**Министерство науки и высшего образования РФ**

**Алтайский государственный технический университет им. И. И. Ползунова**

**Научно-техническое предприятие Специальная электроника**

**Центр информационной безопасности**

**Кафедра информатики, вычислительной техники и информационной безопасности**

# ПРОГРАММНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

**Материалы Всероссийской молодежной научно-практической конференции 16 декабря 2020 г., г. Барнаул**

ISBN 978-5-7568-1348-7


**АлтГТУ**
**Барнаул ● 2021**

Об издании – 1, 2

УДК 658.512:004
П 784

Программно-техническое обеспечение автоматизированных систем : материалы Всероссийской молодежной научно-практической конференции (16 декабря 2020 г., г. Барнаул) / Алтайский государственный технический университет им. И. И. Ползунова ; под ред. А. Г. Якунина. – Барнаул : АлтГТУ, 2021. – 141 с. – URL : https://journal.altstu.ru/konf_2020/2021_1/77/. – Текст: электронный.

ISBN 978-5-7568-1348-7

***Ответственный редактор*** – Якунин А. Г., д. т. н., профессор.

В сборнике публикуются материалы Всероссийской молодежной научно-практической конференции «Программно-техническое обеспечение автоматизированных систем» (ПТОАС-2020) (доклады и/или их тезисы), проходившей в г. Барнауле в Алтайском государственном техническом университете 16 декабря 2020 года. В материалах рассмотрены вопросы проектирования, разработки и эксплуатации программно-аппаратных компонентов информационно-измерительных и управляющих систем, подходы к моделированию процессов обработки информации, пути совершенствования программно-технического обеспечения автоматизированных систем, включая технологии и методы защиты информации.

**Материалы публикуются в авторской редакции.**

***Научное издание***
**Материалы конференции**

Минимальные системные требования:
Yandex (20.12.1) или Google Chrome (87.0.4280.141) и т.п.,
скорость подключения - не менее 5 Мб/с, Adobe Reader и т.п.

Дата подписания к использованию 08.02.2021. Объем издания – 4 Мб.
Федеральное государственное образовательное учреждение высшего образования «Алтайский государственный технический университет им. И. И. Ползунова, 656038, г. Барнаул, пр-т Ленина, 46, https://www.altstu.ru.

ISBN 978-5-7568-1348-7

# РАЗДЕЛ 1. ОБЩИЕ ВОПРОСЫ РАСЧЕТА И ПРОЕКТИРОВАНИЯ ПРОГРАММНО-ТЕХНИЧЕСКИХ СРЕДСТВ ДЛЯ РЕШЕНИЯ ЗАДАЧ ИЗМЕРЕНИЯ, КОНТРОЛЯ И АВТОМАТИЗАЦИИ

**УДК 004.89**

## ИССЛЕДОВАНИЕ ПРОГРАММНЫХ ЭМУЛЯТОРОВ СЕТЕВОГО ОБОРУДОВАНИЯ

Е. Е. ИСТРАТОВА, Р. В. АВЕРЬЯНОВ, Н. А. ГАСЬКОВ

Применение программных эмуляторов сетевого оборудования на сегодняшний день достаточно распространено не только в учебном процессе, но и на практике при отработке отдельных моментов организации локальной или корпоративной сети. Благодаря точной передаче ключевых сетевых процессов, подобные программы позволяют имитировать реальные изменения сетевого трафика, выявлять ошибки при передаче данных и прогнозировать изменения пропускной способности сети [1, 2].

**Цель исследования** заключалась в проведении сравнительного анализа программных эмуляторов сетевого оборудования на примере проектирования реальной корпоративной сети.

Для реализации цели были выполнены следующие задачи:

– определение критериев сравнения;
– выбор оптимальных программных продуктов;
– проектирование корпоративной сети с использованием различных инструментов;
– сопоставление результатов.

Наиболее распространенными программными продуктами, используемыми для эмуляции сетевого оборудования, являются следующие:

– Cisco Packet Tracer;
– Graphical Network Simulator (GNS3);
– Virtual Internet Routing Lab (VIRL);
– Emulated Virtual Environment Next Generation (EVE-NG) [3].

Cisco Packet Tracer является проприетарным условно-бесплатным программным обеспечением, относящимся к классу симуляторов, так как обладает возможностями не только программной, но и аппаратной настройки. Данный инструмент включен в группу кроссплатформенного программного обеспечения, он позволяет производить тонкую настройку сетевого оборудования и подключать для симуляции различные сетевые устройства Cisco. К основному недостатку данного симулятора можно

отнести тот факт, что в нем не предусмотрена динамическая настройка сети.

Graphical Network Simulator является кроссплатформенным проектом с открытым исходным кодом и достаточно большим набором документации. Данный инструмент позволяет работать удаленно путем взаимодействия как с виртуальными машинами, так и с реально существующими сетями. К недостаткам данного программного обеспечения можно отнести снижение производительности при увеличении масштабов сети, а также необходимость скачивания и установки драйверов на сетевое оборудование Cisco.

Virtual Internet Routing Lab также является фирменным продуктом из линейки Cisco. Данный программный эмулятор сетевого оборудования не распространяется бесплатно, а предоставляется только по подписке. Его отличительной особенностью является наличие инструмента для настройки базовых устройств в сети, а также функции экспорта схемы сетевой топологии. Наряду со стоимостью, отсутствие возможности работы с последовательными интерфейсами и высокая ресурсоемкость являются сдерживающими факторами распространения данного вида эмуляторов.

Emulated Virtual Environment Next Generation — это кроссплатформенный проект, защищенный лицензией и распространяемый как в бесплатном, так и в платном виде. Отличительной особенностью данного эмулятора является поддержка многопользовательской работы. Это позволяет регистрировать топологию сети во время работы с ней, что дает экономию во времени при работе с узлами. Среди основных недостатков можно обозначить недостаточную и запутанную документацию.

Несмотря на ряд отличий в трендах развития отечественного и зарубежного рынков программного обеспечения, при сравнении программных эмуляторов сетевого оборудования в качестве исходных данных принимают во внимание две базовые метрики:

– наличие вакансий, в которых требуются навыки работы с данным программным обеспечением;

– количество скачиваний конкретного программного продукта в месяц.

Исходя из этого, именно данные метрики целесообразно использовать в качестве критериев при сопоставлении различных программных эмуляторов сетевого оборудования.

Количество вакансий, в которых требуются навыки работы с конкретным эмулятором, можно найти на международном сайте Indeed.com. Ресурс Indeed агрегирует данные разных сервисов по поиску работы по всему миру. Количество упоминаний того или иного программного эмулятора подсчитывается раз в год для того, чтобы понять, что необходимо

работодателям. Число скачиваний программных эмуляторов сетевого оборудования в месяц позволяет оценить их реальное использование. При этом установка пакета, как правило, означает его необходимость для рабочего процесса. Согласно собранным данным, лидерами по количеству скачиваний в первом полугодии 2020 года стали следующие программные продукты: Cisco Packet Tracer (38 %); Graphical Network Simulator (31 %); Emulated Virtual Environment Next Generation (22 %), менее востребованным оказался эмулятор сетевого оборудования Virtual Internet Routing Lab (9 %), что объясняется узкоспециализированной технической спецификой его применения.

При сопоставлении данных о востребованности и числу скачиваний программного обеспечения очевидно, что они подтверждают общую тенденцию отечественного рынка программного обеспечения, согласно которой наиболее распространенными и востребованными являются Cisco Packet Tracer и Graphical Network Simulator. Таким образом, дальнейшее сопоставление и выбор оптимального инструмента для эмуляции сетевого оборудования будет осуществляться на основании результатов сравнительного анализа данных программ.

В качестве задания для проектирования корпоративной сети была выбрана схема (рис. 1) и определен ряд процессов сети, которые необходимо было настроить для ее работоспособности. Для сопоставления результатов исследования фиксировались продолжительность и качество выполнения задания (рис. 2).

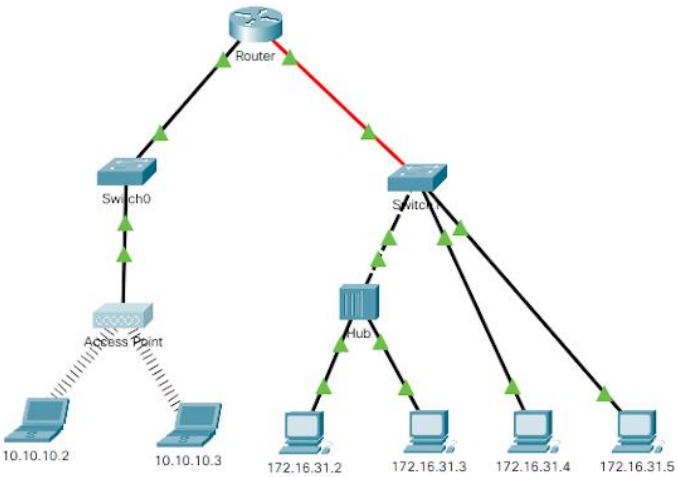



Рисунок 1 – Схема сети

На основе полученных результатов можно сделать вывод о том, что при примерно одинаковом качестве настройки сети (91 % и 92 %) Cisco Packet Tracer является интуитивно более понятным, что и объясняет меньшее значение времени, необходимого для выполнения задания. Таким образом, можно сделать вывод, что каждый из инструментов, несмотря на общее назначение, захватывает разные сферы работы с топологиями сетей и предоставляет различные возможности для работы. Исходя из этого, каждый из эмуляторов подходит для специалистов разных степеней подготовки, а также требует разных финансовых вложений. Поэтому выбирать один из данных эмуляторов стоит, исходя из целей и финансовых возможностей.

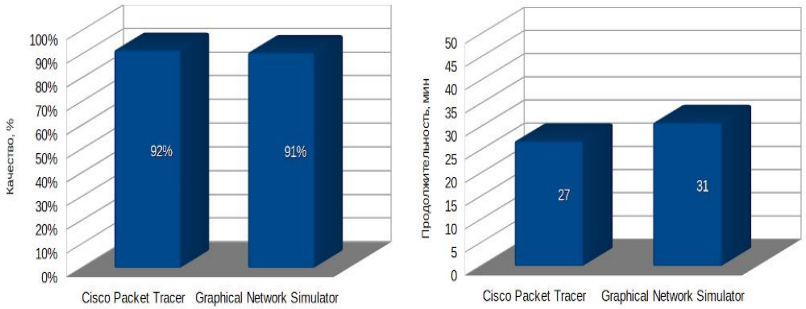



Рисунок 2 – Результаты сравнительного анализа программных эмуляторов сетевого оборудования

**Литература. 1.** Катунцов Е.В., Култан Я., Маховиков А.Б. Применение средств электронного обучения при подготовке специалистов в области информационных технологий / Е.В. Катунов и др. // Записки Горного института. 2017. №. URL: https://cyberleninka.ru/article/n/primenenie-sredstv-elektronnogo-obucheniya-pri-podgotovke-spetsialistov-v-oblasti-informatsionnyh-tehnologiy-dlya-predpriyatiy (дата обращения: 11.12.2020). **2.** Лапонина О.Р. Лабораторный стенд для тестирования возможностей интеграции ПКС-сетей и традиционных сетей / О.Р. Лапонина, М.Р. Сизова // International Journal of Open Information Technologies. 2017. № 9. URL: https://cyberleninka.ru/article/n/laboratornyy-stend-dlya-testirovaniya-vozmozhnostey-integratsii-pks-setey-i-traditsionnyh-setey (дата обращения: 11.12.2020). **3.** Павлов А.А. Проблемы использования средств тестирования многошаговых беспроводных сетей / А.А. Павлов, И.О. Датьев // Труды Кольского научного центра РАН. 2017. №3-8 (8). URL: https://cyberleninka.ru/article/n/problemy-ispolzovaniya-sredstv-testirovaniya-mnogoshagovyh-besprovodnyh-setey (дата обращения: 10.12.2020).

**Реквизиты для справок:** *Россия, 630073, Новосибирск, пр. К. Маркса, 20, Новосибирский государственный технический университет, кандидату технических наук, доценту кафедры автоматизированных систем управления, Истратовой Е.Е., тел. 8-952-921-86-29. E-mail: istratova@mail.ru.*

**УДК 629.331+004.6**

## ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ПОДСИСТЕМ СВЯЗИ АВТОМОБИЛЯ С ОКРУЖАЮЩЕЙ СРЕДОЙ

А. А. АРБУЗОВА, М. С. ЧЕРНОЯРОВА

Современные технологии все больше проникают в окружающий нас мир, постоянно меняя его [1]. Автомобилестроение как раз и является одной из таких областей. Современный автомобиль является не просто механической повозкой с двигателем, каким он был еще 50-60 лет назад. Сейчас это высокотехнологичное устройство со множеством датчиков и сенсоров. Эти приспособления берут на себя многие функции водителя, а в некоторых случаях полностью заменяют его.

Разумеется, взаимодействие между этими устройствами должно происходить на очень большой скорости, при этом объем передаваемой информации весьма значителен. Именно это обусловило использование в автономных автомобилях современных устройств связи, поддерживающих технологию 5G [2].

В целом современные системы связи, применяемые в автомобиле можно разделить на несколько групп [3]:

- для диагностики узлов и агрегатов автомобиля;
- для определения состояния и анализа поведения водителя;
- для определения местоположения транспортного средства;
- для взаимодействия с окружающей средой (технология V2X);
- для обеспечения связи водителя и пассажиров, мобильных устройств, доступ в сеть Интернет.

Статистика показывает, что общество уже не воспринимает автономные автомобили как нечто опасное или враждебное. Так, согласно данным аналитического агентства в сфере IT, McKinsey&Company, в 2018-2019 гг. количество автовладельцев из Германии, США и Китая, готовых сменить бренд автомобиля для улучшения возможностей подключения к глобальной мировой сети, возросло в 2 раза.

При этом необходимо отметить, что все перечисленные выше системы используют сотовую связь, и причем все чаще эта связь – 5G [4].

Наглядно применение 5G для управления движением иллюстрирует рисунок 1.

Сеть 5G сможет обеспечить все потребности современного беспилотного (или автономного) автомобиля. Это обусловлено целым рядом причин. Во-первых, это скорость передачи данных в пределах 10 Гбит – 100 Гбит, что превышает существующие сейчас показатели в десятки и сотни раз. Во-вторых, у данной сети высокая надежность сигнала, а стабильность передачи не будет зависеть от загруженности сети. Сеть выдерживает до одного миллиона соединений на 1 км$^2$.

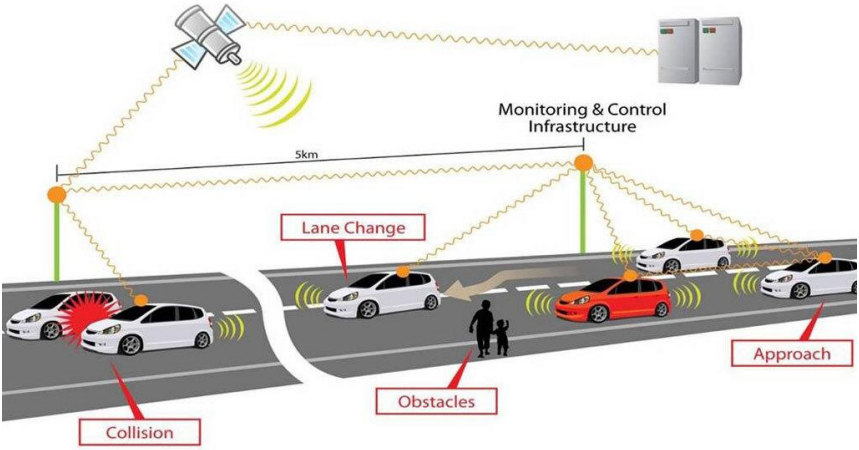



Рисунок 1 – Сеть 5G для управления движением автотранспорта

При отправке данных задержка сигнала составит в пределах 1-10 мс, тогда как сейчас – 40-60 мс. При ухудшении качества связи сеть 5G сможет незаметно для пользователя переключаться в более низкий стандарт – 4G и 3G, за счет чего обеспечивается безотказность работы сети. Все данные параметры позволят широко использовать данную сеть в быстродвижущихся объектах, например, автомобилях.

В настоящее время конструкторы уже разработали (в 2012 г.) стандарт для технологии транспортной модификации сети – V2X, т. е. «Транспорт, подключенный ко всему». Данная технология позволяет осуществлять взаимодействие непосредственно между транспортными средствами (V2V) и между транспортными средствами и окружающей их инфраструктурой (V2I) (см. рис. 2). А еще одна технология C-V2X появилась в 2016 г. и дополняет систему сотовой связью и 5G – V2N. Это

дает возможность автомобилю присутствовать онлайн в общей информационной среде.

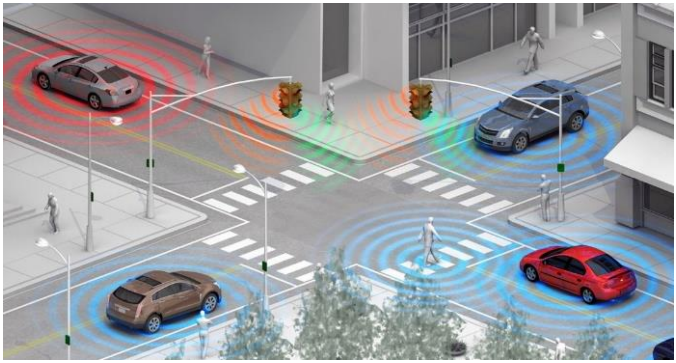


Рисунок 2 – Иллюстрация технологии Vehicle to everything communications

В технологии V2X можно выделить следующие подсистемы (см. рис. 3).

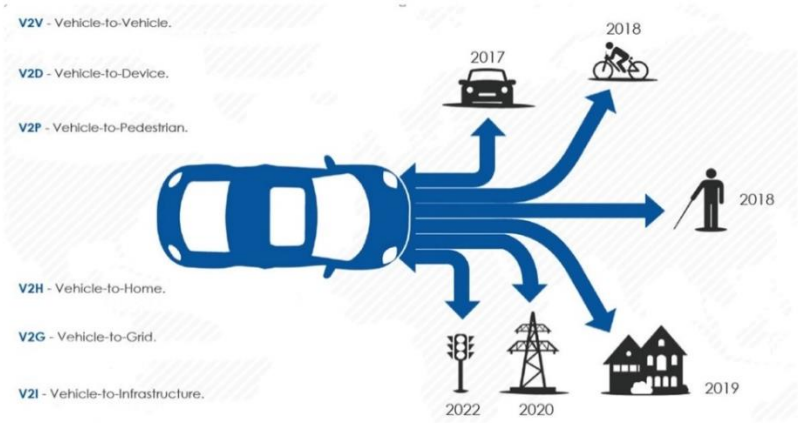



Рисунок 3 – Схематичное представление подсистем V2X

Подсистема V2V осуществляет обработку в режиме on-line данных о скорости движения автомобиля, производимом им манёвре, местонахождении, техническом состоянии и ряде других параметров, а также об его ориентации относительно других участников движения.

Подсистема V2D предусматривает получение и передачу данных с видеокамер, охранных систем или гаджетов, установленных на различных объектах (велосипед, собака, заграждение и т. д.), подключенным к V2X, и с транспортного средства.

Подсистема V2P предусматривает регулирование взаимодействия между автомобилем и пешеходом с целью снижения смертности на нерегулируемых или неосвещённых участках дороги, а также при нарушении правил дорожного движения пешеходами путем своевременного выявления расположения, скорости и направления движения пешеходов.

Подсистема V2I, применяя сенсоры, внедренные в авто, обеспечивает обмен информацией с объектами инфраструктуры (светофоры, дорожные знаки, препятствия, здания и т. п.).

Подсистема V2G направлена на реализацию в будущем более легкого перехода от бензиновых автомобилей к электрическим, и предусматривает реализацию подключения транспорта к общей энергетической сети с целью подзарядки или возвращения лишней электроэнергии.

Подсистема V2H предполагает подключение автомобиля к домашнему информационному пространству.

Использование системы V2X позволяет автомобилю учитывать и прогнозировать дорожную обстановку как в непосредственной близости, так и на заданном участке.

Аналитики Ernst & Young Global Limited указывают, что наличие поддержки V2X в ближайшее время станет обязательным требованием для новых автомобилей, выпускаемых мировой автомобильной промышленность. В целом от внедрения технологии V2X хотелось бы получить сокращение аварийности и смертности на дорогах, а также улучшения ситуации с загруженностью дорог.

В заключение настоящей статьи хотелось бы отметить, что повсеместное распространение технологии 5G станет невероятным прорывом в области эксплуатации и управления высокотехнологичными автомобилями ближайшего будущего. Технология V2X даст возможность раскрыть новые возможности городской инфраструктуры, являясь проводником для дополнительных источников информации о дорожном движении, особенностях ландшафта, расположении автомобилей экстренных служб и т.д. Все это позволит синхронизировать движение всех участников дорожного движения, увеличит безопасность и эффективность передвижения как автомобилей, так и пешеходов.

**Литература. 1.** Леонтьев И.А. Технология айтрекинг и ее использование в UX-исследованиях / И.А. Леонтьев, А.А. Арбузова // Сборник материалов национальной молодежной научно-технической конференции «Молодые ученые - развитию Национальной технологической инициативы (ПОИСК)». 2020. № 1. С. 373-375. **2.** Naderpour M. Privacy of V2X communications

/ M. Naderpour // Conference of Open Innovations Association, FRUCT. 2017. № 21. С. 462. **3.** Heo J. Performance-cost tradeoff of using mobile roadside units for V2X communication / J. Heo, B. Kang, J.M. Yang, S. Bahk, J. Paek // Transactions on Vehicular Technology. 2019. Т. 68. № 9. С. 9049-9059. **4.** Багаева В.Д. Технология V2X как компонент развития 5G / В.Д. Багаева, Е.П. Грахова // Сборник материалов XX Международной научно-технической конференции, XVI Международной научно-технической конференции «Проблемы техники и технологии телекоммуникаций. Оптические технологии в телекоммуникациях». 2018. С. 244-245.

**Реквизиты для справок:** *Россия, 153000, Иваново, Шереметевский пр., д.21, ФГБОУ ВО Ивановский государственный политехнический университет, доценту кафедры информационных технологий и сервиса, кандидату технических наук, Арбузовой А.А., тел. 8-915-814-63-54. E-mail: annaarb215@gmail.com*

**УДК 004.054**

## МОДУЛЬНОЕ ТЕСТИРОВАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА JAVA С ПРИМЕНЕНИЕМ БИБЛИОТЕК JUNIT И MOCKITO

И. В. КОНДУРОВ

Тестирование - процесс испытания программного кода, целью которого является проверка соответствия фактического результата выполнения функции ожидаемому. В разное время по-разному трактовалось понятие «тестирование», но практически всегда оно обозначало подтверждение качества программного продукта.

На сегодняшний день существует немалое количество видов тестирования. Классификация обеспечения качества программного продукта зависит от:

- целевого объекта;
- уровня знания внутренней системы;
- степени автоматизации;
- степени изолированности;
- затрат времени на проведение тестирования;
- признака позитивности сценария;
- степени готовности к процессу тестирования.

Одним из самых важных видов тестирования с точки зрения разработки программ принято считать модульное тестирование. Такое тестирование даёт не только обеспечение качества программных модулей и функций, но и предоставляет начало разработки. Изначально такой меха-

низм кодирования носил название «сначала тест». Позднее подобный механизм выделился в отдельную методологию, называемую «разработка через тестирование». Разработка через тестирование - важнейшая часть экстремального программирования, применяемая многими крупнейшими IT гигантами двадцать первого века.

Целью данной работы является анализ модульного тестирования программного обеспечения в языке программирования высокого уровня Java. Поскольку данный язык имеет как широкое применение среди ряда крупнейших организаций по разработке и внедрении программного обеспечения, так и является одним из лидеров среди всех существующих языков программирования, целесообразно провести исследование юнит-тестирования именно на Java.

Модульное или юнит тестирование - тестирование, позволяющее проверить качество отдельного программного компонента системы, его работоспособность и соответствие ожидаемым результатам выполнения. Юнит-тесты значительно облегчили работу программистов и тестировщиков, освободив от необходимости развёртывания всех технических инструментов для воспроизведения целостной системы. В число таких инструментов, как правило, включают:

- браузер (если это веб-приложение);
- СУБД;
- сервер.

Даже если существует необходимость проверить, к примеру, механизм пользовательской авторизации, нужно будет поднять систему целиком, то есть выполнить интеграционное тестирование. Зачастую таких возможностей у некоторых участников команды разработки нет, к тому же такой процесс весьма ресурсозатратен по времени. Впервые упоминание о таком понятии, как модульное тестирование, появилось в 1989 году в статье Кента Бекома «Simple Smalltalk Testing: With Patterns». Юнит-тесты позволили значительно ускорить процесс разработки программного обеспечения и улучшить качество разрабатываемой системы в целом. Юнит-тестирование расположилось на самой нижней позиции пирамиды тестирования, тем самым обеспечивая качество программного кода на самом нижнем уровне (тестирование ядра системы). На рис. 1 представлена пирамида тестирования, трактуемая по Кону Майку, на которой в качестве базовой основы конструкции является модульное тестирование. Кон Майк – известный американский scrum-мастер, основатель методологии разработки scrum, создатель нескольких трудов по Agile методологии. Среди таковых «Agile – оценка и планирование проектов» [1].

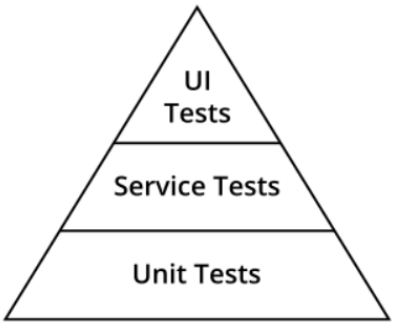



Рисунок 1 – Пирамида тестирования

Рассмотрим технологию модульного тестирования на Java.

Сегодня, в 2020 году, существует достаточное количество фреймворков, позволяющих java-разработчикам писать качественные и понятные юнит-тесты. Перечень наиболее популярных библиотек и сходным кодом для написания модульных тестов:

- JBehave;
- JUnit;
- Serenity;
- TestNG;
- Selenide;
- Gauge;
- Geb;
- Spock;
- HttpUnit;
- JWebUnit.

Среди представителей java-сообщества принято считать фреймворк JUnit наиболее адаптированным и комфортным для работы в проектах любой сложности. Причина такого выбора заключается в хорошей рекомендации данного фреймворка со стороны опытных программистов на протяжении многих лет. Кроме того, JUnit последней версии (пятая версия) позволяет создавать интеграционные тесты. Данная open–source библиотека поддерживается практически во всех ведущих средах разработки на java (IntelliJIDEA, NetBeans, Eclipse и другие). Также JUnit можно использовать с Java 5 и другими версиями [2].

Рассмотрим основные возможности библиотеки с открытым исходным кодом JUnit.

Для начала работы с JUnit её необходимо подключить к проекту. Реализуется это двумя способами:

1) Подключение jar-файла к проекту.

2) Добавление зависимости (в случае применения сборщиков Maven, Gradle).

Работа с фреймворком осуществляется через аннотации. Аннотация – это специальная форма метаданных, добавляемая в исходный код. Аннотация начинается с символа «@». Например, @Test. Основные аннотации, применяемые при работе с библиотекой для модульного тестирования JUnit, приведены в таблице 1.

Таблица 1 – Детальный анализ аннотаций в JUnit

| Аннотации JUnit | | |
|---|---|---|
| Название аннотации | Характеристика | Применение |
| @Test | Аннотация @Test определяет, что метод method() является тестовым. | public void method() |
| @Before | Аннотация @Before указывает на то, что метод будет выполняться перед каждым тестируемым методом @Test. | public void method() |
| @After | Аннотация @After указывает на то, что метод будет выполняться после каждого тестируемого метода @Test. | public void method() |
| @BeforeClass | Аннотация @BeforeClass указывает на то, что метод будет выполняться в начале всех тестов, а точнее - в момент запуска тестов (перед всеми тестами @Test). | public static void method() |
| @AfterClass | Аннотация @AfterClass указывает на то, что метод будет выполяться после всех тестов. | public static void method() |
| @Ignore | Аннотация @Ignore говорит, что метод будет проигнорирован в момент проведения тестирования. | public static void method() |
| @Test (expected = Exception.class) | (expected = Exception.class) – указывает на то, что в данном тестовом методе преднамеренно ожидается Exception. | public static void method() |
| @Test (timeout=100) | (timeout=100) – указывает, что тестируемый метод не должен занимать больше, чем 100 миллисекунд. | public static void method() |

Помимо аннотаций, JUnit располагает удобными в использовании методами класса Assert (junit.framework.Assert.*). Рассмотрим самые популярные методы для проверки произвольных данных в произвольном месте кода в таблице 2.

Таблица 2 – исследование методов класса Assert библиотеки JUnit

| Метод класса Assert | Характеристика метода |
|---|---|
| fail(String) | Указывает на то, чтобы тестовый метод завалился, при этом выводя текстовое сообщение. |
| assertTrue([message], boolean condition) | Проверяет, что логическое условие истинно. |
| assertsEquals([String message], expected, actual) | Проверяет, что два значения совпадают. Примечание: для массивов проверяются ссылки, а не содержание массивов. |
| assertNull([message], object) | Проверяет, что объект является пустым null. |
| assertNotNull([message], object) | Проверяет, что объект не является пустым null. |
| assertSame([String], expected, actual) | Проверяет, что обе переменные относятся к одному объекту. |
| assertNotSame([String], expected, actual) | Проверяет, что обе переменные относятся к разным объектам. |

При написании модульных тестов java-разработчики зачастую используют библиотеку Mockito.

Mockito - библиотека с открытым исходным кодом, обеспечивающая работу с заглушками, написанная на java.

Иногда у программистов возникает необходимость протестировать написанный метод, в котором присутствуют внешние зависимости. В качестве примеров таких зависимостей могут быть:

- обращение к базе данных;
- обращение к сервису;
- обращение к другой библиотеке.

Рассмотрим ситуацию, когда программист пишет очередную бизнес-логику приложения и в каком-то из своих методов использует сервис для вызова метода сохранения сущности в базе данных. При написании юнит-теста на свой метод программист может столкнуться с проблемой той самой строчки кода, в которой вызывается сервис для работы с БД. Ему нет необходимости проверять, какой ответ получает приложение от сервера БД, поскольку механизм работы с базой данных уже давно про-

тестирован другими разработчиками. Ему необходимо проверить написанный им функционал. Возникает проблема, которая влечёт за собой множество ошибок, среди которых самая распространённая – Null Pointer Exception. Избежать ошибки, связанной с внешними зависимостями, можно несколькими путями. Первый путь – написание альтернативных сервисов и интерфейсов с целью обеспечения фейкового механизма специально для юнит-тестирования. Второй путь – создание заглушек (мок-объектов).

Для реализации второго пути потребуется библиотека с открытым исходным кодом Mockito. Основная работа с методами библиотеки Mockito ведётся через класс Mockito [3].

Рассмотрим тот же самый сервис для работы с базой данных. Назовём его DataService. В классе, где программист использует данный сервис, необходимо его инициализировать следующим образом:

DataService dataServiceMock = Mockito.mock(DataService.class).

Такая форма инициализации означает, что мок-объект dataServiceMock становится абсолютно безликим. К примеру, если программа вызывает метод данного сервиса с возвращаемым параметром, то метод вернёт 0 в случае примитивного типа параметра и null в случае ссылочного. Если тип возвращаемого параметра метода мок-объекта – список, то метод вернёт пустые экземпляры коллекции.

Mockito позволяет задавать поведение мок-объектам. Рассмотрим ситуацию на примере уже написанного ранее сервиса dataServiceMock. С помощью метода when программист может задать нужное поведение методу объекта. Метод when позволяет задать такое поведение сервису dataServiceMock, которое будет характеризовать определённый возвращаемый параметр. С его помощью можно получить не пустые экземпляры коллекции, а заполненные так, как нужно. Следующая запись позволяет задать поведение сервису при вызове метода сохранения:

Mockito.when(dataService.getAllEntities()).thenReturn(new ArrayList< Entity>()).

Такое поведение заключается в следующем: при вызове метода getAllEntities() сервиса DataService программа вернёт новый список new ArrayList<Entity>(). Можно также заранее инициализировать список ожидаемыми значениями в переменную, к примеру, ArrayList< Entity> entities и сделать следующую запись:

Mockito.when(dataService.getAllEntities()).thenReturn(entities).

В таком случае метод getAllEntities() вернёт список объектов entities.

Работая с библиотекой Mockito при написании модульных тестов, рекомендуется использовать следующие методы:

verify() – позволяет проверить количество вызовов метода в программе;

thenThrow() – позволяет выбросить исключение при вызове метода;

thenReturn().thenReturn() – позволяет возвращать определённые значения при последовательных вызовах метода.

Последние два метода используются в комбинации с методом Mockito.when().

При работе с библиотекой Mockito становится возможным использовать матчеры при задании поведения mock-объектам. Например, методы any(), anyInt(). При задании поведения объекту можно использовать матчеры: when(dataService.getEntityByData(eq("true"), anyInt())). thenReturn(new Entity()). Метод eq() трактуется следующим образом: в качестве первого параметра вызываемого метода должно быть истинное булево значение. Метод anyInt(): параметр типа int.

И это только основная и наиболее популярная часть библиотеки Mockito. Данный фреймворк позволяет облегчить работу программистов при написании юнит-тестов с внешними зависимостями.

В завершении исследования модульного тестирования в языке программирования высокого уровня Java следует отметить прежде всего особую важность юнит-тестов при создании программного продукта, которые позволяют повысить качество программного кода отдельных модулей системы, и отличные технические инструменты в виде java-фреймворков JUnit и Mockito, которые значительно упрощают и ускоряют работу программистов.

**Литература. 1.** Шарма Р., Гулати Ш. Java Unit Testing with JUnit 5: Test Driven Development with JUnit 5 / Р. Шарма, Ш. Гулати – Нью-Дели,: apress, 2014. – 76-124 с. **2.** Mastering Unit Testing Using Mockito and JUnit /С. Ачария - Нью-Дели: PACKT PUBLISHING, 2014. – 21-130 с. **3.** Искусство тестирования программ /М. Гленфорд, Б. Том - Киев: Вильямс, 2020. – 121-130 с.

**Реквизиты для справок: 1.** *Россия, 656038, Барнаул, проспект Ленина, д. 46, Алтайский государственный технический университет им. И.И. Ползунова, бакалавру кафедры ИВТ и ИБ Кондурову Игорю Витальевичу, E-mail:igorkondurov@mail.ru.*

**УДК 004.054**

## ЛИДЕРСТВО БИЗНЕС- И СИСТЕМНОГО АНАЛИТИКА НА IT-РЫНКЕ

И. В. КОНДУРОВ, А. Н. ТУШЕВ

В 2000-х годах на IT-рынке была введена самостоятельная роль аналитика. Аналитик — это специалист, способный определить истинную

проблему заказчика и полностью удовлетворить его потребности. Основная деятельность такого специалиста направлена как на интервьюирование заказчика, в ходе которого происходит выявление, сбор и формирование бизнес-требований, стейкхолдеров (заинтересованных лиц бизнеса) и сценариев работы организации, так и системный анализ полученных требований, составление композиции системы, её модулей и компонентов, постановка задач на разработку и коммуникацию с командой разработки.

Стоит отметить, что изначально аналитик - сотрудник, способный совмещать в себе абсолютно все роли, касающиеся анализа разрабатываемой системы: бизнес анализ, системный анализ, анализ данных и информационной безопасности, анализ UI и UX. Но, начиная со второго десятилетия двадцать первого века, ситуация существенно изменилась [1].

При поиске работы аналитиком можно заметить такие вакансии, как бизнес-аналитик, системный аналитик, аналитик данных, аналитик, финансовый аналитик, продуктовый аналитик, маркетолог-аналитик. Столь сильное разделение одной общей роли связано с увеличением сложности разрабатываемых систем. Данная специфика на IT-рынке показала, что такое решение оказалось абсолютно разумным. Огромный стек работ аналитика был распределён между подролями, в результате чего значительно повысились качество и скорость разработки программных продуктов.

Несмотря на множественное существование видов профессии аналитика, лидирующие позиции все же занимают такие роли, как бизнес-аналитик и системный аналитик. Причём можно смело утверждать, что эти две роли лидируют не только в рамках локальной роли «аналитик», но и в рамках всех существующих глобальных ролей в программной инженерии. В число таковых включают менеджера по программным продуктам, архитектора системы, разработчиков бэкенда и фронтенда, мануальных тестировщиков и разработчиков автотестов, дизайнеров UI, UX, специалистов по внедрению и сопровождению продукта.

Определим значение двух ведущих видов аналитиков на современном IT-рынке и причину их лидерства.

Бизнес-аналитик. Данная роль подразумевает, что специалист сосредоточен на аналитике бизнес-процессов. Иначе говоря, бизнес-аналитик занимается коммуникациями с заказчиком. Основной стек обязанностей бизнес-аналитика следующий:

- изучение предметной области;
- выявление требований к системе со стороны заказчика;
- постоянная интеграция информации от заказчика к команде разработки и наоборот;

- презентация результатов работ команды разработки заказчику и всем заинтересованным лицам;
- командная дипломатия и коммуникация;
- участие в тестировании системы (приёмочные тесты);
- участие в планировании спринтов разработки;
- участие в командных конференциях;

Более детальный анализ работы бизнес-аналитика приведён на рис. 1.


Рисунок 1 – Стек работ бизнес-аналитика

Надо сказать, что бизнес-аналитик обеспокоен именно целями и заботами заказчика. Для такого специалиста самое важное – полностью удовлетворить все потребности заказчика и заинтересованных лиц любым путём, не думая о технологиях и о технической возможности реализации системы. От того, насколько точно и объёмно бизнес-аналитик проведёт интервью с заказчиком и стейкхолдерами, зависит успешность удовлетворения потребностей стороны заказчика разрабатываемой системы. По данным сайтов исследования современного IT-рынка, эта успешность может достигать до 80 %. Также стоит отметить, что крайне важно связующее звено между бизнес-аналитиком и системным аналитиком, ведь именно через этот и по существу единственный канал связи с командой разработки, бизнес-аналитик может разработанные требования перенести на их реализацию [2].

