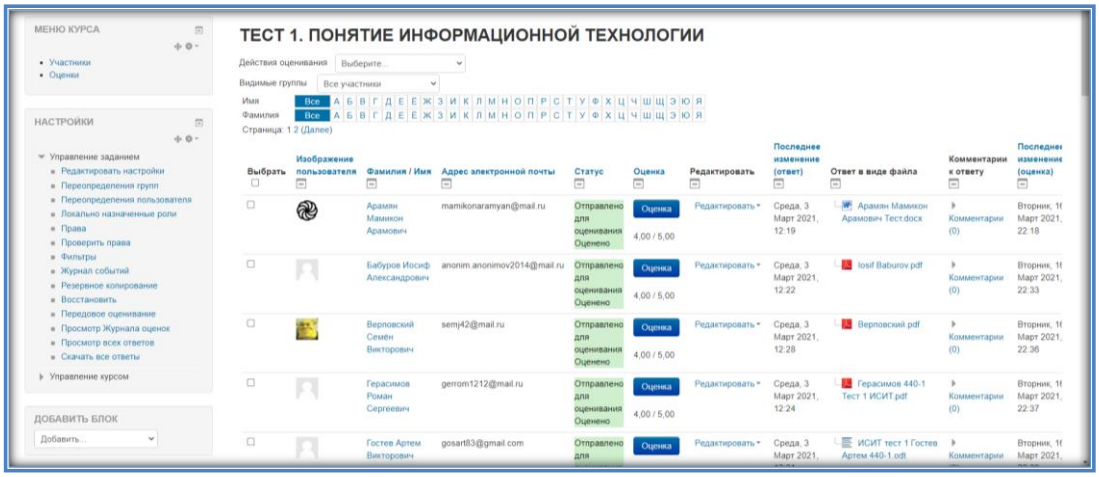

Рисунок 4. Итоговый журнал оценок по проверке конкретного задания

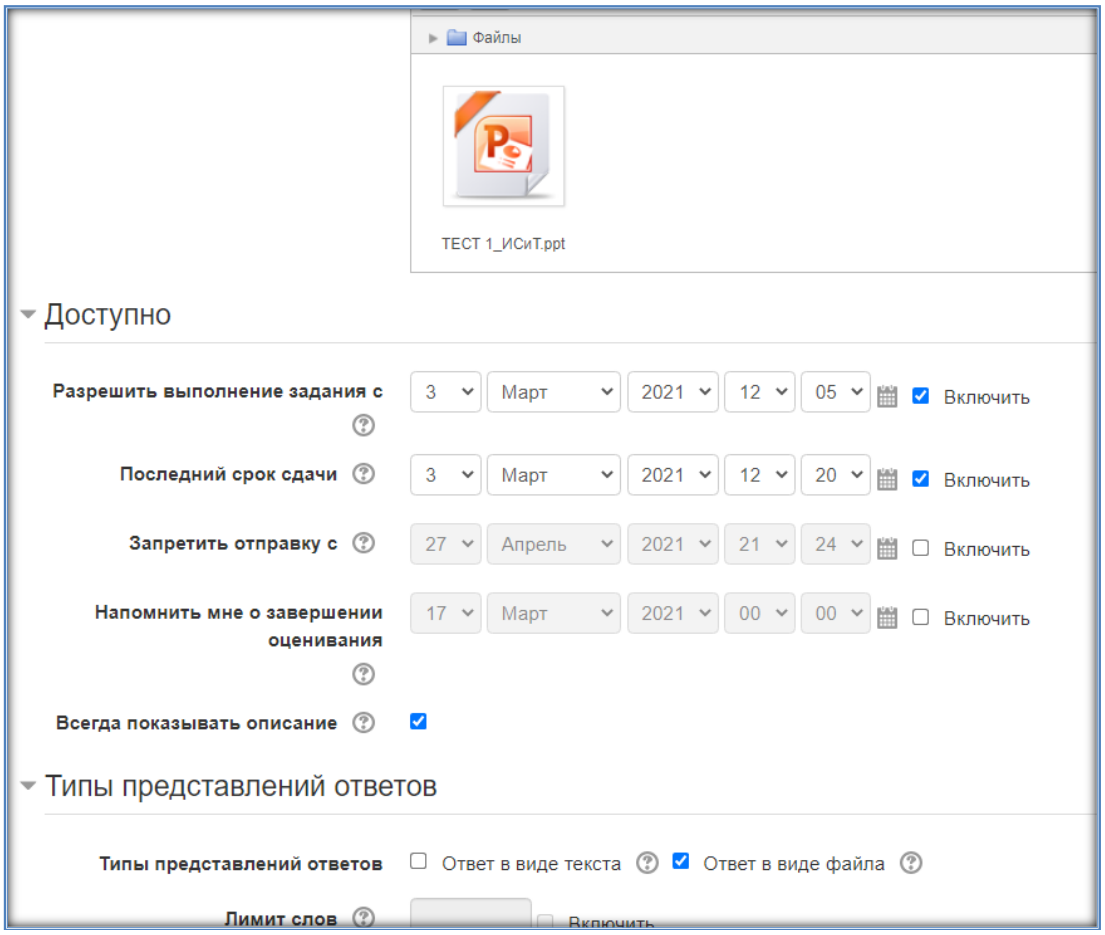

Рисунок 5. Настройка времени сдачи задания

В системе Moodle преподаватель может видеть статистику выполнения заданий всеми участниками образовательного процесса или статистику одного определённого участника (рисунок 6).

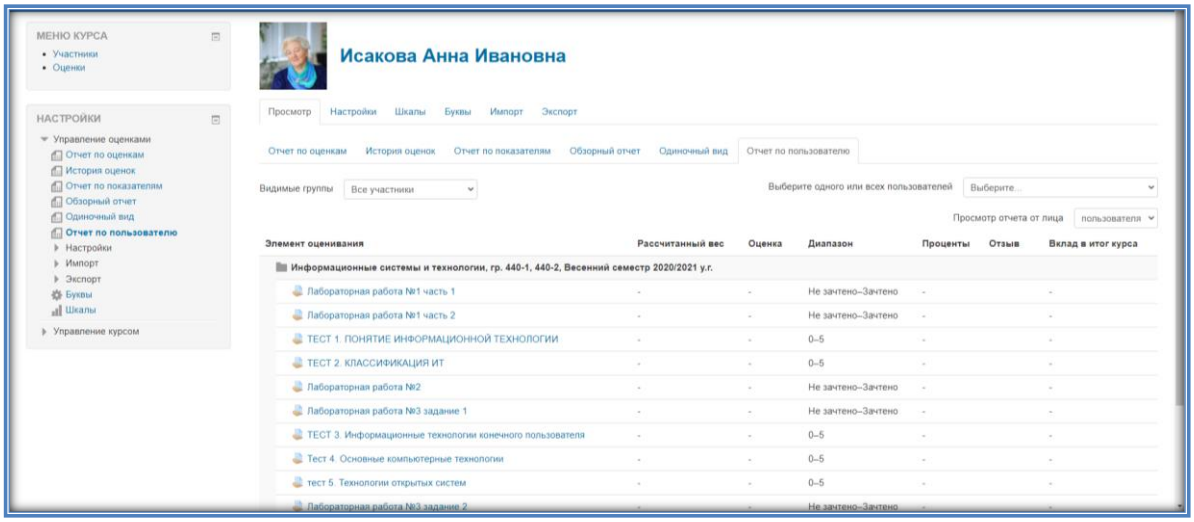

Рисунок 6. Статистика оценивания заданий в целом всех участников

Выводы

Таким образом, система управления обучением Moodle позволяет расширить возможности образовательного процесса в вузе, создать условия для активной и мотивированной деятельности всех его участников.

Основными преимущества использования Moodle для формирования персонализированной среды электронного обучения студентов вуза являются:

– четкая структуризация и наглядное представление учебного материала в начале изучения дисциплины;

– проверка знаний и контроля успеваемости студентов;

– ведение статистики посещаемости, активности студентов;

– составление индивидуальной траектории обучения студента;

– хранение выполненных работ студентов в портфолио.

Электронный курс по дисциплине «Информационные системы и технологии» предоставил студентам первого курса новые возможности – в любое время просмотреть необходимый материал в режиме онлайн, прослушать аудиолекцию по теме, задать вопрос преподавателю, пройти тестирование, проверить свои знания по изучаемой дисциплине, просмотреть свои оценки в журнале и исправить неаттестованные работы.

Литература

1. Исакова, А.И., Кориков, А.М., Левин, С.М. Платформы взаимодействия со студентами в условиях пандемии COVID-19 и дистанционного обучения // Современное образование: повышение конкурентоспособности университетов: В 2 ч. Ч. 2: материалы междунар. науч.-метод. конф., 28-29 января 2021 г., Томск, Россия. – Томск: Изд-во Томск. гос. ун-та систем упр. и радиоэлектроники, 2021. – С. 189-195.

