ISSN 2618 - 7167

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СТРОИТЕЛЬНЫХ, СОЦИАЛЬНЫХ И ЭКОНОМИЧЕСКИХ СИСТЕМАХ

НАУЧНО - ТЕХНИЧЕСКИЙ ЖУРНАЛ

Выпуск №3-4 (17-18)

Декабрь, 2019

- **МАТЕМАТИЧЕСКИЕ МЕТОДЫ СИСТЕМНОГО АНАЛИЗА И УПРАВЛЕНИЯ**
- **ИНФОРМАЦИОННО - ВЫЧИСЛИТЕЛЬНЫЕ, УПРАВЛЯЮЩИЕ И СЕТЕВЫЕ СИСТЕМЫ**
- **СИНТЕЗ, АНАЛИЗ И ПРИНЯТИЕ РЕШЕНИЙ**
- **АЛГОРИТМЫ, ПРОГРАММЫ И БАЗЫ ЗНАНИЙ**

ВОРОНЕЖ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СТРОИТЕЛЬНЫХ, СОЦИАЛЬНЫХ И ЭКОНОМИЧЕСКИХ СИСТЕМАХ

ВЫХОДИТ ЧЕТЫРЕ РАЗА В ГОД

НАУЧНО - ТЕХНИЧЕСКИЙ ЖУРНАЛ

Учредитель и издатель: Федеральное государственное бюджетное образовательное учреждение высшего образования «Воронежский государственный технический университет»

Адрес учредителя и издателя: 394026 г. Воронеж, Московский просп., 14

Территория распространения - Российская Федерация

РЕДАКЦИОННАЯ КОЛЛЕГИЯ ЖУРНАЛА:

Главный редактор - Д.К. Проскурин, канд. физ.-мат. наук, доц.
Зам. главного редактора - Д.В. Сысоев, канд. техн. наук, доц.
Ответственный секретарь - Н.В. Акамсина, канд. техн. наук, доц.

ЧЛЕНЫ РЕДКОЛЛЕГИИ:

Авдеев В.П., д-р техн. наук, проф. (ВГТУ)
Алгазинов Э.К., д-р техн. наук, проф. (ВГУ)
Баркалов С.А., д-р техн. наук, проф. (ВГТУ)
Голиков В.К., канд. техн. наук, доц. (РАП)
Головинский П.А., д-р физ.-мат. наук, проф.(ВГТУ)
Зольников В.К., д-р техн. наук, проф. (ВГЛТУ)
Князева Т.Н., д-р техн. наук, проф. (ВГМУ)
Курипта О.В., канд. техн. наук, доц. (ВГТУ)
Лавлинский В.В., д-р техн. наук, доц.(ВГЛТУ)
Ряжских В.И., д-р техн. наук, проф. (ВГТУ)
Хаустов И.А., д-р техн. наук, проф. (ВВА)
Хвостов А.А., д-р техн. наук, проф. (ВВА)

Статьи, поступившие в редакцию, рецензируются. За достоверность сведений, изложенных с статьях, ответственность несут авторы публикаций. Мнение редакции может не совпадать с мнением авторов материалов. Перепечатка без разрешения редакции запрещена, ссылки на журнал при цитировании обязательны.

Материалы публикуются в авторской редакции.

16+

© ВГТУ, 2019

Дата выхода в свет 30.12.2019. Формат 60x84/8. Бумага писчая. Усл. печ. л. 21,6.
Уч.-изд. л. 16,4. Тираж 500 экз. Заказ № 257. Цена свободная.

ФГБОУ ВО «Воронежский государственный технический университет»
394026 Воронеж, Московский проспект, 14

Отпечатано: отдел оперативной полиграфии издательства ВГТУ
394006, г.Воронеж, ул. 20-летия Октября, 84

МАТЕМАТИЧЕСКИЕ МЕТОДЫ СИСТЕМНОГО АНАЛИЗА И УПРАВЛЕНИЯ

Литвин Н.В. Моделирование полумарковского прибора для многоканальной системы обслуживания …….. 7

Глущенко С.В. О факторном анализе в целеполагаемых системах …….. 13

Кущев А.Б. О существовании периодических решений одного класса дифференциальных уравнений 3-го порядка с существенной нелинейностью в случае отсутствия второй производной в линейной части …….. 16

Лавлинская О.Ю. Универсальная мера измерения как инструмент динамики развития инновационных систем …….. 19

Бырдин А.П., Сидоренко А.А., Соколова О.А., Сысоева А.А. Деформации в плоской задаче для материалов с функциональной реологией …….. 22

Кузнецова О.Н., Кузнецов А.А., Несмеянов Н.Н. Сравнительный анализ технических средств для ведения воздушной радиационной разведки …… 25

Хвостов А.А., Журавлев А.А., Журавлев Е.А., Сысоев Д.В. Математическая модель динамики конфликта на основе Марковской цепи …… 30

Litvin N.V. Semi-Markov device for multi-channel system of maintenance …….. 7

Gluschenko S.V. On factor analysis in purpose systems …… 13

Kushchev A.B. Existence periodic solution one class differential equation third order with essential nonlinearity without two derivative in linear part …… 16

Lavlinskaya O.Yu. Universal measure as a tool for the dynamics of the development of innovative systems …….. 19

Byrdin A.P., Sidorenko A.A., Sokolova O.A., Sysoeva A.A. The deformations in plane problem for the material with functional equation state …….. 22

Kuznetsov O.N., Kuznetsov A.A., Nesmeyanov N.N. Comparative analysis of technical means for conducting aerial radiation reconnaissance …… 25

Khvostov A.A., Zhuravlev A.A., Zhuravlev E.A., Sysoev D.V. Mathematical model of conflict dynamics based on Markov chain …….. 30

ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫЕ, УПРАВЛЯЮЩИЕ И СЕТЕВЫЕ СИСТЕМЫ

Гильмутдинов В.И., Кононов А.А. Определение энтропии принимаемого двумерного сигнала с М-распределением огибающих ортогонально-поляризованных компонент …….. 36

Жидко Е.А., Кирьянов К.А. Теоретический подход к исследованиям по проблеме информационных конфликтов хозяйствующего субъекта …….. 40

Мешков Д.А., Стариков А.В. Определение формальной структуры процесса проектирования в мультиагентной среде ВКБМ …….. 46

Давнис В.В., Добрина М.В., Чекмарев А.В. Компаративный анализ различных типов инвестиционных портфелей …….. 48

Gilmutdinov V.I., Kononov A.A. Determination of the entropy of the received two-dimensional signal with M-distribution of envelopes of orthogonally polarized components …….. 36

Zhidko E.A., Kiryanov K.A. Theoretical approach to research on the problem of information conflicts of the economic subject … 40

Meshkov D.A., Starikov A.V. Determination of the formal structure of the design process in the multiaagent environment of virtual design office furniture …….. 46

Davnis V.V., Dobrina M.V., Chekmarev A.V. Comparative analysis of different types for investment portfolios …….. 48

Паршина Е.М. ERP-системы. Анализ оценки рисков при использовании ERP-систем …… 52