Системный аналитик. Данная роль присуща специалисту, способному работать с требованиями с технической точки зрения. Данный анали-

тик должен иметь знания по корпоративному стеку технологий. В число таковых включают, как правило, СУБД, язык программирования системы, среду разработки, методы проектирования, архитектуру системы.

Определим основные аспекты работы системного аналитика.

- Коммуникация с бизнес-аналитиком.
- Конвертирование бизнес-требований в системные требования и обратно.
- Постановка задач на разработку.
- Коммуникация с разработчиками.
- Участие в архитектурных решениях системы.
- Исследование системы и её компонентов.
- Анализ данных (SQL, Python).
- Участие в тестировании системы (модульные, интеграционные системные тесты).
- Участие в планировании спринтов разработки.

На рис. 2 показан перечень основных видов деятельности системного аналитика в проекте по разработке ПО.


Рисунок 2 – Стек работ бизнес-аналитика

Системный аналитик всегда мыслит с учётом возможностей технической стороны. Проще говоря, при принятии важных системных решений и переговорах с заказчиком, и всей командой разработки и эксплуатации продукта, системный аналитик при ответе на любой вопрос учитывает возможности технической реализации без учёта бизнес-требований. Такая сторона аналитика связана с его ответственностью за возможности технической реализации, поставленной разработчикам проекта. Системный аналитик несёт ответственность за своевременное изменение требований ввиду невозможности технической реализации.

Успешность IT-проекта напрямую определяется взаимодействием бизнес и системного аналитика, поскольку данные роли неразрывно связаны. Один не может существовать без другого. На одном ответствен-

ность за погружение в предметную область и общение с заказчиком, на другом - ответственность за принятие глобальных технический решений в команде, коммуникацию с командой разработки и её курирование.

Работа аналитиков, как и деятельность многих специалистов в области бизнеса, может быть так или иначе частично или полностью автоматизирована. В качестве автоматизации коммуникативной работы аналитиков может послужить программное обеспечение, способное генерировать аналитиками тестовые модули, позволяющие провести объёмный информативный опрос среди заинтересованных лиц организации, деятельность бизнес-процесса которой необходимо автоматизировать. Таким образом, создавая тестовый материал по системным требованиям, бизнес-сценариям и пользовательским историям, аналитики могут значительно сэкономить на времени по сбору информации со стейкхолдеров. Программное обеспечение синхронно отправляет созданные аналитиками в системе тестовые вопросы и задания заинтересованным лицам. После успешного прохождения последними всех модулей тестирования, информация по результатам автоматически отправляется аналитикам. Те, в свою очередь, имеют готовый материал по ожиданиям и требованиям заинтересованных лиц к разрабатываемой системе. Данное программное обеспечение позволяет частично автоматизировать работу аналитиков, тем самым давая ощутимую экономию по времени работы [3].

На сегодняшний день бизнес и системный анализ занимают одну из передовых позиций на рынке разработки программных продуктов.

Набирающая обороты актуальность и значимость такой аналитики обусловлена созданием связующего звена между методистами, бизнес-аналитиками и командой разработки, которое впоследствии повышает качество программного продукта и сокращает время его разработки.

Если рассмотреть текущую ситуацию на рынке IT, то можно заметить определённый дефицит системных и бизнес - аналитиков среди организаций по разработке и внедрению программных продуктов. Возникающий дефицит требует большого количества высококвалифицированных специалистов в области анализа системы, способных удовлетворить потребности рынка в проработке концепции автоматизированных систем с технической точки зрения, написании требований и постановке задач на разработку.

Лидирующая позиция бизнес-аналитика и системного аналитика в программной инженерии характеризуется их, пожалуй, самой важной ролью при разработке системы - качественное и количественное исследование предметной области и проектирование технической реализации. От того, насколько хорошо эти специалисты поработают, зависит успешность проекта и степень удовлетворённости заказчика и заинтересованных лиц. Поскольку на сегодняшний день данным специальностям не обучают в высших учебных заведениях, рынок крайне нуждается в ана-

литиках высокого уровня и не может их получить от государственных вузов.

Подводя итоги по лидерской позиции бизнес и системного аналитика, стоит отметить два аспекта, отдающих им пальму первенства в IT:

1. Огромная ответственность за качество разрабатываемой системы и степень удовлетворённости заказчика;

2. Сильный дефицит на рынке, обусловленный как невозможностью предоставления профильных специалистов со стороны вузов, так и сложностью изучения специфики работы аналитика.

**Литература. 1.** Купер А. Психбольница в руках пациентов / А. Купер – Санкт-Петербург: ПИТЕР, 2020. – 280-282 с. **2.** Чистый код /Р. Мартин - Санкт-Петербург: ПИТЕР, 2020. – 121-130 с. **3.** Чистая архитектура / Р. Мартин - Санкт-Петербург: ПИТЕР, 2020. – 121-130 с.

**Реквизиты для справок: 1.** *Россия, 656038, Барнаул, проспект Ленина, д. 46, Алтайский государственный технический университет им. И.И. Ползунова, бакалавру кафедры ИВТ и ИБ Кондурову Игорю Витальевичу, E-mail:igorkondurov@mail.ru* **2.** *Россия, 656038, Барнаул, проспект Ленина, д. 46, Алтайский государственный технический университет им. И.И. Ползунова, , кандидату технических наук, доценту, кафедры Информатики, вычислительной техники и информационной безопасности, Тушеву Александру Николаевичу, E-mail:tushev51@mail.ru*

**УДК 004.82**

## ИЗВЛЕЧЕНИЕ КОНЦЕПТОВ ИЗ ПОЛЬЗОВАТЕЛЬСКИХ ИСТОРИЙ НА ОСНОВЕ АНАЛИЗА ДЕРЕВЬЕВ ЗАВИСИМОСТЕЙ

Т. А. ПЕРЕПЕЛКИНА

Как правило, разработка программного продукта начинается со сбора и анализа требований, которые заинтересованные стороны проекта предоставляют команде разработки. Этот этап является важной ступенью при проектировании системы. Упущения на этапе сбора и анализа требований могут повлиять на эффективность работы команды разработки, сроки сдачи и стоимость проекта. Кроме того, учитывая динамичность современного мира, требования к проекту могут быть изменены или скорректированы заинтересованными сторонами в момент, когда система уже находится на этапе разработки.

Отсюда возникает потребность в структурировании накопленного в процессе жизни проекта знания. Под знанием в данном случае подразумеваются: ключевые понятия и термины предметной области, требования и история их изменений, типы пользователей и функциональное напол-

нение продукта, особенности реализации, описание используемых технологий и т. п.

Тема представления знаний в области инженерии требований неоднократно поднималась в научных работах последних лет. В работе [1] предлагается подход к формированию системы онтологий в области инженерии требований, а также описан анализ требований на основе онтологической и продукционной моделей. В работе [2] предлагается улучшенный подход, основанный на скрытом семантическом индексировании, и проверяется его эффективность на шести наборах артефактов требований. В работе [3] описаны типы подходов к проектированию требования в инженерии требований и приведены результаты их сравнительного анализа. В работе [4] предлагается подход к определению конфликтующих нефункциональных требований к проекту, представленных на естественном языке, при помощи онтологии.

**Целью текущей работы** является разработка подхода к извлечению концептов предметной области из текста пользовательских историй.

Пользовательская история представляет собой инструмент для описания функциональной возможности программного обеспечения простыми, общими словами, составленного с точки зрения конечного пользователя [5]. Шаблон написания пользовательской истории имеет следующий вид: «Как [тип пользователя], Я хочу [потребность], чтобы [цель]». Применение пользовательской истории характерно, как правило, для проектов, реализуемых с использованием гибких методологий разработки (agile).

В данной работе предлагается организовать ключевые концепты предметной области в виде онтологии. Пользовательские истории содержат в себе описание типов пользователей, функциональных возможностей системы и целей, для которой они разработаны. С помощью обработки синтаксических деревьев, построенных для пользовательских историй, можно определить характеристики, которым обладают слова, и извлечь значимые, с точки зрения предметной области, концепты.

Для построения деревьев синтаксических зависимостей пользовательских историй использовался инструмент UDPipe, который приводит словоформу исходного предложения к лемме (словарной форме), а также автоматически определяет часть речи и грамматические характеристики приведенных слов в тексте с приписыванием им соответствующих тегов [6].

При анализе пользовательских историй были собраны и проанализированы следующие характеристики:

– часть речи (Upos Tag),

– часть предложения (DepRel),

– наличие зависимого слова (has Attrib).

Для проведения анализа были подобраны примеры пользовательских историй, разработанных в рамках учебных проектов. Пользовательские истории были загружены и проанализированы с помощью UDPipe.

В таблице 1 представлен фрагмент полученного результата на примере пользовательской истории проекта по созданию сайта для книжного магазина.

Таблица 1 – Фрагмент результата анализа пользовательских историй

| Как пользователь, я хочу сортировать товар по цене, чтобы выбрать подходящий товар | | | | | | |
|---|---|---|---|---|---|---|
| | Как | пользователь | Я | хочу | сортировать | товар |
| Upos Tag | SCONJ | NOUN | PRON | VERB | VERB | NOUN |
| Dep Rel | mark | Advcl | nsubj | root | xcomp | obj |
| has Attrib | 0 | 0 | 0 | 0 | 0 | 0 |
| | по | цене | чтобы | выбрать | подходящий | товар |
| Upos Tag | ADP | NOUN | SCONJ | VERB | ADJ | NOUN |
| Dep Rel | case | Obl | mark | advcl | amod | obj |
| has Attrib | 0 | 0 | 0 | 0 | 0 | 1 |

Таким образом, индикатором роли выступает слово «Как», индикатором потребности «я хочу», индикатором конечной цели «чтобы». В приведенном примере тип пользователь – «аналитик», потребность – редактировать требования», цель – «поддерживать документацию в актуальном состоянии».

Рассмотрим подробнее каждую полученную часть пользовательской истории.

Описание типа пользователя на текущем примере полное и не содержит дополнений (уточняющих прилагательных или причастий).

Часть, отвечающая за потребность, звучит как «сортировать товар по цене». Слово «сортировать» выступает в роли основного глагола. Объект, на который направлено действие – существительное «товар». Словосочетание из предлога и существительное «по цене» дополняет описание выполняемого действия.

Фрагмент предложения, отвечающий за конечную цель, на приведенном примере звучит как «выбрать подходящий товар». Фраза состоит из: глагола «выбрать», объекта «товар» и зависимого от него слова «подходящий», которые даёт характеристику объекту

Упростим предложение и выделим в нём 3 основных элемента: роль («покупатель»), потребность («сортировать товар»), цель («выбрать товар»). Полученная структура имеет упрощенную форму пользовательской истории и помогает быстрее выделить ключевые элементы из целого предложения.

Аналогичным образом были проанализированы около 50 пользовательских историй и сделан вывод о том, что, благодаря фиксированной структуре предложения, можно выделить характеристики основных его элементов. В таблице 2 представлены характеристики фрагментов пользовательских историй для слов, входящих в выделенные группы.

Таблица 2 – Характеристики фрагментов дерева объектов предметной области

| Группа | Upos Tag | DepRel | has Attrib |
|---|---|---|---|
| Индикатор роли | SCONJ | mark | 0 |
| Индикатор потребности | PRON | nsubj | 0 |
| | VERB | root | 0 |
| Индикатор цели | SCONJ | mark | 0 |
| Роль | NOUN | advcl | 0\1 |
| Атрибут роли | VERB | amod | 0 |
| Потребность - действие | VERB | xcomp | 0 |
| Потребность - объект | NOUN | obj | 0\1 |
| Цель – действие | VERB | advcl | 0 |
| Цель – объект | NOUN | obj | 0\1 |

Зная характеристики слов, содержащихся в структуре пользовательской истории, можно выделить их и составить дерево из роли (типа пользователя), потребности (функционального действия) и цели (рис 1.)


Рисунок 1 – Фрагмент дерева основных объектов предметной области для проекта разработки сайта книжного магазина

Выделив элементы и создав дерево концептов предметной области, можно ускорить процесс изучения сведения о проекте. Просматривая дерево, формируется представление о ключевых функциональных возможностях проекта и типах пользователя. Информация, собранная в одном месте, поможет сформировать представления о масштабах проекта и обязательных его элементах.

Дерево основных концептов предметной области может быть полезно команде разработки в следующих случаях:

– работа с типовыми проектами для разных заказчиков,

– формирование плана по обучению основным дистрибутивным функциям продукта для новых сотрудников,

– сопровождения работы дистрибутивной версии продукта,

– оказания консультации заказчику по вопросам дистрибутивного наполнения продукта,

– отображение актуального состояния требований при разработке продукта,

– сохранение и передача накопленного в ходе работы над проектом опыта.

Таким образом, с помощью проведенного анализа, были разработаны правила извлечения концептов из текста пользовательской истории, которые могут быть использованы для формирования модели представления знаний по проекту.

**Литература. 1.** Муртазина М.Ш., Авдеенко Т.В. Онтологический подход к интеллектуальной поддержке инженерии требований при гибкой разработке программных продуктов // Информационные технологии и нанотехнологии (ИТНТ-2020). В 4 т. Т. 4 : Науки о данных : сб. тр. 6 междунар. конф. и молодеж. шк., Самара, 26–29 мая 2020 г. – Самара : Изд-во Самар. нац. исслед. ун-та, 2020. – С. 183–191. **2.** Eder S. et al. Configuring latent semantic indexing for requirements tracing //2015 IEEE/ACM 2nd International Workshop on Requirements Engineering and Testing. – IEEE, 2015. – С. 27-33. **3.** Outfarouin A., Zahid N., Abdali A. A Comparative Study of the Decisional Needs Engineering Approaches // International journal of Advanced Computer Science and Applications. – 2018. – Т. 9. – №. 8. – С. 433-441. **4.** Shah U., Patel S., Jinwala D. An Ontological Approach to Specify Conflicts among Non-Functional Requirements //Proceedings of the 2019 2nd International Conference on Geoinformatics and Data Analysis. – 2019. – С. 145-149. **5.** Пользовательские истории с примерами и шаблоном [Электронные ресурс]. URL: https://www.atlassian.com/ ru/agile/project-management/user-stories. **6.** UDPipe [Электронный ресурс]. URL: https://lindat.mff.cuni.cz/services/udpipe/.

**Реквизиты для справок:** *Россия, 630073, г. Новосибирск, пр. К. Маркса 20, Новосибирский Государственный Университет, факуль-*

*тет АВТФ, кафедра АСУ, магистрант Перепелкина Т.А. E-mail: perepelkina.2015@stud.nstu.ru*

**УДК 681.51**

## ЧИСЛЕННЫЙ МЕТОД РЕШЕНИЯ ОБРАТНОЙ ЗАДАЧИ ДЛЯ ПЕРЕМЕЩЕНИЯ РОБОТА МАНИПУЛЯТОРА

Д. Р. МАЛАХОВ, О. В. ЗАХАРОВ

Роботы манипуляторы широко применяются в технике для решения различных задач в соответствии с их назначением [1-4]. Манипуляторы обычно состоят из последовательно соединенных жестких звеньев и связей между ними – соединений. Одной из наиболее сложных разновидностей роботов манипуляторов является сочлененный робот, также получивший название Robotic Arm. Он имеет структуру, подобную человеческой руке с тремя жесткими звеньями и только вращательными соединениями. Такая структура обеспечивает большую гибкость, управляемость и универсальность [5, 6]. Вместе тем снижается точность и усложняется кинематический расчет. Прямая кинематическая задача достаточно хорошо описана в литературе и однозначно решается с помощью углов Эйлера или кватернионных матриц [7-9]. Обратная кинематическая задача имеет многовариантное решение и поэтому может быть сформулирована как оптимизационная. В настоящее время разработано много методов для решения обратной задачи кинематики для роботов манипуляторов, получение аналитических решений для которых затруднительно [10].

Прямая задача кинематики манипулятора заключается в вычислении декартовых координат конечного звена по его кинематической схеме и заданным углам всех звеньев. Известные методы решения прямой задачи построены на преобразовании координат с помощью матриц направляющих косинусов, углов Эйлера, аппарата кватернионов, дробно-линейных преобразований с параметрами Кейли-Клейна. Прямая кинематическая задача достаточно подробно описана в работах для определенных типов манипуляторов [11, 12].

Обратная задача кинематики манипулятора заключается обобщенных координат (углов) звеньев по известному конечному положению схвата. Большинство кинематических схем роботов построены таким образом, что имеется аналитическое решение. Однако известно, что в общем случае обратная задача кинематики даже для манипуляторов без кинематической избыточности допускает многовариантность решения. Единственно верным подходом будет задача параметрической оптимизации. Для этого требуется найти все множество решений, а затем выбрать

из них одно по какому-либо критерию. Поэтому актуальным вопросом становится выбор критерия оптимизации.

В настоящее время существующие методы получения решения обратной задачи можно разделить на геометрические, аналитические и численные. Нахождение обобщенных координат в явном виде представляет собой сложную вычислительную задачу ввиду того, что получаемые уравнения нелинейны. Поэтому аналитическое решение существует только для роботов с определенной конструкцией. В методе углов Эйлера предлагается последовательно умножать слева обе части уравнения на матрицы обратных преобразований и определять искомые углы из полученных таким образом матричных уравнений. Также известно решение обратной задачи кинематики в дуальных параметрах Родрига–Гамильтона, а именно с помощью бикватернионных матриц. Геометрический подход связан с использованием аналитического решения с учетом особенностей кинематической схемы, позволяющий уменьшить число независимых уравнений.

К недостаткам аналитического решения относятся неоднозначность получаемого результата, обусловленная используемыми тригонометрическими функциями. При этом требуется дополнительный анализ выбора правильного решения. Поэтому в статье предлагается численный метод решения обратной задачи кинематики манипулятора на основе параметрической оптимизации. Математическое описание строится на векторно-матричных преобразованиях декартовых координат звеньев в соответствии со схемой робота. Полученные формулы прямой задачи кинематики выступают в качестве исходных данных, где углы поворота звеньев неизвестны. Для их нахождения ищется минимум целевой функции, представляющей собой суммы квадратов разности заданных и полученных декартовых координат схвата. В статье рассматривается трехзвенный манипулятор с шестью степенями свободы, имеющий только вращательные соединения. Данная схема робота является более общей, чем известные роботы схемы PUMA.

Координатная схема манипулятора представлена на рис. 1. Для аналитического описания используем следующие системы координат:

1) система ($x_0$, $y_0$, $z_0$) - условно неподвижная система первого звена манипулятора (основание);

2) системы ($x_1$, $y_1$, $z_1$), ($x_2$, $y_2$, $z_2$) - соответственно подвижные системы координат первого и второго звена;

3) система ($x_3$, $y_3$, $z_3$) - подвижная система координат конечного звена (схвата).

Выполним последовательные векторно-матричные преобразования систем координат, начиная от основания и заканчивая схватом.

Уравнение для декартовых координат первого звена:

$$\begin{cases} x_1 = x_0 + l_1 \cos\alpha_1 \sin\alpha_2; \\ y_1 = y_0 + l_1 \sin\alpha_1; \\ z_1 = z_0 + l_1 \cos\alpha_1 \cos\alpha_2, \end{cases} \quad (1)$$

где $l_1$ – длина первого звена; $x_0$, $y_0$, $z_0$ – координаты основания; $\alpha_1$, $\alpha_2$ – углы поворота первого звена вокруг соответственно осей *Y* и *X*.

Уравнение для декартовых координат второго звена:

$$\begin{cases} x_2 = x_1 + l_2 \cos(\alpha_1 + \alpha_3) \sin(\alpha_2 + \alpha_4); \\ y_2 = y_1 + l_2 \sin(\alpha_1 + \alpha_3); \\ z_2 = z_1 + l_2 \cos(\alpha_1 + \alpha_3) \cos(\alpha_2 + \alpha_4), \end{cases} \quad (2)$$

где $l_2$ – длина второго звена; $x_1$, $y_1$, $z_1$ – координаты первого соединения; $\alpha_3$, $\alpha_4$ – углы поворота второго звена вокруг соответственно осей *Y* и *X*.

Уравнение для декартовых координат третьего звена:

$$\begin{cases} x_3 = x_2 + l_3 \cos(\alpha_1 + \alpha_3 + \alpha_5) \sin(\alpha_2 + \alpha_4 + \alpha_6); \\ y_3 = y_2 + l_3 \sin(\alpha_1 + \alpha_3 + \alpha_5); \\ z_3 = z_2 + l_3 \cos(\alpha_1 + \alpha_3 + \alpha_5) \cos(\alpha_2 + \alpha_4 + \alpha_6), \end{cases} \quad (3)$$

где $l_3$ – длина третьего звена; $x_2$, $y_2$, $z_2$ – координаты второго соединения; $\alpha_5$, $\alpha_6$ – углы поворота третьего звена вокруг соответственно осей *Y* и *X*.

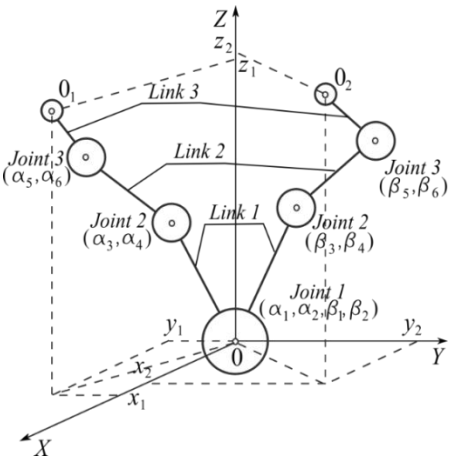



Рисунок 1 – Кинематическая схема манипулятора

Уравнения (3) представляют собой решение прямой задачи кинематики манипулятора. В этом случае задают значения углов α и определяют декартовы координаты *x*, *y*, *z*. Если задать координаты *x*, *y*, *z*, а неизвестными считать углы β, то получим обратную задачу кинематики. Для

ее решения применим параметрическую оптимизацию. Искомую целевую функцию запишем в виде суммы квадратов разности искомых и заданных декартовых координат схвата:

$$F(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6,\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6)=\sum(X_1-X_2)^2+(Y_1-Y_2)^2+(Z_1-Z_2)^2, \quad (4)$$

где $X_1$, $Y_1$, $Z_1$ – искомые координаты схвата; $X_2$, $Y_2$, $Z_2$ – требуемые координаты схвата; $\alpha_1$, $\alpha_2$, $\alpha_3$, $\alpha_4$, $\alpha_5$, $\alpha_6$ – исходные углы поворота звеньев; $\beta_1$, $\beta_2$, $\beta_3$, $\beta_4$, $\beta_5$, $\beta_6$ – неизвестные углы поворота звеньев.

Рассмотренный подход и математическая модель реализованы в программной среде MATLAB. Проведенный численный эксперимент показал, что независимо от исходных условий обратная задача кинематики манипулятора имеет множество решений. При этом целевая функция достигает принимает значение, близкое к нулю (порядка $10^{-8}$). Тот или иной вариант решения определяется выбором начальных значений параметров.

Выполнен расчет обратной кинематической задачи для рассмотренного манипулятора с шестью степенями свободы и с длинами звеньев $l_1$ = 200 мм, $l_2$ = 150 мм, $l_3$ = 50 мм. Четыре варианта расчета проиллюстрированы на рис. 2.

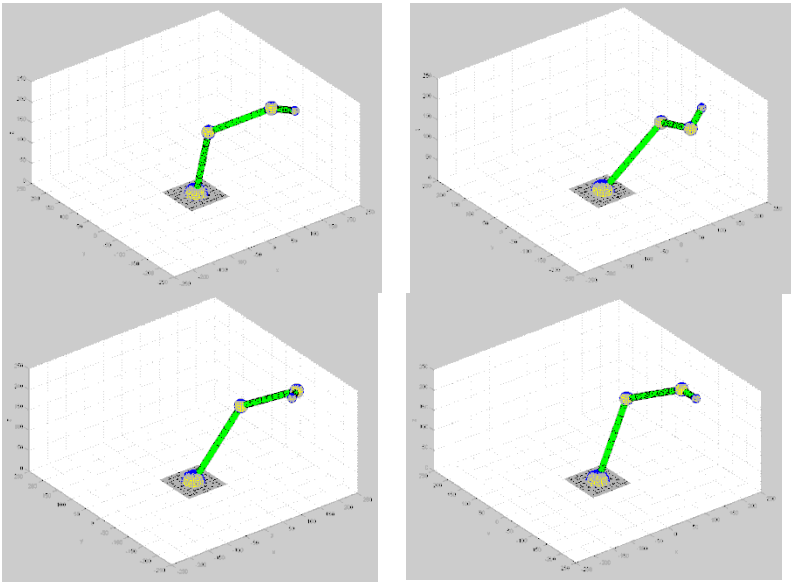


Рисунок 2 – Расчетные положения робота манипулятора

Анализ полученных данных показал, что при различных вариантах решения суммы углов звеньев манипулятора существенно различаются. Результаты в виде сумм углов поворота всех звеньев робота и их суммы даны на рис. 3. Из рисунка видно, что максимальная разница в суммах углов звеньев может достигать двух раз.

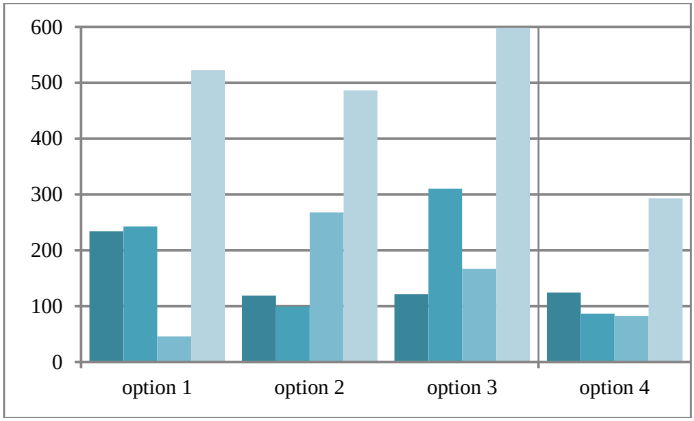



Рисунок 3 – Сумма углов звеньев робота манипулятора

Выполненные численные эксперименты показал, что решение обратной задачи кинематики робота манипулятора с шестью степенями свободы является многовариантным. Имеется множество вариантов решения в обобщенной системе координат с различными значениями углов соединений. Поэтому требуется решение оптимизационной задачи. В качестве критерия предложена сумма углов всех звеньев манипулятора. На примерах расчета показано, что оптимальное решение позволяют до двух раз уменьшить сумму углов соединений и тем самым минимизировать повороты звеньев манипулятора.

**Литература. 1.** Юревич Е.И. Управление роботами и робототехническими системами / Е.И. Юревич. СПб, 2001. 168 с. **2.** Хомченко В.Г. Мехатронные и робототехнические системы / В.Г. Хомченко, В.Ю. Соломин. Омск: Изд-во ОмГТУ, 2008. 160 с. **3.** Зенкевич С.Л. Основы управления манипуляционными роботами / С.Л. Зенкевич, А.С. Ющенко. М.: Изд-во МГТУ им. Н. Э. Баумана. 2004. 480 с. **4.** Челпанов И.Б. Устройство промышленных роботов. 2-ое изд. СПб: Политехника, 2001. 204 с. **5.** Захаров О.В. Минимизация погрешностей формообразования при бесцентровой абразивной обработке: монография / О.В. Захаров. Саратов: СГТУ, 2006. 152 с. **6.** Гречников Ф.В. Минимизация объема измерений при контроле

цилиндрических поверхностей на основе статистического моделирования / Ф.В. Гречников, А.С. Яковишин, О.В. Захаров // Вестник Пермского национального исследовательского политехнического университета. Машиностроение, материаловедение. 2017. № 4. С. 101-110. **7.** Челноков Ю.Н. Кватернионные модели и методы динамики, навигации и управления движением / Ю.Н. Челноков. М.: ФИЗМАТЛИТ, 2011. 560 с. **8.** Борисов О.И. Методы управления робототехническими приложениями / О.И. Борисов, В.С. Громов, А.А. Пыркин. СПб, 2016. 108 с. **9.** Гречников Ф.В. Итерационный метод коррекции радиуса сферического щупа мобильных координатно-измерительных машин при контроле поверхностей вращения / Ф.В. Гречников, А.Ф. Резчиков, О.В. Захаров // Измерительная техника. 2018. № 4. С. 21-24. **10.** Каргинов Л.А. Иерархический подход к решению обратной задачи кинематики / Л.А. Каргинов // Наука и Образование. МГТУ им. Н.Э. Баумана. 2016. № 3. С. 37–63.**11.** Данилов А.В. Общий подход к решению обратной задачи кинематики для манипулятора последовательной структуры с помощью конечного поворота и смещения / А.В. Данилов, А.Н. Кропотов, О.В. Трифонов // Препринты ИПМ им. М.В. Келдыша. 2018. № 81. С. 1-15. **12.** Дыда А.А. Решение обратной задачи кинематики для манипуляционного робота методом штрафных функций / А.А. Дыда, Д.А. Оськин // Фундаментальные исследования. 2015. № 11-4. С. 673-677.

***Захаров Олег Владимирович,*** *д.т.н., профессор кафедры «Технология и системы управления в машиностроении», Саратовский государственный технический университет имени Гагарина Ю.А. E-mail: zov@sstu.ru.*

**УДК 004.8**

## МЕТОДЫ ВЫЯВЛЕНИЯ ТЕМПОРАЛЬНЫХ ЗАКОНОМЕРНОСТЕЙ В ГРУППАХ ВРЕМЕННЫХ РЯДОВ

К. М. МАЛЕВАН

В наше время существует значительное количество областей деятельности человека, которые связаны с постепенным накоплением информации о протекании процессов, характеризуемых набором параметров. Каждый из параметров изменяется с течением времени, причем характер данных изменений может свидетельствовать о предвестниках нештатной ситуации или характеризовать некоторое состояние объектов, по которым происходит накопление информации. Таким образом, выявление темпоральных закономерностей является актуальной задачей, от способа решения которой зависит, например, разработка алгоритмов и программного обеспечения подсистемы принятия решений в информацион-

но-измерительных системах. Механизм принятия решений связан с процессами выработки информирующих сообщений и управления. Исходя из того, что часто приходится учитывать ранее полученную информацию, только первичных данных для формирования управляющих воздействий недостаточно. Первичные данные, помимо информационной части, должны включать темпоральную составляющую, которая фиксирует, в какой момент времени данные были обработаны и/или получены.

Для анализа классических временных рядов используют машинное обучение и методы статистики, практическими аспектами обработки временных рядов являются кластеризация, прогнозирование и выявление аномалий.

Для получения новых знаний о закономерностях и об объекте может быть рассмотрена нечеткая форма представления данных, при которой уменьшается степень их детализации [2]. С помощью лингвистических переменных осуществляется описание темпоральных явлений в лингвистической форме. Каждой из переменных соответствует некоторое количество словесных значений, соответствующих различным интервалам числовых значений временных рядов и задаваемых с помощью функции принадлежности. Большое количество сложных объектов анализа обладают объективной неопределенностью, и поэтому требуется дальнейшее расширение инструментария прогностики.

Нечеткие временные ряды позволяют учитывать неполноту и неопределенность информации о происходящем событии в условиях недостаточности объема статистической базы данных, которая обязательна для применения традиционных вероятностных методов [2].

В последние десятилетия в работах многих ученых рассмотрены методы нечеткой регрессии, а также методы анализа данных нечетких временных рядов [2, 3]. Данные работы посвящены этой теме. В развитии теории нечетких временных рядов рассматривались такие методы анализа, как:

1) Нечеткая регрессия.

2) Мягкие вычисления. Анализ нечетких тенденций является наиболее перспективным направлением с использованием мягких вычислений. Он заключается в описании и распознавании тенденций, прогнозирования на основе нечетких тенденций, а также извлечении ассоциативных правил.

3) Применение лингвистических методов анализа нечетких временных рядов.

4) Извлечение правил (Data Mining) из нечетких временных рядов. Для этого необходимо развитие методов Data Mining для реляционных баз данных и методов нечетких баз данных.

В основу анализа нечетких временных рядов могут быть положены распознавание образцов – паттернов и извлечение ассоциативных правил в лингвистической форме.

В работах зарубежных ученых, например, Х. Танаки, К Хироты, Я. Капржика [5] использованы методы линейного программирования и представлены модели линейной регрессии с нечетким коэффициентом.

Если рассматривать работы отечественных ученых, то можно обратить внимание на труды И. З. Батыршина, С. М. Ковалева, Н. Г. Ярушкиной и др.

Н. Г. Ярушкина в своей работе [3] рассматривает основные аспекты теории нечетких систем, генетических алгоритмов и нейронных сетей. В ней значительное внимание уделено алгоритмам обучения нечетких нейронных сетей и структуре гибридных сетей. Раскрыты основные подходы к интеллектуальному анализу временных рядов, в числе которых присутствуют технологии анализа именно нечетких временных рядов и нечеткие модели, но данные алгоритмы подробно не рассмотрены.

Анализ операций нечеткой логики и их обобщения, а также подходы к компьютерному и математическому моделированию обработки нечетких данных рассмотрены ученым И. З. Батыршиным [5]. В его работе предлагается методология обнаружения аномалий в темпоральных данных, которая базируется на анализе динамики вероятностных значений аномалии с поступлением каждого нового отсчета в потоке данных.

Также с помощью темпоральных данных предлагается методология обнаружения аномалий на объекте наблюдения, которая основывается на выявлении аномалий путем анализа динамики вероятностных свойств с поступлением каждого нового отсчета в потоке данных. Но для применения данной методологии с целью вычисления вероятностей аномалий необходимо накопление значительного объема данных.

Матричный паттерн является одним из способов хранения темпоральных шаблонов для группы нечетких и четких временных рядов.

Однако данный способ предполагает наличие в рядах незначащих для анализа элементов, и это не позволяет осуществить компактное хранение шаблона, а также сократить время на выполнение операции сравнения паттерна с реальными данными.

Для группы временных рядов гибридный ОЛС-паттерн, предложенный в работах [4] основан на применении классических односвязных линейных списков (ОЛС) для хранения и последующего выявления темпоральных закономерностей в данных.

В работе [1] рассмотрены алгоритмы применения ОЛС-паттерна для нечеткого временного ряда для различных вариантов следования нечетких данных, однако перспективным является разработка алгоритмов и моделей принятия решений для группы нечетких временных рядов с

различным шагом временной детализации. Указанные алгоритмы и модели востребованы для автоматизированных систем, где скорость принятия решений является критически важной, например, в медицинских комплексах, контролирующих группу жизненно важных параметров здоровья человека. Выявление темпоральных закономерностей на архивных данных также способствует получению новых знаний о контролируемых объектах и процессов с учетом их взаимосвязей.

**Литература. 1.** Дульцев Д.В., Сучкова Л.И. Материалы IV Всероссийской междисциплинарной молодежной научной конференции «Проблемы правовой и технической защиты информации – 2016» (г. Барнаул, Алтайский государственный университет, 20-21 мая 2016 г.). Проблемы правовой и технической защиты информации. Выпуск IV / Сборник научных статей. - Барнаул: Издательство «Новый формат», 2016. – 318 с. – с. 37-43**. 2. Кизбикенов, К.О.** Прогнозирование и временные ряды : учебное пособие. [Текст] / К.О. Кизбикенов; Алтайский гос. пед. ун-т. – Барнаул : АлтГПУ, 2017. – 113 с. **3.** Ярушкина, Н.Г. Интеллектуальный анализ временных рядов [Текст]: учеб. пособие / Н.Г. Ярушкина, И.Г. Перфильева, Т.В. Афанасьева. – Ульяновск: УлГТУ, 2010. – 320 с. **4.** Дульцев Д.В., Сучкова Л.И. Описание и идентификация темпоральных закономерностей для нечеткого временного ряда с применением гибридных ОЛС-паттернов. Вестник Дагестанского государственного технического университета. Технические науки. 2018; 45(2):104-113. https://doi.org/10.21822/2073-6185-2018-45-2-104-113 **5.** Нечеткие гибридные системы. Теория и практика [Текст] / И.З. Батыршин [и др.]; под ред. Н.Г. Ярушкиной. – Москва.: Физматлит, 2007. – 208 с.

**Реквизиты для справок:** *Россия, 656038, Барнаул, пр. Ленина 46, Алтайский Государственный Университет им. И.И. Ползунова, ст. преподаватель каф. ИВТиИБ, тел. 8 (3852) 29-07-86. E-mail: kristya_22@mail.ru.*

**УДК 51-74; 664.665**

## МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ СОСТАВА БЕЗГЛЮТЕНОВЫХ ХЛЕБОПЕКАРНЫХ СМЕСЕЙ

А. Г. БЛЕМ, Л. А. КОЗУБАЕВА, Я. Ю. МУЗОВАТОВА

В настоящее время заметен всплеск интереса потребителей к функциональным пищевым продуктам. Одним из сегментов данного рынка являются продукты для безглютенового питания. Несмотря на возросший спрос, ассортимент безглютеновых хлебобулочных изделий в торговых предприятиях Алтайского края довольно беден. Кроме того, в крае практи-

чески отсутствуют предприятия, занимающиеся выпуском безглютеновых хлебобулочных продуктов. Вероятно, это связано с тем, что производство безглютеновых мучных изделий достаточно трудозатратный и наукоемкий процесс, требующий специальных условий. Для решения этой проблемы была разработана соответствующая информационная система управления хлебопекарным производством, включающая в себя и способы формирования рецептур хлеба. Примером может служить рецептура хлеба из смеси различных видов безглютеновой муки, созданная на основе рецептуры хлеба из кукурузной муки. Разработка рецептур осуществлялась путем планирования полного факторного эксперимента [1-3].

В соответствии с планом (таблица 1) были рассчитаны экспериментальные рецептуры, по которым были проведены пробные выпечки. У готового продукта хлеба анализировали массу, объем, пористость и давали органолептическую оценку. В качестве целевой функции были выбраны наиболее информативные показатели качества хлеба – удельный объем и органолептическая оценка. Для этих показателей были рассчитаны уравнения регрессии, представленные в таблице 2.