2. About Moodle. URL: https://docs.moodle.org/310/en/About_Moodle#All-in-one_learning_platform

3. Moodle. Scalable to any size. URL: https://docs.moodle.org/310/en/About_ Moodle#Scalable_to_any_size

4. Рекомендуемые системы дистанционной работы. URL: https://wiki.cs.msu.ru/Main/СистемыУдаленнойРаботы

5. Moodle. Activities. URL: https://docs.moodle.org/310/en/Activities

6. Learning_Tools_Interoperability. URL: https://en.wikipedia.org/wiki/Learning _Tools _Interoperability

7. Исакова А.И., Левин С.М. Модели повышения мотивации студентов в образовательном процессе вуза // Инженерное образование. 2020. №28. С. 20-30.

8. Alie M., Casany M.J., Llorens A., Alcober J., Prat J.d. Atenea. Exams, an IMS LTI Application to Solve Scalability Problems: A Study Case // Applied Sciences. 2021. №11(1). P. 80. URL: https://dx.doi.org/10.3390/app11010080

9. Бабичева И.В. Реализация когнитивно-визуального подхода к обучению математике с использованием SCORM-технологий//Вестник Сибирского института бизнеса и информационных технологий. 2020. №2 (34). С. 5-15. DOI: 10.24411/2225-8264-2020-10014

УДК 004

МЕТОДОЛОГИЧЕСКИЕ ПОДХОДЫ ФОРМИРОВАНИЯ ГОТОВНОСТИ СТУДЕНТОВ К САМОСТОЯТЕЛЬНОЙ РАБОТЕ ПОСРЕДСТВОМ БЕНЧМАРКИНГ-ТЕХНОЛОГИИ

METHODOLOGICAL APPROACHES OF FORMATION OF STUDENTS READINESS FOR INDEPENDENT WORK BY MEANS OF BENCHMARKING TECHNOLOGY

Зиязиева Л.Р.,
Кокшетауский государственный университет им. Ш. Уалиханова,
г. Кокшетау, Республика Казахстан
ФГБОУ ВО «Горно-Алтайский государственный университет»
г. Горно-Алтайск, Российская Федерация

L.R. Ziyazieva,
Kokshetau State University named after Sh. Ualikhanova,
Kokshetau, Republic of Kazakhstan
FSBEI HE “Gorno-Altai State University”
Gorno-Altaysk, Russian Federation

e-mail: liliyazr@mail.ru.

Аннотация. В статье рассмотрены методологические подходы, которые автор использовал для разработки и реализации модели формирования готовности студентов к организации СРС посредством бенчмаркин-технологий. Был использован комплексный подход, который включал в себя системный, деятельностный, компетентностный подходы, взаимосвязанные друг с другом. Кроме того, раскрыто понятие «бенчмаркинг», как поиск лучших практик, инноваций и идей в системе образования. Раскрыта актуальность формирования готовности студентов посредством бенчмаркинг-технологий, а также предложена модель формирования готовности студентов. Рассмотрены вопросы влияния бенчмаркинг-технологии на процесс организации самостоятельной деятельности обучающихся. При формировании готовности студентов к самообразованию и самообучению особую значимость приобретают бенчмаркинг-технологии. Возможность получения лучшего опыта делает эту технологию все более привлекательной в образовательной среде. Применение бенчмаркинга в образовании представляет собой довольно сложный процесс, так как включает в себя очень много факторов, которые необходимо изучить. Вместе с тем, бенчмаркинг – это стимул к развитию у учебного заведения стремления к непрерывному совершенствованию и самосозиданию, а также непрерывный поиск новых идей, их адаптация и использование на практике.

Abstract. The article discusses the methodological approaches that the author used to develop and implement a model for the formation of students' readiness to organize CDS through benchmarking technologies. An integrated approach was used, which included systemic, activity-based, competency-based approaches interconnected with each other. In addition, the concept of “benchmarking” is disclosed as a search for best practices, innovations and ideas in the educational system. The relevance of students 'readiness formation through benchmarking technologies is disclosed, and a model of students' readiness formation is also

proposed. The questions of the impact of benchmarking technology on the process of organizing students' independent activities are examined. In the formation of students' readiness for self-education and self-learning, benchmarking technologies are of particular importance. The opportunity to gain better experience makes this technology more attractive in the educational environment. The use of benchmarking in education is a rather complicated process, since it includes a lot of factors that need to be studied. At the same time, benchmarking is an incentive for the development of the institution's desire for continuous improvement and self-creation, as well as the continuous search for new ideas, their adaptation and use in practice.