Колыхалова Е.В., Андреева К.А. Анализ жизненного цикла продукта с учетом будущих изменений ……..... 57

Лупаренко Е.В. Экспертная система первичной диагностики заболеваний ……... 60

Акимов В.И., Полуказаков А.В., Какалов В.А. Система климат-контроля в информационном ресурсе «Умного дома» …….. 66

Звягинцева А.В., Сазонова С.А., Ефремов В.В. Воздействие электромагнитных излучений на развитие радиоволновых заболеваний……. 72

Пырнова О.А., Зарипова Р.С. Перспективы развития искусственного интеллекта и кибернетики ……. 78

Аснина Н.Г., Еремина Т.В. Разработка функциональных моделей процедуры проверки обвинительного заключения прокурором ……. 81

Parshina E.M. ERP-systems. Risk assessment analysis when using ERP-systems …….. 52

Kolyhalova E.V., Andreeva K.A. Product life cycle analysis for future changes …… 57

Luparenko E.V. Expert system of primary diagnostics of diseases …… 60

Akimov V.I., Polozakakov A.V., Kakalov V.A. Climate control system in the information resource of Smart Home ……. 66

Zvyagintseva A.V., Sazonova S.A., Efremov V.V. The impact of electromagnetic radiation on the development of radio wave diseases ……... 72

Pyrnova O.A., Zaripova R.S. Prospects for the development of artificial intelligence and cybernetics …….. 78

Asnina N.G., Eremina T.V. Development of functional models of the procedure for checking a charge conclusion by the prosecutor …… 81

СИНТЕЗ, АНАЛИЗ И ПРИНЯТИЕ РЕШЕНИЙ

Добрина М.В. Путевой анализ в пакете STATISTICA …… 86

Волобуева Т.В. Управление складом. Оптимизация затрат хранения товаров на складе …… 90

Звягинцева А.В., Сазонова С.А., Пакин В.С. Исследование уровня экологической безопасности и радиационной защиты на примере НВАЭС …….. 97

Ефремов В.В., Патраков Л.В., Пакин В.С. Анализ рекомендаций для повышения эффективности системы контроля электромагнитных полей …… 104

Жидко Е.А., Недоносков А.Б. Подход к оценке возможностей разрешения информационного конфликта хозяйствующих субъектов …….. 109

Гуляева Д.А. Декомпозиция задачи синтеза деятельности организации на стадии формирования задания на ее разработку …….. 114

Паршина Е.М. Моделирование и анализ эпидимических процессов в корпоративной сети с внедренной ERP –системой …… 117

Ефремов В.В., Патраков Л.В., Пакин В.С. Экологическая характеристика естественных источников радиации 120

Мозговой Н.В., Фадеев Б.И. Анализ риска при транспортировке газа на территории сельского поселения 125

Dobrina M.V. Path analysis in the STATISTICA package ……... 86

Volobueva T.V. Warehouse menegement. Optimization of storage costs of goods in the wsrehouse ……... 90

Zvyagintseva A.V., Sazonova S.A., Pakin V.S. Research of the level of ecological safety and radiation protection on the example of NNPP … 97

Efremov V.V., Petrakov L.V., Bakin V.S. Analysis of recommendations to improve the efficiency of the electromagnetic field control system ……. 104

Zhidko E.A., Nedonoskov A.B. Approach to the evaluation of the possibilities of resolving the information conflict of economic subjects …..... 109

Gulyaeva D.A. Decomposition of synthesis problems of the organization at the stage of formation tasks for its development ……... 114

Parshina E.M. Modeling and analysis of epidymic processes in the corporate network with the embedded ERP-system ……. 117

Efremov V.V., Patrakov L.V., Pakin V.S. Ecological characteristics of natural radiation sources …… 120

Mozgovoj N.V., Fadeev B.I. Risk analysis during gas transportation in the territory of a rural settlement ……... 125

АЛГОРИТМЫ, ПРОГРАММЫ И БАЗЫ ЗНАНИЙ

Галиуллина Э.Р., Зарипова Р.С. Проблемы кибербезопасности для виртуальной образовательной среды ……... 129

Звягинцева А.В., Сазонова С.А., Мозговой Н.В. Анализ показателей степени экологических рисков и разработка организационных и технических мероприятий на ООО «ПРИДОНХИМСТРОЙ» ….. 132

Кульнева В.В., Свиридова С.В. Разработка алгоритма процесса управления в социально-экономических системах …… 138

Кузнецова О.Н., Побережнюк Н.С., Богданов А.П. Разработка беспилотного летательного аппарата для ведения воздушной радиационной разведки … 145

Шакиров А.А., Зарипова Р.С. Проблемы обеспечения информационной безопасности больших данных …….. 150

Гречишников А.Л. Методы математической статистики в применении экспериментальной методики развития координационных способностей у юных игроков в «русский» хоккей 152

Коноплёв С.В. Выбор программных инструментов анализа данных для студенческого научного исследования …… 157

Галиуллина Э.Р., Шакиров А.А., Зарипова Р.С. Информационная безопасность в финансовых транзакциях через мобильный телефон: алгоритмы 162

Добрина М.В., Чекмарев А.В. Потенциал больших данных для финансовой сферы …….. 166

Аснина Н.Г., Емельяненко Е.А. Анализ технологий ведения проектов разработанных для внедрения программных продуктов на базе «1С: Предприятие 8» ……. 171

Мозговой Н.В., Фадеев Б.И. Пожарная безопасность нефтегазовых промыслов …… 174

Сергеева А.Г., Грибанов А.Н. Применение цифровых технологий на занятиях в рамках дисциплины «физическая культура» для студентов строительных вузов ……. 180

Иванова В.Р., Жидко Е.А. Сравнение вариантов утеплителя для реконструкции жилого дома методом анализа иерархий ……. 183

Galiullina E.R., Zaripova R.S. Cyber security problems for virtual educational environment …… 129

Zvyagintseva A.V., Sazonova S.A., Mozgovoj N.V. Analysis of indicators of the degree of ecological risks and development of organizational and technical events at LLC «PRIDONKHIMSTROY» …….. 132

Kulneva V.V., Sviridova S.V. Application of the hydrodynamic model of the combustion process in the study of the quality of mixture formation 138

Kuznetsova O.N., Poberezhnyuk N.S., Bogdanov A.P. The development of unmanned aerial vehicle to conduct aerial radiation reconnaissance …… 145

Shakirov A.A., Zaripova R.S. Problems of ensuring information security of big data ……... 150

Grechishnikov A.L. Methods of mathematical statistics in the application of experimental techniques for the development of coordination abilities in young players in “russian” hockey ... 152

Konoplyov S.V. Data analysis software tools for student scientific research ……... 157

Galiullina E.R., Shakirov A.A., Zaripova R.S. Information security in financial transactions via mobile phone: algorithms ……. 162

Dobrina M.V., Chekmarev A.V. The potential of big data for finance ……. 166

Asnina N.G., Emelyanenko E.A. Analysis of technologies for conducting projects designed for the introduction of software products on the basis "1C: Enterprise 8" …….. 171