Таблица 1 – План эксперимента ПФЭ $2^2$

| № опыта | Кодированные значения факторов | | Факторы в натуральном выражении | |
|---|---|---|---|---|
| | X1 | X2 | Количество кукурузной муки, г | Количество гречневой муки, г |
| 1 | + | + | 70 | 30 |
| 2 | + | - | 50 | 10 |
| 3 | - | + | 70 | 30 |
| 4 | - | - | 50 | 10 |
| Центр эксперимента | 60 | 20 | | |
| Интервалы варьирования | 10 | 10 | | |

Таблица 2 – Уравнения регрессии

| Показатель качества | Кодированная форма | Уравнения регрессии |
|---|---|---|
| Удельный объем | У1 | $y_1 = 4{,}22-0{,}17x_2+0{,}88x_1x_2$ |
| Органолептическая оценка | У2 | $y_2 = 28{,}33+4{,}89x_1-10{,}02x_1x_2$ |

На рисунке 1 представлены графики, отражающие влияние того или иного количества гречневой и кукурузной муки на удельный объем и органолептическую оценку [4].

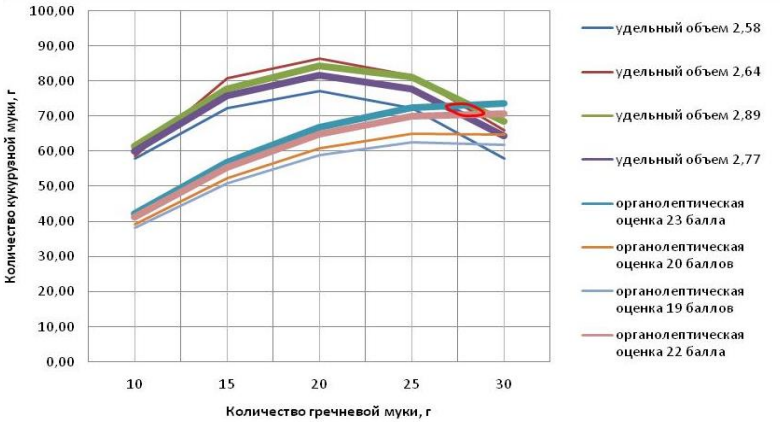



Рисунок 1 – Графическое представление результатов планирования

По результатам планирования была составлена оптимальная рецептура хлеба из смеси кукурузной и гречневой муки, представленная в таблице 3.

Таблица 3 – Рецептура хлеба из смеси рисовой и кукурузной муки

| Наименование сырья | Количество сырья, г |
|---|---|
| Мука кукурузная | 71,0 |
| Мука гречневая | 29,0 |
| Дрожжи хлебопекарные | 7,4 |
| Соль поваренная пищевая | 1,8 |
| Сахар-песок | 3,8 |
| Яичный белок | 38,0 |
| Маргарин столовый | 5,0 |

В результате математического моделирования была составлена оптимальная рецептура хлеба из смеси рисовой и кукурузной муки в зависимости от информативных показателей качества хлеба – удельного объемаи органолептической оценки. При этом количество рисовой муки должно составлять 50 г, кукурузной – 21 г.

**Литература 1.** Казиев, В. М. Введение в анализ, синтез и моделирование систем : учебное пособие / В. М. Казиев. – 3-е изд. – Москва, Саратов :

Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. – 270 с. – ISBN 978-5-4497-0307-1. – Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. – URL: http://www.iprbookshop.ru/89425.html (дата обращения: 20.09.2020). – Режим доступа: для авторизир. пользователей **2.** Панкратьева Н.А., Заворохина Н.В. Моделирование рецептуры хлеба с повышенной пищевой ценностью и улучшенными реологическими свойствами // АПК России. – 2017. – Т. 24. № 5. – С. 1227-1233. **3.** Бочарова-Лескина, А. Л., Иванова,Е. Е. Математическое моделирование в технологии и оценке качества пищевых продуктов // Научный журнал КубГАУ - ScientificJournalofKubSAU. – 2017. – №125. URL: https://cyberleninka.ru/article/n/matematicheskoe-modelirovanie-v-tehnologii-i-otsenke-kachestva-pischevyh-produktov (дата обращения: 20.09.2020). **4.** Сагдеев, Д. И. Основы научных исследований, организация и планирование эксперимента: учебное пособие / Д. И. Сагдеев. – Казань: Казанский национальный исследовательский технологический университет, 2016. – 324 с. – ISBN 978-5-7882-2010-9. – Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. – URL: http://www.iprbookshop.ru/79455.html (дата обращения: 20.09.2020). – Режим доступа: для авторизир. Пользователей.

***Реквизиты для справок: Блем Александр Генрихович****, доцент кафедры ИСЭ ФГБОУ ВО «Алтайский государственный технический университет им. И.И. Ползунова», e-mail: alblem@mail.ru;* ***Музоватова Яна Юрьевна,*** *магистрант кафедры ИСЭ ФГБОУ ВО «Алтайский государственный технический университет им. И.И. Ползунова», e-mail: yana.muzovatova@mail.ru;* ***Козубаева Людмила Алексеевна,*** *доцент кафедры ТХПЗ ФГБОУ ВО «Алтайский государственный технический университет им. И.И. Ползунова», тел. 29-07-30.*

**УДК 004.7**

## АНАЛИЗ НАГРУЗКИ НА ПРОЦЕССОР ПРИ СОЗДАНИИ НОВЫХ ПОТОКОВ И АСИНХРОННОЙ РАБОТЫ ВНУТРИ ОДНОГО ПОТОКА

Н. В. РОГАЧЕВСКИЙ, К. М. МАЛЕВАН

Современные нагруженные системы с множеством пользователей и задач часто требуют оптимизаций и улучшений не только на уровне кода, но и на уровне выполнения кода. Достаточно часто для ускорения выполнения программы используют создание нового потока, который совместно с другим потоком выполняет вычисления и тем самым ускоряет

выполнение кода в целом, однако в масштабе нагруженных систем необходимо учитывать следующие проблемы:

• создание потока занимает некоторое время, так как при создании потока, должен быть присвоен контекст и передана часть управления;

• каждому потоку нужна память под стек, а соответственно, потребуется больше памяти, чем для одного потока;

• есть крайние ситуации, когда в пуле не останется свободных потоков (если все потоки занять, например ожиданием ответа от базы данных).

Решением данных проблем можно считать более эффективное использование одного потока: Асинхронное выполнение программы.

**Целью работы** является экспериментальное определение эффективности применения асинхронного метода обработки информации по сравнению с синхронным многопоточным методом.

При использовании асинхронности, пока поток ожидает ответ от чего-либо, например, от базы данных, операции Write, Read, Input, Output, он продолжает выполнять следующие операции, а когда ожидаемый ответ будет получен, поток продолжит выполнение не законченной операции. Такой подход позволяет не создавать новые потоки (сохранить время и память), а к тому же и продолжить вычисления во время простоя.

Важно уточнить, что в современных системах новый поток создается, чаще всего, ориентируясь на задержку другого потока, а именно получается такая цепочка: работает основной поток => задержка => поток занят => создать новый => потеря времени. Задержка возникает из-за синхронных запросов.

Для проверки этой гипотезы была составлена модель обращений пользователей к сервису, реализованная на языке Java, которая состоит из серверной и пользовательской части. Пользовательская сторона отправляет много разных рандомизированных hash-строк, а сервер их обрабатывает и возвращает результат. Нагрузка процессора состояла в конвертации полученного сервером hash-тэга в ключ, который далее искался в базе данных и если такой ключ уже существовал, то возвращался объект с этим ключом, а если ключа в базе данных не находилось, то он создавался, и в его поля помещалась информация, полученная сложными для компьютера математическими функциями из присланного hash-тэга. Все эти действия записывались в файл логов программы.

Сначала был реализован асинхронный метод обработки данных, далее была подключена синхронная нагрузка, которая заключалась в том, что пакет сначала должен отобразиться пользователю и только после этого продолжалась обработка других запросов. На рисунке 1 можно увидеть переход между методами. Для большей реалистичности, а также чистоты эксперимента, нагрузка усиливалась днем и снижалась к вечеру

(количество пользователей изменялось), а также была разнообразной при помощи средств рандомизации отправляемых пакетов.

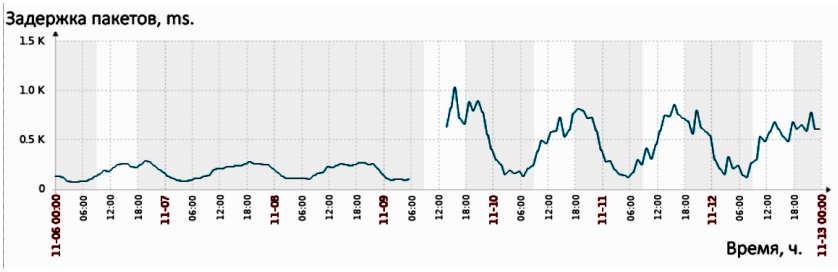



Рисунок 1 – Задержка пакетов при асинхронной (слева) и синхронной (справа) нагрузке

Из графика видно, что в пиковые моменты задержка пакетов составляла 0.75 секунды с синхронной обработкой и 0.25 секунды с асинхронной обработкой. То есть время, через которое пользователь получает ответ на свой запрос, увеличилось в 3 раза. При этом в обоих случаях если какой-либо поток был долго занят и не отвечал, создавался новый, так как иначе с созданной нагрузкой один поток бы не справился. На рисунке 2 представлена нагрузка на процессор в это время.

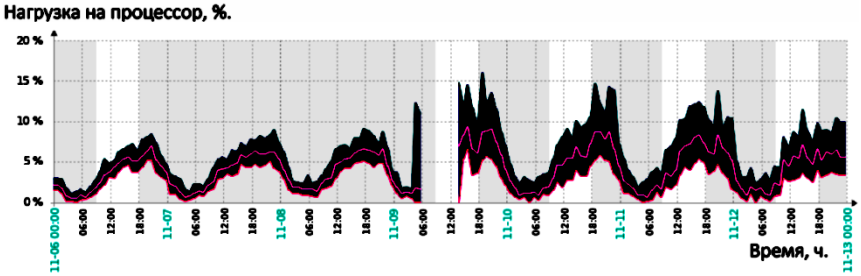



Рисунок 2 – Нагрузка на процессор при асинхронной (слева) и синхронной (справа) нагрузке

Из графика видно, что нагрузка на процессор стала выше при синхронном методе обработки, а также появились резкие возрастания и падения, потому что как раз в эти моменты создаются новые потоки и происходят изменения контекстов. При этом также видно, что нагрузка на процессор не была приближена к 100 %. Это означает, что эксперимент на других вычислительных машинах покажет примерно те же результа-

ты, если вычислительной мощности будет хватать. Сама система, на которой тестировались задержки, была разработана на языке Java, поэтому на других устройствах результаты будут схожими в процентном соотношении.

Наконец, можно оценить последний показатель работы – это среднее время простоя основного потока (рис. 3, 4).

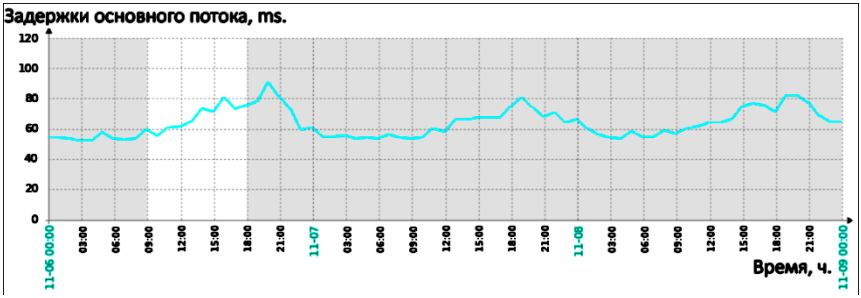



Рисунок 3 – Время простоя основного потока при асинхронной работе

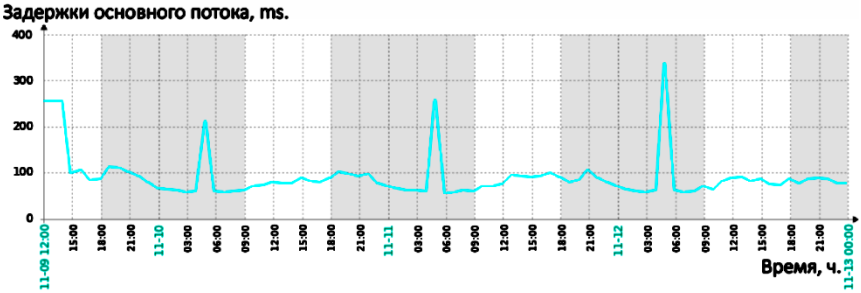



Рисунок 4 – Время простоя основного потока при синхронной работе

Из графика видно, что в целом основной поток стал дольше работать из-за того, что передавал свои данные в другие потоки для обработки, а затем, получая результат, возвращался к продолжению работы с этим результатом.

Таким образом, полученные экспериментально данные позволяют заключить, что в нагруженных системах заметна эффективность от применения метода асинхронной обработки данных. Конечно, без многопоточности в таких системах не обойтись, так как рано или поздно один поток не сможет обрабатывать все запросы. Но вот использование потока в других задачах, пока он ждет ответа по текущей задаче, значительно

повышает эффективность этого потока, поскольку он постоянно занят работой. При этом нет нужны создавать дополнительные потоки, на изменение контекста которых тратится лишнее время и память компьютера.

**Литература. 1.** Дэвис, Алекс Асинхронное программирование в C# 5.0 / Алекс Дэвис. - М.: ДМК Пресс, 2015. – 120 с. **2.** Рассел, Джесси Многопоточность / Джесси Рассел. - М.: VSD, 2012. – 404 с. **3.** Герберт Java 2 v5.0 (Tiger). Новые возможности / Герберт, Шилдт. – М.: СПб: БХВ-Петербург, 2005. – 208 с.

**Реквизиты для справок:** *Россия, 656038, Барнаул, пр. Ленина 46, Алтайский Государственный Университет им. И. И. Ползунова, старшему преподавателю каф. ИВТиИБ, Малеван К.М., тел. 8(983)-542-02-19. E-mail:kristya_22@mail.ru.*

# РАЗДЕЛ 2. ИНФОРМАЦИОННЫЕ СИСТЕМЫ, ИЗМЕРИТЕЛЬНЫЕ И УПРАВЛЯЮЩИЕ КОМПЛЕКСЫ

**УДК 656.13.062:004**

## РАЗРАБОТКА САЙТА АВТОСЕРВИСА

Е. А. БОРОЗДУН, С. Ю. ФЕТИСОВА

Автосервис – это организация, предоставляющая услуги физическим лицам и организациям по диагностике, техническому обслуживанию и ремонту автотранспортных средств.

В функции автосервиса входит:

- информирование клиентов о предоставляемых услугах;
- прием заявок на оказание услуг;
- регистрация новых клиентов;
- выполнение заявок на услуги;
- информирование и отчётность по выполненным заявкам.

Как и любая другая коммерческая организация, автосервис нуждается в рекламе для привлечения клиентуры, поскольку реклама – двигатель торговли и услуг.

Современные инструменты продвижения рекламы очень разнообразны. Чтобы повысить свою конкурентоспособность, организации применяют как типовые рекламные механизмы, так и высокотехнологичные.

Не все автосервисы заказывают разработку сайта, а ведь сайт организации сегодня – очень востребованный рекламный инструмент. Раньше информация об открытии нового магазина или сервисного центра активно передавалась путем «сарафанного радио», рекламные материалы размещались в печатных СМИ, рекламных буклетах, крутилась по телевизору в бегущей строке или мельком упоминалось по радио. Но информация в бегущей строке далеко не всегда отслеживается зрителями (чаще раздражает), радио сегодня востребовано мало, буклет, попавший к незаинтересованному лицу, оказывается в мусорной корзине. С другой стороны, продвигать сайт куда проще и экономичнее, а масштабы распространения рекламной информации несравнимо больше. Каждый владелец компьютера или смартфона ищет интересующую его информацию, например, с помощью таких поисковых систем, как Google, Yandex, Mozilla и т. д. Найти в Интернете сайт автосервиса несложно, но действительно качественных сайтов не так много: на одних бывает представлена неактуальная информация, другие грешат слабым дизайном.

**Целью работы** является создание сайта автосервисного предприятия для повышения эффективности его деятельности, в частности, для увеличения прибыли за счёт привлечения дополнительных клиентов.

Ремонт и обслуживание автомобилей, по сравнению с банковской сферой, сферой страхования или продажей электроники - не самая сложная услуга для продвижения через Интернет. Это связано с невысоким объемом инвестиций. Чтобы сайт приносил результат, нужно проработать структуру сайта, оптимизировать его техническую часть, продумать полезные «фишки», и самое главное – оперативно заполнять его страницы актуальным контентом.

Любой сайт обязательно должен содержать главную страницу или страницу с информацией о компании. Некоторые разработчики делают обе страницы: «Главная» и «О компании», но в таком случае информация на этих страницах не должна дублироваться. Надо заметить, что не стоит нагружать потенциального клиента большим количеством текста, он пришел на сайт с конкретным вопросом и копаться в истории создания компании ему будет, скорее всего, не интересно.

Такие данные, как адрес, контактный телефон, график работы и карта расположения автосервиса должны быть на видном месте, чтобы потенциальный клиент мог понять, насколько удобно для него расположен автосервис и работает ли он в данный момент.

Виды предоставляемых услуг лучше всего расположить на отдельных страницах с соответствующими заголовками. Если клиент интересуется ремонтом топливной системы, то он точно видит, смогут ли ему помочь в решении его вопроса или стоит искать другой автосервис.

Визуальное оформление должно быть приятным для глаз и аккуратным. Приветствуется разборчивый шрифт и чёткие изображения.

На рынке информационных технологий средства web-дизайна и web-программирования представлены достаточно широко.

Одина из самых популярных платформ для создания сайтов – WordPress ― характеризуется большим количеством бесплатных шаблонов, понятным интерфейсом. Сайт на WordPress’е можно создать самостоятельно без базовых знаний языков программирования [1].

Конструктор подходит для небольших площадок с базовым функционалом: блоки информации, форма обратной связи, отзывы клиентов и так далее.

При создании контента страниц сайта необходимо соблюдать определенные правила, описанные ниже.

1. При создании рекламных материалов нужно учитывать, что качество услуг автосервисов далеко не всегда полностью отвечает ожиданиям клиентов.

2. Громкие слоганы, такие как: «У нас самые лучшие запчасти», «Пожизненная гарантия» и т. п., воспринимаются как публичная оферта.

Ведь все мы прекрасно понимаем, что эти слоганы нередко противоречат действительности.

3. Оправдывайте ожидания клиента и держите слово.

4. Зачастую, когда клиент узнает по телефону о какой-либо услуге, ему озвучивают ее стоимость, но в действительности,с учетом нюансов, о которых не сообщается, эта цена оказывается гораздо выше.

5. Используйте реальные фотографии деятельности автосервиса.

Многие предприниматели поддаются соблазну сэкономить время, публикуя вместо оригинальных изображений скачанные в интернете фотографии аналогичных автомобилей в чужих боксах. Когда клиент приедет за услугой, то сразу отметит для себя: «на сайте я видел другое». Это настораживает, не способствуя установлению доверительного контакта и появлению желания продолжать деловые отношения.

Поэтому нашими принципами разработки сайта будут достоверность, полнота и актуальность информации, адекватные дизайн страниц и навигация по сайту (дружественный интерфейс).

На рисунке 1 представлен макет главной страницы сайта. Планируется, что на ней будет представлено главное меню и ссылки на разделы, описывающие услуги по конкретным подсистемам автомобиля.

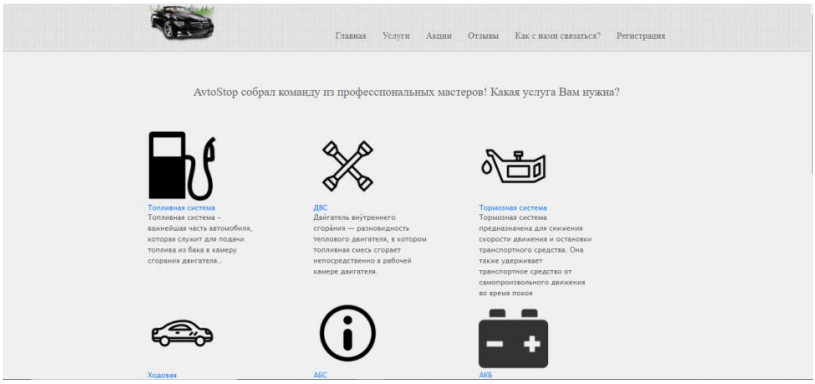



Рисунок 1 – Макет главной страницы

Планируется, что на сайте можно будет не только ознакомиться с предлагаемыми услугами, но и подать заявку на получение одной или нескольких услуг, которая будет зарегистрирована и отслежена. Также можно будет сразу оценить стоимость заказанных услуг и принять решение, подтверждать ли заявку или отказаться.

Автосервис планирует проведение рекламных акций, которые могут способствовать поддержанию интереса к сервису постоянных клиентов и привлечению дополнительных клиентов.

При желании клиент сможет оставить на сайте отзыв о качестве оказанных услуг. С одной стороны, положительные отзывы также позволят привлечь к деятельности автосервиса внимание потенциальных клиентов, с другой – послужат дополнительными данными для руководства предприятия при проведении анализа деятельности сервиса, оценки качества обслуживания и принятия соответствующих управленческих решений.

На рисунке 2 представлен макет страницы с контактной информацией предприятия.

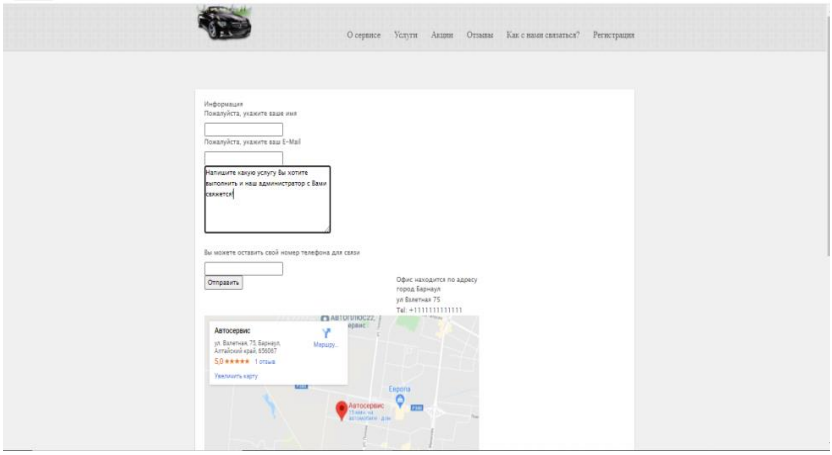



Рисунок 2 – Макет страницы «Как с нами связаться?»

Как показывает практика, разработка подобных автоматизированных информационных систем не требует больших финансовых затрат.

Поскольку услуги автосервиса очень востребованы населением и организациями, руководство предприятия планирует, что затраты на разработку web-сервиса окупятся в течение двух лет.

**Литература. 1.** Как создать сайт на WordPress:[сайт]/ URL.: https://hostiq.ua/wiki/wordpress-guide/ (дата обращения 10.12.2020)

**Реквизиты для справок:** *Россия, 656038, Барнаул, пр-т Ленина, 46, Алтайский государственный технический университет им. И.И. Ползунова, старшему преподавателю кафедры ИСЭ, Фетисовой С.Ю., тел. (385-2) 290-870. E-mail:kamch6336@mail.ru*

**УДК 004.7**

# ВИРТУАЛЬНЫЕ ЛАБОРАТОРИИ КАК СРЕДА ОБУЧЕНИЯ

А. С. ГИРЁВ, Е. В. ШАРЛАЕВ

В настоящее время невозможно представить мир без использования сетевых технологий. Необходимость в высококвалифицированных специалистов, способных поддерживать инфраструктуру, особенно актуальна сегодня, так как все больше компаний стремится к цифровизации.

Обучение специалистов сетевым технологиям не является чем-то простым. Многие учреждения не имеют достаточных финансовых ресурсов для приобретения нескольких видов оборудования, сделав их доступными для обучения будущих специалистов.

Однако, в современных реалиях можно обойтись и без приобретения множества дорогостоящего сетевого оборудования, а осуществить задуманное при помощи виртуального моделирования. Существует множество инструментов сетевого моделирования. Рассмотрим самые популярные на сегодняшний день.

Cisco Packet Tracer (Cisco PT) – один из самых популярных инструментов моделирования сети. Этот уникальный инструмент моделирования позволяет построить топологию сети и воспроизвести ее в современных компьютерных сетях. Он позволяет имитировать соответствующую конфигурацию через интерфейс командной строки [1].

Виртуальная лаборатория Cisco VIRL – еще один продукт фирмы Cisco. Однако подписка на данное программное обеспечение является платной, к тому же есть ограничение на количество виртуальных сетевых узлов.

GNS 3 – популярная программа эмуляции сети, распространяющаяся бесплатно, и позволяющая имитировать взаимодействие сетевых устройств в различных топологиях сетей. GNS 3 обладает полным функционалом эмулируемых устройств, в отличии от Cisco Packet Tracer, где часть функционала недоступна, так как это всего лишь симулятор – программное обеспечение, содержащие упрощения и предназначенное только для воспроизведения внешнего поведения исследуемого объекта. В отличии от продуктов Cisco, GNS 3 позволяет работать и с продуктами других производителей, например MikroTik, Juniper, Fortinet и другие. Однако главным недостатком GNS 3 является отсутствие возможности эмулировать коммутаторы [2].

EVE-NG: Emulated Virtual Environment Next Generation или EVEN-NG — это единственный в своем роде многопользовательский сетевой симулятор. EVE-NG схож по функционалу с GNS3. Есть как платная, так и бесплатная реализация этого инструмента моделирования виртуальной

сети. Бесплатная версия имеет ограничение в 63 узла на лабораторию. Для виртуализации, связывания и настройки сетевых устройств нет необходимости загружать и устанавливать дополнительное приложение помимо сервера. Все проектирование, подключение и управление сетевыми топологиями можно легко выполнить с помощью интегрированного HTML5- клиента. Несмотря на изоляцию среды в виртуальной машине, для работы с ней можно также использовать PuTTY, SecureCRT, Wireshark и другие продукты [3].

EVE-NG поддерживает многопользовательскую работу с лабораторией. Например, с симулятором одновременно может работать студент, выполняющий лабораторную работу, и преподаватель, наблюдающий за корректностью её выполнения.

Системные требования для с представлены в таблице 1 и 2. EVE-NG работает на операционных системах Windows 7,8,10, Linux Desktop, на VMware Workstation 12.5 и выше, VMware Player 12.5 и выше.

Таблица 1 – Минимальные системные требования для EVE-NG

| | Аппаратные требования для ПК | Аппаратные требования для виртуальных машин EVE |
|---|---|---|
| CPU | Intel i5/7 (4 логических процессора), включённая виртуализация в BIOS | 4/1 (число процессоров/число ядер) поддержка Intel VT-x/EPT |
| Ram | 8 Гб | 6 Гб |
| Место на HDD | 40 Гб | 40 Гб |
| Network | Наличие сетевой карты | VMware NAT или соединение типа мост |

Таблица 2 – Рекомендуемые системные требования для EVE-NG

| | Аппаратные требования для ПК | Аппаратные требования для виртуальных машин EVE |
|---|---|---|
| CPU | Intel i7 (8 логических процессоров), включенная поддержка виртуализации BIOS | 8/1 (Число процессоров/Число ядер) поддержка Intel VTx/EPT |
| Ram | 32 Гб | 24 Гб |
| Место на HDD | 200 Гб | 200 Гб |
| Network | Наличие сетевой карты | VMware NAT или соединение типа мост |

Минимальные требования позволяют запускать в EVE-NG только маленькие лаборатории и общая производительность работы симулятора будет сильно зависеть от числа узлов, задействованных в схеме.

Важным фактором, который делает EVE-NG одним из лучших инструментов моделирования сети, является то, что приложение экономит

время, позволяя вносить изменения в топологию сетей во время их одновременного запуска. Кроме того, симулятор подходит как для Ethernet, так и для последовательных интерфейсов.

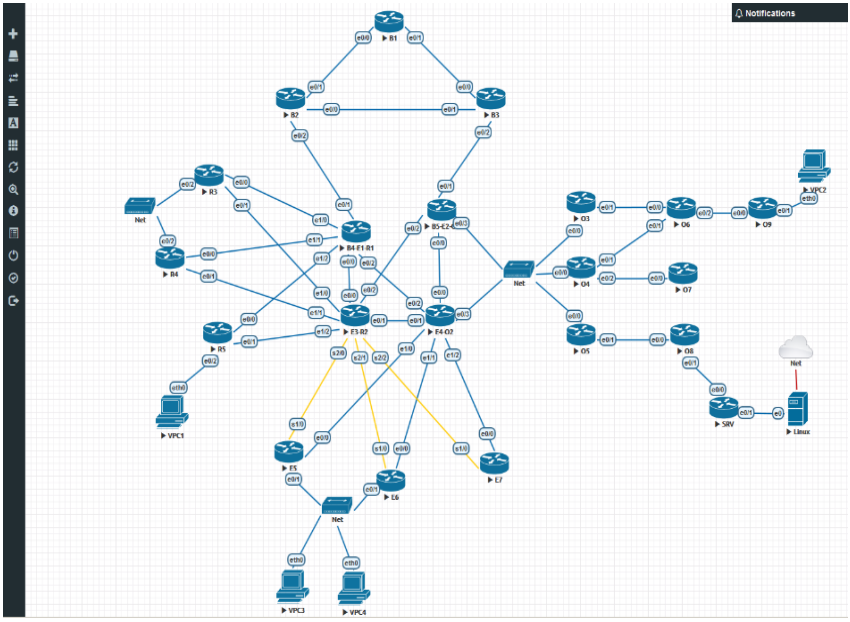



Рисунок 1 – Пример построения сети в EVE-NG

Моделирование позволяет приобрести профессиональные навыки и получить опыт работы с сетью без серьезных аппаратных вложений. На сегодняшний день одним из лучших решений для обучения специалистов работе с сетевыми технологиями является EVE-NG.

**Литература: 1.** Топ 5 инструментов моделирования сетей в 2020 году. – [Электронный ресурс]. – Режим доступа: https://wiki.merionet.ru/seti/34/ top-5-instrumentov-modelirovaniya-setej-v-2020-godu/. **2.** Основы GNS3. Обзор – [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/ 266503/. **3.** Имитированные Cisco, идентичные натуральным. – [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/494504/.

**Реквизиты для справок:** *Россия, 659305, Барнаул, пр. Ленина 46, Алтайский государственный технический университет им. И. И. Ползунова, доценту кафедры «Информатика, вычислительная техника и информационная безопасность», Шарлаеву Е.В. E-mail: sharlaev@mail.ru*

**УДК 681.382**

# АВТОМАТИЗИРОВАННЫЙ РЕАНИМАЦИОННЫЙ КОМПЛЕКС ДЛЯ НЕОНАТОЛОГИИ

М. А. ХАЗАМОВА, З. А. КАМИЛОВА

Одной из важнейших задач сохранения здоровья новорожденного с патологией в первые дни жизни является обеспечение соответствующего микроклимата в зоне его обитания с необходимыми параметрами температуры и влажности [1]. Для этих целей в настоящее время используются специализированные неонатологические реанимационные комплексы, снабженные специальной системой термо- и влагорегулирования. Данная система, как правило, включает в себя кондиционирующую аппаратуру, дающую возможность осуществлять как нагрев, так и охлаждение объема кювета с ребенком. Для нагрева обычно используются электрические нагреватели, а для охлаждения - компрессионное оборудование. В большинстве случаев, подобные системы кондиционирования громоздки, имеют высокую стоимость, не обеспечивают должную точность поддержания микроклимата в кювете с новорожденным.

В этой связи авторами предлагается к рассмотрению неонатологический реанимационный комплекс, в котором функции источника теплоты выполняют термоэлектрические батареи [2]. Структурная схема комплекса изображена на рис. 1.

В состав комплекса входят: передвижной стол 1 с противопролежневым матрасом 5 (6 – ячейки в матрасе, заполненные гелем 7), размещенный в инкубаторе 2, снабженном верхней откидной 3 и боковой выдвижной 4 крышками; блок термоэлектрических батарей 9, разделенный на секции, с рабочими спаями 8 и опорными спаями 10, снабженными радиаторной системой 11; приспособление для гипотермии головы 12, выполненное в виде полого стакана 13 со сферической внутренней полостью 14, на которую также нанесена гелевая прослойка 15; дополнительный термоэлектрический модуль 17 с рабочими спаями 16 и опорными спаями, контактирующими с жидкостным теплообменником 18; датчики температуры 19 и блок управления 20 для регулирования микроклимата в инкубаторе.

Новорожденного размещают на матрасе в инкубаторе и с помощью терморегулирующей аппаратуры, включающей в себя блок термоэлектрических батарей и управления выставляют в нем необходимые параметры микроклимата. В зависимости от сигналов с датчиков данные параметры контролируются и регулируются путем включения и отключения секций блока термоэлектрических батарей на протяжении всего вре-

мени нахождения новорожденного в инкубаторе. Для дополнительной гипо- и гипертермии головы ребенка используется дополнительный термоэлектрический модуль.

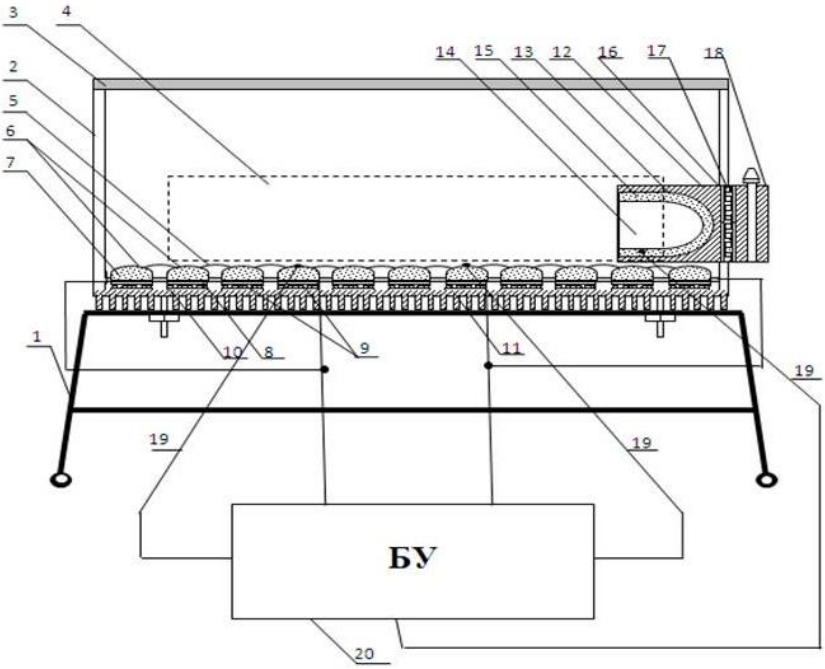



Рисунок 1 – Структурная схема автоматизированного реанимационного комплекса для новорожденных

Данная система обеспечения микроклимата в кювете с новорожденным отличается малыми габаритными размерами, относительно невысокой стоимостью и высокой точностью регулирования параметров температуры.

**Литература. 1.** Шабалов, Н.П. Неонатология / Н.П. Шабалов. М.:МЕДпресс-информ, 2009. 2**.** Пат. 2494715 Рос. Федерация: МПК A61G 10/02, A61G 11/00, Реанимационный комплекс для новорожденных/ Исмаилов Т.А., Хазамова М.А., Евдулов О.В., Камилова З.А.; заявитель и патентообладатель ФГБОУ ВПО «Дагестанский государственный технический университет». - №2012102167/14; заявл. 23.01.2012; опубл. 10.10.2013, Бюл. № 28.

**Реквизиты для справок:** *Россия, 367030, Махачкала, пр. Им. Шамиля 70, ФГБОУ ВО «ДГТУ»,ассистенту, Камиловой З.А., тел. (8722) 62-82-69. E-mail:zuri2408@mail.ru*

**УДК 543.54**

# ОБЗОР МЕТОДОВ ИЗМЕРЕНИЯ МАССОВОЙ КОНЦЕНТРАЦИИ БЕНЗ(А)ПИРЕНА В ПИЩЕВЫХ ПРОДУКТАХ

Е. А. ЕНГИБАРЯН, В. В. НАДВОЦКАЯ

Бенз(а)пирен является суперэкотоксикантом 1-го класса опасности. Вещество может содержаться в любой пище, приготовленной при неполном сгорании органических веществ, то есть на гриле или при жарке. Массовая доля бенз(а)пирена в продуктах питания допускается до 1 мкг/кг и определена такими нормативными документами, как технический регламент Таможенного союза "О безопасности пищевой продукции", ГОСТы, регламент комиссии ЕС, и пр. Поскольку вещество является биоаккумулирующим соединением, то его выявление в пищевых продуктах крайне важно для сохранения здоровья и жизни человека. Жиросодержащие продукты питания абсорбируют бенз(а)пирен при транспортировке, хранении, в технологическом процессе изготовления, поэтому актуальным является исследование, в первую очередь, жиросодержащих продуктов – растительные масла, майонез, жареная пища [1].

**Цель работы** – обзор методов измерения бенз(а)пирена в пищевых продуктах.

В настоящее время методы обнаружения бенз(а)пирена разнообразны, выбор метода зависит от чувствительности средства измерения, диапазона измерения массовой доли бенз(а)пирена для исследования различных объектов: от снега на улице до масла, оставшегося после жарки котлет, от питьевой воды до промышленных отходов и т.д. В настоящее время для определения бенз(а)пирена применяют в основном газовую хроматографию-масс-спектрометрию, ацетилированную бумажную хроматографию, флуоресцентную спектрофотометрию, тонкослойную хроматографию, высокоэффективную жидкостную хроматографию и другие методы [2].

Достаточно традиционным методом измерений является флуоресцентная спектрофотометрия, так как результаты измерения данным методом стабильны. Вследствие этого флуоресцентная спектрофотометрия стала национальным стандартным методом, указанным в китайских стандартах гигиены пищевых продуктов. Оптимальный диапазон определения массовых концентраций бенз(а)пирена в исследуемых пищевых продуктах составляет 0,0002-0,005 мг/кг. Данный метод включает в себя этапы экстракции органических растворов, экстракции омыления, очистки и разделения ацетила и других форм, количественной флуоресцентной спектрофотометрии [2].

Метод высокоэффективной жидкостной хроматографии (ВЭЖХ)

включает в себя твердофазную экстракцию и хроматографию с флуориметрическим детектированием (HPLC-FLD) - комбинированное определение содержания бенз(а)пирена в пищевых продуктах в соответствии с различными условиями экстракции образца. Достоинства данного метода измерения - простой метод предварительной обработки, минимальное время анализа, хорошая чувствительность и точность. Поэтому он хорошо подходит для определения бенз(а)пирена во всех видах пищевых продуктов в диапазоне величин массовой доли бенз(а)пирена в анализируемых продуктах 0,0001-0,002 мг/кг [2].