Ключевые слова: бенчмаркинг-технологии, системный подход, самообразования, формирование готовности, профессиональное образование.

Keywords: benchmarking technology, a systematic approach, self-education, readiness formation, professional education.

Современный взгляд на образование требует абсолютного обновления системы высшего профессионального образования.

С недавних пор высшее образование перестало соответствовать потребностям государства. В период, когда на рынке труда наметилось значительное оживление, стал остро ощущаться недостаток творческих, активных специалистов, способных удовлетворить требования производства.

Современное образование должно быть направлено на формирование знаниевой культуры посредством творческого развития и готовностью студентов к самостоятельной работе. Так, Г. Щедровицкий писал: «Люди уже заранее должны быть максимально подготовлены к возможным сменам профессии, они должны иметь общее научное и техническое образование, которое бы обеспечило им необходимую основу для широкой группы профессий и свело процесс переучивания к минимуму». Чтобы соответствовать требованиям современного производства, специалисту необходимо постоянно повышать свою профессиональную квалификацию.

При формировании готовности студентов к самообразованию и самообучению особую значимость приобретают бенчмаркинг-технологии. Возможность получения лучшего опыта делает эту технологию все более привлекательной в образовательной среде.

Большинство зарубежных и отечественных исследователей (Е.А. Князев, Я.Ш. Евдокимова, С. Гарлик, А. Карялайнен, Д.В. Маслова и др.) под бенчмаркингом в образовании понимают анализ результатов между образовательными организациями с целью получения информации для самосовершенствования процесса.

Применительно к образовательной системе понятие «бенчмаркинг», на наш взгляд, может быть объяснено как систематический процесс поиска лучшей практики, инновационных идей и высокоэффективных процедур, которые позволяют совершенствовать учебно-воспитательный процесс.

Не всегда стоит обращаться к лучшим практикам других вузов, можно также присмотреться и перенять опыт у других кафедр или факультетов своего учебного заведения, так как бенчмаркинг в образовательной среде предназначен сравнить общие действия и адаптировать лучшие, не конкурируя между собой.

Таким образом, польза бенчмаркинга состоит в том, что образовательные функции становятся наиболее управляемыми, когда исследуются и внедряются лучшие методы и технологии других.

На наш взгляд, применение бенчмаркинга в образовании представляет собой сложный процесс, так как включает в себя много факторов, которые необходимо

изучить. Вместе с тем, бенчмаркинг – это стимул к развитию у учебного заведения стремления к непрерывному совершенствованию, а также непрерывный поиск новых идей, их адаптация и использование на практике.

Как известно, доля самостоятельной работы составляет порядка 70% в общем объеме дисциплины.

Как показывают данные Forrester Research, отвечая на вопрос о приоритетах своей деятельности:

– 58% руководителей в сфере высшего образования назвали своей основной задачей «Обучение студентов практическим навыкам и получение ими знаний, необходимых для их дальнейшей профессиональной деятельности через самообразование»,

– 56% руководителей назвали своим приоритетом привлечение и удержание студентов, которые соответствуют стандартам академической успеваемости [1].

Также по их данным больше половины студентов, начинающих курс обучения, не могут его окончить, так как не умеют правильно организовать процесс самостоятельной работы.

Практика показывает, что не все студенты готовы к активному самообразованию, не умеют ориентироваться в потоке информации, пользоваться учебной и научной литературой, интернет ресурсами для нахождения нужной информации.

Анализ педагогических исследований в этой области позволил выделить противоречие между повышением требований к готовности СРС студентов и их фактическими возможностями к самообучению и творческому развитию.

В научно-педагогических трудах исследователя Р.Б. Срода под самостоятельной работой обучающихся понимается такую деятельность, которая сопровождается максимумом творчества, активности, самостоятельного суждения, инициативы. Но работа в условиях непонимания, когда обучающийся сам должен организовать процесс СР, приводит к определенным трудностям [2].

Исходя из этого, проблема формирования готовности у студентов к самостоятельной работе и самосозиданию посредством бенчмаркинг-технологии становится весьма актуальной.

Бенчмаркинг-технологии позволят улучшить процесс формирования готовности у студентов к самостоятельной работе опираясь на опыт и знания лучших в этой сфере, помогая студентам перейти от пассивного слушателя к творчески активной личности, автономно выстраивая и организовывая собственную учебную деятельность [3].