Mozgovoj N.V., Fadeev B.I. Fire safety of oil and gas fields …….. 174

Sergeeva A.G., Gribanov A.N. Use of digital technologies in classes «Physical Education» for students of construction universities ……. 180

Ivanova V.R., Zhidko E.A. A comparison of insulation options for reconstruction of residential house method of analysis of hierarchies ……... 183

УДК 004

Казанский государственный энергетический университет
Студентка О.А. Пырнова, тел.: 8(843) 519-43-26
Канд. техн. наук, доцент Р.С. Зарипова
E-mail: zarim@rambler.ru
Россия, г. Казань

Kazan State Power Engineering University
Student O.A. Pyrnova, Ph.: 8(843) 519-43-26
Cand. tech. Sci., Assoc. R.S. Zaripova
E-mail: zarim@rambler.ru
Russia, Kazan

О.А. Пырнова, Р.С. Зарипова

ПЕРСПЕКТИВЫ РАЗВИТИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И КИБЕРНЕТИКИ

Аннотация: В данной статье затрагивается тема искусственного интеллекта и такого отдельного направления, как кибернетика. Описана роль данного направления как в информационных технологиях, так и в повседневной жизни людей. Кроме того, затрагиваются принцип работы и строение нейронных сетей

Ключевые слова: искусственный интеллект, «умные» технологии, кибернетика, нейронные сети, нейрон, информационные технологии

O.A. Pyrnova, R.S. Zaripova

PROSPECTS FOR THE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE AND CYBERNETICS

Annotation: This article addresses the topic of artificial intelligence and such a separate direction as cybernetics. The role of people in everyday life is described. In addition, it affects the principle of operation and structure of neural networks

Keywords: artificial intelligence, “smart” technologies, cybernetics, neural networks, neuron, information technology

Искусственный интеллект – область, появившаяся в сфере информационных технологий значительно недавно, однако развивающаяся огромными темпами. Началом истории искусственного интеллекта послужило предложение Джона МакКартни, Марвина Л. Мински и других ученых, сделанное в 1955 году, о том, что интеллектуальная машина будет стремиться создавать в себе абстрактную модель среды, в которой она будет размещена. То есть если бы ей была задана какая-либо проблема, то она могла бы сначала исследовать решения внутри своей внутренней абстрактной модели окружающей среды, а уже после сделать попытку в проведении внешних экспериментов. Ученые, сделавшие огромный вклад в этой области, добились впечатляющих успехов. Были построены машины, которые могли бы решить проблемы школьной математики, а программа под названием Eliza стала первым чатботом в мире, изредка обманывая пользователей, думая, что это было сознательно. В 1980-х годах последовал очередной бум, благодаря появлению экспертных систем и японской компьютерной инициативе пятого поколения, которая приняла параллельное программирование. Экспертные системы широко использовались в промышленности. В течение 1990-х и 2000-х годов были достигнуты многие из знаковых целей искусственного интеллекта. В 1997 году правящий чемпион мира по шахматам и гроссмейстер Гари Каспаров был побежден компьютерной программой Deep Blue, играющей в шахматы. Этот высокооплачиваемый матч был впервые поражением чемпиона мира по шахматам на компьютере и стал огромным шагом к искусственно интеллектуальной программе принятия решений. В том же году программное обеспечение распознавания речи, разработанное Dragon Systems, было реализовано в Windows. Это был еще один большой шаг вперед, но в направлении устной интерпретации речи. Сейчас мы живем в эпоху «Big Data», в которой находиться

© Пырнова О.А., Зарипова Р.С., 2019

огромное количество необходимой нам информации [1]. Однако человеческому мозгу сложно ее обрабатывать в полной мере. Применение искусственного интеллекта в этом отношении уже довольно плодотворно в ряде отраслей, таких как технологии, банковское дело, маркетинг и развлечения. Развитие искусственного интеллекта не прекращается ни на минуту и проникает во все сферы деятельности человека [2].

На данный момент искусственный интеллект делится на огромное количество направлений и сфер деятельности [3]. Например, разработка таких систем, как экспертные системы, экзоскелеты, машинное творчество. Однако наиболее важную роль в наши дни занимает изучение кибернетики.

Кибернетика изначально была наукой о сложных системах и процессах, их моделировании, управлении и связи. История кибернетики началась с изобретения Джеймса Ватта – паровой машины в 1765 году. В наши дни кибернетика подразумевает под собой управление обратной связью, стохастические системы, независимые динамические системы, физиологию, в частности, физиологию нервной системы. Большую роль в кибернетике играют «контроллеры», которые могут быть мозгом человека, получающим сигналы от «монитора». Информация, отправленная монитором контроллеру, называется обратной связью, и на основании этой обратной связи контроллер может выдавать инструкции, чтобы приблизить наблюдаемое поведение к желаемому [4]. Некоторые из самых ранних работ, выполненных в кибернетике, это изучение правил контроля, с помощью которых происходит человеческое действие, с целью создания искусственных конечностей, связанных с мозгом [5].

В последующие годы компьютер и связанные с ним области математики (например, математическая логика) оказали большое влияние на развитие кибернетики по той простой причине, что компьютеры могут использоваться не только для автоматического расчета, но и для всех преобразований информации, включая различные типы обработки информации, используемые в системах управления [6]. Эта улучшенная способность компьютеров сделала возможным два разных взгляда на кибернетику. Более узкий взгляд, распространенный в западных странах, определяет кибернетику как науку об управлении сложными системами различных типов – техническими, биологическими или социальными. Во многих западных странах особое внимание уделяется аспектам кибернетики, используемой при создании систем управления в технологии и живых организмах. Более широкий взгляд на кибернетику возник в России и других советских республиках и преобладал там на протяжении многих лет. Таким образом, информатика, считающаяся отдельной дисциплиной на Западе, включена как одна из составных частей кибернетики.

Значительную роль в искусственном интеллекте и кибернетике играют искусственные нейронные сети. Это вычислительные системы, созданные по образу и подобию биологических нейронных сетей, которые составляют нервную систему человека. Сама нейронная сеть не является алгоритмом, а скорее является основой многих различных алгоритмов машинного обучения для совместной работы и обработки сложных данных. Вся нейронная система, достигая цели, обычно не использует программирование конкретных задач. К примеру, для распознавания объектов они учатся идентифицировать изображения с нужным им объектом через анализирование различных картин, которые помечены, присутствует ли данный предмет или нет. Изучив объект, они могут безошибочно сообщать находиться ли нужный объект, при этом не имея предварительных знаний. Учебный материал помогает им генерировать идентифицирующие свойства.

Сами нейронные сети созданы благодаря связанным узлам – искусственным нейронам. Именно они моделируют нейроны в нервной системе живых существ. Алгоритм работы нейронных сетей заключается в том, что соединения (синапсы) передают сигнал от нейрона к нейрону, которые обрабатываются, и формируются в выходящий сигнал (рис.1).