Тонкослойная хроматография использует неподвижную фазу в виде пластинки с различными сорбентами для разделения веществ в составе исследуемой пробы. Минимальное количество обнаружения массовых концентраций бенз(а)пирена в исследуемых пищевых продуктах составляет 0,005 мг/кг.

Газовая хроматография-масс-спектрометрия в дополнение к вышеуказанным методам обнаружения бензопирена тоже может быть использована для определения характеристик бенз(а)пирена.

Проведем эксперимент – исследование пробы растительного масла, на котором 60 минут жарили котлеты, на наличие бенз(а)пирена. Для исследования используем метод ВЭЖХ. Хроматографическая установка представлена на рис. 1. Для проведения экспериментов использовалось следующее оборудование: стандартный набор лабораторной посуды, весы аналитические, центрифуга, пресс-форма ПФ-13, «Люмахром» с флуориметрическим детектором «Люмахром ФЛД 2410 Флюорат-02-2М», колонка C18 Kromasil 2,1x150, зерно 6,2, микрошприц на 100 мкл [3].

Рисунок 1 – Хроматографическая установка

В настоящей работе содержание бензо(а)пирена в воде было определено при скорости потока 1 мл/мин и температуре колонки 25 ℃ с использованием дихлорметана в качестве экстрагента и W(ацетонитрил): w (вода) = 85 : 15 в качестве подвижной фазы.

Попробуем обнаружить по хроматограмме наличие бенз(а)пирена в пробе масла после жарки на нем покупных котлет. Пик бенз(а)пирена обнаруживается с помощью специального программного обеспечения (ПО) «МультиХром» компании Люмекс.

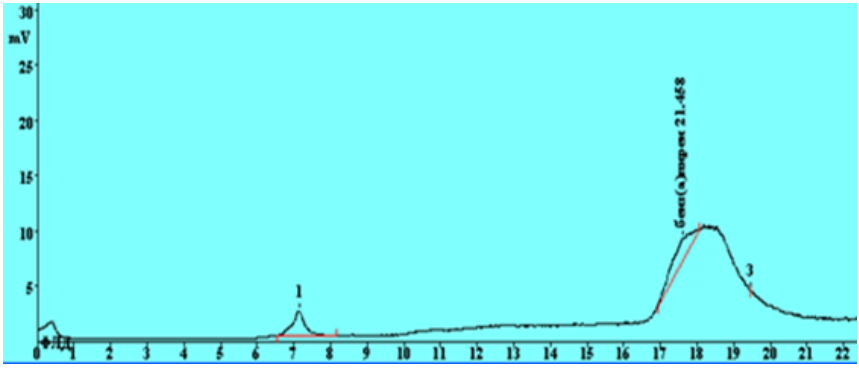



Рисунок 2 – Хроматограмма пробы подсолнечного масла после его использования

Бенз(а)пирен при использовании метода ВЖЭХ можно отличить от других веществ, содержащихся в исследуемой пробе растительного масла, по характерному изображению пика на хроматограмме (рис. 2). Биоаккумулянт проявляется на хроматограмме в период 17-22 минуты проведения эксперименты. Полученный результат превышает более чем в 100 раз ПДК бенз(а)пирена. Это подтверждает необходимость проведения исследований содержания бенз(а)пирена и мониторинг содержания вредных веществ в пищевых продуктах в целом.

**Выводы:** в работе проведен обзор методов измерения бенз(а)пирена в пищевых продуктах, а также был проведен эксперимент по обнаружению в пробе использованного подсолнечного масла и визуализация хроматограммы при помощи специального ПО «МультиХром».

**Литература: 1.** Надвоцкая В.В., Горелова О.М., Котлубовская Т.В., Андреева А.А., Шапоренко А.Г. Экстракция бенз(а)пирена из проб воды для исследования методом ВЭЖХ // Ползуновский альманах. – Барнаул: Изд-во АлтГТУ, 2019. – №4. – С. 77-80. **2.** ГОСТ Р 51650-2000 Методы определения массовой доли бенз(а)пирена [Электронный ресурс] – М.: ИПК Издательство стандартов, 2000. – Режим доступа: http://docs.cntd.ru/document/gost-r-51650-

2000. – Загл. с экрана (дата обращения 01.12.2020). **3.** ГОСТ 32123-2013 (ISO 15302:2007) Жиры и масла животные и растительные. Определение содержания бенз(а)пирена. Метод с применением высокоразрешающей жидкостной хроматографии с обратной фазой. – АО "Кодекс", 2013. – 62 с.

**Реквизиты для справок:** *Россия, 656038, Барнаул, ул. Ленина 46, АлтГТУ им. И.И.Ползунова, доцент Надвоцкая В..В., тел.: (3852) 290-823, E-mail: nadvotskaya7@mail.ru*

**УДК 543.54**

## ИССЛЕДОВАНИЕ МАССОВОЙ КОНЦЕНТРАЦИИ БЕНЗ(А)ПИРЕНА В ПРОДУКЦИИ МАСЛОЗАВОДА МЕТОДОМ ВЫСОКОЭФФЕКТИВНОЙ ЖИДКОСТНОЙ ХРОМАТОГРАФИИ

В. В. НАДВОЦКИЙ, Т. В. КОТЛУБОВСКАЯ

Растительные масла широко используются в питании человека – для приготовления кулинарных блюд, изготовления консервов, в пищевой промышленности и непосредственно в пищу. К факторам, которые обусловливают сферу использования растительных масел, относятся качество сырья и технология их производства [1]. Свойства растительного масла и содержание в нем вредных веществ зависят от чистоты выращенных семян подсолнечника, способа их хранения и переработки. Если за качеством технологии получения масла из семян подсолнечника – холодного прессования, горячего отжима, рафинирования – производители смотрят на производстве, то контроль использования посевных площадей рядом с трассой, способ сушки, хранения семян в хозяйствах остается под вопросом. Например, при длительной сушке на элеваторах при использовании «жестких» температур в семенах образуется бенз(а)пирен (канцероген первого класса опасности по классификации ВОЗ). В связи с этим маслозавод ООО «Эскадо» обратился к представителям АлтГТУ с предложением комплексной проверки материала, используемого для получения растительного масла из семян подсолнечника, закупаемого в различных районах Алтайского края.

**Цель работы** – исследование массовой концентрации бенз(а)пирена в продукции маслозавода методом высокоэффективной жидкостной хроматографии.

Этапы пробоподготовки предполагается проводить в химической лаборатории кафедры «Химическая техника и инженерная экология» АлтГТУ. Далее работы будут продолжаться в лаборатории хроматографических исследований кафедры информационных технологий.

Алтайский край входит в перечень регионов, в которых производит-

ся массовое выращивание подсолнечника. Условно Алтайский край делят на семь аграрных зон, которые поставляют материал на завод (рис. 1). Растительные масла одного товарного наименования, но выделенные из семян растений, выращенных в разных районах, отличаются по показателям. Поэтому при проведении исследований будем пользоваться зональным разделением [2].


Рисунок 1 – Аграрные зоны Алтайского края

Для определения бенз(а)пирена используются различные методы и средства измерения, но поскольку наиболее информативным методом определения массовой доли бенз(а)пирена является высокоэффективная жидкостная хроматография с флуориметрическим детектированием, то проведение начальных исследований проводилось согласно ГОСТ 32123-2013 (ISO 15302:2007) «Жиры и масла животные и растительные. Определение содержания бенз(а)пирена. Метод с применением высокоразрешающей жидкостной хроматографии с обратной фазой» [3].

Процесс проведения работы поэтапный. Первый этап подготовительный, второй - непосредственная работа с самим хроматографом. На подготовительном этапе работа ведется с подготовкой пробы к анализу. По методике необходимо выделить бенз(а)пирен из образца растительного масла путем щелочного гидролиза. Затем отделить исследуемое вещество. Образец помещают в делительную воронку и добавляют гексан объемом 20–25 мл. Необходимо перемешать жидкости специальным оборудованием в течение двух минут. После появления границы раздела двух фаз приступаем к удалению нижнего слоя.

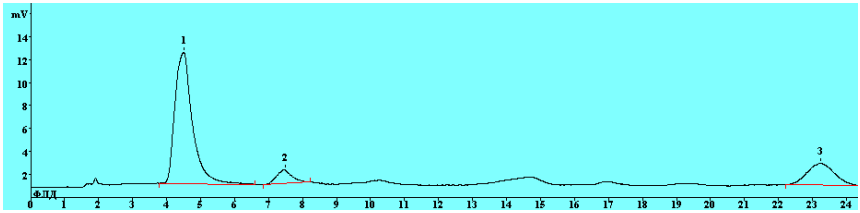



Рисунок 2 – Хроматограмма пробы №1

Второй этап работы предполагает работу с прибором. Хроматограф – это совокупность приборов: флюорат, насос и персональный компьютер (ПК). Также в данный этап входит подготовка подвижной фазы. При проведении измерений подвижной фазой являлась смесь ацетонитрила и дистиллированной воды в отношении 4:1. Включив все необходимые приборы, выполняется промывка системы подвижной фазой. Как только линия отклика детектора на ПК станет стабильной, можно проводить анализ. На рис. 2 представлена хроматограмма, полученная при обработке результатов пробы №1 (масло, полученное из семян хозяйства "Новичихинское", Приалейская степь).

После получения хроматограммы осуществляется расчет концентрации в пробе.

При обработке пробы (рис. 2) бенз(а)пирен не обнаружен. Можно предположить, что это связано с чистотой материала пробы и соблюдением технологии изготовления растительного масла из семян подсолнечника Новичихинского хозяйства.

На основе полученных данных делаем выводы о пригодности метода высокоэффективной жидкостной хроматографии на основе флуориметрического детектирования для исследования массовой концентрации бенз(а)пирена в продукции маслозавода методом высокоэффективной жидкостной хроматографии.

Выводы: начальная цель исследования достигнута – в работе представлен алгоритм проведения исследований массовой концентрации бенз(а)пирена в продукции маслозавода методом высокоэффективной жидкостной хроматографии. В дальнейшем необходимо получить зависимость чистоты проб получаемого масла от районов Алтайского края и сделать вывод о качестве выращиваемого подсолнечника в различных регионах Алтайского края.

**Литература: 1.** Кищенко В.А. Определение токоферолов в маслах и маслосодержащих продуктах методом высокоэффективной жидкостной хроматографии // Масличные культуры, №2(137), 2007. – Режим доступа: https://readera.org/opredelenie-tokoferolov-v-maslah-i-maslosoderzhashhih-

produktah-metodom-142150823 (дата обращения 10.11.2020). **2**. Смолякова В.Л., Крылова А.П. Влияние качества сырья на качество растительного масла // Современные инновации: тенденции и перспективы современной науки, №8(22), 2017. - (Россия. Москва. 18 сентября 2017). – Режим доступа: https://moderninnovation.ru/h/blizhajshij-nomer/tekhnicheskie-nauki99.html?start=40 (дата обращения 15.11.2020). **3.** ГОСТ 32123-2013 (ISO 15302:2007) Жиры и масла животные и растительные. Определение содержания бенз(а)пирена. Метод с применением высокоразрешающей жидкостной хроматографии с обратной фазой. – АО "Кодекс", 2013. – 62 с.

**Реквизиты для справок:** *Россия, 656038, Барнаул, ул. Ленина 46, АлтГТУ им. И.И.Ползунова, доцент Котлубовская Т.В., тел.: (3852) 290-913, E-mail: tavikot2010@mail.ru*

**УДК 331.1:004.02**

## ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ПРОЦЕССА ВНЕДРЕНИЯ МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ ПУТЕМ ПРИМЕНЕНИЯ МОТИВАЦИОННОГО ПРОГРАММНО-ЦЕЛЕВОГО ПОДХОДА

А. И. ПОПКОВА

В 2020 году в связи с пандемией новой коронавирусной инфекции существенно возросла роль медицинских информационных систем, систем телемедицинских консультаций и интеллектуального анализа медицинской информации. В зависимости от того, насколько эффективно современные информационные технологии используются врачами, руководителями медицинских организаций, управляющими органами, зависит качество медицинской помощи населению.

Комплексный анализ данных о состоянии пациентов, динамике и результативности обращений к врачам, диагностика здоровья на основании машинного обучения, аналитика эффективности медицинских производственных процессов являются глобальными задачами интегрированных медицинских информационных систем (МИС). МИС должны быть позиционированы на рынке как целостный продукт, позволяющий на качественно новом уровне осуществлять руководство деятельностью медучреждения и оказывать медицинские услуги из единой информационной среды [1].

Несмотря прогрессивность МИС, их внедрение тормозится рядом факторов:

- низкая квалификация пользователей МИС в сфере IT-технологий;

- отсутствие мотивации работников сферы здравоохранения к овладеванию инструментальными средствами МИС из-за боязни увольнения из-за передачи части выполняемого функционала в МИС;

- слабая материальная IT-база большинства государственных медицинских учреждений;

- отсутствие интегральных решений при информатизации здравоохранения [2].

МИС требуют для своего внедрения всесторонней вовлеченности управленческого персонала, IT-специалистов, врачей, младшего медицинского персонала, по сути, всех работников, осуществляющих сбор и обработку медицинских данных. При этом при реализации функций управления в МИС рекомендуется применение специальных управленческих методов, ориентированных на рост мотивации людей к работе в новых IT-системах. При разработке и внедрении МИС предлагается мотивационный программно-целевой подход (МПЦП) [3]. Этапами МПЦП являются:

1. Предварительный системный анализ текущего уровня и перспектив развития IT-технологий и внедрения МИС в государственной медицинской организации;

2. Структурирование древовидной иерархии глобальной и локальных этапных целей управленческого процесса внедрения МИС для автоматизации процесса сбора и обработки медицинских данных;

3. Проектирование системы достижения глобальной и локальных целей процесса внедрения МИС с учетом выстраивания последовательности мероприятий;

4. Разработка мероприятий, обеспечивающих мотивационную и технологическую подготовку экторов медицинского государственного учреждения к внедрению МИС методом «step-by-step» в логике «хочу-могу-исполняю-получаю»;

5. Формализация критериальных характеристик эффективности внедрения МИС в деятельность медицинского учреждения, разработка прозрачных алгоритмов расчета.

МПЦП предусматривает наличие, регулирование и контроль достижения образцов деятельности для реализации локальных целей [4].

Процесс внедрения МИС в государственном медицинском учреждении должен начинаться с формирования мотивации экторов в процессе системного анализа управленческих процессов. Иерархическая структура целей позволяет детализировать комплекс мероприятий по достижению генеральной цели. Одновременно выявляются негативные факторы риска достижения цели и предусматриваются методы реагирования на риски успешного внедрения МИС.

Иерархичность достижения целей означает, что цель более высокого уровня иерархии может быть достигнута только при наличии достижения целей низлежащих уровней с приемлемым качеством исполнения.

МПЦП позволяет пошагово формировать мотивацию экторов через обучение и контроль полученных компетенций методом «step-by-step», обеспечивая стабильную причинно-следственную связь между психологической, технологической подготовкой экторов и достижением целей внедрения МИС.

Если главной целью является успешное внедрение МИС, то администрации государственного медицинского учреждения необходимо обеспечить не только технологическую готовность к процессу, но и сформировать подцели для каждого субъекта и объекта управления с учетом когнитивного, деятельностного и креативного аспектов овладения новой МИС.

Функции управления внедрением должны быть сформулированы с учетом мотивации, познавательной деятельности, адаптации и контроля деятельности экторов.

Результаты внедрения МИС зависят от активности и мотивации экторов при овладении новой МИС, на которые влияет психологическая готовность и наличие стимульных ситуаций. Главным назначением стимульных ситуаций является обеспечение воздействия на сферу познания, эмоций и чувств [4].

Мероприятия по внедрению МИС предлагается описывать в виде норм-образцов деятельности по достижению цели по типу: для достижения цели Цi необходимо выполнить Д1i, Д2i,...).

Таким образом, применение МПЦП, предполагающего последовательность и систематизацию шагов для каждого уровня иерархии, формирование психологической готовности экторов к внедрению МИС, создает предпосылки для роста эффективности внедрения МИС и новых управленческих решений в медицинском учреждении.

**Литература. 1.** Сухомлин, В. А. Введение в анализ информационных технологий/ В.А. Сухомлин. − М.: Горячая линия - Телеком, 2016. - 432 с **2.** Парахонский А.П. Использование новейших информационно-коммуникационных технологий в медицине и здравоохранении/А.П. Парахонский, А.П. Миносян//Успехи современного естествознания. - 2009. № 7. - С. 83 **3.** Горячих, А.И. Практический уровень моделирования содержания обучающих программ в логике мотивационного программно-целевого управления /А.И. Горячих - Перспективы науки №6(08) – Тамбов, 2010 – С. 20-23. **4.** Шалаев, И. К. Повышение эффективности управления образованием: Методические рекомендации /И.К. Шалаев - г. Барнаул: АКИПКРО, 2007. - 108с.

**Реквизиты для справок:** *656038, Российская Федерация, Алтайский край, г. Барнаул, пр. Ленина, 46 ,доценту кафедры информатики, вычислительной техники и информационной безопасности Попковой А.И.., тел +7 902 -143-9635. E-mail:goryac-anna@yandex.ru*

**УДК 621.362: 537.322**

## АВТОМАТИЗИРОВАННАЯ СИСТЕМА ДЛЯ ЛЕЧЕНИЯ ВОСПАЛИТЕЛЬНЫХ ЗАБОЛЕВАНИЙ ПАРОДОНТА

О. В. ЕВДУЛОВ, С. Г. МАГОМЕДОВА, И. Ш. МИСПАХОВ

Одним из эффективных методов лечения воспалительных заболеваний пародонта, имеющий все большее распространение на сегодняшний день в стоматологической практике, является метод, основанный на локальном замораживании пораженных участков при температуре до -40 °С. Подобное воздействие на зону пародонта имеет противовоспалительное, гемостатическое, спазмолитическое, анальгезирующее действие, улучшает трофик тканей, стимулирует репаративно-трофические реакции.

Для реализации таких процедур применяются аппаратные средства, работающие на основе жидкого азота. Среди промышленно выпускаемых приборов, предназначенных для данных целей, используются системы Ятрань, Cryolaser, CryoSkin, КриоИней, Азокриод, АЛК-Криомед, Криоэлектроника-1 и др. Общим недостатком перечисленных технических средств является наличие криоагента, возможности и сроки хранения которого вдали от специальных хранилищ ограничены. Другим недостатком этих приборов является неудобство проведения лечебных процедур (криоагент может попасть на близлежащие ткани), а также невозможность контролировать уровень теплового воздействия (возможно либо чрезмерная, либо недостаточная заморозка области пародонта).

В этих условиях представляет интерес разработка новых типов приборов и систем для реализации метода локального замораживания области пародонта.

Авторами предлагается автоматизированная система для локального замораживания области пародонта, исполнительным элементом в которой является термоэлектрический охладитель [1], отличающаяся высокой надежностью, эффективностью и комфортностью проведения процедур.

Конструкция системы представлена на рис. 1. В состав прибора входит воздействующий элемент 1 и блок регулирования температуры 2. Воздействующий элемент 1 состоит из двух высокотеплопроводных пластин 3, одной поверхностью контактирующих с зоной пародонта через

образованные с помощью пленки 4 специальные контейнеры 5, заполненные высокотеплопроводным гранулятом, а второй с термоэлектрическими модулями 6, оснащенными радиаторной системой 7. Воздействующий элемент 1 с помощью крепежного приспособления 8 образует жесткую конструкцию с возможностью регулирования расстояния между пластинами 3 и областью пародонта. При проведении процедур система фиксируется на соответствующей области пародонта и запитывается постоянным электрическим током, величина которого регулируется блоком регулирования температуры 2.

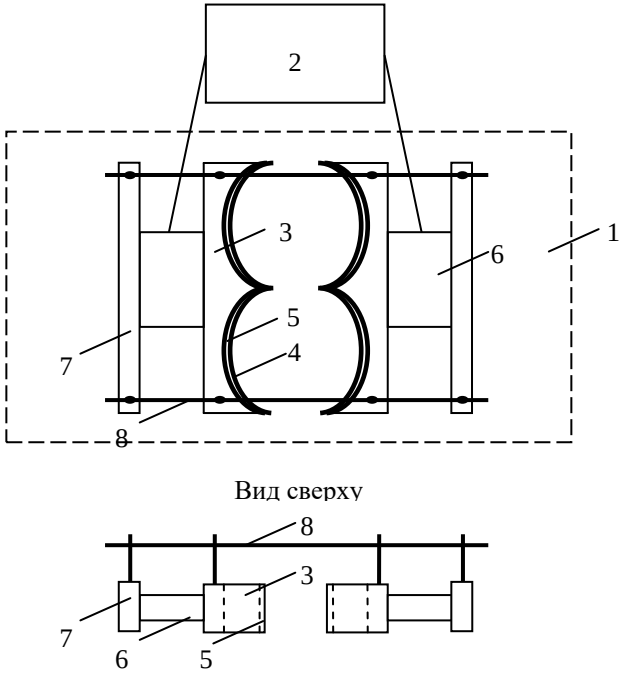



Рисунок 1 – Конструкция автоматизированной системы для лечения воспалительных заболеваний пародонта

Произведен расчет прибора. Установлено, что необходимый уровень проведения процедур, может быть реализован при холодопроизводительности термоэлектрических модулей 6000 Вт/м$^2$. При этом время выхода на режим системы составит примерно 3 мин.

**Литература**. **1**. Исмаилов Т.А., Евдулов О.В., Аминов Г.И., Юсуфов Ш.А. Приборы для локального температурного воздействия на человеческий организм // Известия вузов. Северо-Кавказский регион. Технические науки. – 2003. – №2. – С. 3-6.

**Реквизиты для справок:** *Россия, 367026, Махачкала, пр. Имама Шамиля 70, ФГБОУ ВО "Дагестанский государственный технический университет", кафедра теоретической и общей электротехники, к.т.н., доцент Евдулов О.В. – ole-ole-ole@rambler.ru, тел.(8722)628269.*

**УДК 004.896**

## ПРИМЕНЕНИЕ «БЕЗЛЮДНОЙ» ТЕХНОЛОГИИ В ПЕРИОД ПАНДЕМИИ COVID-19

А. А. АРБУЗОВА, Е. С. КУСТОВА

Наиболее существенным событием, оказавшим влияние не только на 2020 год, но и, скорее всего, на ближайшее будущее, стала пандемия COVID- 19.

Кроме тяжелых симптомов протекания заболевания инфекция накладывает целый ряд ограничений на различные сферы жизнедеятельности людей и изменяет традиционные бизнес-процессы. Одним из основных ограничений является ограничение контактов между людьми. В работе активно используются дистанционные подходы, а в личной жизни – мессенджеры и социальные сети. Однако есть такие сферы, где присутствие человека является необходимым. Например, медицина. Врачам, в силу своей профессиональной деятельности, постоянно приходится контактировать с пациентами. При этом существуют так называемые «безлюдные» технологии [1-3], которые могут помочь медикам осуществлять профилактику, диагностику и лечение инфекции, помочь справиться с нехваткой кадров в больницах, обеспечить повышенную безопасность медперсонала при лечении пациентов и облегчить их социальное дистанцирование.

Так, например, отечественная компания «Promobot» предлагает использование автономного робота Promobot V.4 (см. рис. 1), который может провести экспресс-опрос пациентов и тем самым помочь определить, есть ли у человека первичные симптомы COVID-19. Это особенно необходимо для того, чтобы постоянно привлекать внимание населения к необходимости защиты от инфекции и информировании о методах определения заболевания.

Рисунок 1 – Внешний вид автономного робота Promobot V.4

Данный робот обладает функциями распознавания лиц и голоса, генерацией ответов на общие вопросы и поддержание разговора с человеком, может хаотично менять свое положение и автоматически подъезжать к людям [4]. Применять его можно как в помещениях больниц для общения с пациентами, так и на открытых площадках, например, для проведения просветительской деятельности.

Одним из опасных этапов работы для медицинских сотрудников является операция взятия мазка из горла потенциально заболевшего пациента, т.к. высок риск заражения. Китайские учёные из Гуанчжоуского института по здоровью дыхательных органов и инженеры Шэньянского института автоматизации при Академии наук разработали мобильный манипулятор для осуществления данной медицинской процедуры (см. рис. 2). Основной рабочий инструмент робота - механическая рука, в которую встроен эндоскоп. Он направляется в горло пациента и показывает трехмерную анатомическую картину в высоком разрешении. Также манипулятор дистанционно получает команды от медика и берёт мазок из горла [5].

Рисунок 2 – Роботизированная механическая рука для взятия мазка из горла потенциально заболевшего пациента

В больницах ряда стран: Китая (Ухань), Италии (Сирколо в Варесе), США, Германии, Польши применяют гуманоидных роботов CloudMinds 5G (см. рис. 3). Данные роботы предназначены в большей степени для организации обмена информацией между медицинским персоналом и пациентами. А также управляют потоками пациентов [6].

а б

Рисунок 3 – Роботы CloudMinds 5G

Такие роботы (см. рис. 3а) могут общаться с поступающими в медицинское учреждение больными, направлять их на дезинфекцию рук и выдачу защитных масок, задавать соответствующие вопросы для дальнейшей сортировки нуждающихся в медицинской помощи.

Также роботы (см. рис. 3б) находятся у постели пациентов, круглосуточно контролируют показатели жизнедеятельности и передают их лечащим врачам.

Применение таких роботов дает возможность медицинским учреждениям ограничить количество прямых контактов врачей и медсестер с пациентами, снизить риск прямого и перекрестного заражения, количества расходных материалов (масок, костюмов и дезинфекторов).

В заключении необходимо отметить, что рассмотренная «безлюдная» технология, за счет применения разнообразных роботов, действительно может существенно помочь медикам и пациентам медицинских учреждений во время эпидемии инфекционных заболеваний, когда контакты между людьми необходимо ограничить. Она является достаточно перспективной, но при этом остается открытым вопрос возможности широкого внедрения данной технологии в лечебных заведениях в современных реалиях. Поскольку для ее полноценного использования требуются существенные финансовые вложения и дополнительные компетенции у медицинских работников.

**Литература. 1.** Морозов А.Д. Беспилотная авиация на службе МЧС России / А.Д. Морозов, А.А. Арбузова // Сборник материалов IX Всероссийской научно-практической конференции «Надежность и долговечность машин и механизмов». – 2018. С. 164-167. **2.** Морозов А.Д. Исследование возможности использования биспилотных летательных аппаратов в деятельности МЧС России / А.Д. Морозов, А.А. Арбузова // Сборник научных трудов XIII Международной научно-практической конференции «Современные инструментальные системы, информационные технологии и инновации». – 2018. С. 140-143. **3.** Арбузова А.А. Биомеханический костюм как средство повышения функциональных показателей пожарных и спасателей /А.А. Арбузова // Сборник материалов II Всероссийской национальной научной конференции студентов, аспирантов и молодых ученых «Молодежь и наука: актуальные проблемы фундаментальных и прикладных исследований». – 2019. С. 199-202. **4.** Официальный сайт компании Promobot. Сервисный робот для бизнеса // https://promo-bot.ru/production/promobot-v4/. **5.** Ефимов А.Р., Гонноченко А.С., Пайсон Д.Б., Дюгованец Ю.И., Цыганков В.А., Морошкин С.Д., Левицкий Б.И., Вольнова Т.А., Зуев А.В. Практическое применение роботов и сопутствующих технологий в борьбе с пандемией COVID-19 // Робототехника и техническая кибернетика. 2020. Т. 8. № 2. С. 87-100. **6.** Новостной портал ASSIETTE.RU - Все главные новости в одном месте! // https://assiette.ru/

**Реквизиты для справок:** *Россия, 153000, Иваново, Шереметевский пр., д.21, ФГБОУ ВО Ивановский государственный политехнический университет, доценту кафедры информационных технологий и сервиса, кандидату технических наук, Арбузовой А.А., тел. 8-915-814-63-54. E-mail: annaarb215@gmail.com*

**УДК 004.934.2**

## СОЗДАНИЕ ДОСТУПНОЙ СРЕДЫ ДЛЯ ОБУЧЕНИЯ В СИСТЕМАХ LMS С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ РАСПОЗНАВАНИЯ И СИНТЕЗА РЕЧИ

И. Е. БЕЛОВОЛОВ, А. Н. ТУШЕВ

В настоящее время все более актуальными становятся LMS (Learning Management System) – системы управления обучением, так как эти системы позволяют организовать полноценное удаленное обучение студентов и школьников. LMS представляет из себя продвинутое хранилище материалов для учебы, позволяющее обмениваться сообщениями

между пользователями системы, фиксировать проведенное в системе время, оценивать уровень подготовки. Данные системы пока еще не способны полностью вытеснить традиционные виды обучения, но, тем не менее, для них характерен больший уровень свободы доступа к информации. Высокий уровень свободы доступа к информации также подразумевает создание доступной среды, обеспечивающей облегчение доступа к информации людям с ограниченными возможностями.

**Целью работы** является упрощение взаимодействия с LMS и тем самым создание более доступной среды для обучения при помощи использования технологий распознавания и синтеза речи,.

Распознавание речи представляет собой поэтапную задачу распознавания образов: система получает информацию о колебаниях воздуха через аппаратное устройство (микрофон), затем полученный аналоговый сигнал конвертируется в цифровую форму, проходит фильтрацию и предварительную коррекцию, разбивается на участки, в которых происходит выделение акустических параметров для дальнейшего анализа, основанного на сравнении полученных данных с ранее записанными образцами.

Самостоятельная реализация непосредственного процесса распознавания речи сложна, к тому же существует множество доступных API, позволяющих его реализовать. Одни из самых известных систем, имеющие поддержку русского языка – Google Cloud Speech API и Yandex Speech Kit. Обе системы способны осуществить и синтез речи, и ее распознавание.

Технологии распознавания и синтезирования речи на данный момент не способны полностью заменить процесс взаимодействия с традиционными для рабочего места манипуляторами и средствами вывода (клавиатурой и мышью, монитором), однако в некоторых случаях они способны значительно сократить количество физического контакта с манипуляторами.

Для облегчения взаимодействия пользователя с LMS системой с помощью распознавания речи нужно обратить внимание на следующие варианты взаимодействия:

1. Пользователю необходимо осуществить навигацию в интерфейсе LMS системы (перейти из одного пункта меню системы в другой, выбрать учебный курс для изучения, переместиться между страницами учебного материала). Для реализации подобной функций необходимо составить несколько словарей ключевых слов: статический словарь доступных команд («перейти в…», «выбрать…», «следующая страница», «предыдущая страница») и динамически генерирующийся словарь, уникальный для отдельно взятой страницы системы (например, словарь до-

ступных для пользователя курсов, на просмотр которых у него есть права, чтобы иметь возможность перейти к изучению курса, название которого произнесет пользователь);

2. Пользователю нужно связаться с другими пользователями системы, создать и отправить текстовое сообщение для преподавателя, для одногруппников при помощи голоса. В данном случае для перевода речи в текст локальные словари ключевых слов уже не понадобятся.

Не только распознавание речи, но также и синтез речи может найти применение в следующих ситуациях:

1. При взаимодействии пользователя с интерфейсом системы пользователь должен получать обратную связь, отклик от системы (реакция на голосовые команды, которые дает пользователь; описание элементов, на которые пользователь наводит курсор мыши). Для каждого элемента системы необходимо заполнить поля с описанием выделяемого элемента;

2. Автоматическое озвучивание текстового содержимого электронного курса, если у курса отсутствует видео или аудио версия;

3. Голосовое уведомление пользователя о поступивших сообщениях, появлении новых материалов, выставлении преподавателем оценки пользователю;

4. Озвучивание входящих сообщений от преподавателя;

5. Автоматическая генерация мультимедийных звуковых файлов на основе содержания текста электронного курса для дальнейшего прослушивания на устройствах, поддерживающих воспроизведение таких файлов;

Таким образом, использование технологий распознавания и синтеза речи может помочь создать доступную среду для пользователей LMS систем и облегчить работу с информацией, размещенной в этих системах.

**Литература. 1.** Бабаринов С.Л., Будникова М.А. О распознавании речи // Экономика. Информатика. 2014. №21-1 (192). URL: https://cyberleninka.ru/article/n/o-raspoznavanii-rechi. Загл. с экрана. (дата обращения: 12.12.2020). **2**. Алимурадов А.К. Параметры и классификация систем распознавания речи // Модели, системы, сети в экономике, технике, природе и обществе. 2014. №1 (9). URL: https://cyberleninka.ru/article/n/parametry-i-klassifikatsiya-sistem-raspoznavaniya-rechi. Загл. с экрана. (дата обращения: 12.12.2020). **3.** Колесникова Д.С., Рудниченко А.К., Верещагина Е.А., Фоминова Е.Р. Применение современных технологий распознавания речи при создании лингвистического тренажера для повышения уровня языковой компетенции в сфере межкультурной коммуникации // Интернет-журнал «Науковедение» Том 9, №6 (2017) URL: https://naukovedenie.ru/PDF/20TVN617.pdf. Загл. с экрана. (дата обращения: 12.12.2020). **4**. Андрюшкова О. В., Горбунов М. А., Козлова А. В. Learning

management system как необходимый элемент blended Learning // Открытое образование. 2017. №3. URL: https://cyberleninka.ru/article/n/learning-management-system-kak-neobhodimyy-element-blended-learning. Загл. с экрана. (дата обращения: 12.12.2020).

**Реквизиты для справок:** ***1.*** *Россия, 656038, Барнаул, проспект Ленина, д. 46, Алтайский государственный технический университет им. И.И. Ползунова, бакалавру кафедры ИВТ и ИБ Беловолову Илье Евгеньевичу, E-mail: belovolov.ilya@yandex.ru* ***2.*** *Россия, 656038, Барнаул, проспект Ленина, д. 46, Алтайский государственный технический университет им. И.И. Ползунова, , кандидату технических наук, доценту кафедры Информатики, вычислительной техники и информационной безопасности, Тушеву Александру Николаевичу, E-mail:tushev51@mail.ru*

**УДК 681.2.084**

# ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ МЕТОДИК ПОВЫШЕНИЯ ТОЧНОСТИ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА ДЛЯ ИЗМЕРЕНИЯ И РЕГИСТРАЦИИ МЫШЕЧНОЙ АКТИВНОСТИ

С. А. ГАВРИЛОВ, И. Н. МАЛЬЧИКОВ, Н. А. ДУДАРЕНКО.

**Целью данной работы** является практическое применение методов повышения точности измерений мышечной активности для мобильного программно-аппаратного комплекса интерференционной (поверхностной) электромиографии (иЭМГ) [1]. Ранее была разработана модель фильтра сигналов от датчиков для контроллера мышечной [2]. Фильтр несущей составляющей сигнала на основе RC-фильтра высоких частот обеспечивает отвязку блока измерения от опорного напряжения датчика, а активный фильтр низких частот усиливает сигнал от датчика и фильтрует шумы выше диапазона частот сигналов мышечной активности. Данная работа проводится в рамках разработки нейрокомпьютерного интерфейса для управления бионическими устройствами [3]. В связи с этим, была поставлена задача физической реализации данных методов.

**Оценка практического применения методов повышения точности**

Для проверки методов повышения точности измерений был разработана схема блока усилителя (рисунок 1) с входным фильтром высоких частот (ФВЧ) и выходным активным фильтром низких частот 2-го порядка. Изготовлен прототип платы (рисунок 2) программно-аппаратного комплекса.

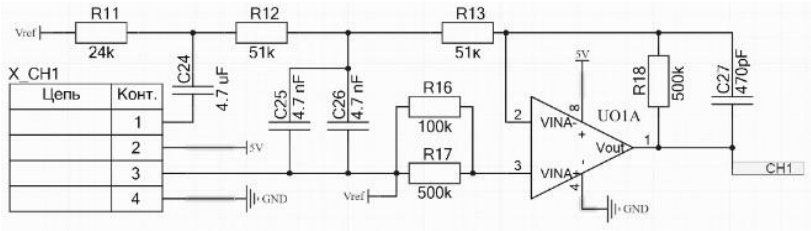



Рисунок 1 – Схема блока усилителя прототипа с входным ФВЧ и выходным активным ФНЧ 2-го порядка

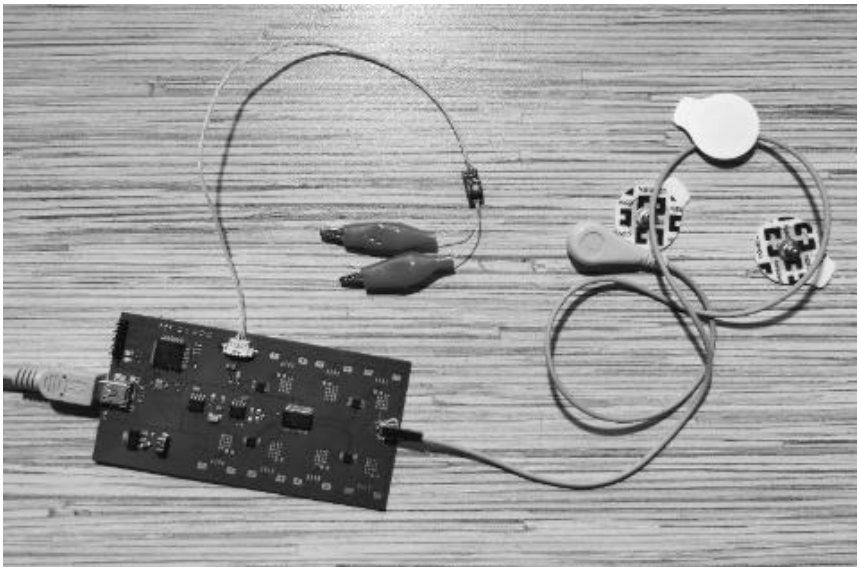


Рисунок 2 – Модернизированная плата прототипа программно-аппаратного комплекса интерференционной электромиографии

Для проверки работы фильтров блока усилителя был разработан источник шумового сигнала на основе генератора случайных чисел отладочной платы NUCLEO-F746ZG от STMicroelectronics. Стенд (рисунок 3) генерирует сигнал нормально распределенной случайной величины на частоте 2 кГц. Осциллограмма и спектрограмма генерируемого сигнала представлены на рисунке 4. Данный сигнал подается на вход усилителя прототипа (1 вывод разъема X_CH1 на рисунке 1).