В нашем исследовании для разработки и реализации модели формирования готовности студентов к организации СРС посредством бенчмаркин-технологий мы использовали комплексный подход, который включал в себя системный, деятельностный, компетентностный подходы, взаимосвязанные друг с другом.

Для повышения эффективности формирования готовности к самостоятельной работе студентов применяется *системный подход.*

Основоположниками системного подхода являются: И.В. Блауберг, Э.Г. Юдина А.А. Богданов, Л. фон Берталанфи, Э. де Боно, Л. ла Руш, Г. Саймон, П. Друкер, А. Чандлер, С.А. Черногор, А.Н. Малюта и др.

И.В. Блауберга и Э.Г. Юдина считают, что системный подход – это методологическое направление, задачей которого является разработка принципов, методов и средств изучения объектов, представляющих собой системы [4].

Э.С. Маркарян отмечает, что системный подход способен поставить перед социальными науками проблемы, наметить новые подходы и перспективы исследования, выполнить роль необходимого связующего звена этих наук с другими областями знания, роль определенного методологического средства [5].

Системный подход включает в себя элементы формирования готовности студентов к самостоятельной работе: цели, организация процесса, индивидуальный подход, корректировка процесса организации с учетом способностей студентов, оценка и учет её результатов, мотивация и т.д.

Формирование готовности студентов к СР включает обеспечение необходимой информацией, грамотное использование бюджета времени студентов, умение использования интернет-ресурсов.

Важность системного подхода можно проследить в структуре готовности к СРС, схематически указанной на рисунке 1:

Рисунок 1. Структура формирования готовности
к самостоятельной работе студентов

Относительно самостоятельной работы системный подход представляет собой понимание формирования готовности к самостоятельной работе как системному совершенствованию и упорядочению всех составных элементов: организация времени, форм и методов проведения, обеспечение информацией и т.д. Для эффективной реализации описанного подхода необходимо разработать модель формирования готовности студентов к СР с составляющими элементами для обеспечения системности.

Аспекты *компетентностного* подхода отражены в трудах И.А. Зимней, В.В. Краевского, А.К. Марковой. Основоположниками системного подхода являются: А.А. Богданов, Л. фон Берталанфи, Э. де Боно, Л. ла Руш, Г. Саймон, П. Друкер, А.Чандлер, С. А. Черногор, А.Н. Малюта.

Деятельностный подход в педагогической психологии исследовали отечественные ученые, а именно Л.С. Выготский, С.Л. Рубинштейн, А.Н. Леонтьев и др. К активным их сторонникам и продолжателям следует отнести Л.В. Занкова, Д.Б. Эльконина, В.В. Давыдова, П.Я. Гальперина, Н.Ф. Талызину, А.К. Маркову и др. Они определяют деятельностный подход как организацию обучения и воспитания, при которой ученик действует с позиции активного субъекта познания, труда и общения, у которого целенаправленно формируются учебные умения по осознанию цели, планированию хода предстоящей деятельности, ее исполнению и регулированию, выполнению самоконтроля, анализа и оценки результатов своей деятельности [5].

Рисунок 2. Модель формирования готовности студентов к самостоятельной работе посредством бенчмаркинг-технологии

Выводы

Таким образом, модель формирования готовности студентов к самостоятельной работе посредством бенчмаркинг-технологии должна объединять в себе преимущества системного, деятельностного, компетентностного подходов (рисунок 2).

Литература

1. Джородж Р. Боггс «Колледжи демократии: развитие местных колледжей в Америке» // Американская ассоциация местных колледжей, 2010 г. URL: http://www2.ed.gov/PDFDocs/college-completion/01-democracys-colleges.pdf.

2. Срода Р.Б. Воспитание активности и самостоятельности учащихся в учении. М., 1956.

3. Данилова Т.В. Бенчмаркинг как инструмент обеспечения конкурентоспособности образовательных услуг вуза: дис. канд. пед. наук. – Казань, 2007. 188 с.

4. Блауберг И.В. Становление и сущность системного подхода // И.В. Блауберг, Э.П. Юдин. – М.: Наука, 1973. 270 с.

5. Маркарян Э.С. Вопросы системного рассмотрения культуры в человеческой деятельности. История материализма как теория социального познания и деятельности // Э.С. Маркарян. URL: http://ej.kubagro.ru/2015/07/pdf/59.pdf. Научный журнал КубГАУ, №111(07), 2015. М.: Наука, 1972. 452 с.

6. Эльконин Б.Д. Действие как единица развития // Вопросы психологии. 2004, №1. с. 35-49.