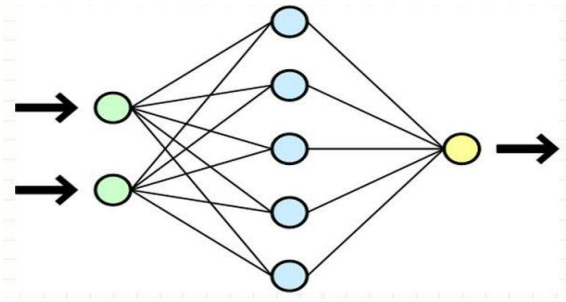

Рис.1. Схема простой нейросети

Первоначальной целью подхода к нейронным сетям было решение проблем таким же способом, как их решает мозг человека. Однако со временем внимание перешло к выполнению конкретных задач, что привело к отклонениям от биологии. В настоящее время искусственные нейронные сети используются по целому ряду задач, включая компьютерное зрение, распознавание речи, машинный перевод, фильтрацию социальных сетей, игровые доски и видеоигры и медицинскую диагностику [8].

Кибернетика в чистом виде изучает системы управления, чтобы понять основные принципы, которые лежат в основе таких вещей как: искусственный интеллект, робототехника, компьютерное зрение; системы управления; новая кибернетика; теория диалога. Ее участие в биологии также играет значительную роль. Она изучает кибернетические системы, присутствующие в процессах организмов. Во-первых, все внимание сосредоточено на то, как живые организмы адаптируются к своему местообитанию и как генетическая информация передается из поколения в поколение. Также данное направление присутствует в таких сферах, как компьютерные технологии (робототехника, моделирование), инженерия (эргономика, адаптивные системы), менеджмент (предпринимательская кибернетика, организационная кибернетика), математика (динамически системы, информационные системы), психология (системная психология, психокибернетика), социология (меметика, социокибернетика).

В наши дни кибернетика является очень востребованной. Одним из последних изобретений HRP-4C является черноволосая кибернетическая модель. Она оснащена тридцатью моторами, помогающими кибермодели двигать руками, ходить, а еще восемь моторов отвечают за эмоции: гнев, удивление и так далее. Также существует робот, который еще не до конца доработан. Он способен разговаривать, а самое интересное в этом то, что рот двигается, подражая речи человека.

Таким образом, исследования в кибернетике проводятся уже на протяжении многих лет и приносят прекрасные результаты. Она безусловно занимает одно из главных мест в претенденты наук будущего. Даже несмотря на захватывающие перспективы для науки, промышленности и экономики, трудно предсказать достижения, которые кибернетика может сделать в будущем. Прогресс в техническом прогрессе является результатом, прежде всего таланта, изобретательности и усилий человека - этого великого регенератора и мастера природы.

Библиографический список

1. Шакиров А.А. Технологии больших данных в области информационной безопасности / А.А. Шакиров, Р.С. Зарипова / International Journal of Advanced Studies in Computer Engineering. – 2018. –№2. –С.74-77.

2. Пырнова О.А. Технологии искусственного интеллекта в образовании / О.А. Пырнова, Р.С. Зарипова / Russian Journal of Education and Psychology. – 2019. – Т. 10. – №3. – С. 41-44.

3. Пырнова О.А. Искусственный интеллект в камерах смартфонов / О.А. Пырнова, Р.С. Зарипова / Информационные технологии в строительных, социальных и экономических системах. – 2019. – № 1 (15). – С. 82-84.

4. Хайруллин А.М. Обучение будущих инженеров робототехнике – вложение в конкурентоспособность страны / А.М. Хайруллин, Р.С. Зарипова / Сборник статей XX Всероссийской студенческой научно - практической конференции Нижневартовского государственного университета. – 2018. – С.141-142.

5. Пырнова О.А. Применение робототехники в медицине / О.А. Пырнова, Р.С. За-

рипова / Сборник статей XX Всероссийской студенческой научно - практической конференции Нижневартовского государственного университета. – 2018. – С. 384-386.

6. Шакиров А.А. Обучение компьютерному моделированию с использованием интерактивных сред / А.А. Шакиров, Р.С. Зарипова / International Journal of Advanced Studies in Education and Sociology. –2019. – № 1. – С. 56-59.

7. Байнов А.М. Робототехника и компьютерное моделирование: задачи и перспективы применения / А.М. Байнов, Р.С. Зарипова / International Journal of Advanced Studies in Computer Engineering. – 2018. – № 2. – С. 4-7.

8. Антипова Т.С. Компьютерное моделирование цифровых приборов / Т.С. Антипова, Р.С. Зарипова / Состояние и перспективы развития ИТ - образования: Сборник докладов и научных статей Всероссийской научно - практической конференции. – Чебоксары, 2018. – С. 193-198.

9. Зарипова Р.С. Использование сред схемотехнического проектирования и машиностроительных САПР для моделирования виртуальных прототипов приборов / Р.С. Зарипова, А.А. Шакиров / International Journal of Advanced Studies. – 2018. – Т. 8. – № 4-2. – С. 29-32.

10. Зарипова Р.С. Особенности и тенденции развития современного инженерного образования / Р.С. Зарипова, О.А. Пырнова / Современные исследования социальных проблем. – Красноярск: Научно - Инновационный Центр, 2018. – Т.9. – №8-2. – С.43-46.

УДК 681.3:516.8

Воронежский государственный университет
Канд. техн. наук, доцент Н.Г. Аснина
E-mail: andrey050569@yandex.ru
Студентка факультета ПММ Т.В. Еремина
E-mail: eremina.tanya1995@yandex.ru
Россия, г. Воронеж

Voronezh State University
Ph. D. in Engineering, associate professor N.G. Asnina
E-mail: andrey050569@yandex.ru
Student of the faculty PMM T.V. Eremina
E-mail: eremina.tanya1995@yandex.ru
Russia, Voronezh

Н.Г. Аснина, Т.В. Еремина

РАЗРАБОТКА ФУНКЦИОНАЛЬНЫХ МОДЕЛЕЙ ПРОЦЕДУРЫ ПРОВЕРКИ ОБВИНИТЕЛЬНОГО ЗАКЛЮЧЕНИЯ ПРОКУРОРОМ

Аннотация: В статье предпринята попытка визуализации процедуры проверки обвинительного заключения на основе функциональных моделей ARIS и сетей Петри

Ключевые слова: функциональное моделирование, модели ARIS, сети Петри

N.G. Asnina, T.V. Eremin

DEVELOPMENT OF FUNCTIONAL MODELS OF THE PROCEDURE FOR CHECKING A CHARGE CONCLUSION BY THE PROSECUTOR

Abstract: The article attempts to visualize the procedure for verifying the indictment based on functional models of ARIS and Petri nets

Keywords: functional modeling, ARIS models, Petri nets

Уголовное дело – это дело, возбуждаемое в установленном законом порядке в каждом случае обнаружения признаков преступления.