Рисунок 3 – Стенд генерации, сигнал нормально распределенной случайной величины с подключенной платой прототипа

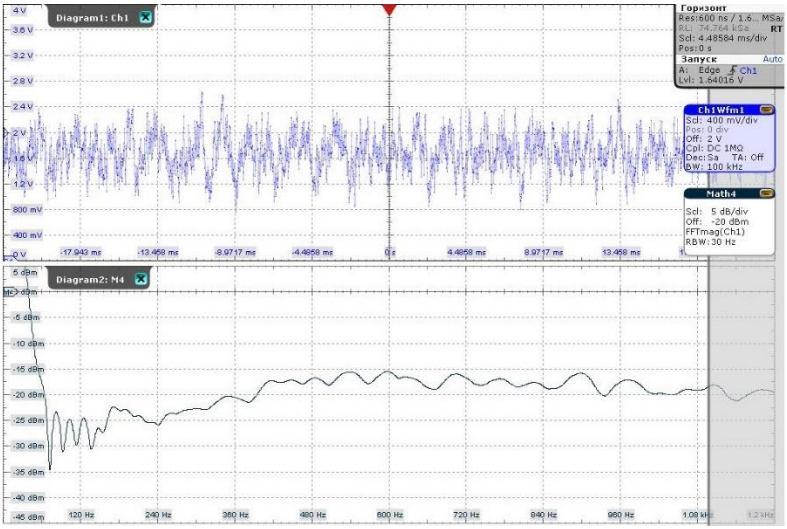
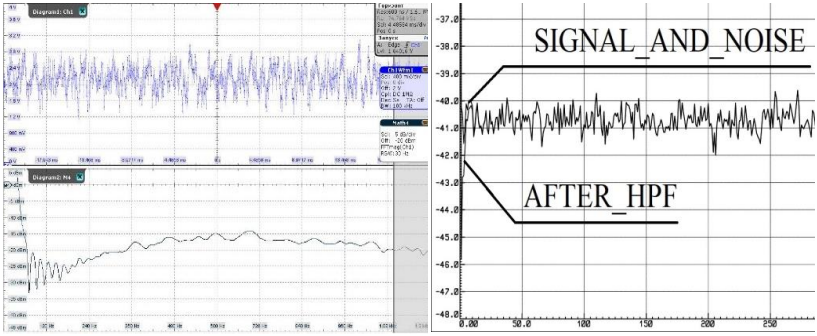



Рисунок 4 – Осциллограмма и спектрограмма генерируемого сигнала нормально распределенной случайной величины

Для проверки работы RC-ФВЧ выход фильтра (точка между R12 и R13 на рисунке 1) подключен к осциллографу. Осциллограмма (Diagram1) и спектрограмма (Diagram2) работы RC-ФВЧ представлены на рисунке 5а. Для сравнения на рисунке 5б представлена спектрограмма модели.




а) б)

Рисунок 5 – а) осциллограмма и спектрограмма RC-ФВЧ,
б) спектрограмма модели

Из сравнения 2-х спектрограмм можно сделать вывод, что работа RC-ФВЧ соответствует модели и обеспечивает крутизну подавления приблизительно 6 дБ. Частота среза RC-ФВЧ находится по формуле:

$$f_{HPF} = \frac{1}{2 \times \pi \times R11 \times C24} = \frac{1}{2 \times 3{,}14 \times 4{,}7\,mF \times 24\,kOhm} \approx 1{,}4109\,Hz$$

где $f_{HPF}$ – частота среза ФВЧ;

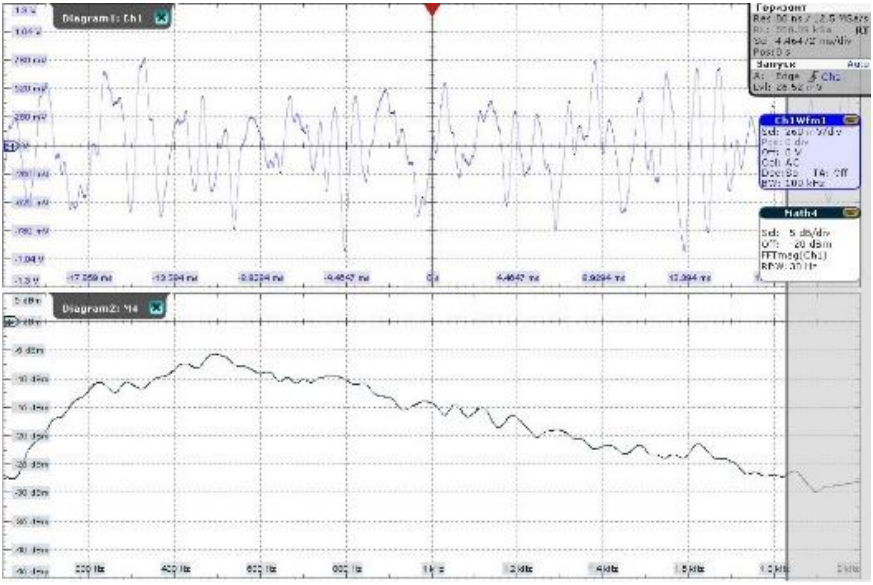
$\pi$ – математическая постоянная, равная отношению длины окружности к её диаметру;

$R11$ – сопротивление резистора R11 (рисунок 1);

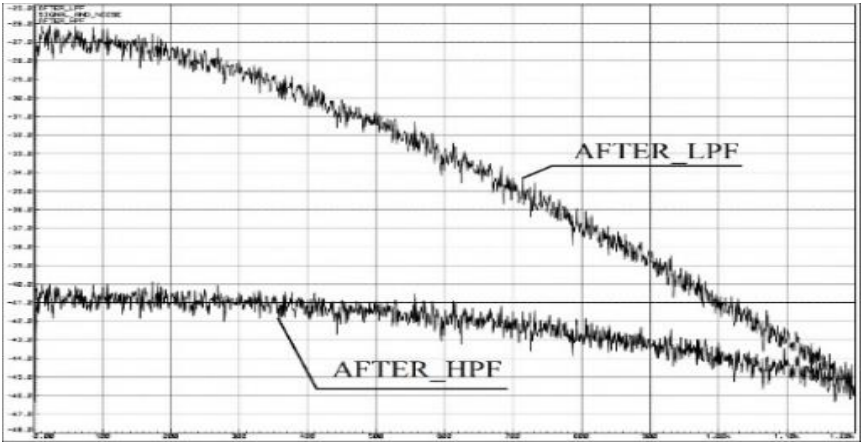
$C24$ – емкость конденсатора C24 (рисунок 1).

Для проверки работы активного ФНЧ 2-го порядка выход фильтра (точка CH1 на рисунке 1) подключен к осциллографу. Осциллограмма (Diagram1) и спектрограмма (Diagram2) работы активного ФНЧ 2-го порядка представлены на рисунке 6а. Для сравнения на рисунке 6б представлена спектрограмма модели.

Из сравнения 2-х спектрограмм можно сделать аналогичный вывод, что работа активного ФНЧ 2-го порядка соответствует модели и обеспечивает крутизну подавления приблизительно 12 дБ. Коэффициент усиления усилителя и частота среза ФНЧ находятся по формулам соответственно:



а)




б)

Рисунок 6 – а) осциллограмма и спектрограмма активного ФНЧ 2-го порядка,
б) спектрограмма модели

$$G_{ch} = -\frac{R1}{R4 + R5} = -\frac{500\ kOhm}{50\ kOhm + 50\ kOhm} = -5$$

$$f_{AFC} = \frac{1}{2 \times \pi \times (R4 + R5) \times C1} = \frac{1}{2 \times 3.14 \times (50\ kOhm + 50\ kOhm) \times 470\ pF} \approx 677{,}25\ Hz$$

где $G_{ch}$ – коэффициент усиления усилителя;
$f_{LPF}$ – частота среза ФНЧ;
$R1$ – сопротивление резистора R1 (рисунок 1);
$R4$ – сопротивление резистора R4 (рисунок 1);
$C1$ – емкость конденсатора C1 (рисунок 1).

**Заключение.** Такие методы, как фильтрация несущей составляющей сигнала и повышение порядка фильтра низких частот, на практике показали положительные результаты повышения точности измерений мышечной активности для мобильного программно-аппаратного комплекса интерференционной электромиографии. Результаты данной работы позволят снизить влияние таких внешних источников шума, как сервоприводы экзоскелетов, отрезов и протезов.

Далее, планируется реализовать цифровой режекторный фильтр частоты бытовой сети электропитания и приступить к разработке алгоритма адаптивного анализа сигналов мышечной активности.

**Литература. 1.** Rangayyan R.M. (Ed.). (2015). Biomedical Signal Analysis. doi:10.1002/9781119068129. **2.** Gavrilov S.A., Kyzdarbekova A.S., Reznikov S.S. (2020). Accuracy increase of software and hardware appliance for muscle activity measuring and monitoring by filtration of carrier component and frequencies higher than measured signal range // Scientific and Technical Journal of Information Technologies, Mechanics and Optics, 2020, vol. 20, no. 4, pp. 617–624. **3.** Гаврилов С.А., Кыздарбекова А.А., Резников С.С. (2019). «Разработка прототипа программно-аппаратного комплекса для регистрации мышечной активности» // Сборник трудов VIII конгресса молодых ученых, Санкт-Петербург, 2019, 35-38.

**Реквизиты для справок:** *Россия, 197101, Санкт-Петербург, ул. Кронверкский пр., 49, Университет ИТМО, аспиранту, Гаврилову С.А., тел. +7(968) 193-74-66. E-mail:itgavrilov@gmail.com*

**УДК 621.362**

# ЭКСПЕРИМЕНТАЛЬНЫЙ СТЕНД ДЛЯ ИЗМЕРЕНИЯ ХАРАКТЕРИСТИК ТЕРМОЭЛЕКТРИЧЕСКОЙ СИСТЕМЫ ДЛЯ ИЗВЛЕЧЕНИЯ ИНОРОДНЫХ ОБЪЕКТОВ ИЗ ТЕЛА ЧЕЛОВЕКА МЕТОДОМ ПРИМОРАЖИВАНИЯ

О. В. ЕВДУЛОВ, А. М. НАСРУЛАЕВ

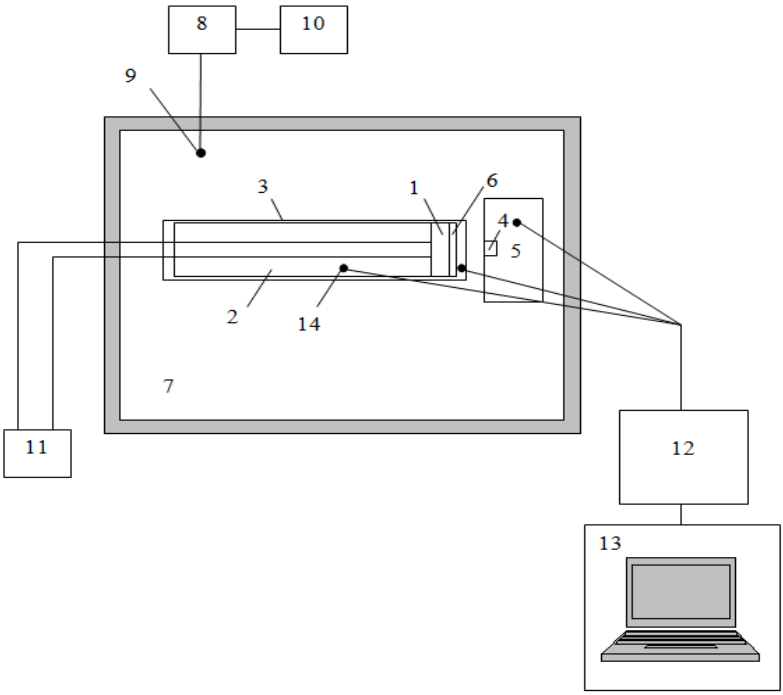
При попадании в организм человека инородных объектов (ИО), последние могут вызвать существенные дисфункции организма. В частности, болезненные ощущения дискомфорт, воспаление и заражение близлежащих тканей, вызывающие дальнейшее нагноение и некроз ткани. Поэтому операции по извлечению инородных объектов (ИО) из тела человека являются важными и ответственными мероприятиями, качество и оперативность проведения которых напрямую влияет на здоровье и жизнь человека.

Проведенный литературный обзор [1-3] показал, что в настоящее время извлечение ИО из тела человека производится в основном хирургическим методом с использованием различного оборудования, в состав которого входят разнообразные механические приспособления. В случае извлечения ферромагнитных ИО могут быть также применены намагниченные зонды. Методики проведения операций по извлечению посторонних тел также могут быть разнообразными. Они зависят от местоположения ИО объекта, его формы, размеров и состава и включают в себя такие мероприятия, как отыскание местоположения ИО, приведение его в наиболее удобное для извлечения положение и непосредственно выем из тела человека.

Анализирую данные методики по извлечению ИО из тела человека и технические средства для их реализации необходимо отметить их недостаточную надежность, связанную, прежде всего с качеством фиксации постороннего объекта в приспособлении, зависимость от квалификации персонала, проводящего операцию, болезненность и продолжительность процедуры. Поэтому представляет интерес разработка новых технических средств для извлечения ИО из тела человека и методик, реализованных на их основе. В этих условиях перспективным является использование методики локального приморaживания ИО к специальному зонду с охлажденным наконечником. Надежность фиксации ИО в извлекающем приспособлении в данном случае будет обеспечиваться за счет высокой степени сцепления наконечника зонда и объекта при их приморaживании друг к другу. В качестве источника холода в зонде может быть использован компактный термоэлектрический модуль (ТЭМ), обладающий высоким ресурсом работы, надежностью, экологичностью, обеспечивающий

требуемую мощность для надежной фиксации ИО на извлекающем приспособлении [4].

Разработан экспериментальный стенд для измерения рабочих характеристик такого прибора (рис.1). В качестве объекта экспериментальных исследований выступал лабораторный образец термоэлектрической системы (ТЭС), состоящий из ТЭМ 1, закрепленного на торцевой поверхности латунного зонда 2, имеющего возможность перемещаться по направляющим в специальной пластиковой трубке 3. Зонд имеет цилиндрическую форму с сквозным отверстием вдоль центральной продольной оси, через которое производится вывод электрических контактов ТЭМ. В качестве источника холода использовался ТЭМ типа TES1-04303 (производитель Hebei Yuxiang Electronic Co., Ltd., Китай).




Риунок 1 – Принципиальная схема экспериментального стенда для измерения характеристик ТЭС для извлечения ИО из тела человека

При проведении натурных испытаний опытный образец ТЭС приводился в контакт с ИО (дюралюминиевый диск диаметром 15 мм и толщи-

ной 4 мм) 4, находящемся в имитаторе биологического объекта 5. Имитатор биологического объекта представлял собой некоторый объем, заполненный силиконом, внутри которого на определенной глубине размещается ИО. На поверхности ТЭМ, предназначенной для контакта с ИО 4 размещалась влажная губка 6, при полном промерзании выполняющая функцию ледяного моста между извлекаемым объектом и модулем.

Исследования проводились в климатической камере 7. Блок управления 8 и датчик температуры и влажности 9, показания которых выводились на цифровое табло 10, использовались для регулирования указанных характеристик среды в объеме камеры. ТЭМ питался от источника постоянного электрического тока 11. Для измерения температуры в контрольных точках прибора использовался многоканальный измеритель температуры ИРТМ 2402/ М3 12, подключаемый к персональному компьютеру 13. В качестве датчиков температуры использовались отградуированные медь-константановые термопары 14.

При проведении натурных испытаний системы измерялись ток и напряжение ТЭМ, температура у поверхности влажной губки, в имитаторе биологического объекта, по длине зонда и в окружающей среде. Одновременно проводилось визуальное наблюдение за процессом образования ледяного моста и примораживания ИО к ТЭС с фиксированием времени, необходимым для этого при тех или иных условиях (в зависимости от температуры внутри климатической камеры, величины тока питания ТЭМ).

Результаты измерений показали, что при использовании данного типа ТЭМ с максимальным током питания $I_{max} = 3,3$ А, напряжением $U_{max} = 5,07$ В и холодопроизводительностью $Q_{max} = 10$ Вт продолжительность процедуры фиксации ИО к прибору составит порядка 40 с.

**Литература. 1**. Блоцкий, А.А. Травмы и инородные тела ЛОР-органов / А.А. Блоцкий, С.А. Карпищенко, В.В. Антипенко, Р.А. Блоцкий. – СПб.: Диалог, 2018. – 217 с. **2**. Блоцкий, А.А. Неотложные состояния в оториноларингологии / А.А. Блоцкий, С.А Карпищенко. – СПб.: Диалог, 2016. – 203 с. **3**. Юнусов, А.С. Эпидемиология инородных тел полости носа в условиях крупного мегаполиса / А.С. Юнусов, [и др.] // Российская оториноларингология. – 2017. – № 5. – С. 83-87. **4.** Евдулов, О.В. Термоэлектрическая система для извлечения инородных объектов из тела человека / О.В. Евдулов, А.М. Насрулаев, С.Г. Магомедова, И.Ш. Миспахов, Н.А. Набиев // Вестник ДГТУ. Технические науки. – 2019. – т.46, №1. – С. 32-41.

**Реквизиты для справок:** *Россия, 367026, Махачкала, пр. Имама Шамиля, д.70, ФГБОУ ВО "Дагестанский государственный технический университет", кафедра теоретической и общей электротехники, д.т.н., доцент Евдулов О.В. – ole-ole-ole@rambler.ru, тел.(8722)628269.*

**УДК 621.362**

# ТЕРМОЭЛЕКТРИЧЕСКОЕ УСТРОЙСТВО ДЛЯ ИЗМЕРЕНИЯ И ВИЗУАЛИЗАЦИИ ТЕМПЕРАТУРНЫХ ПОЛЕЙ ПЛОСКИХ ОБЪЕКТОВ

О. В. ЕВДУЛОВ, К. А. МАГОМЕДОВА

В настоящее время в таких областях жизнедеятельности человека, как машиностроение, приборостроение, энергетика, медицина одной из актуальных задач является задача определения и визуализации температурных полей различных объектов. Решение данной задачи дает возможность повысить эффективность анализа надежности работы разрабатываемой аппаратуры, а в области медицины осуществлять экспресс диагностику различных заболеваний по аномально высокой или низкой температуры человека.

На данный момент одним из методов решения описанной задачи является использование для целей визуализации температурных полей объектов жидкокристаллических пленок, изменяющих свой цвет в зависимости от температуры. Реализованные на их основе системы дешевы, конструктивно просты и технологичны [1]. Однако им присущи недостатки, заключающиеся в значительном влияния на эффективность их работы таких параметров, как точность сопряжения с объектом, температурное поле которого подлежит измерению, и шероховатость сопрягаемой поверхности.

В ФГБОУ ВО "Дагестанский государственный технический университет" разработан ряд конструкций приборов, предназначенных для определения и визуализации температурных полей плоских объектов [2], описание одного из вариантов которых приводится в данной работе.

Конструкция прибора изображена на рис. 1. В состав устройства входит высокотеплопроводное основание, выполненное в виде рамки 1, на внутренней торцевой поверхности которой закреплена жидкокристаллическая пленка 2 выпуклой формы. Радиус кривизны пленки находится в пределах 80-90 % от максимального значения, соответствующего абсолютно плоской поверхности. С внешней торцевой поверхностью рамки по ее периметру сопряжены термоэлектрические модули (ТЭМ) 3, снабженные на опорных спаях радиаторной системой 4.

При определении и визуализации температурного поля плоского объекта устройство сопрягается с его поверхностью. При этом первоначально с помощью ТЭМ, работающих в режиме охлаждения, либо нагрева, цвет жидкокристаллической пленки устанавливается равномерным и одинаковым по всей ее поверхности. Например, жидкокристаллическая пленка индикатора ТЖК608 (производство ООО "Инновационная компа-

ния Ялос", г. Москва) имеет голубой цвет при температуре 17 °С. При сопряжении жидкокристаллической пленки с объектом за счет неравномерности температуры поверхности последнего она изменит цвет, причем цветовая картина будет соответствовать температурному полю поверхности. Непосредственно температура в каждой точке поверхности определяется по градуировочной цветовой шкале.

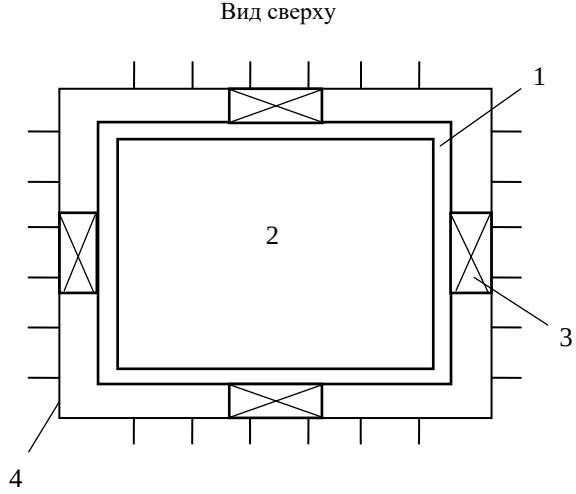



Рисунок 1 – Конструкция термоэлектрического устройства для измерения и визуализации температурных полей плоских объектов

Проведено математическое моделирование прибора, выполненное на основе решения нестационарной двумерной задачи теплопроводности с локальными истоками и стоками теплоты по площади жидкокристаллической пленки. При этом в качестве граничных условиях по ее периметру принималось наличие определенного теплового потока от ТЭМ. Нас

рис. 2 показано температурное поле, плоского объекта, полученное в результате моделирования.

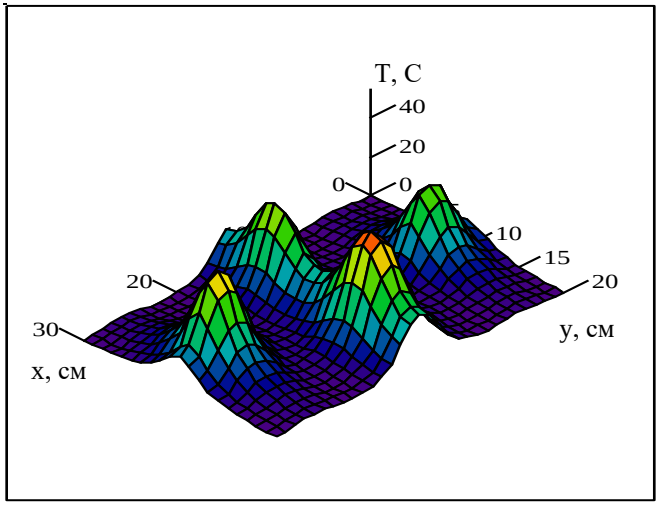



Рисунок 2 – Температурное поле плоского объекта

Использование разработанного прибора на практике даст возможность повысить точность определения и визуализации температурного поля плоской поверхности за счет обеспечения более плотного контакта жидкокристаллической пленки с ней.

**Литература**. **1**. Исмаилов Т.А. Термоэлектрические полупроводниковые устройства и интенсификаторы теплопередачи. СПб.: Политехника, 2005. – 533 с. **2**. Евдулов О.В., Магомедова К.А., Миспахов И.Ш. Устройство для определения и визуализации температурных полей плоских объектов // Материалы Всероссийской молодежной НПК "Программно-техническое обеспечение автоматизированных систем". Барнаул: АГТУ. – 2018. – С.115-117.

**Реквизиты для справок:** *Россия, 367026, Махачкала, пр. Имама Шамиля 70, ФГБОУ ВО "Дагестанский государственный технический университет", кафедра теоретической и общей электротехники, д.т.н., доцент Евдулов О.В. – ole-ole-ole@rambler.ru, тел.(8722)628269* .

**УДК 531.717**

# ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ БЕСЦЕНТРОВОГО ИЗМЕРЕНИЯ КРУГЛОСТИ

П. В. ШИРИНИНА, А. А. ТРОШИН, О. В. ЗАХАРОВ

Измерение круглости согласно ГОСТ Р 53442-2015 представляет собой актуальную задачу в машиностроении, так как большая часть изделий содержит поверхности, номинальным сечением которых является окружность. Однако функциональное назначение изделия, тип сопряжения деталей, размеры и требования точности и тип производства определяют различные требования к применяемым измерительным приборам.

Известны следующие методы и приборы для измерения круглости: прецизионного вращения на кругломере, координатного измерения на координатно-измерительной машине (КИМ), бесцентровый с помощью призмы и датчика малых линейных перемещений [1-3]. Наиболее точным из указанных методов является первый. Вместе с тем этот метод требует лабораторных условий и высококвалифицированного персонала, а также высокая стоимость самих приборов. Получил применение в основном в подшипниковой промышленности. Наиболее известными приборами являются прецизионные кругломеры Talyrond фирмы Taylor Hobson (Великобритания).

КИМ представляет собой наиболее дорогостоящее оборудование, применение которого целесообразно для сложных изделий. Обладая высокой универсальностью процесса измерения и программного обеспечения, он значительно уступает по точности прецизионным кругломерам.

Бесцентровый метод измерения относится к трехточечным методам и использует различные комбинации призм и датчика малых линейных перемещений [4-6]. Достоинством метода является высокая производительность, простота и как следствие высокая надежность прибора. Однако метод получил распространение в цеховых условиях машиностроительных предприятий для контроля изделий средней точности. Такая ситуация обусловлена тем, что методу присуща методическая погрешность измерения [7, 8]. В результате погрешность измерения может достигать 100 % [9-11].

За последние десятилетия неоднократно предпринимались попытки минимизировать погрешность бесцентрового измерения. Для этого разрабатывались сложные методики обработки результатов измерения или проектировались более сложные конструкции прибора (например, многоступенчатая призма с самоустанавливающимся контактом [5]). Такие подходы позволили снизить методическую погрешность, но не решили проблему в целом.

Для исследования процесса бесцентрового измерения круглости и методической погрешности необходима математическая модель достаточной степени адекватности реальному процессу. Анализ известных математических моделей показал, что все они построены на простых геометрических соотношениях и не позволяют рассчитать точки контакта детали с гранями призмы. Используемое допущение о постоянстве точек контакта при измерении вносит основную составляющую погрешности в математическую модель. Другим некорректным допущением является рассмотрение суперпозиции гармоник без учета их начальных фаз при описании профиля детали с помощью тригонометрического полинома.

Поэтому разработана математическая модель бесцентрового измерения более высокой степени адекватности реальному процессу, использующая численные методы и гармонический анализ [12]. В ней точки контакта определяются на основе численного алгоритма при каждом повороте детали на небольшой угол. Разработанная программный комплекс для моделирования процесса бесцентрового измерения визуально подтвердил правильность предложенного подхода и математической модели. С помощью программного комплекса было выполнено моделирование и обоснована возможность минимизации систематической погрешности измерения до 5 % на основе создания прибора, реализующего адаптивную наладку.

Математическое описание процесса измерения рассматривается в три этапа: нахождение центра средней окружности профиля детали после базирования, определение радиусов измеренных датчиком точек профиля, расчёт круглости по измеренным точкам. Расчет круглости может выполняться как методом наименьших квадратов, так и по окружности минимальной зоны. В результате разработаны алгоритм и программа на языке C++ (рис. 1). В программе используется интерактивный ввод исходных данных о профиле измеряемой детали в виде совокупности амплитуд и начальных фаз гармоник. С помощью полос прокрутки или численно меняется угол призмы и угол положения датчика. Все изменения в режиме реального времени отображаются на экране программы.

В центральном окне программы происходит анимация процесса измерения. Настройки предусматривают возможность изменения параметров анимации (скорость и дискретность движения) и возможность включения или отключения начального положения профиля, смещенного положения профиля в процессе базирования, измеренного профиля, а также вектора центра профиля при вращении. На экран после анимации измерения выводятся следующие результаты: фактическое, измеренное и уточненное значения круглости; погрешности измерения и базирования (в виде среднеарифметического значения) и модуль эксцентриситета. Уточненное значение круглости получают после исключения эксцентриситета по результатам гармонического анализа окончательно измеренного профиля.

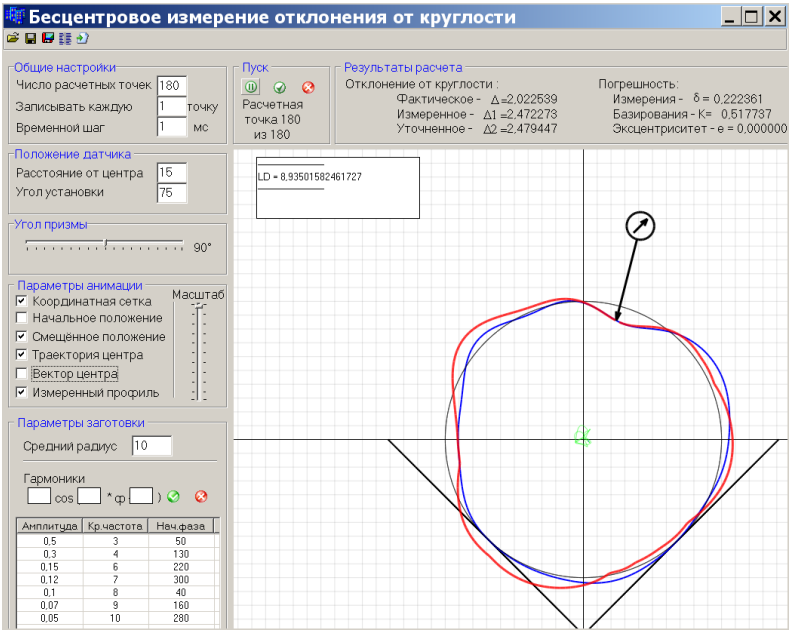



Рисунок 1 – Моделирование бесцентрового измерения круглости

Представленный программный комплекс для моделирования бесцентрового измерения круглости применяется в учебных целях в лаборатории метрологии, стандартизации и сертификации. После добавления в программно-измерительный комплекс аппаратного модуля для ввода и подготовки данных с датчика малых линейных перемещений может быть использован на машино- и приборостроительных предприятиях при серийном и массовом производстве высокоточных деталей.

**Литература. 1.** Уайтхауз Д. Метрология поверхностей. Принципы, промышленные методы и приборы. М.: ИД Интеллект. 2009. 472 с. 2. Авдулов А. Н. Контроль и оценка круглости деталей машин / А. Н. Авдулов. М.: Изд-во стандартов, 1974. 176 с. 3. Гречников Ф.В. Минимизация объема измерений при контроле цилиндрических поверхностей на основе статистического моделирования / Ф.В. Гречников, А.С. Яковишин, О.В. Захаров // Вестник Пермского национального исследовательского политехнического университета. Машиностроение, материаловедение. 2017. № 4. С. 101-110. 4. Палей М.А., Чудов В.А. О возможностях седлообразных приборов при контроле диаметров и отклонений формы // Измерительная техника. 1972. № 4. С. 20-21. 5. Прецизионный кругломер / Я.И. Биндер, И.Д. Гебель, А.И. Нефедов и др. // Измерительная техника. 1999. № 8. С. 25-27. 6. Гречников Ф.В. Итераци-

онный метод коррекции радиуса сферического щупа мобильных координатно-измерительных машин при контроле поверхностей вращения / Ф.В. Гречников, А.Ф. Резчиков, О.В. Захаров // Измерительная техника. 2018. № 4. С. 21-24. 7. Моделирование сопряжения деталей по плоскоцилиндрическим поверхностям / М.А. Болотов, В.А. Печенин, Н.В. Рузанов, И.А. Грачев, И.В. Щербаков, Н.Д. Проничев // СТИН. 2017. № 3. С. 22-28. 8. Прогнозирование погрешностей сборки изделий с использова нием действительных моделей деталей / Ю.С. Елисеев, М.А. Болотов, В.А. Печенин, И.А. Грачев, Е.В. Кудашов // Вестник Самарского университета. Аэрокосмическая техника, технологии и машиностроение. 2019. Т. 18. № 2. С. 128-137. 9. Захаров О. В. Методические основы гармонического анализа круглограмм / О. В. Захаров, В. В. Погораздов, А. В. Кочетков // Метрология. 2004. № 6. С. 3-10. 10. Печенин В.А. Модель координатных измерений геометрии поверхностей сложной формы / В.А. Печенин, М.А. Болотов, Н.В. Рузанов // Вестник Тамбовского государственного технического университета. 2015. Т. 21. № 4. С. 675-685. 11. Сысоев Ю.С. Координатные методы определения параметров средней окружности при анализе профиля реальной поверхности // Измерительная техника. 1995. № 10. С. 22-25. 12. Захаров О.В. Минимизация систематической погрешности при бесцентровом измерении круглости деталей / О.В. Захаров, А.В. Кочетков // Метрология. 2015. № 4. С. 20-28.

***Захаров Олег Владимирович,*** *д.т.н., профессор кафедры «Технология и системы управления в машиностроении», Саратовский государственный технический университет имени Гагарина Ю.А. E-mail: zov@sstu.ru.*

**УДК 531.7**

## АЛГОРИТМЫ ОБРАБОТКИ СИГНАЛОВ ПРИ КООРДИНАТНЫХ ИЗМЕРЕНИЯХ

А. А. ТРОШИН, О. В. ЗАХАРОВ

Координатно-измерительные машины обладают широкими возможностями и высокой точностью для измерения большинства изделий машиностроения. Значительная часть измерений выполняется контактным методом. Результатом является облако точек с декартовыми координатами.

Измеренный сигнал представляет собой сложный геометрический объект, состоящий из комбинации геометрических погрешностей изделия и погрешностей измерения. Поэтому при обработке измеренного сигнала возникает необходимость разделения погрешностей формы, волнистости и шероховатости. Кроме того, в полезном сигнале присутствует так называемый шум, который складывается из случайных ошибок измере-

ния от прибора и окружающей среды. Помимо случайных погрешностей необходимо исключение грубых ошибок измерения. Для технологии производства изделий важно знать причины появления погрешностей. Для этого предназначен гармонический анализ, который выявляет систематические погрешности из общих погрешностей формы изделия. Также необходимо удаление шума, представляющего собой сумму случайной погрешности средства измерения и внешних факторов. Обязательным этапом в обработке сигнала является исключение грубых ошибок. Также в ряде случаев полезно выявление систематических составляющих погрешности поверхности детали для установления причин их возникновения при обработке.

При измерении на координатно-измерительных машинах (КИМ) могут применяться различные методы фильтрации, так как стандарт отсутствует. Поэтому известно большое число работ, посвящённых этой проблеме [1-5]. Общепринятые рекомендации по фильтрации сигнала при измерениях на КИМ отсутствуют. Поэтому целесообразно руководствоваться стандартом ISO 16610-1:2015 и результатами, полученными при измерении круглости и шероховатости [6-8]. Так для измерения шероховатости используется линейный фильтр Гаусса, а для круглости – гармонический анализ на основе дискретного преобразования Фурье.

Выделяют два типа фильтрации – пространственную и временную. В метрологии поверхностей традиционно применяют пространственную фильтрацию. Фильтр Гаусса относится к линейным методам пространственной фильтрации, в то время как преобразование Фурье – к частотным методам. При измерении шероховатости традиционно используют линейный фильтр Гаусса с коррекцией фазы. Для анализа замкнутых профилей (круглости) обычно применяют гармонический анализ, реализуемый с помощью дискретного преобразования Фурье. Из двух типов фильтрации (временной и пространственной) в метрологии поверхностей наибольшее применение получила пространственная фильтрация. Также получили применение фрактальные методы для анализа пространственных параметров шероховатости.

Погрешности, полученные в результате измерения, можно условно разделить на две группы: детали и измерения. Первая группа погрешностей представляет собой объективную информацию, которую необходимо установить. Вторая группа погрешностей возникает в процессе измерения и может считаться шумом или ошибками. От этих погрешностей следует избавляться в результате фильтрации полученного сигнала.

Полученный при измерении поверхности сигнал содержит полезную информацию и шум. Полезная информация представляет собой геометрические погрешности формы изделия. Эти погрешности являются реальными и поэтому могут быть отнесены к первой группе. Другие погрешности являются ошибками измерения. Эти ошибки могут быть слу-

чайными или грубыми ошибками. В обоих случаях методы фильтрации должны их исключить или по крайне мере минимизировать. Данные погрешности можно отнести ко второй группе.

Фильтрация сигнала при измерении на КИМ решает следующие задачи:

1) исключение грубых ошибок измерения;
2) минимизация случайных ошибок датчика касания;
3) выявление и исключение изъянов поверхности;
4) выявление систематических погрешностей поверхности;
5) выделение волнистости;
6) выделение шероховатости.

Появление грубых ошибок в измерении приводит к погрешностям совмещения систем координат измеренных точек и математической модели. Даже одна грубая ошибка может существенно исказить оценку среднего значения размеров или формы изделия. По этой причине исключение грубых ошибок должно выполняться на первом этапе фильтрации.

Известные критерии исключения выбивающихся из общего ряда результатов измерения исходят из предположения о том, что измеренные случайные величины распределены по нормальному закону. Стандарт ISO 5725-2:1994 рекомендует использование критерия Граббса. Идея проверки заключается в проверке на аномальность резко выделяющихся результатов измерений. Статистики критерия Граббса позволяют проверять в выборке один аномальный результат измерения (наименьший или наибольший) или два (два наименьших в выборке или два наибольших).

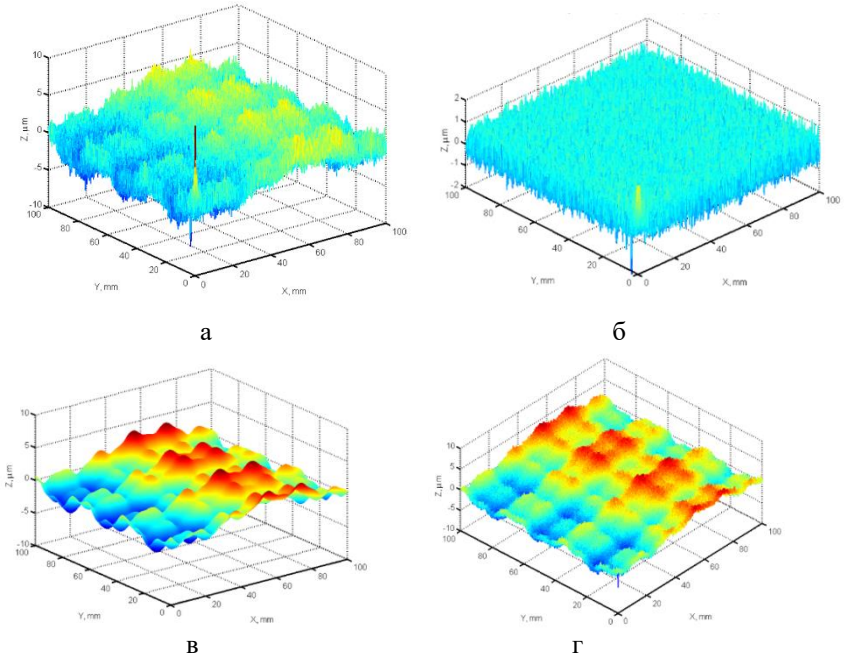
Разделение составляющих погрешностей поверхности (профиля) на погрешности формы, волнистость и шероховатость также осуществляется с помощью фильтров. В соответствии с ISO 16610-21:2011 фильтр Гаусса является стандартным фильтром для текстуры поверхности. Этот стандарт определяет два типа фильтров. Длинноволновый (нижний) гауссовский фильтр представляет собой непрерывную взвешенную свертку для открытого профиля, с весами, принимающими классическую гауссову колоколообразную форму и срезающую длину волны 50 % сигнала. Коротковолновый фильтр Гаусса (высокая частота) определяется как разность между профилем поверхности и компонентом профиля длинной волны, возникающим в результате длинноволнового гауссовского фильтра с 50%-ной длиной волны отсечки. Стандарт ISO 16610-21:2011 не дает информации об алгоритмах реализации фильтра Гаусса.

Известно, что любую функцию с определенной погрешностью можно представить рядом Фурье. Поэтому погрешности поверхности также можно представить конечной суммой гармонических функций. Определить совокупность гармонических функций можно посредством преобразования Фурье. Используя полученный ряд Фурье, можно решать две задачи. Во-первых, удаление шума как высокочастотных составляющих с малой амплитудой. Во-вторых, определить амплитуды и длины волн,

отвечающих за систематические составляющие погрешностей поверхности. Для определения значимых гармоник используется величина поверхностной спектральной плотности мощности:

Для проверки предлагаемой методики было проведено измерение плоскости размера 100×100 мм после плоского шлифования. Измерения проводились на координатно-измерительной машине. Плоскость была равномерно разбита совокупностью точек через 10 мм с отступом от краев 5 мм. В итоге был получен массив из 121 точки.

Исходно измеренное значение для плоскости по 121 точке составило 7.13 мкм, среднеарифметическое значение 0.02 мкм, стандартное отклонение 0.17 мкм. В результате преобразования Фурье выявлены 3 гармоники с частотами n = 3, 5, 12 и амплитудами a = 1.12, 0.67, 0.32 мкм по оси x и 2 гармоники с частотами n = 4, 8 и амплитудами a = 1.18, 0.65 мкм по оси y. После фильтрации и восстановления поверхности получено максимальное значение погрешности 5.82 мкм, среднеарифметическое значение 0.01 мкм, стандартное отклонение 0.09 мкм. Результаты даны на рис. 1.




а б в г

Рисунок 1 – Пример фильтрации сигнала: а – исходные погрешности;
б – случайные погрешности после исключения систематических;
в – выявленные ДПФ систематические погрешности;
г – восстановленные погрешности после фильтрации

Для фильтрации случайных погрешностей в условиях реального производства отсутствует возможность многократных измерений поверхностей и определения статистических параметров. Поэтому алгоритмы обработки сигналов необходимо строить для данных, полученных после однократного измерения. Таким образом, важной задачей становится подбор подходящего математического аппарата для фильтрации случайных погрешностей и определение параметров выбранного фильтра. Предлагается в качестве оптимизируемых параметров выбирать уровень спектральной плотности мощности ДПФ и дисперсию для пространственной и ранговой функций Гаусса билатерального фильтра.

**Литература. 1.** Уайтхауз Д. Метрология поверхностей. Принципы, промышленные методы и приборы / Д. Уайтхауз. М.: Интеллект, 2009. 472 с. **2.** Печенин В.А. Модель распознания элементов геометрии пера лопаток газотурбинных двигателей / В.А. Печенин, М.А. Болотов, Н.В. Рузанов // Проблемы машиностроения и надёжности машин. 2018. № 3. С. 102-108. **3.** Гречников Ф.В. Минимизация объема измерений при контроле цилиндрических поверхностей на основе статистического моделирования / Ф.В. Гречников, А.С. Яковишин, О.В. Захаров // Вестник Пермского национального исследовательского политехнического университета. Машиностроение, материаловедение. 2017. № 4. С. 101-110. **4.** Порошин В.В. Исследование погрешности фильтрации неровностей поверхности сплайновым пространственным фильтром / В.В. Порошин, Д.Ю. Богомолов, В.Г. Лысенко // Измерительная техника. 2018. № 3. С. 27-32. **5.** Гречников Ф.В. Итерационный метод коррекции радиуса сферического щупа мобильных координатно-измерительных машин при контроле поверхностей вращения / Ф.В. Гречников, А.Ф. Резчиков, О.В. Захаров // Измерительная техника. 2018. № 4. С. 21-24. **6.** Елисеев Ю. С. Прогнозирование погрешностей сборки изделий с использованием действительных моделей деталей / Ю.С. Елисеев, М.А. Болотов, В.А. Печенин, И.А. Грачев, Е.В. Кудашов // Вестник Самарского университета. Аэрокосмическая техника, технологии и машиностроение. 2019. Т. 18. № 2. С. 128-137. **7.** Порошин В.В. Исследование погрешности фильтрации текстуры поверхности пространственным фильтром Гаусса / В.В. Порошин, Д.Ю. Богомолов, В.Г. Лысенко // Измерительная техника. 2017. № 8. С. 19-23. **8.** Хаймович И.Н. Формирование поверхностей пера лопаток с использованием интерполяционных сглаживающих сплайнов / И.Н. Хаймович // Кузнечно-штамповочное производство. Обработка материалов давлением. 2014. № 2. С. 41-44.

**Реквизиты для справок:** *Россия, 410054, Саратов, ул. Политехническая 77, Саратовский государственный технический университет имени Гагарина Ю.А., доктору технических наук, профессору, Захарову Олегу Владимировичу, тел. (8452) 99-87-96. E-mail: zov@sstu.ru.*

**УДК 004.42**

# РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ УЧЕТА ЛЬГОТНОГО ПИТАНИЯ ОБУЧАЮЩИХСЯ

Е. Е. ИСТРАТОВА, А. С. КАРПУХИНА

Применение информационных систем актуально практически для любых организаций, причем для многих принципы их работы схожи. Однако автоматизация предприятий общественного питания, например, столовых, имеет свои особенности, которые значительно отличают ее от остальных. Одной из таких особенностей является необходимость обеспечения возможности льготного питания или питания за счет предприятия [1]. На одних предприятиях общественного питания этот вопрос решается использованием талонов на еду, в других – предлагается скидка или питание по себестоимости [2]. В любом случае, информационная система должна фиксировать не только учет предоставленных льгот и финансовую оценку затрат, но и вопросы корректного налогообложения, поскольку выплаченная дотация на питание является доходом, и организация обязана включить ее в налоговую базу по НДФЛ.

Однако, в случае отсутствия автоматизации учет и контроль дотационных денежных средств, выделяемых на питание обучающихся, невозможно назвать на 100 % прозрачным. Ведь при отсутствии льготника в образовательном учреждении, его правом на неполное покрытие расходов на питание может воспользоваться другой ученик. Также составление списков обучающихся, посетивших столовую, разбиение их на группы и предоставление отчетов вручную требует затрат человеческих и временных ресурсов. Для устранения этих недостатков и для повышения эффективности функционирования столовой была решено спроектировать информационную систему.

**Целью исследования** являлась разработка информационной системы для учета фактических расходов на питание обучающихся, имеющих льготы.

Объектом информатизации стал лицей города Новосибирска № 22 «Надежда Сибири». На момент начала работы в лицее процесс учета и составления отчетов не был автоматизирован.

В соответствии с нормативно-правовыми актами по организации питания и предоставлению мер социальной поддержки, учащиеся из малообеспеченных или малоимущих семей, а также сироты имеют право на льготное питание за счет финансирования администрации города [3]. На уровне муниципального образования отделом образования Новосибирской области принят порядок, регламентирующий вопросы организации питания школьников. Так, раз в месяц школы должны отчитываться об

использовании бюджетных средств, выделенных на организацию льготного питания обучающихся.

Актуальность темы работы заключалась в возможности как фиксации расходов на питание, так и формирования требуемой отчетности. На основании отчетов поступает финансирование. Разные виды льгот имеют разные источники финансирования. Исходя из этого, разрабатываемая структура информационной системы сможет регистрировать нахождение обучающегося, имеющего льготы на питание, в учебном заведении, а также определять вид льгот. Отчетность можно рассматривать в разрезе видов льгот, источников финансирования, возраста детей и других критериев. Информационная система должна фиксировать не только учет предоставленных льгот и финансовую оценку затрат, но и вопросы корректного налогообложения, поскольку выплаченная дотация на питание является доходом, и организация обязана включить ее в налоговую базу по НДФЛ.

Для реализации поставленной цели были решены следующие задачи:

1) изучение теоретического материала и действующих в учебном заведении локальных нормативных актов в сфере учета льготного питания;

2) определение основных ролей пользователей;

3) корректировка структуры базы данных;

4) осуществление функций контроля за использованием бюджетных средств;

5) формирование необходимых отчетов для администрации лицея;

6) получение персонифицированной информации в режиме реального времени для администрации по категориям питающихся.

На основе исходных данных была составлена диаграмма процесса составления отчетности об исполнении бюджета (рис. 1).

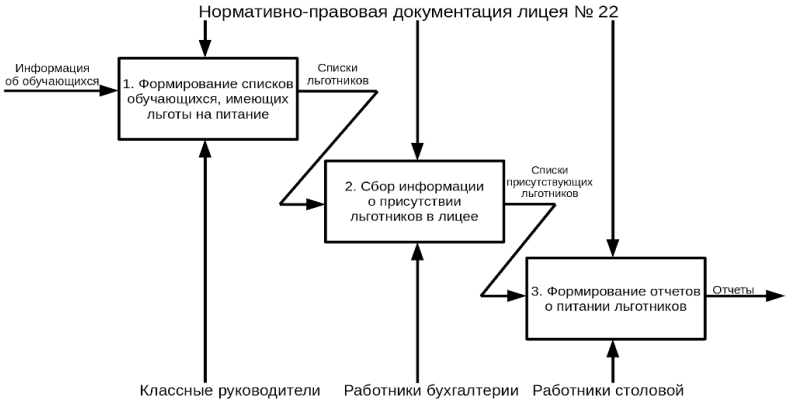



Рисунок 1 – Диаграмма формирования отчетности об использовании бюджетных средств

Как видно из диаграммы, ключевыми участниками информационной системы являются следующие пользователи:

– классный руководитель – составляет списки школьников;

– работник столовой – ведет табель питающихся учеников в разрезе категорий (льготная или полная оплата питания), составляет отчет об использовании бюджетных средств;

– работник бухгалтерии – вносит данные о бюджете;

– системный администратор (имеет полные права на использование и редактирование информации, обслуживает информационную систему, разграничивает права пользователей).

Первоначальным этапом разработки информационной системы являлось проектирование структуры базы данных. Для реализация данной задачи были выполнены следующие этапы:

1. Формулирование цели проектирования структуры базы данных.
2. Определение функций пользователей базы данных.
3. Выявление ключевых сущностей, атрибутов, доменов.
4. Выполнение физического проектирования базы данных.

Цель разработки структуры базы данных заключалась в учете фактических расходов на питание обучающихся, имеющих льготы.

Функциями пользователей проектируемой базы данных являлись:

– фиксация посещаемости учебного заведения обучающимися, имеющими льготы (классный руководитель);

– регистрация учета назначаемых льгот (работник бухгалтерии);

– формирование отчетов (работник столовой).

Следующий этап заключался в разработке интерфейса информационной системы. В начале была настроена панель пользователя, в которой были размещены все требующиеся страницы и справочники. После настройки панели, была спроектирована главная страница со ссылками на страницы и с функцией учета хранимых на них данных.

В результате проектирования информационной системы было разработано веб-приложение, при запуске которого пользователь авторизуется и получает право на доступ к информации в соответствии с его ролью в системе. Причем верхнее меню с необходимым функционалом формируется автоматически в зависимости от прав пользователя. После авторизации пользователя информационной системы ему становится доступен раздел с документами «Льготы». Данный раздел содержит реестр всех документов на право предоставления льгот на питание в столовой лицея № 22 (рис. 2).

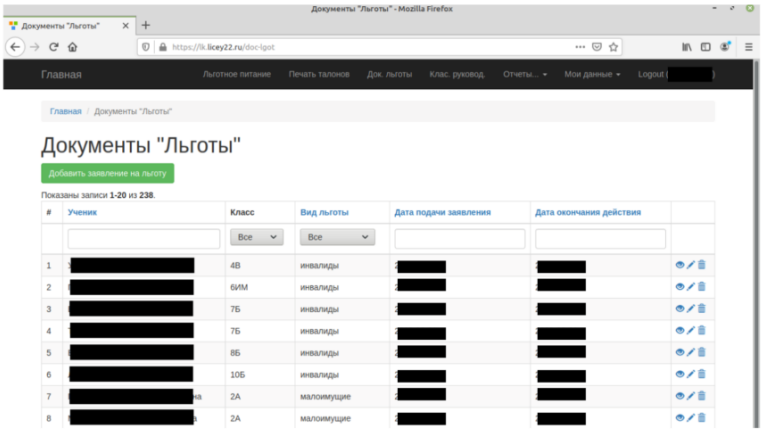



Рисунок 2 – Перечень документов «Льготы»

Раздел меню «Льготное питание» доступен только пользователям системы с ролью «классный руководитель». При этом классный руководитель может подать заявку на льготное питание ученика только на текущую дату. На рис. 3 представлена таблица, содержащая список учеников класса, имеющих право на льготное питание. После отправки заявки, данные сохраняются в базу данных, а в информационной системе учета льготного питания отображаются сведения о присутствии ученика в лицее.

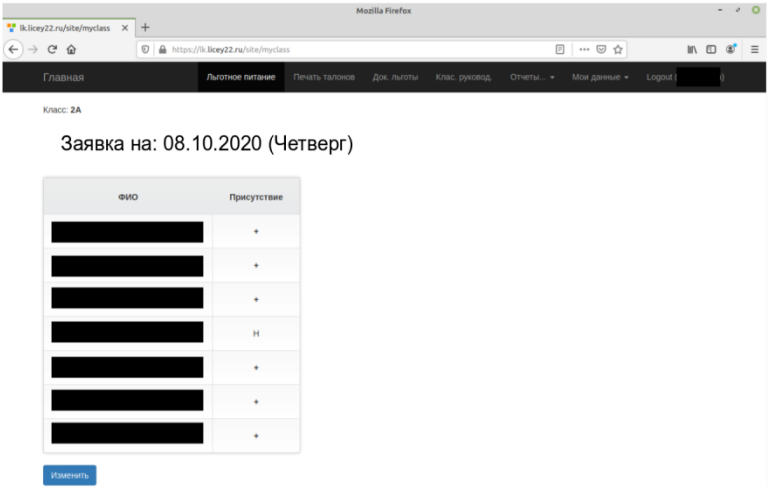



Рисунок 3 – Пример заполненной формы

Разработанная информационная система также обладает возможностью формирования различных видов отчетов по льготному питанию учеников лицея (рис. 4). Данный раздел доступен только для пользователя системы с ролью «бухгалтер».

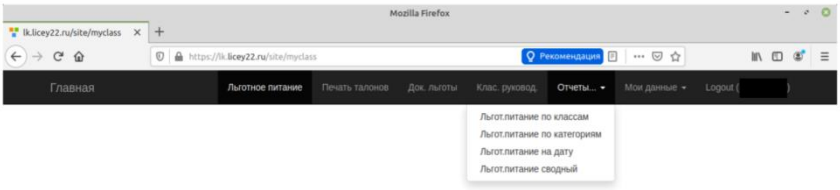
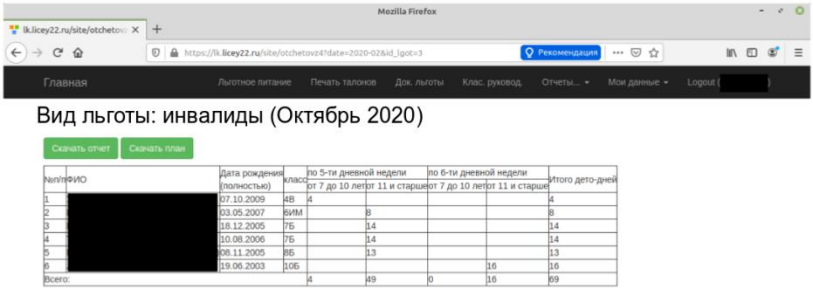



Рисунок 4 – Виды отчетов

Отчет по льготному питанию на конкретную дату формируется ежедневно и применяется для сопоставления данных сотрудников бухгалтерии и столовой. Данный отчет показывает количество учеников, имеющих право на льготное питание и присутствующих в лицее в конкретный день, с разбивкой на категории, отличающиеся по стоимости питания. Таким образом, стоимость льготного питания зависит от возраста ученика на первое число месяца и вида его льготы.

Итоговым видом отчета является сводный отчет, формируемый один раз в месяц в разрезе видов льгот и предоставляемый в администрацию области (рис. 5).




| №п/п | ФИО | Дата рождения (полностью) | класс | по 5-ти дневной недели | | по 6-ти дневной недели | | Итого дето-дней |
|---|---|---|---|---|---|---|---|---|
| | | | | от 7 до 10 лет | от 11 и старше | от 7 до 10 лет | от 11 и старше | |
| 1 | [redacted] | 07.10.2009 | 4В | 4 | | | | 4 |
| 2 | | 03.05.2007 | 6ИМ | | 8 | | | 8 |
| 3 | | 18.12.2005 | 7Б | | 14 | | | 14 |
| 4 | | 10.08.2006 | 7Б | | 14 | | | 14 |
| 5 | | 08.11.2005 | 8Б | | 13 | | | 13 |
| 6 | | 19.06.2003 | 10Б | | | | 16 | 16 |
| Всего: | | | | 4 | 49 | 0 | 16 | 69 |

Рисунок 5 – Сводный отчет

В информационной системе предусмотрен раздел «Печать талонов». В конце каждого месяца бухгалтер лицея, ответственный за выдачу талонов ученикам, распечатывает талоны на следующий месяц и раздает их ученикам, имеющим право на льготное питание. По этим талонам учащиеся питаются в столовой лицея.

Разработанная информационная система также обладает возможностью формирования различных видов отчетов по льготному питанию учеников лицея. Данный раздел доступен только для пользователя системы с ролью «бухгалтер». Отчет по льготному питанию на конкретную дату формируется ежедневно и применяется для сопоставления данных сотрудников бухгалтерии и столовой. Данный отчет показывает количество учеников, имеющих право на льготное питание и присутствующих в лицее в конкретный день с разбивкой на категории, отличающиеся по стоимости питания. Итоговым видом отчета является сводный отчет, формируемый один раз в месяц в разрезе видов льгот и предоставляемый в администрацию области.

В результате была спроектирована информационная система с функциями фиксации посещаемости учебного заведения обучающимися, имеющими льготы, регистрацией учета назначаемых льгот и формирования отчетов. Отличительной особенностью данной информационной системы является то, что отчетность в ней может быть рассмотрена в разрезе видов льгот, источников финансирования, возраста детей и других критериев.

**Литература. 1.** Маюрникова Л.А. Модернизация школьного питания на основе бизнес-процесса развития предприятия в региональных условиях / Л.А. Маюрникова, С.В. Новоселов // Food industry. 2018. №2. URL: https://cyberleninka.ru/article/n/modernizatsiya-shkolnogo-pitaniya-na-osnove-biznes-protsessa-razvitiya-predpriyatiya-v-regionalnyh-usloviyah (дата обращения: 10.12.2020). **2.** Стафиевская М.В. Инновации в системе управленческого учета затрат предприятий агробизнеса / М.В. Стафиевская, Е.А. Минина // Вестник евразийской науки. 2019. №4. URL: https://cyberleninka.ru/article/n/innovatsii-v-sistemeupravlencheskogo-ucheta-zatrat-predpriyatiy-agrobiznesa (дата обращения: 11.12.2020). **3.** Гарант.Ру [Электронный ресурс]: Приказ Министерства здравоохранения и социального развития РФ и Министерства образования и науки РФ от 11 марта 2012г. № 213н/178 «Об утверждении методических рекомендаций по организации питания обучающихся и воспитанников образовательных учреждений». – URL: http://www.garant.ru/products/ipo/prime/doc/70063904 (дата обращения: 10.12.2020).

***Реквизиты для справок:*** *Россия, 630073, Новосибирск, пр. К. Маркса, 20, Новосибирский государственный технический университет, кандидату технических наук, доценту кафедры автоматизированных систем управления, Истратовой Е.Е., тел. 8-952-921-86-29. E-mail: istratova@mail.ru*

**УДК 531.717**

# МЕТОДИКА ИЗМЕРЕНИЯ ПЛОСКОСТНОСТИ НА МОБИЛЬНОЙ КООРДИНАТНО-ИЗМЕРИТЕЛЬНОЙ МАШИНЕ

А. А. ТРОШИН, О. В. ЗАХАРОВ

Плоские поверхности являются одними из наиболее распространенных на деталях машин и механизмов. Поэтому от точности их формы зависит качество сопряжения и точность работы узла в целом. В связи с этим измерению плоскостности уделяют много внимания в метрологии [1-3]. Для этих целей наиболее эффективно применение высокоточных координатно-измерительных машин.

Основным вопросом при обработке результатов измерения плоскостности является определение базового положения плоскости. Тогда величина плоскостности рассчитывается как наибольшее расстояние от измеренных точек до базовой плоскости. В качестве базовых используются следующие плоскости: средняя (полученная по методу наименьших квадратов), прилегающая (внешняя или внутренняя), минимальной зоны (две параллельные плоскости, охватывающие измеренные точки).

Целью данной работы является разработка новой методики расчета плоскостности на координатно – измерительной машине методом наименьших квадратов по нормали, рассчитанном при помощи среды MATLAB.

Расчет прилегающей плоскости сопряжен с большими вычислительными затратами, т. к. подразумевает последовательный перебор плоскостей, построенных по трем точкам. Плоскость минимальной зоны в большинстве случаев обеспечивает меньшее значение плоскостности по сравнению с другими вариантами. Вместе с тем, алгоритм расчета на основе минимизации целевой функции в виде минимальной зоны не всегда гарантирует хорошую сходимость.

Наибольшее распространение получила базовая плоскость, получаемая на основе метода наименьших квадратов. Несомненным преимуществом является однозначность получаемого решения и быстрая сходимость численного алгоритма. Известная методика расчета плоскостности описана в книге [4]. Неплоскостность можно рассматривать как непрямолинейность в любом из направлений на плоскости, заданной уравнением:

$$z = c + m_1 x + m_2 y, \qquad (1)$$

где $x$ и $y$ – независимые переменные, определяющие область измерений;
z – координаты точек плоскости.

Для нахождения параметров $c$, $m_1$, $m_2$ минимизируют целевую функцию в виде суммы квадратов отклонений измеренных точек от плоскости:

$$F = \sum_{i=1}^{n} (z_i - (c + m_1 x_i + m_2 y_i))^2 , \qquad (2)$$

где *xi*, *yi*, *zi* – декартовы координаты i-й измеренной точки, n – число измеренных точек.

Недостаток известной модели заключается в том, что минимизируются расстояния от измеренных точек до плоскости, отсчитываемые по оси *z*. Если плоскость имеет малое отклонение от плоскости *x0y*, то можно считать, что указанные расстояния мало отличаются от перпендикуляров к плоскости. При положении плоскости, характеризуемом большим углом наклона к координатной плоскости *x0y*, эти отклонения становятся значимыми и погрешность расчета существенно увеличивается (рис. 1).

Поэтому предложено минимизировать целевую функцию в виде суммы расстояний от измеренных точек до плоскости:

$$F = \sum_{i=1}^{n} \frac{\left| Ax_i + By_i + Cz_i + D \right|}{\sqrt{A^2 + B^2 + C^2}}, \qquad (3)$$

где плоскость задана уравнением $Ax + By + Cz + D = 0$.

Так как расстояние есть положительная величина, то нет необходимости возводить ее в квадрат в (3).

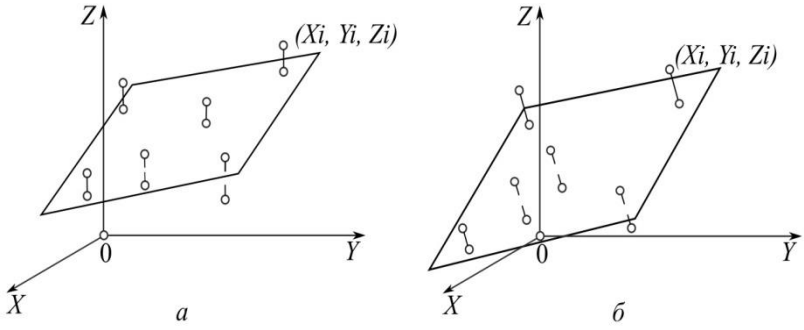



Рисунок 1 – Расчетная схема измерения плоскостности:
а – методика [4], б – предлагаемая методика

Пример построения базовой плоскости методом наименьших квадратов в программной среде MATLAB показан на рис. 2.

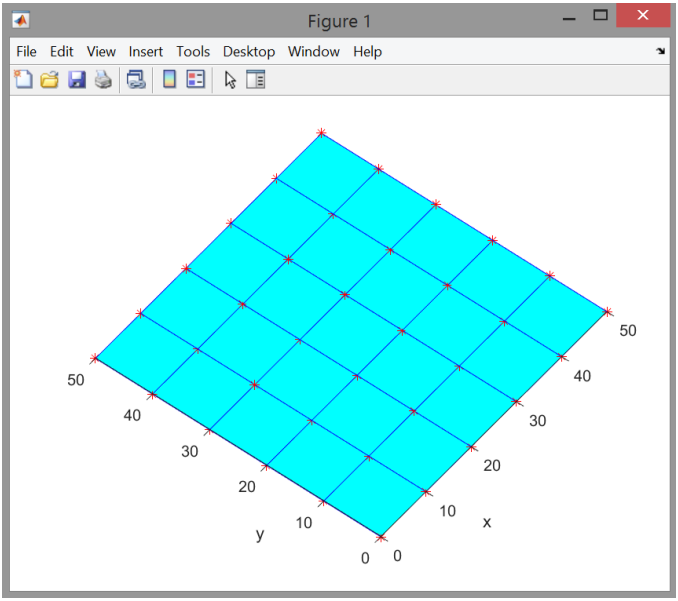



Рисунок 2 – Расчет плоскостности в программе MATLAB

Вопросы выбора числа и расположения контрольных точек на поверхности рассмотрены в [5-8], а фильтрации – в [9-12].

Проведены экспериментальные исследования для сравнительного анализа точности определения плоскостности по известному (2) и предложенному (3) алгоритмам. Измерялись две плоскости высокоточной призмы под различными углами наклона измеряемой поверхности с размерами граней 50×50 мм. На каждой грани призмы измерялись 5 равномерно расположенных точек. В результате обработки данных получены данные о статистическом распределении, а также проведено моделирование для пяти различных углов наклона плоскости. Полученные данные моделирования в виде среднего показателя плоскостности приведены в табл. 1.

Таблица 1 – Плоскостность при обработке результатов по методикам

| Среднее значение плоскостности, мкм | | |
|---|---|---|
| Угол наклона плоскости | Стандартная методика | Разработанная методика |
| 1 | 8.04 | 7.96 |
| 5 | 8.68 | 8.01 |
| 25 | 9.22 | 8.04 |
| 45 | 9.85 | 8.09 |
| 60 | 10.06 | 8.12 |

Таким образом, проведенное моделирование на основе экспериментальных данных показало, что новый алгоритм расчета при измерениях уменьшает значение плоскостности. При этом с увеличением угла наклона поверхности к координатной плоскости *x0y* до показателей наклона 45-60 градусов, разница в значениях плоскостности при использовании базового алгоритма возрастает и составляет 20 %.

**Литература. 1.** Моделирование сопряжения деталей по плоскоцилиндрическим поверхностям / М.А. Болотов, В.А. Печенин, Н.В. Рузанов, И.А. Грачев, И.В. Щербаков, Н.Д. Проничев // СТИН. 2017. № 3. С. 22-28. **2.** Васильева А.А. Исследование процесса измерения корпусных деталей на координатно-измерительной машине Carl Zeiss Contura G2 / А.А. Васильева, Т.Р. Абляз // Вестник Пермского национального политехнического университета. Сер. Машиностроение, материаловедение. 2015. № 3. С. 32-40. **3.** Гречников Ф.В. Минимизация объема измерений плоских поверхностей деталей при сборке / Ф.В. Гречников, А.С. Яковишин, О.В. Захаров // Сборка в машиностроении, приборостроении. 2018. № 2. С. 56-58. **4.** Уайтхауз Д. Метрология поверхностей. Принципы, промышленные методы и приборы. М.: ИД Интеллект. 2009. 472 с. **5.** Гречников Ф.В. Минимизация объема измерений плоских поверхностей деталей при сборке / Ф.В. Гречников, А.С. Яковишин, О.В. Захаров // Сборка в машиностроении, приборостроении. 2018. № 2. С. 56-58. **6.** Порошин В.В. Исследование погрешности фильтрации неровностей поверхности сплайновым пространственным фильтром / В.В. Порошин, Д.Ю. Богомолов, В.Г. Лысенко // Измерительная техника. 2018. № 3. С. 27-32. **7.** Захаров О.В. Минимизация погрешностей формообразования при бесцентровой абразивной обработке: монография / О.В. Захаров. Саратов: СГТУ, 2006. 152 с. **8.** Гречников Ф.В. Минимизация объема измерений при контроле цилиндрических поверхностей на основе статистического моделирования / Ф.В. Гречников, А.С. Яковишин, О.В. Захаров // Вестник Пермского национального исследовательского политехнического университета. Машиностроение, материаловедение. 2017. № 4. С. 101-110. **9.** Гречни-

ков Ф.В., Резчиков А.Ф., Захаров О.В. Итерационный метод коррекции радиуса сферического щупа мобильных координатно-измерительных машин при контроле поверхностей вращения. Измерительная техника. 2018. № 4. С. 21-24. **10.** Фомин А.А. Обеспечение микрогеометрии поверхностей при обработке заготовок с неоднородными свойствами / А.А. Фомин // Сборка в машиностроении, приборостроении, 2012. № 12 С. 27-29. **11.** Прогнозирование погрешностей сборки изделий с использованием действительных моделей деталей / Ю.С. Елисеев, М.А. Болотов, В.А. Печенин, И.А. Грачев, Е.В. Кудашов // Вестник Самарского университета. Аэрокосмическая техника, технологии и машиностроение. 2019. Т. 18. № 2. С. 128-137. **12.** Печенин В.А., Болотов М.А., Рузанов Н.В. Модель координатных измерений геометрии поверхностей сложной формы // Вестник Тамбовского государственного технического университета. 2015. Т. 21. № 4. С. 675-685.

**Реквизиты для справок:** *Россия, 410054, Саратов, ул. Политехническая 77, Саратовский государственный технический университет имени Гагарина Ю.А., доктору технических наук, профессору, Захарову Олегу Владимировичу, тел. (8452) 99-87-96. E-mail: zov@sstu.ru*

# РАЗДЕЛ 3. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

**УДК 004.056.53**

## ИДЕНТИФИКАЦИЯ ОБЪЕКТОВ ПРИ ОГРАНИЧЕННОЙ ВИДИМОСТИ И НЕСТАБИЛЬНОМ ПОЗИЦИОНИРОВАНИИ

А. А. АГАФОНОВА, Е. А. БОГЕР, Ю. А. ОСОКИН

**Цель исследования** – проверить метод идентификации объектов на примере распознавания по геометрии лица. Для этого проведем корреляционный анализ нескольких фотографий с различными ограничениями видимости лица объекта или его нестабильным позиционированием.

Идентификация является одним из аспектов защиты информации. Она позволяет распознать личность и решить: имеет ли человек доступ к контролируемой зоне или нет. Кроме распознавания личности, идентификация позволяет распознать какой-либо иной объект, который может служить злоумышленникам для получения нужной информации [1].

Идентификация и аутентификация как аспекты защиты информации от несанкционированного доступа тесно связаны между собой. Идентификация представляет собой распознавание объекта при помощи анализа его идентификаторов. Аутентификация – это проверка подлинности предоставленного идентификатора пользователя. Также задачей аутентификации является проверка личности на наличие доступа к данной информационной системе. Вместе эти процессы позволяют нам разграничить права доступа к информации для разных пользователей и предотвратить несанкционированный доступ злоумышленников к конфиденциальной информации.

Для аутентификации пользователя могут применяться два метода: статистический и динамический.

Статистический метод позволяет распознать некоторые физические параметры человека, например, отпечаток пальца, рисунок глазной сетчатки или геометрию лица.

Динамический метод анализирует особенности поведения пользователя (например, голос или подпись).

Рассмотрим некоторые методы аутентификации:

Аутентификацию по сетчатке глаза начали использовать еще в 50-х годах прошлого века. Именно в те времена была определена уникальность рисунка кровеносных сосудов глазного дна. Данный вид аутентификации имеет самую высокую степень защищенности, потому что рисунок кровеносных сосудов не повторяется даже у близнецов. Сканеры сетчатки глаза отличаются высокой надежностью: обмануть сканер сетчатки

глаза практически невозможно, а также вероятность ошибки при распознавании глазного рисунка слишком мала – примерно один случай сбоя на миллион тестов.

Но у этого типа аутентификации есть и недостатки: сканеры сетчатки имеют более высокую цену по сравнению с другими сканерами.

Сканер сетчатки глаза действует следующим образом: инфракрасное излучение, характеризующееся низкой частотой, направляется к кровеносным сосудам глазного дна через зрачок. После этого сигнал отображает характерные точки, которые записываются в шаблон и далее сравниваются с полученными ранее данными в ходе обучения системы.

Аутентификация по отпечатку пальца также начала развиваться в прошлом столетии. Именно в те времена, когда компьютеры научились сканировать отпечаток пальца. Первым предложенным способом сбора данных с помощью данной технологии является оптический.

Отпечаток пальца представляет собой уникальный для каждого человека рисунок, состоящий из бугорков и впадин на поверхности кожи. Для работы сканера отпечаток достаточно сфотографировать и в дальнейшем сравнивать с полученной фотографией в ходе работы.

Существуют и другие методы сбора данных, которые основаны на работе радиочастотных сканеров, термосканеров, сканеров, чувствительных к давлению, ультразвуковых сканеров и других. Каждый из перечисленных способов имеет свои достоинства и недостатки [1].

Аутентификация по геометрии лица представляет собой биометрический метод, который основан на распознавании лица по его очертанию и некоторым показателям, например, расстоянии между бровями, глубине глазных впадин и т.д. Данный метод подразделяется на двухмерное и трехмерное распознавание. Двухмерное распознавание лица с каждым годом совершенствуется, тем самым повышая уровень надежности. Однако вероятность ложных срабатываний данного метода до сих пор можно считать высоким – вероятность ложных срабатываний варьируется от 0,1% до 1%, частота ошибок непризнания еще выше.

При трёхмерном распознавании лиц используется множество сложных алгоритмов, эффективность которых зависит от условий их применения. В основном, шаблон составляется из таких неизменных характеристик, как глубина глазных впадин, форма черепа, надбровных дуг, высота и ширина скул и прочих ярко выраженных особенностей. Благодаря им впоследствии система сможет распознать лицо даже при наличии бороды, очков, шрамов, головного убора и прочего [2].

**Проведение исследований**

Для проведения исследований был выбран метод двухмерной аутентификации по геометрии лица.

В качестве оценки схожести объектов было решено провести корреляционный анализ. Корреляцией называется статистическая зависимость одной случайной величины от другой. Математической мерой корреляции двух случайных величин является коэффициент корреляции, который может принимать значения от –1 до 1 [3]. Рассчитывается он следующим образом:

Для начала необходимо рассчитать среднее значение для каждого параметра по формуле (1).

$$\bar{x} = \frac{\sum_{i=1}^{n} x_i}{n} \qquad \bar{y} = \frac{\sum_{i=1}^{n} y_i}{n}; \tag{1}$$

Далее производится расчет коэффициента корреляции по формуле (2).

$$r = \frac{\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i-\bar{x})^2}\sqrt{\sum_{i=1}^{n}(y_i-\bar{y})^2}}; \tag{2}$$

Для удобства работы была составлена программа для расчета коэффициента корреляции на языке программирования Python (рисунок 1).


Рисунок 1 – Окно программы. Пример вводимых данных

Для анализа было взято несколько вариантов видеоизображений с «эталонным» фото и фото с различными изменениями. На каждом фото были отмечены 8 характерных точек в соответствии с изначальным снимком, который представлен на рисунке 2.

Рисунок 2 – «Эталонное» фото

Далее для каждой точки были определены координаты x и y (начало координат находится в верхнем левом углу фотографии). Далее, внося координаты в программу, находился коэффициент корреляции, на основе которого можно было сделать выводы: чем ближе к 1 модуль коэффициента корреляции, тем более схожими являются фото и, наоборот, чем он ближе к 0, тем более различны фотографии.

Ниже представлены фото с различными ограничениями видимости лица и разнообразными изменениями позиционирования головы. Результаты анализа для каждого эксперимента приведены в верхней части соответствующего рисунка.