«Обвинительное заключение - это завершающий предварительное следствие процессуальный документ, содержащий сформулированное по делу обвинение, определяющее пределы судебного разбирательства, а также систему и анализ доказательств и фокусирующее процессуальное решение компетентных органов и должностных лиц о возможности направления уголовного дела в суд для рассмотрения его по

© Аснина Н.Г., Еремина Т.В., 2019

УДК 004: 378

Казанский государственный энергетический университет
Студентка Э.Р. Галиуллина, E-mail: zarim@rambler.ru
Канд. техн. наук, доцент Р.С. Зарипова, тел.: 8(843) 519-43-26
Россия, г. Казань

Kazan State Power Engineering University
Student E.R. Galiullina, E-mail: zarim@rambler.ru
Cand. tech. Sci., Assoc. R.S. Zaripova, Ph.: 8(843) 519-43-26
Russia, Kazan

Э.Р. Галиуллина, Р.С. Зарипова

ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ ДЛЯ ВИРТУАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ

Аннотация: В данной работе дается обзор наиболее важных проблем кибербезопасности, имеющих отношение к системам высшего образования и будущим распределенным системам электронного обучения. Охвачены основные разделы: кибербезопасность и образование; угрозы безопасности, обнаружение и защита в распределенных системах электронного обучения; разработка модели управления безопасностью для систем электронного обучения; и представлены некоторые выводы

Ключевые слова: образовательная среда**,** электронное обучение, высшее учебное заведение, кибербезопасность, электронные системы, информация

E.R. Galiullina, R.S. Zaripova

CYBER SECURITY PROBLEMS FOR VIRTUAL EDUCATIONAL ENVIRONMENT

Annotation: This paper gives an overview of the most important cybersecurity issues related to higher education systems and future distributed e-learning systems. The main sections are covered: cybersecurity and education; security threats, detection and protection in distributed e-learning systems; development of a security management model for e-learning systems; and some conclusions are presented

Keywords: educational environment, e-learning, higher education institution, cybersecurity, electronic systems, information

Системы электронного обучения являются сложными системами, направленными на обеспечение потребностей учащихся и поддерживать хороший имидж учебного процесса. Имеются четкие доказательства того, что инновационные образовательные технологии, такие как электронное обучение, предоставляют беспрецедентные возможности для студентов, слушателей и преподавателей получать, развивать и поддерживать основные навыки и знания [1]. Однако системы электронного обучения используют Интернет как место для получения всей необходимой информации и знаний. К сожалению, Интернет также стал местом проведения новомодной незаконной деятельности, так называемой киберпреступности. Информация, связанная с электронной средой обучения, часть которой может носить личный, защищенный или конфиденциальный характер, постоянно подвергающаяся угрозами безопасности, поскольку системы электронного обучения являются открытыми, распределенными и взаимосвязанными.

За последние годы электронное обучение получило впечатляющее развитие. Системы электронного обучения разнообразны и широко распространены, например,

© Галиуллина Э.Р., Зарипова Р.С., 2019

WebCT, Moodle и Blackboard. Они большие и динамичные с различными пользовательскими надстройками и ресурсами. Обмен информацией, сотрудничество и взаимодействие являются основными элементами любой системы электронного обучения [2]. Из этого следует, что все данные должны быть защищены для обеспечения конфиденциальности, целостности и доступности. Защита от манипулирования данными, мошеннической аутентификации пользователей и компромиссов в конфиденциальности является важным вопросом безопасности в электронном обучении. В то же время тенденции в области электронного обучения требуют повышения уровня совместимости приложений, учебных сред и гетерогенных систем.

Системы электронного обучения имеют те же характеристики и проблемы, что и другие электронные услуги, требующие обмена и распространения информации. Более конкретно, они связаны с доступностью услуг через Интернет, потреблением услуг человеком через Интернет и оплатой услуг клиентом. Организации должны уделять больше внимания управлению рисками безопасности, принимая во внимание тип и серьезность различных угроз и уязвимостей, а также признавая разнообразное взаимодействие и интеграцию между клиентами, серверами, базами данных и другими компонентами.

Электронные системы уязвимы перед рядом угроз: серьезные угрозы безопасности включают программные атаки (вирусы, черви, макросы, отказ в обслуживании), шпионаж, акты кражи (незаконное оборудование или информация) и интеллектуальную собственность (пиратство, нарушение авторских прав). Системы электронного обучения имеют некоторые особенности, имея множество пользователей, множество приложений и информации для загрузки и выгрузки.

Электронные системы уязвимы для целого ряда угроз безопасности:

• аутентификация – нарушенная аутентификация и управление сеансами;

• доступность – отказ в обслуживании;

• конфиденциальность – небезопасное криптографическое хранилище; небезопасная прямая ссылка на объект; утечка информации;

• целостность - переполнение буфера; подделка межсайтовых запросов; межсайтовый скриптинг; невозможность ограничить доступ к URL.

Угроза определяется как категория объекта, человека или других объектов, представляющих опасность, таких как трояны или фишинг. Схемы, включающие аутентификацию пользователей на основе паролей, очень чувствительны к фишинговым атакам, которые становятся все более изощренными и требуют решительных профилактических и контрмер.

Высшие учебные заведения должны применять корпоративные подходы к управлению рисками информационной безопасности в рамках существующих структур управления [3]. Учреждения должны идентифицировать «контроли» данных, чтобы установить четкие линии информации в учреждении, которое безопасно распространяет информацию в распределенной среде. Реализация управления кибербезопасностью требует соответствующего уровня понимания угроз, стоящих перед университетом, и мер, которые были приняты. Это потребует повседневной ответственности за надлежащую оценку, управление и отчетность по рискам. Руководители учреждений, весь академический персонал и ИТ-группа в высшем учебном заведении должны быть в курсе информации об их обязанностях и предупреждать о возникающих угрозах и рисках для пользователей данных.

Все высшие учебные заведения должны осознавать свои обязанности в отноше-

нии защиты институциональных и исследовательских данных и иметь соответствующие меры для обеспечения их соответствия Федеральному закону «О персональных данных» (2006). Большинство высших учебных заведений будут иметь различные структуры для управления данными и исследованиями, а также соответствующие уровни контроля. У большинства из этих учреждений и исследователей будет различная политика и планы по управлению данными, и при этом очень мало будет проблем с ошибками. Эти функции представляют собой проблему для корпоративного управления, чтобы понять, как проблемы, так и необходимость модели процессов угроз кибербезопасности сотрудников.

В конце концов, безопасность сети – это ответственность всего учреждения. Сетевые администраторы могут постоянно получать информацию об угрозах и мерах противодействия путем обмена информацией с коллегами и другими руководствующими структурами. Более важны пользователи, для которых они имеют решающее значение для безопасности любой сети и информации. Они должны играть центральную роль в оценке риска, с которым сталкиваются информация, приоритеты безопасности и, наконец, как пользователи, они несут ответственность за реализацию мер контроля.

Потребность в электронном обучении изменила способ, которым Высшее образование ведет повседневную деятельность, проявляя все большую активность в создании или поиске новых услуг, которые могут позволить студентам учиться в виртуальной среде. Повышенная потребность в мобильности и расширении возможностей электронного обучения представляет собой серьезную проблему для ИТ-отделов высшего образования, которым все труднее поддерживать контроль над тем, как данные используются, хранятся и совместно используются внутри и за пределами стен университета. Понимание потребностей пользователей и внедрение новых услуг требует создания безопасных, стандартизированных, высокодоступных сред электронного обучения, а также централизованного управления приложениями.

Библиографический список

1. Зарипова Р.С. Особенности и тенденции развития современного инженерного образования / Р.С. Зарипова, О.А. Пырнова / Современные исследования социальных проблем. – Красноярск: Научно - Инновационный Центр, 2018. – Т.9. – №8-2. – С.43-46.

2. Кривоногова А.Е. Современные информационные технологии и их применение в сфере образования / А.Е. Кривоногова, Р.С. Зарипова / Russian Journal of Education and Psychology. – 2019. –Т. 10. – №5. – С. 44-47.

3. Ширмамедова З.Н. Роль открытых электронных образовательных ресурсов в современном информационно - образовательном пространстве / З.Н. Ширмамедова, Р.С. Зарипова / Учёные записки ИСГЗ. – 2019. – Т.17. – №1. – С.536-539.

4. Галиуллина Э.Р. Образовательные цифровые игры как способ обучения студентов / Э.Р. Галиуллина, Р.С. Зарипова / International Journal of Advanced Studies in Education and Sociology. – 2019. – № 1. – С. 9-13.

5. Шакиров А.А. Технологии больших данных в области информационной безопасности / А.А. Шакиров, Р.С. Зарипова / International Journal of Advanced Studies in Computer Engineering. –2018. –№2. –С. 74-77.

6. Пырнова О.А. Интернет как средство обучения / О.А. Пырнова, Р.С. Зарипова / International Journal of Advanced Studies in Education and Sociology. – 2018. – № 2. – С. 41-44.

УДК 004

Казанский государственный энергетический университет
Студент А.А. Шакиров, тел.: 8 (843) 519-42-63
Канд. техн. наук, доцент Р.С. Зарипова, E-mail: zarim@rambler.ru
Россия, г. Казань

Kazan state power engineering University
Student A.A. Shakirov, Ph.: 8 (843) 519-42-63
Cand. tech. Sciences, associate Professor R.S. Zaripova,
E-mail: zarim@rambler.ru, Russia, Kazan

А.А. Шакиров, Р.С. Зарипова

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БОЛЬШИХ ДАННЫХ

Аннотация: На сегодняшний день во многих сферах общественной жизни набирает популярность такое понятие, как «большие данные» или же «Big data». Эта технология необходима для управления и анализа огромного количества различных данных. В статье рассмотрен вопрос, почему в настоящее время так важно хранить огромный массив данных и обеспечивать его целостность

Ключевые слова: большие данные, Big data, массив данных, система больших данных

A.A. Shakirov, R.S. Zaripova

PROBLEMS OF ENSURING INFORMATION SECURITY OF BIG DATA

Abstract: Today, in many areas of public life, such a notion as “big database data” or “Big data” is gaining popularity. This technology is needed to manage and analyze a huge amount of different data. The article discusses the question of why it is now so important to store a huge array of data

Keywords: big data, Big data, data array, big data system

Ни для кого не секрет, что существование и рост большого массива данных влечет за собой последствия в виде отсутствия необходимой инфраструктуры, которая помогала бы охранять собранные массивы данных в надлежащем виде. Отсутствие необходимой инфраструктуры для хранения «больших данных» создает проблему в сфере информационной безопасности, главными аспектами которого являются целостность информации, ее конфиденциальность и доступность [1].

Почему в наше время так важно хранить огромный массив данных? На этот вопрос можно ответить несколькими примерами из реальной жизни, в которых объясняется ценность данных и необходимость защиты их конфиденциальности и целостности.

Приведем пример из медицины. Представим ситуацию, когда врач должен поставить своему пациенту точный диагноз, но он колеблется между двумя диагнозами в связи с полученными результатами анализов своего пациента. Для того чтобы определиться с выбором он опирается не только на результаты анализов и историю болезни больного, но и извлекает информацию из опытов других врачей или из достоверных источников об экологическом состоянии района проживания своего пациента. Проанализировав полученные данные, врач легко сможет дать точный диагноз.

Второй пример приведем из сферы торговли. Допустим, человек принял решение открыть свою торговую точку, но для этого он должен выбрать правильное местоположение, где всегда будет наличие огромного потока людей. Для того, чтобы определиться с местом открытия торговой точки можно обратиться к существующему массиву данных и посмотреть наличие локаций с мощным потоком людей.

Очевидно, что технология big data необходима для каждой сферы общественной жизни. Но как же обезопасить огромный объем данных и не нарушить целостность и конфиденциальность информационной безопасности? Уязвимость информационной безопасности возникает вследствие утечки данных, многообразия источников данных, их форматов, а также вследствие потоковой природы сбора данных и передачи этих данных между распределенными облачными инфраструктурами [2]. Если вовремя не за-

© Шакиров А.А., Зарипова Р.С., 2019

думаться над проблемой обеспечения безопасности информации, можно ожидать в будущем увеличения утечки информации на порядок выше, чем было ранее.

На сегодняшний день еще не существует какого-то универсального и эффективного метода по обеспечению защиты огромного массива данных. На данном этапе разработана новая методология, затрагивающая вопросы информационной безопасности [3]. Эта методология представляет собой систему больших данных, состоящих из пяти логических функциональных компонентов, связанных интерфейсами функциональной совместимости:

1) интерфейс, позволяющий взаимодействовать провайдеру данных и провайдеру приложений: одна из свойств системы больших данных – это введение и применение различных данных из разнообразных источников, как внутренних, так и внешних. Исходя из этого, все введенные данные должны проверяться на целостность и отсутствие факторов, наносящих вред системе;

2) интерфейс взаимодействия провайдера приложений и потребителей данных: потребителями больших данных являются пользователи или иные системы, осуществляющие поиск данных, их анализ или визуализацию операций данных [4]. Необходимо защитить интерфейсы доступа пользователей к информации и предоставить полную конфиденциальность данных в соответствии с законодательством;

3) интерфейс взаимодействия провайдера приложений и платформы работы с большими данными: площадь с огромным количеством данным может иметь запутанную и сложную структуру, состоящую из различных уровней и очень часто используются различные технологические подходы к хранению собранной информации [5]. Необходимо создать такой уровень контроля доступа, который смог бы гарантировать доступ к данным, согласованным с правилами разграничения доступа;

4) защита данных при внутреннем взаимодействии различных технологий и платформ больших данных. Гарантия защиты платформы больших данных – это сложный процесс. Нужно обеспечить безопасность систем, программ, защиту собранной информации методами систем управления базами данных (СУБД). Должна обеспечиваться также защита данных и журналов транзакций, а для контроля доступа и отслеживания ключей нужно предусмотреть управление ключами;

5) защита средств управления системой больших данных. Методы регулирования системой больших данных предоставляют большие возможности внедрению механизмов безопасности, при помощи которых можно наблюдать за состоянием элементов, управлением правилами разграничения доступа, идентификацией источников данных и т.д.

Но сами методы регулирования такой системы тоже нуждаются в защите, так как они являются особенной ценностью для нарушителя.