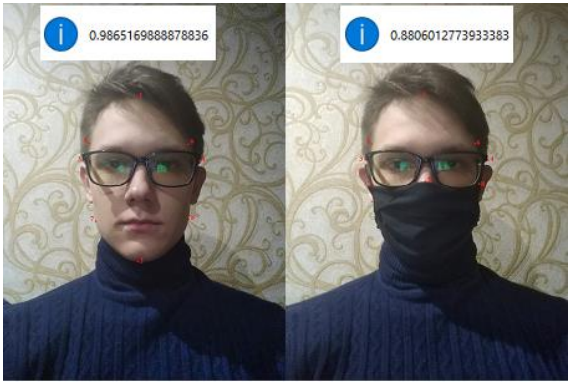



Рисунок 3 – Фото с ограничением видимости лица

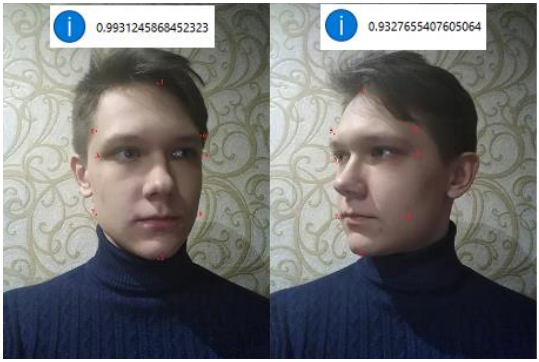



Рисунок 4 – Фото с нестабильным позиционированием (поворот головы)

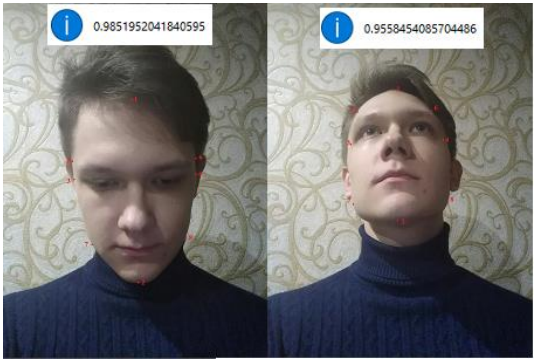



Рисунок 5 – Фото с нестабильным позиционированием (наклон головы)

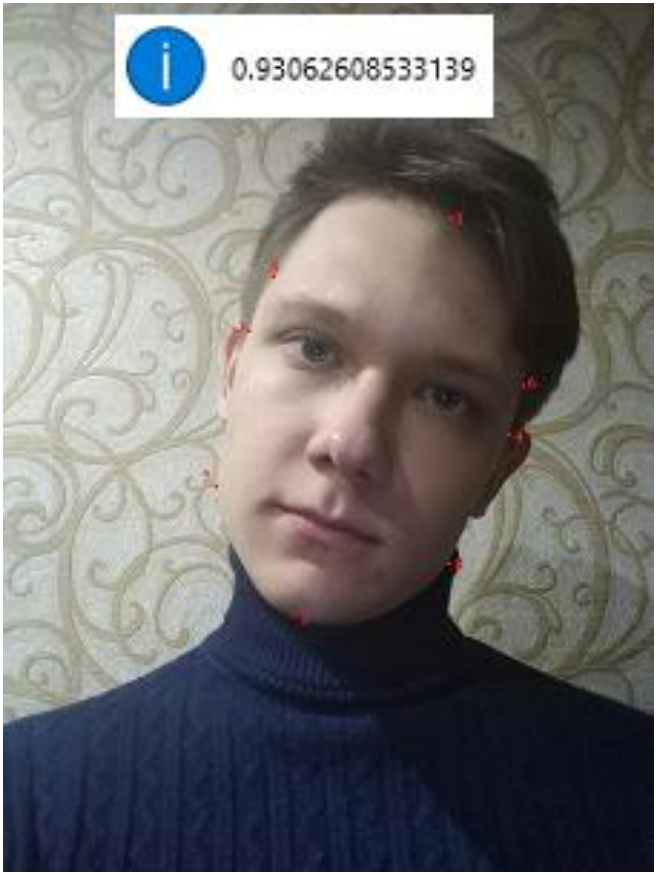



Рисунок 6 – Фото с нестабильным позиционированием (наклон головы влево)

Таким образом, в ходе проведения исследования можно сделать вывод, что метод аутентификации по геометрии лица имеет некоторые недостатки: наличие помех на изображении лица, возможные ограничение видимости, изменения мимики лица или поворота головы приводят к ухудшению надежности метода, приводя к ошибкам непризнания или, наоборот, ложным заключениям.

**Литература. 1.** Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации / Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. - М.: Риор: Инфра-М, 2015. — 392 с. **2.** Аутентификация по геометрии лица [Электронный ресурс]. – Режим доступа: https://studbooks.net/2249892/informatika/autentifikatsiya_geometrii_litsa,

свободный – (13.12.2020). **3.** Харченко М.А. Корреляционный анализ: учебное пособие для вузов / Харченко М.А. – В.: Издательско-полиграфический центр Воронежского государственного университета, 2008. – 31 с.

**Реквизиты для справок:** ***Агафонова Александрина Александровна****, студент 4-го курса кафедры «ИВТиИБ», Факультета информационных технологий ФГБОУ ВО «Алтайский государственный технический университет им. И.И. Ползунова», e-mail:Agafonova.99@list.ru;* ***Богер Егор Андреевич****, студент 4-го курса кафедры «ИВТиИБ», Факультета информационных технологий ФГБОУ ВО «Алтайский государственный технический университет им. И.И. Ползунова», e-mail: bogegor1999@mail.ru;* ***Осокин Юрий Анатольевич****, кандидат технических наук, доцент кафедры «ИВТиИБ», Факультета информационных технологий ФГБОУ ВО «Алтайский государственный технический университет им. И.И. Ползунова», e-mail: y-osokin@mail.*

**УДК 004.054**

## НЕЙРОННЫЕ СЕТИ В КРИПТОГРАФИИ

О. В. МИЛЛЕР, А. Н. ТУШЕВ

Защита информации является неотъемлемой частью любого информационного процесса. С каждым годом злоумышленники придумывают все новые и новые способы получения нужной информации, однако и защитники информации тоже не дремлют. Защита информации предоставляет нам несколько методов, таких как физическая защита, правовая защита информации и криптографическая защита. Рассмотрим более подробно последний метод.

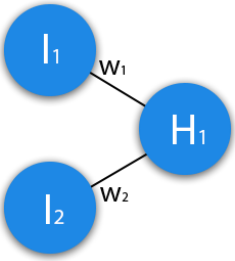
Сама по себе криптография - это наука о методах обеспечения конфиденциальности (недоступности информации третьим лицам), целостности (невозможности изменения исходной информации), аутентификации (проверки подлинности авторства). Криптографический метод защиты предполагает преобразование информации, с целью сокрытия ее смысла для потенциального противника. Как использовать последние достижения в области машинного обучения и, в частности, достижения нейронных сетей в криптографии?

**Целью работы** является исследование роли нейронных сетей в информационной безопасности, в построении хеш-функций на основе нейронных сетей и шифрования.

Нейронная сеть – это математическая модель организации и функционирования биологических нейронных сетей.

Нейрон – это вычислительная единица, которая получает информацию и производит над ней простые вычисления. Для каждого из нейронов характерны два типа данных: входные и выходные. Несколько нейронов объединяются в нейронный слой. Выделяют три типа нейронных слоёв: входной, скрытый, выходной. Из нейронных слоёв, связанных между собой, состоит нейронная сеть.

На рисунке 1 представлена часть нейронной сети, где I – это нейроны входного слоя, H – скрытый нейрон, а W – веса. Входная информация вычисляется путем сложения произведений всех входных данных на соответствующие веса. Путём подстановки входных данных в функцию активации вычисляются выходные значения нейронного слоя. Функция активации представляет собой функцию, нормализующую входные данные, т.е. если на входе находится большое число, то, проходя через такую функцию, получается число в нужном диапазоне. На сегодняшний день наиболее популярными функциями активации являются: линейная пороговая функция (ReLU), сигмоид, гиперболический тангенс. Выходные данные текущего слоя передаются на вход следующего, пока не будет получен отклик от выходов последнего слоя. Путем многократной подачи векторов входного набора и плавной регулировки весов w можно, как правило, добиться хороших результатов в задаче распознавания.




$$1)H1_{input} = (I_1 * w_1) + (I_2 * w_2)$$

$$2)H1_{output} = f_{activation}(H1_{input})$$

Рисунок 1 – Алгоритм работы нейронной сети

Рассмотрим применение принципов обучения нейронных сетей для решения задач информационной безопасности.

Архитектура нейронных сетей позволяет выполнять работы по распознаванию образов и классификации объектов по какому-либо признаку. Системы цифровых водяных знаков, которые позволяют обеспечить защиту авторского права, построены с использованием нейронных сетей [1].

В области криптографии нейронные сети нашли своё применение в построении функций хеширования, а также шифровании.

Рассмотрим модель искусственного нейрона, входящего в состав сети для построения хеш-функций. На рисунке 2 приведено схематическое изображение нейрона сети, которая как раз подходит для решения задач по построению хеш-функций. Из этого рисунка становится понятно, что сеть – трехслойная и является сетью прямого распространения. Также отличительной особенностью данной сети является то, что она использует «хаотическое отображение» [2]. Однако, для построения алгоритма хеширования одной нейронной сети будет недостаточно. Необходимо также использовать генератор ключей, который будет преобразовывать ключ пользователя в набор весовых характеристик сети.

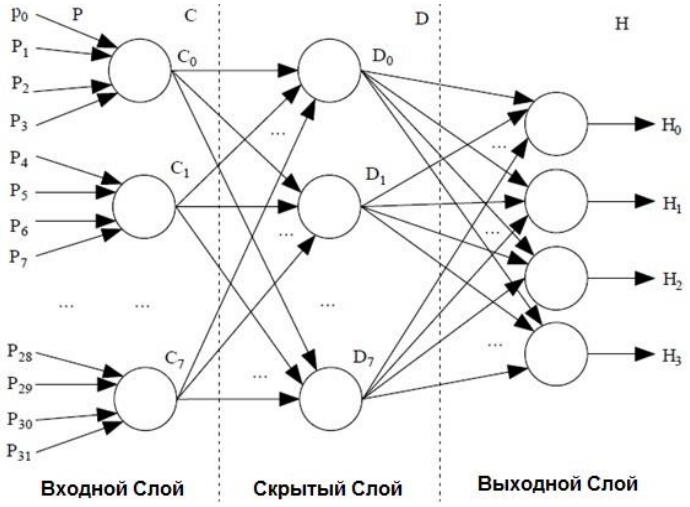



Рисунок 2 – Схема нейронной сети, используемой для построения хеш-функции

При анализе алгоритмов хеширования, основой которых являются нейронные сети, можно выделить следующие преимущества:

- однонаправленность;
- высокая чувствительность выходного значения к входным данным и ключу;
- защита от атак «дней рождения» и «встреча посередине»
- параллельные вычисления

Недостатки: требуется ключ для генерации параметров нейронной сети.

Нейронные сети также используются в области шифрования. Рассмотрим их применение на примере алгоритма AES. Для того, чтобы сделать данный алгоритм устойчивым к атакам злоумышленников, нужно внедрить в него нелинейную нейронную сеть.

Для достижения хорошей производительности, а также малого количества ошибок, необходимо использовать сеть с обратной связью, которая, как было сказано выше, является нелинейной. Сама нелинейность поможет сделать алгоритм более устойчивым к взломам. Также стоит отметить, что нелинейность данной сети достигается при помощи нелинейной функции активации [3].

Рассмотрим алгоритм «многослойный персептрон (MLP)» [3]. В качестве входного вектора для данной нейронной сети будет использоваться незашифрованный текст. Зашифрованным текстом будет являться выходной вектор. Функцией активации будет «log-сигмоида», а ключ шифрования пользователя будет использован в качестве первоначальных весов.

В ходе своего обучения алгоритм шифрования будет создавать зашифрованный текст из незашифрованного. Общий алгоритм обучения достаточно прост. Во время своего обучения нейронная сеть использует незашифрованный текст не только в качестве входного параметра, но и в качестве ориентира на результат дешифрования. Ведь важно не только просто зашифровать исходный текст, но и получить данные в первоначальном виде после их дешифрования. [3].

Преимущества нейронных сетей в алгоритмах шифрования. При сравнении результатов алгоритма AES и «нейро - AES» исследователи отметили тот факт, что расхождения в результате имеются, однако их количество становится меньшим после определенного количества итераций алгоритма «нейро - AES», где нейронная сеть уже обучена на всех входных данных. Стоит отметить, что криптосистема с использование нейронной сети более устойчива к известным атакам на алгоритм AES.

Недостатки нейронных сетей в алгоритмах шифрования. После полного обучения нейронной сети могут остаться небольшие отклонения значений шифрования от значений, которые дает обычный алгоритм AES, а это значит, что в шифрованном и дешифрованном тексте могут появиться искажения. Вторым недостатком при использовании нейронных сетей является усложнение алгоритма шифрования относительно более простого AES.

Подводя итоги, можно сказать, что нейронные сети, несомненно, нашли своё применение в криптографической защите информации. Очевидно, создать идеальный алгоритм хеширования и шифрования крайне сложно, ведь с каждым днём злоумышленники ведут активный анализ и проводят огромное количество атак на известные алгоритмы. Внедрение

нейронных сетей помогает избежать уже известных атак и предотвратить появление некоторого числа новых.

**Литература. 1.** Bansal A., Singh Bhadauria S. Watermarking using Neural Network and Hiding the Trained Network within the cover Image / A. Bansal, S. Singh Bhadauria// Journal of Theoretical and Applied Information Technology. 2008. − P. 663−670. **2.** Shiguo Lian, Jinsheng Sun, Zhiquan Wang. One-way Hash Function Based on Neural / L. Shiguo, S. Jinsheng, W. Zhiquan// 2007. **3.** Siddeeq. Y. Ameen, Ali H. Mahdi, AES Cryptosystem Development Using Neural Networks/A. Siddeeq, M. Ali// International Journal of Computer and Electrical Engineering, Vol. 3, No. 2. 2011. − P. 315- 318.

**Реквизиты для справок: 1.** *Россия, 656038, Барнаул, проспект Ленина, д. 46, Алтайский государственный технический университет им. И.И. Ползунова, бакалавру кафедры ИВТ и ИБ Миллеру Олегу Витальевичу, E-mail:milleroleg99@yandex.ru* **2.** *Россия, 656038, Барнаул, проспект Ленина, д. 46, Алтайский государственный технический университет им. И.И. Ползунова, , кандидату технических наук, доценту, кафедры Информатики, вычислительной техники и информационной безопасности, Тушеву Александру Николаевичу, E-mail:tushev51@mail.ru*

**УДК 004.7**

## МЕТОДЫ АНАЛИЗА SSL/TLS ОТПЕЧАТКОВ ДЛЯ КЛАССИФИКАЦИИ ЗАЩИЩЕННОГО ТРАФИКА

А. Ю. МЫСИН, Е. В. ШАРЛАЕВ

**Введение.** В настоящее время все большее количество видов традиционной деятельности человека переходит из привычного всем состояния в сферу цифровых технологий. Такая тенденция сложилась не сразу с появлением компьютерных сетей, в частности сети Интернет, а лишь тогда, когда человечество оценило возможности передачи информации на расстояние и убедилось, что такой тип передачи информации действительно имеет больше плюсов, чем недостатков. Исходя из того, что в начале развития сетевых технологий недостаточно внимания уделялось безопасности при передаче какой-либо конфиденциальной информации, разработчики стандартов передачи данных мало заботились о безопасности внутри таких сетей. С развитием бизнеса в сети Интернет возникло немало потребностей в обеспечении безопасности. Одним из решений по обеспечению передаваемой информации являются стандарты семейства SSL/TLS.

Данное семейство стандартов постоянно развивается и на данный момент актуальными являются стандарты TLS 1.2 и TLS 1.3

**Целью работы** является теоретическое и экспериментальное исследование способов получения информации из SSL/TLS соединений и HTTPS-пакетов.

В процессе установления соединения взаимодействующие устройства обмениваются ключами по алгоритму RSA или алгоритму Диффи-Хеллмана. Важно также отметить, что на практике используется не один, а два ключа. То есть один для отправки сообщений, а другой для получения. Серверному ключу для передаваемых сообщений (Write) соответствует клиентский ключ для принимаемых (Read), и наоборот. В TLS 1.3 используются несколько уровней ключей (для Handshake, для защиты трафика), каждый из которых включает два значения.

Ранее для шифрования использовался исключительно протокол шифрования RSA, и, соответственно, возможность получить анализ зашифрованного трафика целиком и полностью зависела от наличия приватного ключа. Однако, со временем стала набирать тенденция PFS (Perfect Forward Security или совершенная прямая секретность) и поэтому расшифровка только лишь приватным ключом стала невозможна. Теперь для расшифровки стал требоваться сессионный ключ.

В настоящее время существует два основных способа расшифровки TLS-трафика. Первый основан на использовании сессионных ключей и требует создания переменной окружения среды или дополнительных аргументов при запуске JVM. Второй же работает через создание доверенных сертификатов и имитацию веб-сервера на клиентском компьютере. В ходе работы будут реализованы оба способа перехвата и расшифровки трафика.

**Расшифровка трафика на основе сессионных ключей** при помощи Wireshark. Расшифровка трафика таким методом возможна, только если пользователь взаимодействует с сетью Интернет при помощи браузеров Firefox или версии для разработчиков браузеров на Chromium Engine. Для начала нужно создать переменную среды, в которую будет записываться SSL-ключ (sslkeylog). После этого необходимо настроить саму программу перехвата трафика. Здесь могут возникнуть проблемы с версией, так как последняя версия, в которой можно указать лог-файл для SSl – версия 1.6. После нее Wireshark перешел на поддержку протокола TLS. Итак, указав в настройках протокола в зависимости от версии (SSL для версий ниже 1.6 и, соответственно, TLS для версий выше) можно перейти к дешифровке трафика. Структура дампа без дешифровки представлена на ниже (рис. 1).

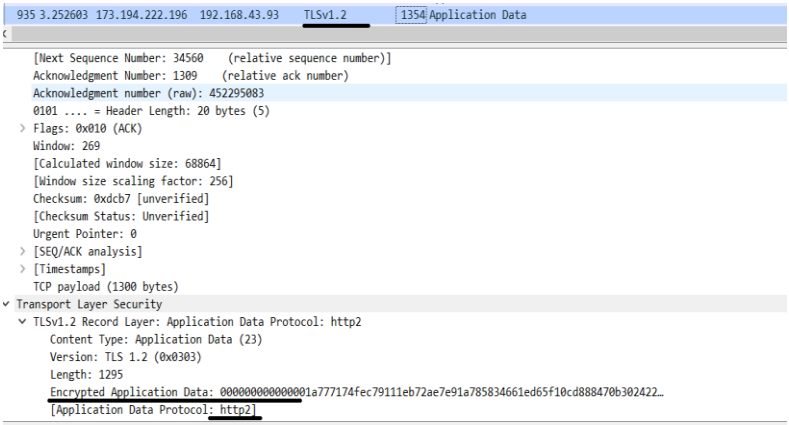



Рисунок 1 – Структура дампа без дешифрования

Добавив лог-файл системы, пакеты, передаваемые по SSL/TLS, расшифровываются. Теперь в списке пакетов появляется HTTP или HTTP2 пакет. В нем содержится информация о протоколе TLS и расшифрованные сведения HTTP-пакета, в частности, метод запроса, длина или его тело. Пример расшифрованного пакета представлен на рис. 2.

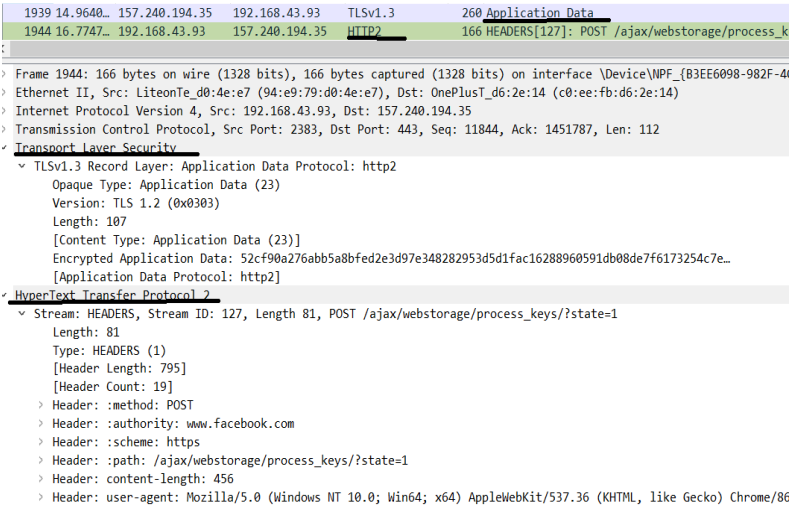



Рисунок 2 – Расшифрованный пакет

**Дешифрование трафика с использованием сертификатов** при помощи Fiddler4. Еще одним инструментом для дешифрования защищенного трафика является Fiddler. Данная программа крайне проста в использовании. Fiddler полагается на подход «in-the-middle» при перехвате HTTPS. Для веб-браузера, делающего запрос к серверу Fiddler утверждает, что он является безопасным веб-сервером, а для веб-сервера Fiddler имитирует веб-браузер. Чтобы выдать себя за веб-сервер, Fiddler динамически генерирует сертификат HTTPS. Однако возникает проблема в недоверии браузера к сертификату. На этом моменте нужно дать свое согласие на доверие этому сертификату. В случае, если этого не сделать, дешифровка не произойдет. Далее нужно просто нажать на Decrypt и информация в пакете будет находиться в открытом виде (рис. 3).

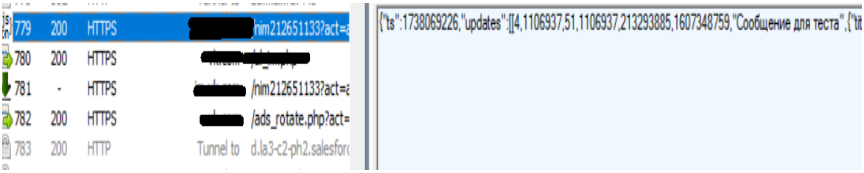



Рисунок 3 – Дешифровка пакета при помощи Fiddler

**Выводы.** В настоящее время задача расшифровки TLS-трафика является крайне важной. Благодаря возможности проверки содержимого защищенных пакетов, для органов безопасности появляется дополнительный механизм предотвращения различных преступлений, будь то терроризм или различные экономические нарушения. С другой же стороны, для людей, которые ценят свою конфиденциальность, примеры, показанные выше – напоминание, что использование чужих сетей для доступа в Интернет влечет за собой множество рисков, связанных с нарушением конфиденциальности. Поэтому для передачи ценных данных необходимо пользоваться дополнительной криптографической защитой.

**Литература. 1.** Ключи, шифры, сообщения: как работает TLS – [Электронный ресурс]. – Режим доступа: https://tls.dxdt.ru/tls.html **2.** Decrypting TLS Browser Traffic With Wireshark – The Easy Way! – [Электронный ресурс]. – Режим доступа: https://redflagsecurity.net/2019/03/10/decrypting-tls-wireshark/ **3.** Configure Fiddler to Decrypt HTTPS Traffic – [Электронный ресурс]. – Режим доступа: https://docs.telerik.com/fiddler/Configure-Fiddler/Tasks/DecryptHTTPS

**Реквизиты для справок:** Россия, 656038, Барнаул, пр. Ленина 46, Алтайский государственный технический университет им. И.И. Ползунова, Мысин А.Ю., тел. 8(923)7949620, e-mail: mysin.alexander99@gmail.com

**УДК 004.7**

# ОСОБЕННОСТИ ПРИМЕНЕНИЯ ПРОТОКОЛА OPENVPN В ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЯХ

Д. И. ЕРБОЛОВ, Е. В.ШАРЛАЕВ

В нынешнее время в условиях пандемии тысячи организаций вынуждены переводить своих сотрудников на удаленный режим работы. В данной ситуации на помощь приходят технологии виртуальных частных сетей (VPN). Хоть технология VPN и была довольно популярна до перевода людей на дистанционный режим работы, но именно сейчас эта технология обрела пик своей популярности.

Однако в целях быстрого и удобного удаленного доступа к рабочему месту специалисты забывают об обеспечении информационной безопасности. Число атак, направленных на удаленных сотрудников, возрастает, поскольку защита систем вне корпоративной сети легче поддается взлому, что позволяет злоумышленникам получить доступ к данным этой организации.

**Целью данной работы** является предложение дополнительных мер по усилению защиты виртуальных частных сетей.

Существует несколько протоколов, обеспечивающих работу виртуальных частных сетей. Одним из наиболее защищенных протоколов является Layer 2 Tunneling Protocol (L2TP)/IPSec. Если быть точнее, то это связка протоколов. L2TP не шифрует проходящий через него трафик, поэтому его и используют в связке с IPSec, что приводит к снижению производительности, поскольку происходит двойная инкапсуляция данных. Криптографически L2TP/IPSec защищен такими алгоритмами шифрования, как 3DES и AES. Наиболее используемым алгоритмом является AES, так как 3DES уязвим к атакам типа «человек по середине» и «sweet32». Одной из серьезных проблем L2TP/IPSec является то, что из-за его сложной настройки данный протокол реализуется недостаточно безопасно. При использовании pre-shared keys (PSK), атакующий может выдать себя за VPN-сервер и далее подслушивать зашифрованный трафик. Безопасность IPSec также может быть ограничена из-за того, что он находится в пространстве ядра.

Поэтому в настоящее время наибольшей популярностью обладает протокол OpenVPN – протокол с открытым исходным кодом, который использует библиотеку OpenSSL для обеспечения шифрования и аутентификации и TLS в качестве канала управления. Одним из главных преимуществ является его гибкая настройка, OpenVPN может быть настроен на работу на любом порту TCP и UDP. Библиотека OpenSSL, используе-

мая OpenVPN, поддерживает наиболее распространенные криптографические алгоритмы – AES и Blowfish [1].

Однако большинство организаций, которые переходят на удаленный режим работы с использованием протокола OpenVPN, используют в своем большинстве конфигурацию OpenVPN, опирающихся на настройки OpenVPN по умолчанию. Эти настройки используются не для повышенного уровня безопасности, а скорее для широкой совместимости. Следовательно, ниже будут приведены рекомендации по усилению защиты протокола.

В OpenVPN происходит взаимная аутентификация сертификатов, что может повлечь за собой компрометацию сертификата и возможность проведения атаки «человек по середине» (MITM) [2]. Чтобы повысить уровень безопасности соединений, необходимо создать файл списка аннулированных сертификатов (CRL), который нужно будет обновлять вручную, так как OpenVPN не содержит механизм протокола состояния сетевого сертификата (OCSP). Также существует возможность создавать краткосрочные сертификаты, которые нужно автоматически обновлять.

Как упоминалось выше, OpenVPN использует TLS в качестве канала управления. Он практически защищен от всех известных атак, но именно в его корне находятся несколько недостатков, позволяющих вывести работу из строя. При использовании UDP в качестве транспорта возникает риск атак отражения UDP, так как исходные пакеты TLS UDP не требуют аутентификации. Также существует возможность инициализировать множество подключений одновременно при аутентификации, поскольку она происходит после стартового рукопожатия.

Для решения этих проблем в OpenVPN используется такая опция, как «tls-crypt», которая редко пользуется популярностью у специалистов, так как в конфигурации по умолчанию предусмотрена уже устаревшая опция «tls-auth». С помощью «tls-crypt» шифруется и аутентифицируется весь TLS-канал. Опция использует предварительный общий симметричный ключ и все неправильно зашифрованные и аутентифицированные пакеты попросту отбрасываются. Отсюда вытекает решение проблем с устранением уязвимостей с отражением UDP, злоумышленники также не смогут инициализировать множество подключений, что предотвращает DoS-атаки, а также не представляется возможным расшифровать предварительное рукопожатие. Опция «tls-crypt» более безопасна при своем использовании, нежели «tls-auth», которая имеет возможность лишь предотвращения DoS-атак [3].

Для установления соединения OpenVPN достаточно лишь наличия сертификата. Поэтому после того, как пользователь установил TLS-соединение, необходимо осуществить дополнительный шаг аутентификации – запрос логина и пароля у пользователя. Такой шаг достаточно

часто игнорируется, поскольку предполагается, что наличие сертификата является достаточным условием установления соединения. Хранение списков пользователей и их паролей можно осуществить, например, на LDAP. Использование многофакторной аутентификации сводит шансы злоумышленников на доступ практически к нулю.

Таким образом, применение дополнительных опций и средств позволяет повысить уровень проверки аутентификационных данных и, соответственно, усилить защиту виртуальной частной сети организации.

**Литература. 1.** Сравнительный обзор реализаций технологий VPN [Электронный ресурс] – Режим доступа: https://1cloud.ru/help/network/comparevpntypes **2.** VPN [Электронный ресурс] – Режим доступа: http://vmk.ugatu.ac.ru/book/vpn.pdf **3.** OpenVPN 2.4 tls-crypt and dh vs eliptic curve [Электронный ресурс] – Режим доступа: https://serverfault.com/questions/1007688/openvpn-2-4-tls-crypt-and-dh-vs-elliptic-curve

**Реквизиты для справок:** *Россия, 656038, Барнаул, ул. Ленина 46, Алтайский государственный технический университет им. И.И.Ползунова, Ерболову Д.И., тел. 8(964)0846335, e-mail: diaserbolovv@yandex.ru, кандидату технических наук, доценту, Шарлаеву Е.В., E-mail: sharlaev@mail.ru*

**УДК 004.056.53**

## СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ В ВЕБ-ПРИЛОЖЕНИИ

А. Д. ШАДРИНА

В мире быстро развивающихся информационных технологий все большую популярность приобретают веб-приложения. Они становятся востребованными благодаря следующим свойствам: кроссплатформенность (пользователь не зависит от определенной операционной системы), могут использоваться большим количеством человек одновременно, не требуют установки, облегчают организацию хранения данных, не требуют обновления. Злоумышленники интересуются способами взлома веб-приложений для разных целей, например, для доступа к ценным ресурсам, управлению чужим контентом и др. Таким образом, возрастает потребность в защите данных веб-приложения [2].

**Целью работы** является определение актуальных угроз безопасности веб-приложения и анализ способов защиты от этих угроз.

Можно выделить несколько основных типов угроз информационной безопасности веб-приложений:

– нарушение целостности – угрозы, связанные с несанкционированным изменением или намеренным повреждением данных;

– нарушение конфиденциальности – угрозы, связанные с неправомерным доступом к данным;

– нарушение доступности – угрозы, связанные с неправомерным ограничением или затруднением доступа к данным [3].

К самым распространенным уязвимостям веб-приложений на данный момент можно отнести следующие: Security Misconfiguration – небезопасная конфигурация; Cross-Site Scripting, XSS – межсайтовый скриптинг; SQL-инъекции – позволяет злоумышленнику получить доступ к базе данных; Broken Authentication – «сломанная» аутентификация; Broken Access Control – недостатки контроля доступа; Sensitive Data Exposure – незащищенность критичных данных [4].

Злоумышленник – это нарушитель, имеющий возможность реализовать угрозы безопасности веб-приложения. Выделяют две типа нарушителей: внешние (лица, не имеющие права доступа к системе, реализуют угрозы безопасности вне системы) и внутренние (имеют право постоянного или разового доступа к системе).

Современные веб-приложения написаны на языках программирования высокого уровня, следовательно, злоумышленникам проще найти уязвимости в коде системы. Поэтому большинство веб-приложений нуждаются в комплексной защите данных.

К основным способам защиты информационной безопасности веб-приложения относятся: аудит информационной безопасности, внедрение WAF, использование защищенных протоколов передачи данных, шифрование данных, ограничение доступа пользователей к данным, безопасная аутентификация, защита используемых баз данных, тестирование состояния системы на сканерах защищенности веб-приложений, анализ сайтов на наличие вирусов. Ниже представлено описание перечисленных способов защиты.

Аудит защищенности веб-приложений – это проверка, анализ и независимая оценка уровня безопасности веб-приложения, позволяющая получить сведения об уязвимостях и возможных атаках на систему. Объектами аудита являются программное обеспечение, логика веб-приложения, среда передачи данных между пользователем и сервером. После проведения аудита составляется документ, содержащий результаты анализа безопасности системы. В нем описаны проведенные проверки, выявленные уязвимости, указаны способы их реализации злоумышленниками и предложены меры по их устранению.

Web Application Firewall (WAF) – межсетевой экран для веб-приложений, предназначенный для фильтрации трафика, выявления и блокирования атак на них. Основная задача WAF – защита системы от

несанкционированного доступа. Для обнаружения атак используются такие методы, как сигнатурный анализ, машинное обучение, возможность настройки правил вручную, терминация TLS и SSL [5].

Под использованием защищенных протоколов передачи данных подразумевается эксплуатация HTTPS. HTTPS – расширение протокола HTTP, поддерживающее шифрование через транспортные механизмы SSL и TLS.

Для ограничения доступа к данным пользователям необходимо присвоить привилегии, соответствующие их уровню доступа, и настроить параметры безопасной аутентификации.

Защиту базы данных можно обеспечить предотвращением SQL-инъекций. SQL-инъекция – это произвольный запрос к базе данных веб-приложения через форму или параметр URL. Для защиты от внедрения вредоносного кода на языке Transact SQL необходимо использовать параметризированные запросы. Также для повышения безопасности данных, хранящихся в базах данных, следует предотвратить межсайтовый скриптинг (XSS). Важным параметром безопасности данных пользователя является хранение его пароля в базе данных в виде хеша, а также использование динамической «соли».

Сканеры защищенности веб-приложений (Web Application Security Scanner, WASS) – это система для мониторинга уязвимостей и оценки уровня защищенности программного обеспечения. Существует ряд технологий выявления уязвимостей в веб-приложениях: white box (сканирование по принципу белого ящика), black box – сканирование по принципу черного ящика, penetration test – тест на проникновение, проверка кода вручную. К популярным сканерам относятся OWASP ZAP, W9scan, Wapiti, Arachni, Paros.

Важным аспектом безопасности веб-приложения является регулярная проверка сайта на наличие вирусов. Такая проверка осуществляется с помощью специальных модулей от хостинг-провайдера, или через онлайн сканирование системы на вирусы и наличие вредоносного кода, или установкой в веб-приложение скриптов для защиты.

Можно сделать вывод, что каждое веб-приложение нуждается в комплексной защите данных и постоянном анализе состояния защищенности системы. Компрометация конфиденциальных данных приложения может привести к финансовым и репутационным негативным последствиям. Несмотря на то, что с каждым годом количество веб-приложений с критически опасными уязвимостями уменьшается, вопрос обеспечения информационной безопасности остается актуальным. Для решения этой проблемы и поддержания высокого уровня защищенности данных необходимо сразу исправлять выявленные уязвимости.

**Литература. 1.** Лука Сафонов. Основные угрозы безопасности сайта / Лука Сафонов. – Режим доступа: https://habr.com/ru/post/279787/ **2.** Защите web-приложений / 22.11.2019. – Режим доступа: https://searchinform.ru/services/outsource-ib/zaschita-informatsii/zaschita-web-prilozhenij/ **3.** Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов. – 372с. **4**. SimplePay. OWASP TOP-10: практический взгляд на безопасность веб-приложений / 21.05.2015. – Режим доступа: https://habr.com/ru/company/simplepay/blog/258499/ **5.** Средства защиты веб-сайтов (приложений) / Web Application Fitewall. – Режим доступа: https://www.anti-malware.ru/security/web-application-firewall

**Реквизиты для справок:** *Россия, 656038, Барнаул, пр. Ленина 46, Алтайский государственный университет им. И.И. Ползунова, Шадрина А.Д., E-mail: nastulia99@mail.ru*

**УДК 003.26**

## ПРИМЕНЕНИЕ МНОГОФАЗНОГО КОДИРОВАНИЯ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ ВЫСОКОДИНАМИЧНЫХ ОБЪЕКТОВ

А. М. ТАРАСОВА, Ю. А. ОСОКИН

**Введение.** В настоящее время в автоматизированных системах, получивших широкое распространение в разнообразных сферах деятельности, существует множество нежелательных факторов, из-за которых решение проблем защиты высоко динамичных объектов становится чрезвычайно актуальным.

Работа высоко динамичных объектов сопряжена с частыми случаями возникновения нестабильных фаз движения, с вынужденным применением знакопеременных операций реверсного характера, с выходом с заданных программным алгоритмом траекторий.

При этом работа осуществляется в условиях активных проявлений внешних помеховых воздействий. Поэтому, для осуществления надежной и точной работы существует необходимость применения адекватных защитных методов и средств.

**Цель работы** – разработка высоко динамичных алгоритмов системы управления в условиях активных помеховых воздействий.

В данных условиях требуется применение высоконадежных методов кодирования и декодирования информации.

При этом, важными задачами являются [1].:

— разработка и реализация высокоскоростных алгоритмов работы динамичным объектов;

— разработка алгоритмов с минимальным временем реакции на события;

— обеспечение информационной безопасности данных.

Проанализировав характеристики применяемых устройств защиты, выбран вариант встраиваемой кодирующей системы, дающей возможности повышать степень защиты информации в условиях активных помеховых воздействий.

Встроенные средства кодирования программируются на самостоятельную работу. При этом рассмотрены варианты использования многофазового кодирования. Они применимы для технологических процессов, где развивается числовое программное управление ответственными объектами, требующими особо надежных средств обеспечения информационной безопасности (приводы винчестеров, высокоскоростных лифтов, это все виды транспортных средств: метро, электроподвижной состав, трамвайно-троллейбусные приводы, автотранспорт, беспилотные подвижные объекты (наземные, летающие, плавающие надводные и подводные) [2].

Примером реализации данного метода является система управления автоматическим манипулятором, работающим в четырех степенях свободы. Управление основным рабочим органом (захватом) манипулятора осуществляется на основе программирования операций. Это обеспечивается программной системой (ПС), управляющей формирователем команд (ФК) и далее исполнительными органами (ИО) манипулятора. Вариант структурной схемы системы управления и 4-фазного кодирования информации показан на рисунке 1.