Исходя из всего вышесказанного, становится ясно то, что технологии больших данных в области информационной безопасности представляют собой сложную, состоящую из многих уровней структуру, которая необходима всем сферам общественной жизни и поэтому требует защиты от внешних и внутренних угроз, которые вредят главным аспектам информационной безопасности: целостности, конфиденциальности и доступности.

Библиографический список

1. Шакиров А.А. Технологии больших данных в области информационной безопасности / А.А. Шакиров, Р.С. Зарипова Р.С. / International Journal of Advanced Studies in Computer Engineering. – 2018. – № 2. – С. 74-77.

2. Шакиров А.А. Актуальность обеспечения информационной безопасности в условиях цифровой экономики / Шакиров А.А., Зарипова Р.С. / Инновационное развитие экономики. Будущее России: Сборник материалов и докладов V Всероссийской

УДК 004

Казанский государственный энергетический университет
Студент Э.Р. Галиуллина, тел.: 7 (843) 519-42-02
Студент А.А. Шакиров, тел.: 7 (843) 519-42-63
Канд. техн. наук, доцент Р.С. Зарипова, E-mail: zarim@rambler.ru
Россия, г. Казань

Kazan state power engineering University
Student E.R. Galiullina , Ph.: 7 (843) 519-42-02
Student A.A. Shakirov, Ph.: 7 (843) 519-42-63
Cand. tech. Sciences, associate Professor R.S. Zaripova,
E-mail: zarim@rambler.ru, Russia, Kazan

Э.Р. Галиуллина, А.А. Шакиров, Р.С. Зарипова

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ФИНАНСОВЫХ ТРАНЗАКЦИЯХ ЧЕРЕЗ МОБИЛЬНЫЙ ТЕЛЕФОН: АЛГОРИТМЫ

Аннотация: Сегодня мобильная коммерция рассматривается многими компаниями, бизнесом и организациями. В мобильной коммерции информационная безопасность финансовых транзакций очень важна. Это происходит из-за обмена информацией об учетной записи, включая номер счета, пароль, кредитные счета и т. д., а раскрытие этой информации повлечет за собой большие финансовые и моральные потери. По этой причине следует использовать алгоритмы для их совершения и увеличения защищенности транзакций. Среди этих алгоритмов приложения WAP, J2ME, Toolkit SIM идентифицированы и описаны в этой статье на основе систематического обзора. Кроме того, есть несколько рекомендаций относительно соответствия различным ситуациям для реализации конкретного алгоритма для этой проблемы. Более подробные результаты впоследствии объясняются в этой статье

Ключевые слова: мобильная коммерция, информационная безопасность, финансовый обмен, транзакция, электронная коммерция

E.R. Galiullina, A.A. Shakirov, R.S. Zaripova

INFORMATION SECURITY IN FINANCIAL TRANSACTIONS VIA MOBILE PHONE: ALGORITHMS

Abstract: Today, mobile commerce is considered by many companies, businesses and organizations. In mobile commerce, information security of financial transactions is very important. This is due to the exchange of information about the account, including account number, password, credit accounts, etc. and the disclosure of this information will entail great financial and moral losses. For this reason, algorithms should be used to complete them and increase transaction security. Among these algorithms, WAP, J2ME, Toolkit SIM applications are identified and described in this article based on a systematic review. In addition, there are several recommendations for matching various situations to implement a specific algorithm for this problem. More detailed results are subsequently explained in this article

Keywords: mobile commerce, information security, financial exchange, transaction, electronic commerce

В современном мире мобильная коммерция обсуждается как один из наиболее важных вопросов в деловых организациях и компаниях. Мобильная коммерция – это любая транзакция, в которой финансовый обмен осуществляется через сети мобильной связи. Согласно этому определению, мобильная коммерция представляет собой подмножество всей электронной коммерции, включая как бизнес для потребителя, так и бизнес для бизнеса. Мобильная коммерция использует Интернет для покупки товаров и услуг, а также для отправки и получения сообщений с помощью портативных беспроводных устройств. Мобильная коммерция может быть определена, например: любая электронная транзакция или информационное взаимодействие, проводимое с использованием мобильного устройства и мобильных сетей, которое приводит к передаче реальной или предполагаемой ценности в обмен на информацию, услуги или товары [1-3]. Мобильная коммерция предлагает потребителям удобство и гибкость мобильных услуг в любое время и в любом месте. Мобильная коммерция известна как мобильная электронная коммерция или беспроводная электронная коммерция.

Беспроводная связь является более сложной и опасной, чем проводная связь по многим причинам, включая маршруты передачи сигналов и взаимодействие с окружающей средой, звуками и возможным незаконным прослушиванием телефонных разго-

© Галиуллина Э.Р., Шакиров А.А., Зарипова Р.С., 2019

воров из-за использования радиоволн. Эти проблемы приводят к меньшей пропускной способности, более высокой частоте появления ошибок и повторной неисправности, поэтому качество беспроводной линии связи ниже, чем для проводного соединения. Следовательно, многие компании и организации не желают применять мобильную коммерцию.

Инфраструктуры открытых ключей основаны на криптографии с открытыми ключами, в которой используются два ключа: закрытый ключ, который хранится в секрете, и открытый ключ, который можно разглашать публично. Интересным свойством этой пары ключей является то, что для расшифровки сообщений, зашифрованных одним, нужен другой. Самый популярный алгоритм криптографии с открытым ключом является RSA. Алгоритм эллиптической криптографии начинает получать признание в мобильных устройствах. Они полагаются на различные математические свойства, которые позволяют использовать более короткие ключи, которые обеспечивают более быстрые вычисления, более низкое энергопотребление, меньшие требования к памяти и пропускной способности и, следовательно, довольно привлекательны для мобильных устройств.

Цифровые подписи могут гарантировать подлинность сторон транзакции, целостность и неоспоримость передач. Цифровая подпись создается, когда передаваемый документ шифруется с использованием закрытого ключа. Процесс шифрования документа с использованием закрытого ключа аутентифицирует документ, поскольку документ мог быть зашифрован только с использованием закрытого ключа владельца. Получатели могут проверить подпись, расшифровав с помощью открытого ключа. В реальном мире документы не полностью зашифрованы, чтобы сэкономить время. В таких случаях используются односторонние хэш-функции. Хэш использует одностороннюю математическую функцию для преобразования данных в дайджест фиксированной длины, называемый хэшем, который впоследствии шифруется. Проверка подписи включает воспроизведение хэша, сгенерированного из полученного сообщения, и сравнение его с расшифрованным оригинальным хэшем.

Цифровые подписи не являются достаточными средствами для автоматической проверки, поскольку даже если подпись может быть проверена. Нет гарантии того, что лицо, сделавшее подпись, является тем, кем он себя считает. Сертификаты открытого ключа являются мощным средством установления доверия к криптографии с открытым ключом. Сертификат – это чей-то открытый ключ, подписанный и упакованный для использования в инфраструктуре открытого ключа. Как правило, сертификат содержит следующие три элемента информации: имя субъекта, для которого выдан сертификат; открытый ключ, связанный с этим субъектом, и цифровая подпись, подписанная эмитентом сертификата. Цифровая подпись будет проверять информацию о сертификате и, если проверка прошла успешно, то гарантируется, что открытый ключ в сертификате действительно принадлежит объекту, к которому относится сертификат.

Рассматриваемые функциональные области, связанные с безопасностью в WAP, включают в себя безопасность беспроводного транспортного уровня (WTLS), модуль беспроводной идентификации, инфраструктуру открытого ключа WAP, текстовую подпись сценария WML и сквозную безопасность транспортного уровня. Протокол WTLS (Wireless Transport Layer Security) – это протокол безопасности с поддержкой PKI, разработанный для защиты связи и транзакций по беспроводным сетям. Протокол WTLS, такой как SSL, является одним из

способов защиты WAP-соединения. Он используется с транспортными протоколами WAP для обеспечения безопасности на транспортном уровне между клиентом WAP в мобильном устройстве и WAP-сервером в WAP-шлюзе.

По большей части разработчики WAP используют стандартные протоколы, и широко на всех уровнях в WAP 2.0, из-за нестандартного стека протоколов WAP 1.0. Поскольку WAP основан на IP, на сетевом уровне поддерживается полностью IPsec, а транспортный уровень защищает TCP-соединение с использованием TLS. На верхнем уровне поддерживается HTTP-метод аутентификации. На прикладном уровне имеется система библиотек для шифрования, где размещены средства для точного контроля и неоспоримого сообщения разработчикам WAP. Поскольку WAP 2.0 основан на общепризнанных стандартах, то существует большая вероятность того, что его службы безопасности будут лучше и безопаснее, чем 802.11 и Bluetooth, особенно для служб аутентификации, целостности и конфиденциальности сообщений.

Модуль идентификации абонента GSM (глобальная система мобильной связи), который хранит личные данные абонента, может быть реализован в виде смарт-карты, называемой SIM-картой. SIM-инструментарий – это спецификация SIM-карты и функциональных возможностей терминала, которые позволяют SIM-карте управлять мобильным терминалом для определенных функций. Инструментарий приложения SIM (SAT) используется для создания приложений мобильных платежей на основе службы коротких сообщений (SMS). В системах на основе инструментария SIM-приложения связь между мобильным клиентом и сервером платежей осуществляется с помощью SMS. SMS используется для инициирования и авторизации платежей. Пользователь идентифицируется и аутентифицируется службой аутентификации GSM, и, следовательно, оператор мобильной сети GSM действует как посредник между мобильным клиентом, сервером платежей и продавцом.

Основными преимуществами использования платформы J2ME являются возможность обеспечения динамического контента и информационной безопасности. Кроме того это мощный, объектно-ориентированный язык программирования с большой базой разработчиков. Информационные устройства и другие портативные устройства интегрированы с аудио, мультимедиа, возможностью подключения и услугами, доступными на одной платформе. Растущая и динамичная вычислительная мощность на этих устройствах позволит разработчикам услуг с высокой добавленной стоимостью. Например, местные информационные службы, позволяющие пассажирам подключаться к Интернету с помощью мобильного телефона и получать доступ к необходимой информации, в том числе местонахождению ближайшего отеля, планам и расписанию [4-6]. Одним из приложений мобильной коммерции является использование мобильных платежей на заправке. Успехи этих приложений требуют высокого уровня надежности и безопасности. Мобильные устройства содержат цифровой идентификатор и из-за этого должен быть способ аутентификации пользователей и обеспечения надежности системы. Обеспечение безопасного доступа к данным абсолютно необходимо в мобильной сети. Оно снижает уровень мошенничества в мобильных платежных системах. Современные практики в платформе J2ME основаны на услугах, предоставляемых в защищенной смарт-карте или аналогичном устройстве, для создания доверия и уверенности в том, что безопасное хранение ключей и криптографических операций и вычислений. Чтобы завершить безопасную транзакцию, прода-

вец должен проверить, авторизованы ли беспроводные подписчики или нет. После этого продавец должен отправить квитанцию подписчику.

По преимуществам и недостаткам введенных алгоритмов и исследований, проведенных в этой области, сделан вывод о том, какие алгоритмы используются в мобильных приложениях, связанных с финансами. Платформа J2ME была бы более подходящей по следующим причинам: выполняется с мобильным обменом, возникают проблемы, включая прослушивание, манипулирование сообщением, генерирование поддельных сообщений и прерывание. Поэтому чтобы избежать этих проблем, необходимы следующие процедуры: аутентификация, конфиденциальность, точность мониторинга и любой способ был бы уместен, который обеспечивает эти четыре решения, а также применим в программах Java из-за достижений в технологии и важности сохранения конфиденциальности информации. В общей сложности платформа J2ME используется для удовлетворения потребностей информационных систем в соответствии с Java software environment. Она предоставляет эти четыре способа. И еще одним преимуществом является то, что эти сервисы могут постоянно обновляться с новыми или улучшенными приложениями, установленными на смарт-карте.

Библиографический список

1. Шакиров А.А. Трансформация систем учета и контроля в условиях цифровой экономики / А.А. Шакиров, Р.С. Зарипова / Наука Красноярья. 2019. – Т. 8. – № 3-2. – С. 112-115.

2. Антипова Т.С. Глобализация и глобальные проблемы в мировой экономике / Т.С. Антипова, А.Р. Залилов, Р.С. Зарипова / «Экономика сегодня: современное состояние и перспективы развития (Вектор-2018)»: Сборник материалов Всероссийской научной конференции молодых исследователей. – Мин-во образования и науки РФ; Росс. гос. ун-т им. А.Н. Косыгина. – 2018. – С. 324-325.

3. Шакиров А.А. Современные информационные технологии как инструмент автоматизации бухгалтерского учета / А.А. Шакиров, Р.С. Зарипова / Наука Красноярья. – 2019. – Т. 8. – № 1-3. – С. 75-78.

4. Зарипова Р.С. Управление деятельностью организаций в условиях цифровой экономики / Р.С. Зарипова, О.А. Пырнова / Ученые записки ИСГЗ. – 2018. – Т. 16. – № 2. – С. 70-75.

5. Шакиров А.А. Роль новых технологий в экономике XXI века: угрозы и вызовы цифровой экономики / А.А. Шакиров, Р.С. Зарипова / «Экономика сегодня: современное состояние и перспективы развития (Вектор-2018)»: Сборник материалов Всероссийской научной конференции молодых исследователей. – Мин-во образования и науки РФ; Росс. гос. ун-т им. А.Н. Косыгина. – 2018. – С. 331-334.

6. Злыгостев Д.Д. Информационная безопасность как инструмент обеспечения экономической безопасности предприятий / Д.Д. Злыгостев, Р.С. Зарипова / Инновации в информационных технологиях, машиностроении и автотранспорте: Сборник материалов Международной научно-практической конференции. – Кемерово, 2017. – С. 23-25.

7. Шакиров А.А. Актуальность обеспечения информационной безопасности в условиях цифровой экономики / А.А. Шакиров, Р.С. Зарипова / Инновационное развитие экономики. Будущее России: Сборник материалов и докладов V Всероссийской (национальной) научно - практической конференции. – 2018. – С. 257-260.