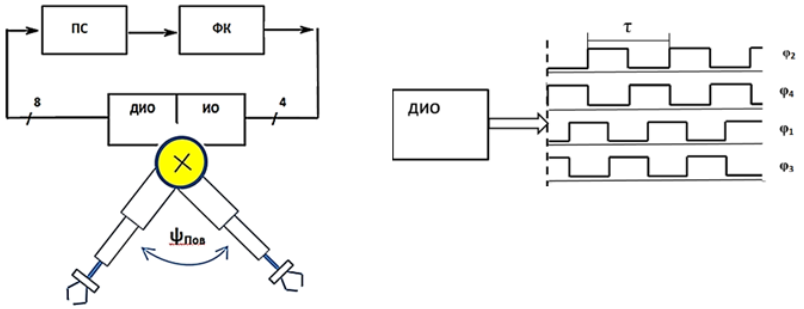



Рисунок 1 – Структурная схема системы управления и 4-фазное кодирование информации

Датчиком исполнительных органов (ДИО) формируется на сенсорном сегменте τ четыре импульса, которые имеют определенный фазовый сдвиг. Контрольная дистанция τ, охватываемая за один период: $\tau = L / N_c$, где L – контрольная дистанция за полный цикл, кадр сенсора, $N_c$ – разрядность датчика

Здесь $N_c$ = 1024 «единичных» сигналов, столько же «нулевых» и 2048 фронтов сигналов. Сдвиговые позиции фаз $\varphi_1$, $\varphi_2$, $\varphi_3$, $\varphi_4$ программно кодируются.

Многофазное кодирование выбрано на том основании, что этот метод дает возможность осуществлять передачу информации с широкими функциональными возможностями. В частности, выявлять и устранять внешние нежелательные воздействия, угрозы, которые, как правило, имеют синфазный характер и угрозы, которые имеют неадекватное кодирование. В рассматриваемой многофазной системе это осуществляется применением противофазных и сдвинутых на определенную величину фазовых контрольных составляющих.

**Многофазовое кодирование.** Многофазное кодирование эффективно для выявления и подавления при появлении импульсных помех в информационных каналах, для подавления внешних умышленных наводок. Для выявления позиционных и динамических помеховых факторов, при возникновении нештатных технологических и траекторных фаз, при появлениях знакопеременных воздействий, при проявлениях внешних помеховых воздействий в сигнальных линиях, цепях.

Основная идея метода фазового кодирования состоит в преобразовании фаз исходных информационных сигналов на кодируемые фазы, характер изменения которых позволяет в итоге отражать собой необходимые данные, которые скрыты в каналах передачи.

Так, распространенные методы передачи информации в форме определенного количества инкрементных импульсов в реальных технологических процессах с вариативной траекторией движения дают завышенное значение перемещения по заданной координате. Для выявления погрешностей при вариативном движении рассмотрен вариант применения многофазового кодирования, которое позволяет определить смену направления и повысить точность управления.

Сенсорная схема датчика многофазного кодирования (рисунок 2) контролирует вариативную траекторию движения, выдает многоканальную информацию с фазовым кодированием по каналу многофазового кодирования.

Система многофазового кодирования в локальном, ограниченном диапазоне контроля может быть 4-фазовой и 6-фазовой в неограниченном диапазоне.

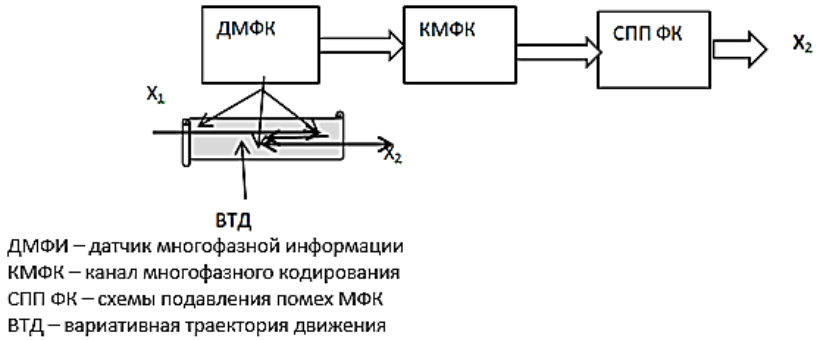



Рисунок 2 – Структурная схема многофазной кодирующей системы

Многофазным кодированием выявляются и устраняются синфазные сигналы, характерные для импульсных помех и внешних умышленных наводок на фоне противофазных, которые исключаются, например, схемами на основе ПЛИС. Данный метод опытно апробирован в экспериментах с применением фазоимпульсных сенсорных датчиков с формированием сигналов на основе 4- и 6-фазового кодирования.

**Выводы.** Метод фазового кодирования имеет лучшие функциональные возможности при высокоточном контроле позиционирования, при измерении динамических характеристик, для оценки направления движения объекта.

Важным преимуществом в сравнении с традиционными методами является быстрое считывание информации о динамике процесса и его направленности.

Фазовое кодирование дает возможность определить направление траектории движения, направленность технологического процесса. Фазоинверсное кодирование позволяет выявлять и устранять помеховое вмешательство. Многократное фазовое смещение позволяет увеличивать информативность сообщения в 2-4 раза. Параллельная обработка информации увеличивает быстродействие и, соответственно, скорость реакции системы на событие. Применение данного метода многофазного кодирования позволяет надежно обмениваться информацией при дистанционном управлении, в том числе при управлении беспилотными объектами [3]. Выполнение этих мер значительно снизит риск искажения информации.

**Литература. 1.** Генри Отт Методы подавления шумов и помех в электронных системах // Москва, 1979г. - [Электронный ресурс]. – Режим доступа: https://www.elec.ru/files/2020/02/13/_G._Ott-__Metodue_podavleniya_shumov_i_pomeh_v_yele.PDF **2.** Osokin Yu.A. High-speed algorithms for au-

tomatic manipulators control systems. // Journal of Physics: Conference Series. 2020. Vol. 1615. Article ID 012026. doi:10.1088/1742-6596/1615/1/012026. **3.** Тарасова А.М., Мысин А.Ю., Осокин Ю.А. “Дистанционный контроль движущегося беспилотного объекта в аграрном секторе” - [Электронный ресурс]. – Режим доступа: http://www.asau.ru/images/Dokument/dok/vestnik_mn_2.pdf

**Реквизиты для справок:** *Россия, 656038, Барнаул, пр. Ленина 46, Алтайский государственный технический университет им. И.И. Ползунова, Тарасова А.М., тел. 8(913)2287653, e-mail: anna.tarasova99@yandex.ru*

**УДК 004.056.53**

## МЕТОДЫ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ В СОВРЕМЕННЫХ СИСТЕМАХ ОБМЕНА МГНОВЕННЫМИ СООБЩЕНИЯМИ

А. Д. ТИХОНОВА, П. А. ТЕПЛЮК

Популярность систем обмена мгновенными сообщениями, или как их обычно называют «мессенджеров», стремительно растёт с каждым годом. Подтверждением тому является их большое разнообразие. Это даёт возможность пользователю в зависимости от его потребностей и желаний выбирать наиболее подходящие сервисы для обмена мгновенными сообщениями.

Системы обмена мгновенными сообщениями, мессенджеры – службы мгновенных сообщений, предназначенные для обмена различного рода информацией в режиме реального времени через сеть Интернет. Передаваемой информацией могут быть текстовые сообщения, файлы, звуковые сигналы, изображения, видео.

В настоящее время мессенджеры используются для различных целей: от повседневного общения до деловых переписок. Неразрывно с этим растёт актуальность проблемы обеспечения информационной безопасности обмена мгновенными сообщениями.

**Целью работы** является выбор эффективного метода обеспечения конфиденциальности для разработки мессенджера. Для достижения цели необходимо провести сравнительный анализ способов защиты в современных системах обмена мгновенными сообщениями.

Для сравнения были выбраны три наиболее популярных мессенджера в России:

– WhatsApp;

– Viber;

– Telegram.

Также был проанализирован мессенджер с открытым исходным кодом Signal, разработчики которого сделали основной акцент на конфиденциальности и безопасности.

Данные приложения имеют схожие базовые методы защиты, такие как авторизация по номеру телефона и двухфакторная аутентификация.

Авторизация при установке приложения и привязка номера телефона к аккаунту осуществляется путём подтверждения номера телефона. Через SMS-сообщение или звонок пользователь получает код, который ему необходимо ввести для подтверждения. При последующем запуске пароль не потребуется, что создаст угрозу информационной безопасности в случае кражи или утери устройства.

Возможность включения функции двухфакторной аутентификации позволяет установить пароль, который будет требоваться при входе в аккаунт с нового устройства [2].

Перечисленные выше мессенджеры главным образом отличаются друг от друга реализацией шифрования и наличием или отсутствием дополнительных функций, обеспечивающих конфиденциальность данных.

Приложение WhatsApp оснащено сквозным шифрованием данных, которое стало доступно в 2016 году. WhatsApp использует криптографический протокол, основанный на протоколе, используемом в другом мессенджере - «Signal» [3]. Сквозное шифрование (end-to-end encryption) – способ передачи данных, при котором информация шифруется в момент её передачи и расшифровывается в момент получения её адресатом, тем самым доступ к зашифрованным данным имеют только пользователи, участвующие при передаче.

В WhatsApp доступна функция подтверждения кода безопасности – общего ключа. Сравнение кодов безопасности даёт уверенность в том, что общение происходит с нужным человеком [2].

Однако WhatsApp имеет плохую репутацию по части информационной безопасности. Компанию неоднократно обвиняли в наличии серьёзных утечек данных пользователей и их переписок. Также, известны многочисленные случаи передачи переписок правоохранительным органам [3].

WhatsApp имеет закрытый исходный код и разработчики тщательно его скрывают. Поэтому нельзя наверняка утверждать, что в коде приложения нет заложенных уязвимостей, при использовании которых можно получить несанкционированный доступ к данным [1].

Также, при создании резервной копии данных, информация уже не шифруется и в дальнейшем хранится в облачном хранилище в незашифрованном виде, будучи потенциально доступной для злоумышленников [2].

Приложение Viber, в отличие от WhatsApp, имеет функцию скрытого чата, которая позволяет скрыть необходимую переписку, установив на неё PIN-код. При этом секретные чаты не синхронизуются на другие устройства. Также функция скрытого чата позволяет установить временной интервал для автоматического удаления сообщений. Скрытый чат защищён от пересылки сообщений и оснащён уведомлениями о скриншотах. Однако данная функция легко обходится фотографией самого экрана устройства с перепиской [5].

Viber также оснащён сквозным шифрованием, работающим по умолчанию. Но, как и в случае с WhatsApp, Viber имеет закрытый исходный код приложения, что также не даёт гарантии отсутствия намеренно введенных уязвимостей [1].

При связи с собеседником в мессенджере присутствует функция подтверждения кода безопасности.

Для данного мессенджера аналогична проблема создания резервных копий данных, хранящихся в облачном хранилище в незашифрованном виде [2].

Telegram – система обмена мгновенными сообщениями с открытым исходным кодом, основанная в 2013 году и позволяющая обмениваться текстовыми сообщениями, аудио, видео, изображениями, документами, а также имеющая функцию аудиозвонка.

Отличительной особенностью Telegram является собственный протокол сквозного шифрования данных MTProto. Данный протокол включает в себя следующий ряд технологий:

– симметричное шифрование AES с размером блоков 256 бит;

– ассиметричное 2048-битное шифрование RSA;

– протокол обмена ключами Диффи-Хеллмана, обеспечивающий мост между AES и RSA и позволяющий передавать по открытому каналу только публичные ключи [3].

Сквозное шифрование реализовано только в секретных чатах, синхронизация на другие устройства таких чатов отсутствует. Также в секретном чате стоит запрет на скриншот, но данная функция работает не на всех устройствах [5]. В случае, когда это возможно, в чате появится уведомление о сделанным пользователем скриншоте. Секретным чатом также поддерживается функция исчезающих по таймеру сообщений.

При передаче информации в обычном режиме она в зашифрованном виде передаётся через сервер. Telegram использует распределённую инфраструктуру хранения, отправки и обработки сообщений с поддержкой CDN-кэширования медиа [1]. Так, ключи шифрования, случайным образом разбитые на части, хранятся на разных серверах Telegram в разных странах, под разной юрисдикцией.

Резервные копии данных хранятся в режиме клиент-сервер с распределением ключа шифрования между разными серверами. Создание резервной копии секретного чата недоступно [3].

В мессенджере доступна функция двусторонней верификация пользователей путём сравнения кодов безопасности.

Для дополнительной защиты существует возможность назначения пароля при входе в мессенджер. Также, Telegram оснащён функцией просмотра активных сессий, в котором отображаются все активные сеансы с информацией об IP-адресе с возможностью завершения конкретной сессии [2].

Signal – система обмена мгновенными сообщениями с открытым исходным кодом, основанная в 2015 году, позволяющая пользователям обмениваться текстовыми сообщениями, аудио, видео, изображениями, файлами и совершать аудио-звонки.

Как и в случае с Telegram, Signal использует собственный разработанный алгоритм сквозного шифрования Signal Protocol, в который входят следующие алгоритмы:

– Curve25519;

– AES-256;

– HMAC-SHA256 [5].

Отличительной особенностью Signal является факт шифрования абсолютно всех данных: от личных и групповых чатов до списка контактов и данных личного профиля, дополнительно обеспечивая защиту персональных данных. Также мессенджер позволяет пользователям автоматически размывать лица людей на фотографиях.

Все переписки хранятся на устройстве пользователя локально и подвергаются локальному шифрованию при помощи парольной фразы перед отправкой на сервер. Перенос данных на другое устройство может осуществляться только напрямую между устройствами. После перемещения на старом устройстве произойдёт выход из аккаунта и удаление переписок с блокировкой возможности отправлять и принимать сообщения [4].

В Signal имеется возможность двухсторонней верификации сессии, при которой происходит сравнение кодов безопасности собеседников. В случае их совпадения сеть считается защищённой [5].

Также, в мессенджере Signal заблокированы функции скриншота и пересылки сообщений, есть возможность установки таймера на удаление сообщений [4].

В таблице 1 приведено сравнение методов обеспечения конфиденциальности в проанализированных системах обмена сообщениями [1].

Таблица 1 – Сравнительная характеристика методов обеспечения конфиденциальности в мессенджерах

| Аспект | WhatsApp | Viber | Telegram | Signal |
|---|---|---|---|---|
| Исходный код | скрыт | скрыт | открыт | открыт |
| Двухфакторная аутентификация | есть | есть | есть | есть |
| Тип шифрования | сквозное | сквозное | сквозное | сквозное |
| Протокол шифрования | основан на Signal | проприетарный | собственный MTProto | собственный Signal Protocol |
| Скрытые чаты | нет | есть | есть | есть |
| Запрет на скриншот | нет | сообщается в уведомлении | не для всех устройств | есть |
| Таймер удаления сообщений | нет | в секретных чатах | в секретных чатах | есть |
| Запрет на пересылку сообщений | нет | в секретных чатах | в секретных чатах | есть |
| Просмотр активных сессий | есть | нет | есть | есть |
| Дополнительный пароль при входе | нет | нет | есть | есть |
| Проверка кода безопасности | есть | есть | есть | есть |

Проанализировав методы обеспечения конфиденциальности в выбранных системах обмена мгновенными сообщениями выяснилось, что наиболее популярные мессенджеры в меньшей степени удовлетворяют требованиям конфиденциальности информации.

Также, на основе проведённого анализа можно сделать вывод, что сквозное шифрование является наиболее эффективным и оптимальным способом обеспечения конфиденциальности при обмене мгновенными сообщениями. В связи с этим, именно этот тип шифрования был выбран в качестве основного алгоритма защиты для разработки защищённого мессенджера.

**Литература. 1.** Подробное сравнение мессенджеров [Электронный ресурс]. Режим доступа: https://jayxt.github.io/MessengerComparison/ru/, свободный. **2.** Обзор безопасности популярных в России мобильных мессенджеров [Электронный ресурс]. Режим доступа: https://www.anti-malware.ru/analytics/Market_Analysis/security-overview-popular-mobile-messengers-in-russia, свободный. **3.** Viber, WhatsApp или Telegram: выясняем, что безопаснее [Электронный ресурс]. Режим доступа: https://www.iguides.ru/blogs/alt_vision_jeronimo/viber-whatsapp-ili-telegram-vyyasnyaem-chto-bezopasnee/, свободный. **4.** Какой мессенджер безопаснее: анализ Signal и iMessage [Электронный ресурс]. Режим доступа: https://www.iguides.ru/blogs/alt_vision_jeronimo/kakoy-messendzher-bezopasnee-teper-o-signal-i-apple-imessage/, свободный. **5.** Шифруйся грамотно! Выбираем мессенджер для безопасной и приватной переписки [Электронный ресурс]. Режим доступа: https://xakep.ru/2018/07/03/messengers/, свободный.

**Реквизиты для справок:** *Россия, 656038, Барнаул, ул. Ленина 46, Алтайский государственный технический университет им. И.И.Ползунова, Тихонова А.Д., тел. 8(903)9955148, e-mail: iam.tixon@mail.ru*

**УДК 004.772**

## СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТЕХНОЛОГИЙ ОРГАНИЗАЦИИ VPN-СОЕДИНЕНИЙ

А. И. ГОСТЕЕВА, Е. Е. ИСТРАТОВА

В век информационных технологий идет активное использование сетевого обмена информацией. Быстрый обмен данными – один из основных инструментов работы успешной корпорации. Однако обеспечить в таком случае защиту данных достаточно сложно. Одним из вариантов обеспечения такой передачи данных является построение VPN-сети. Данная технология позволяет не только обеспечивать надежное соединение поверх другой сети, но и дает возможность объединить удаленных пользователей в единую сеть. В качестве используемой среды в этом случае выступает сеть Интернет [1].

Сети на основе VPN получили широкое распространение среди компаний, которые имеют сотрудников, работающих удаленно. Помимо защищенности передаваемой информации, виртуальные частные сети решают множество задач и проблем для крупных компаний, например, таких, как: легкость администрирования системы, персонализация использования сетевых ресурсов, разграничение прав доступа к сетевым ресурсам и выделение защищенных участков [2]. Все вышеперечисленное делает данную технологию весьма востребованной и актуальной в сфере информационных технологий.

**Целью исследования** являлся сравнительный анализ применяемых в настоящее время технологий организации VPN-сетей.

Для реализации цели были выполнены следующие задачи: выбор наиболее характерных программных продуктов; определение критериев сравнения; сопоставление и анализ результатов.

Предварительно была проведена классификация VPN-сетей. По критерию защищенности виртуальные частные сети могут быть разделены на два вида: доверительные и защищенные.

Доверительный способ организации VPN осуществляется посредством использования протоколов Internet Protocol Security (Ipsec), то есть набора протоколов для обеспечения защиты данных, передаваемых по IP-сети. IPsec работает на сетевом уровне и может использоваться нативно со многими операционными системами, что позволяет использовать его без сторонних приложений, что принципиально отличает его от OpenVPN. IPsec также может работать в транспортном и туннельном режимах. В первом случае шифруются только данные передаваемого пакета, а исходный заголовок сохраняется, а во втором - шифруется весь передаваемый трафик, который затем инкапсулируется в поле данных нового IP-пакета. Транспортный режим IPsec применительно к созданию VPN-сетей используется в связке с другими реализациями, туннельный же сам по себе может являться методом создания VPN-туннеля.

Основными недостатками семейства протоколов IPsec являются небольшое число клиентов и сложность использования, что дополнительно требует применения протокола туннелирования второго уровня — L2TP (Layer 2 Tunneling Protocol). Подобное дополнение позволяет создавать VPN-сети с разграничением прав доступа, обладающие такими важными свойствами, как конфиденциальность и целостность передачи данных. Однако, помимо этого, также требуется обеспечить шифрование и аутентификацию всего трафика, проходящего на пакетном уровне. Именно для этой задачи и используется рассмотренный выше IPsec. Связка L2TP/IPsec присутствует во всех современных операционных системах и имеет простую настройку со стороны клиента. Данное решение на данный момент считается очень безопасным и стабильным при использова-

нии таких алгоритмов шифрования, как AES. Однако, поскольку он инкапсулирует данные дважды, то работает несколько медленнее реализаций, использующих SSL.

В отличие от доверительных, защищенные VPN-сети могут быть организованы за счет применения такого программного продукта, как, например, OpenVPN. Несмотря на то, что это – относительно новая технология с открытом исходным кодом для создания зашифрованного VPN-соединения точка-точка и сервер-клиент, она на данный момент поддерживается почти всеми операционными системами персональных компьютеров и является самой популярной технологией виртуальных частных сетей, которая прошла множество проверок на безопасность и не имеет никаких известных уязвимостей. Это делает данное решение очень надежным и объясняется использованием библиотеки OpenSSL и протоколов SSLv3/TLSv1 для шифрования данных. Благодаря перечисленным особенностям, данная реализация оказывается оперативнее по воздействию на аппаратные ресурсы, в отличие от связки L2TP/Ipsec. OpenVPN имеет возможность проходить через NAT и Firewall без их дополнительной конфигурации по стандартному для HTTPS порту TCP 443, благодаря SSL/TLS-инкапсуляции. В отличие от L2TP/IPsec, при данном способе организации VPN провайдеру сложнее заблокировать трафик. Также предусмотрена и работа по протоколу UDP. Несмотря на то, что TCP обеспечивает высокую надежность передачи данных, он имеет большие задержки по сравнению с UDP, связанные с подтверждением доставки пакетов. Из-за этого при использовании протокола TCP работа OpenVPN может даже оказаться медленнее, чем работа L2TP/Ipsec.

К основным недостаткам OpenVPN можно отнести необходимость установки специального клиентского программного обеспечения для работы с мобильными операционными системами iOS и Android, что не требуется Ipsec.

В качестве ключевых критериев сравнения были выбраны следующие характеристики: вид и стоимость лицензии на программное обеспечение; необходимость установки специализированного программного обеспечения для обеспечения надежности работы; тип используемого шифрования; виды применяемых портов.

Для проведения сравнительного анализа для каждой вида организации VPN-соединений были определены все критерии. Полученные абсолютные значения были переведены в относительные для удобства сопоставления и оценивания. В результате была использована шкала от 1 до 3 баллов, где 1 — минимальное значение критерия, а 3 — максимальное. Результаты представлены в табл. 1.

Таблица 1 – Результаты сравнения OpenVPN и L2TP/IPsec

| Критерии сравнения | OpenVPN | L2TP/IPsec |
|---|---|---|
| Лицензия | 3 | 1 |
| Специализированное ПО | 2 | 3 |
| Шифрование | 3 | 2 |
| Порты | 3 | 1 |

Таким образом, на основе данных таблицы можно сделать вывод о том, что каждая из технологий имеет свои преимущества и недостатки. Так, VPN на базе протокола L2TP/IPsec является лучшим решением для мобильных устройств, благодаря своей простоте настройки, надежности и стабильности. В то время, как VPN на базе протокола OpenVPN подойдет для организации небольшой локальной сети из отдельных персональных компьютеров, благодаря своей защищенности, безопасности и гибкости настроек.

**Литература. 1.** Друк Е.В. Основы организации и управления VPN-сетями современных информационных систем специального назначения / Е.В. Друк. И.В. Левко // T-Comm. 2019. № 6. URL: https://cyberleninka.ru/article/n/osnovy-organizatsii-i-upravleniya-vpn-setyami-sovremennyh-informatsionnyh-sistem-spetsialnogo-naznacheniya (дата обращения: 11.12.2020). **2.** Николахин А.Ю Использование технологии VPN для обеспечения информационной безопасности // Экономика и качество систем связи. 2018. № 3 (9). URL: https://cyberleninka.ru/article/n/ ispolzovanie-tehnologii-vpn-dlya-obespecheniya-informatsionnoy-bezopasnosti (дата обращения: 11.12.2020).

**УДК 004.774.6**

## ОПРЕДЕЛЕНИЕ СТЕКА ТЕХНОЛОГИЙ ДЛЯ РАЗРАБОТКИ ЗАЩИЩЕННОГО ОТ ВНЕШНЕГО ВОЗДЕЙСТВИЯ WEB-РЕСУРСА

И. И. ФРОЛКОВ

В 21 веке происходит глобальная автоматизация всех бизнес процессов, в следствие чего мгновенно увеличивается число web-ресурсов. Сейчас нельзя представить себе какую-либо компанию, организацию, магазин, сервис и так далее без своего собственного web-приложения. Для разработки такого приложения используются самые разнообразные средства и технологии. При этом программисты расходятся во мнении,

какие средства лучше использовать. На выбор средств разработки могут повлиять такие критерии, как требуемая сложность и функциональность сайта, а также надежность, безопасность и затрачиваемые ресурсы. К сожалению, немногие web-программисты уделяют должное внимание защищенности web-ресурса. При этом взлом web-приложений – это на сегодняшний день один из наиболее частых видов атак на различные организации и частные лица. Это приводит к различным неутешительным последствиям как для компаний, так и для простых пользователей.

**Целью работы** является определение наиболее подходящего стека технологий для разработки защищенного от внешнего воздействия web-ресурса.

Стек технологий включает в себя такие компоненты, как операционная система (ОС), система управления базами данных (СУБД), язык программирования, web-сервер, а также frameworks. Чтобы выбрать наиболее подходящий стек технологий для разработки защищенного от внешнего воздействия web-ресурса, возьмем самые используемые компоненты стека и проанализируем их на уязвимости. Для этого изучим банк данных угроз безопасности информации ФСТЭК России [1], базу данных общеизвестных уязвимостей информационной безопасности Common Vulnerabilities and Exposures (CVE) от компании MITRE [2] и CVE-Search от компании CIRCL [3].

Статистика уязвимостей серверных операционных систем представлена в таблице 1.

Таблица 1 – Статистика уязвимостей ОС по версии ФСТЭК\MITRE\CIRCL

| Операционная система | Уязвимости за 2019 год | Уязвимости за 2020 год | Общее число уязвимостей за все время ведения статистики |
|---|---|---|---|
| CentOS | 0\5\5 | 0\27\2 | 990\51\19 |
| Debian | 955\107\7 | 152\871\6 | 5298\10727\189 |
| Red Hat | 448\1\0 | 129\8\3 | 2724\180\171 |
| Ubuntu | 474\139\9 | 113\1204\15 | 1058\7921\132 |
| Windows Server | 133\217\214 | 1\1241\1240 | 751\8196\8190 |

Проанализировав данные таблицы 1, можно сделать вывод, что в различных базах данных количество уязвимостей для каждой системы отличается. Это объясняется тем, что интервалы между обновлениями баз различаются (одни обновляются чаще, другие реже), а также тем, что базы используют индивидуальные системы оценки уязвимостей. Чтобы

обобщить различные источники, мы будем использовать максимальное число уязвимостей для выбранных периодов. Операционные системы Windows Server, Ubuntu и Debian обладают наибольшим числом уязвимостей, поэтому они не подходят для безопасной разработки web-ресурса. Если сравнивать CentOS и Red Hat, то можно заметить, что у CentOS уязвимостей меньше, но данная операционная система – это бесплатный дистрибутив Red Hat, в связи с чем она не обладает поддержкой и доступом к официальным репозиториям RPM, а также не имеет своевременных исправлений безопасности и обновлений программного обеспечения. Из всего вышесказанного можно сделать вывод, что Red Hat – наиболее подходящая операционная система для разработки безопасного web-ресурса.

Для анализа web-серверов мы также будем использовать наибольшее число уязвимостей из каждой базы данных. Обобщенные данные об уязвимостях web-серверов представлены в таблице 2.

Таблица 2 – Статистика уязвимостей web-серверов

| web-сервер | Уязвимости за 2019 год | Уязвимости за 2020 год | Общее число уязвимостей за все время ведения статистики |
|---|---|---|---|
| NGINX | 9 | 28 | 86 |
| LiteSpeed | 0 | 0 | 7 |
| Microsoft IIS | 0 | 3 | 116 |
| Apache | 38 | 204 | 1660 |

Таблица 2 показывает, что наибольшее количество уязвимостей имеют Apache и Microsoft IIS. LiteSpeed – самый безопасный веб-сервер с точки зрения информационной безопасности. Но с точки зрения программирования у него есть ряд недостатков. Например, данный web-сервер используется лишь в 6,8% сайтов. В связи с этим, у LiteSpeed очень мало документации и обсуждений на форумах, что, в случае возникновении какой-либо проблемы, значительно усложнит ее решение. Выводом из всего вышесказанного является то, что NGINX – наиболее подходящий web-сервер. Процент использования NGINX практически такой же, как у Apache, но данный web-сервер обладает значительно меньшим числом уязвимостей.

На основе тех же баз данных проведем анализ уязвимостей систем управления базами данных. Обобщенные данные об уязвимостях систем управления базами данных представлены в таблице 3.

Таблица 3 – Статистика уязвимостей СУБД

| Система управления базами данных | Уязвимости за 2019 год | Уязвимости за 2020 год | Общее число уязвимостей за все время ведения статистики |
|---|---|---|---|
| Microsoft SQL Server | 1 | 9 | 129 |
| PostgreSQL | 3 | 26 | 197 |
| MySQL | 71 | 128 | 1244 |
| Oracle DB | 9 | 46 | 598 |

Проанализировав таблицу 3, можно сказать, что наименьшее число уязвимостей имеют СУБД Microsoft SQL Server и СУБД PostgreSQL. Если речь идет о крупной компании, то несомненно лучше выбрать Microsoft SQL Server, так как он считается наиболее надежным, но частные лица или небольшие конторы данную СУБД использовать не смогут, ведь она имеет огромные потребности в ресурсах. В связи с этим СУБД PostgreSQL – оптимальный вариант в большинстве случаев.

Далее разберем уязвимости PHP-Frameworks. Статистика агрегированных данных уязвимостей фреймворков представлена в таблице 4.

Таблица 4 – Статистика уязвимостей PHP-Frameworks

| framework | Уязвимости за 2019 год | Уязвимости за 2020 год | Общее число уязвимостей за все время ведения статистики |
|---|---|---|---|
| Yii | 0 | 0 | 11 |
| CodeIgniter | 0 | 1 | 18 |
| Laravel | 5 | 2 | 19 |
| Symfony | 12 | 3 | 51 |
| Zend framework | 3 | 2 | 108 |

Из таблицы 4 можно определить, что самое большое число уязвимостей имеют Symfony и Zend framework. Самым безопасным же является Yii. Кроме своей безопасности данный фреймворк очень распространен в Российской Федерации, имеет множество русскоязычной документации и профессиональных форумов.

Проанализировав все компоненты стека технологий, можно сделать вывод, что наилучшим выбором для разработки web-ресурса, защищенного от внешнего воздействия, будет следующий стек технологий:

– серверная операционная система Red Hat Enterprise Linux;

– web-сервер NGINX;
– СУБД PostgreSQL;
– PHP-frameworks Yii.

**Литература. 1.** ФСТЭК России. Банк данных угроз безопасности информации / 11.12.2020. – Режим доступа: https://bdu.fstec.ru/vul **2.** CVE. Search CVE List / 09.12.2020. – Режим доступа: https://cve.mitre.org/cve/search_cve_list.html **3.** CIRCLE. CORCL CVE Search / 11.12.2020. – Режим доступа: https://cve.circl.lu/

**Реквизиты для справок:** *Россия, 656038, Барнаул, пр. Ленина 46, Алтайский государственный университет им. И.И. Ползунова, студент Фролков Илья Игоревич, E-mail: frolkov.1999@mail.ru*

**УДК 004.772**

## МЕТОДЫ ПОДМЕНЫ ПАКЕТОВ ПРИ СЕТЕВОЙ ПЕРЕДАЧЕ ДАННЫХ

Е. Е. ИСТРАТОВА, В. В. ШУМКИН, Б. Д. ЗАХАРОВ

Информационные технологии в наше время проникли во все сферы жизни, они используются в медицине, в банках, в военных и промышленных целях. Все это представляет собой большие потоки данных, которые необходимо защитить от несанкционированного доступа третьих лиц. Несмотря на то, что корпорации тратят огромные средства на обеспечение безопасности в сетях, злоумышленники находят новые способы для проникновения сквозь защиту и кражи данных [1].

Современные сетевые технологии имеют множество уязвимостей, связанных как с возможными программными и аппаратными ошибками, так и с неправильным конфигурированием оборудования. Наличие различных уязвимостей в сети является для злоумышленников возможностью реализовать те или иные виды атак [2]. К наиболее распространенным их видам относятся следующие:

– сканирование и анализ сетевого трафика;
– угроза определения пароля;
– отказ в обслуживании;
– подмена одного объекта сети на другой и его отправка по каналам связи;
– навязывание ложного маршрута сети;
– удаленный запуск приложений.

С точки зрения защиты данных пользователей наиболее опасной является угроза подмены пакетов.

**Цель статьи** заключается в анализе существующих методов подмены пакетов при сетевой передаче данных и определении соответствующих средств обеспечения безопасности в сети.

В компьютерных сетях данные передаются фрагментировано с помощью «пакетов», включающих информацию об источнике и получателе передаваемых по сети данных.

В настоящее время выделяют следующие восемь основных методов подмены пакетов, воздействующих на сеть в процессе передачи данных:

1) UDP Storm приводит к перезагрузке сервера, действуя через открытые UDP-порты. Например, злоумышленник отправляет запрос на какой-нибудь служебный порт, но в качестве отправителя указывает открытый UDP-порт. В результате порты начинают бесконечно отвечать друг другу, что снижает работоспособность сервера. Данный вид атаки останавливается в случае утери пакета или при полной перезагрузке сервера.

2) UDP Bomb вызывает экстренное завершение всех процессов в сети. Принцип действия заключается в том, что злоумышленник отсылает системе некорректно настроенный UDP-пакет, содержащий неправильные поля со служебными данными. В тот момент, когда система принимает и обрабатывает этот пакет, начинаются проблемы, которые могут привести к экстренному завершению всех процессов.

3) Dummy ARP опасен в случае наличия открытого физического доступа к компьютеру в сети, в результате которого злоумышленник может подделать ARP-ответ и выдать себя за другой компьютер в сети, получив его IP-адрес. Это объясняется тем, что такие устройства, как маршрутизатор, коммутатор и ARP- сервер знают какому IP-адресу принадлежит определенный MAC-адрес. Таким образом, он будет принимать все пакеты предназначенные этому узлу, что возможно только в случае отсутствия этого компьютера в сети.

4) Puke вызывает отключение клиента со стороны сервера и связано с тем, что злоумышленник отравляет сфабрикованный ответ ICMP, представляющий собой ошибку удаленной сети, в результате чего сервер считает, что клиент не имеет доступа к данному ресурсу. Данный метод применяется в качестве побочного этапа взлома сервера, если взломщику необходимо отсутствие клиента в сети.

5) Fake unreachable похож на предыдущий метод подмены пакетов и работает по схожему алгоритму, за исключением того, что взломщик фабрикует сообщение о том, что пакет не может быть доставлен, тем самым провоцируя сервер на отключение клиента, ввиду неполадок из-за доставки сообщения.

6) IP-Spoofing представляет собой метод подмены IP-адреса. При этом существует два способа его использования. Первый заключается в

подмене своего реального IP-адреса ложным. Это нужно в том случае, если доступ к ресурсу имеют только определенные IP-адреса. В итоге злоумышленник меняет свой адрес на привилегированный, что позволяет ему получить открытый доступ к необходимому ресурсу. Второй способ заключается в том, что злоумышленник отправляет специально сгенерированные пакеты на адрес пользователя, к которому он подключился с целью вызвать у него перегрузку. Перегрузка позволяет перенаправить чужой трафик на себя, что, в свою очередь, помогает избежать аутентификации.

7) Buffer Overflow является переполнением буфера и относится к опасным методам кибератак, в ходе которых атакующий формирует пакет таким образом, чтобы переполнить графу «данные» пакета, вследствие этого данные, превышающие объем графы «данные», переходят в другие файлы, в том числе в заголовочные, тем самым вызывая обработку процессором тех данных, которые спровоцировали переполнение. Это может быть использовано как для выполнения опасного кода на компьютере, так и для перераспределения прав доступа.

8) Nuke работает только на старых версиях Windows, имеющих некоторые специфические принципы взаимодействия с файлами и устройствами в сети. Для работы с файлами и принтерами система использует протокол NetBIOS, открывающий в системе три TCP-порта (137, 138, 139). Угроза заключается в том, что если послать в открытый 139 порт несколько подобных «сообщений» подряд, то система не сможет корректно обработать данные и приостановит свое действие.

Таким образом, на основе информации о видах угроз и механизмах воздействия злоумышленников, можно предложить следующий ряд мер по предотвращению угроз со стороны методов подмены пакетов при передаче данных по сети. Для предотвращения воздействия первых двух методов необходимо избегать ситуации, когда UDP-порты доступны, а также применения сервисов, принимающих напрямую UDP-пакеты. Также можно экранировать такие порты при помощи межсетевых экранов. Решение проблемы Dummy ARP заключается в использовании программного обеспечения, которое бы отслеживало изменения MAC-адресов и следило бы за файлами ARP-сервера. Самым простым способом предотвращения атаки IP-спуфинг является правильная настройка управления доступом. Чтобы снизить потенциальный вред от данного вида атаки, необходимо контролировать доступ любого трафика, поступающего из внешней сети с адресом, который должен располагаться во внутренней сети. Однако данный способ борьбы может стать менее эффективным, если некоторые адреса внешней сети являются санкционированными.

**Литература. 1.** Галушка В.В. Методика выявления сетевых атак класса «Человек посередине» на основе анализа транзитного трафика / В.В. Галушка и др. // ИВД. 2017. №3 (46). URL: https://cyberleninka.ru/article/n /metodika-vyyavleniya-setevyh-atak-klassa-chelovek-poseredine-na-osnove-analiza-tranzitnogo-trafika (дата обращения: 10.12.2020). **2.** Черкасов Д.Ю. IP-spoofing / Д.Ю. Черкасов, В.В. Иванов // Евразийский научный журнал. 2017. №6. URL: https://cyberleninka.ru/article/n/ip-spoofing (дата обращения: 10.12.2020).

**Реквизиты для справок:** *Россия, 630073, Новосибирск, пр. К. Маркса, 20, Новосибирский государственный технический университет, кандидату технических наук, доценту кафедры автоматизированных систем управления, Истратовой Е.Е., тел. 8-952-921-86-29. E-mail: istratova@mail.ru*

# СОДЕРЖАНИЕ

## РАЗДЕЛ 1. ОБЩИЕ ВОПРОСЫ РАСЧЕТА И ПРОЕКТИРОВАНИЯ ПРОГРАММНО-ТЕХНИЧЕСКИХ СРЕДСТВ ДЛЯ РЕШЕНИЯ ЗАДАЧ ИЗМЕРЕНИЯ, КОНТРОЛЯ И АВТОМАТИЗАЦИИ



## РАЗДЕЛ 2. ИНФОРМАЦИОННЫЕ СИСТЕМЫ, ИЗМЕРИТЕЛЬНЫЕ И УПРАВЛЯЮЩИЕ КОМПЛЕКСЫ

## РАЗДЕЛ 3. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