МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ИТМО

# АЛЬМАНАХ НАУЧНЫХ РАБОТ МОЛОДЫХ УЧЕНЫХ Университета ИТМО

## Том 1


Санкт-Петербург

2018

Альманах научных работ молодых ученых Университета ИТМО. Том 1. – СПб.: Университет ИТМО, 2018. – 297 с.

Издание содержит результаты научных работ молодых ученых, доложенные на XLVII научной и учебно-методической конференции Университета ИТМО по тематике: компьютерные технологии и управление.

ISBN 978-5-7577-0589-7
ISBN 978-5-7577-0590-3 (Том 1)

УНИВЕРСИТЕТ ИТМО

Университет ИТМО – ведущий вуз России в области информационных и фотонных технологий, один из немногих российских вузов, получивших в 2009 году статус национального исследовательского университета. С 2013 года Университет ИТМО – участник программы повышения конкурентоспособности российских университетов среди ведущих мировых научно-образовательных центров, известной как проект «5 в 100». Цель Университета ИТМО – становление исследовательского университета мирового уровня, предпринимательского по типу, ориентированного на интернационализацию всех направлений деятельности.

# ВВЕДЕНИЕ

Издание содержит результаты научных работ молодых ученых, доложенные 30 января – 2 февраля 2018 года на XLVII научной и учебно-методической конференции Университета ИТМО по тематике: компьютерные технологии и управление.

Конференция проводится в целях усиления интегрирующей роли университета в области научных исследований по приоритетным направлениям развития науки, технологий и техники и ознакомления научной общественности с результатами исследований, выполненных в рамках государственного задания Министерства образования и науки РФ, программы развития Университета ИТМО на 2009–2018 годы, программы повышения конкурентоспособности Университета ИТМО среди ведущих мировых научно-образовательных центров на 2013–2020 гг., Федеральной целевой программы «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014–2020 годы», грантов Президента РФ для поддержки молодых российских ученых и ведущих научных школ, грантов РФФИ, РГНФ, РНФ и Правительства РФ (по постановлению № 220 от 09.04.2010 г.) и по инициативным научно-исследовательским проектам, проводимым учеными, преподавателями, научными сотрудниками, аспирантами, магистрантами и студентами университета, в том числе в содружестве с предприятиями и организациями Санкт-Петербурга, а также с целью повышения эффективности научно-исследовательской деятельности и ее вклада в повышение качества подготовки специалистов.

**Гайфулина Диана Альбертовна**
Год рождения: 1995
Университет ИТМО, факультет безопасности информационных технологий, кафедра безопасности киберфизических систем, студент группы № N4159
Направление подготовки: 10.04.01 – Информационная безопасность
e-mail: wing7803@yandex.ru

**УДК 004.056**

# АНАЛИТИЧЕСКИЙ ОБЗОР МЕТОДОВ ОБНАРУЖЕНИЯ АНОМАЛИЙ СЕТЕВОГО УРОВНЯ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

**Гайфулина Д.А.**
**Научный руководитель – д.т.н., доцент Беззатеев С.В.**

Работа выполнена в рамках темы НИР № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность».

В работе проводилось исследование экспертных знаний, которые используются для разработки методик выявления аномалий функционирования киберфизических систем. Для этого выполнен аналитический обзор существующих методов обнаружения аномалий с выявлением их основных преимуществ и недостатков.
**Ключевые слова:** киберфизические системы, обнаружение аномалий, методы интеллектуального анализа, поведенческие методы.

**Введение.** В настоящее время находят все более широкое применение киберфизические системы (КФС), представляющие собой совокупность устройств, вычислительный процесс которых тесно связан с реакцией на процессы физического окружения и выполняется в рамках некоторой физической платформы [1]. В рамках обеспечения безопасного функционирования КФС в работе ставилась цель: выявление достоинств и недостатков существующих методов обнаружения аномалий для оценки их применения при разработке методик выявления аномалий в КФС. В соответствии с ней, определяются следующие задачи:

- выявить особенности аномальной активности функционирования КФС;
- провести сравнительный анализ существующих методов обнаружения аномалий.

**Особенности аномальной активности функционирования КФС.** Общая структура любой КФС может быть разделена на три уровня [2]: прикладной уровень (включает физические устройства и контроллеры), сетевой уровень (реализует связь устройств между собой и с модулями обработки данных) и уровень восприятия (выполняются функции по обработке и хранению данных).

Под аномалиями понимаются, главным образом, отклонения значений данных, передаваемых и обрабатываемых в системе, от определенного нормального поведения. На рис. 1 отображена общая структура КФС с возможным проявлением аномальной активности.

Причинами возникновения аномалий могут являться случайное отклонение от штатного режима работы или намеренное нарушение безопасности – внедрение вредоносного программного обеспечения, физическое воздействие и сетевые атаки. Способы проявления аномалий в КФС выделяют как отключение и отказ ее элементов, перегрузку сетевого оборудования и сервисов [3], т.е. как результаты реализации угроз безопасности КФС. Основные угрозы безопасности на прикладном уровне представляют собой угрозы физической безопасности объектов и сбора информации. Угрозы сетевого уровня

направлены на нарушение безопасной передачи информации и целостности сетевой архитектуры. Угрозы уровня восприятия имеют целью нарушение выполнений функций по сбору, хранению и обработке данных.

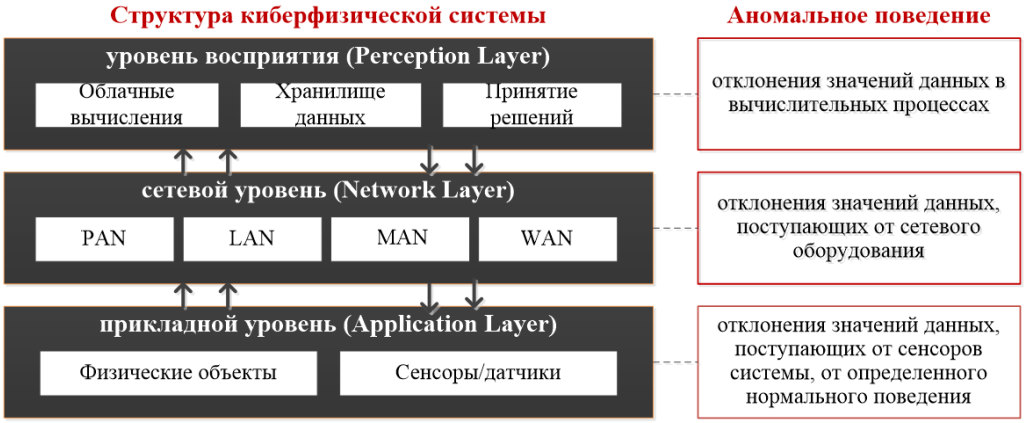



Рис. 1. Проявление аномальной активности на различных уровнях КФС

**Сравнительный анализ методов обнаружения аномалий.** Обнаружение аномалий в КФС – это процесс идентификации подозрительной деятельности, направленной на ресурсы киберфизической системы, путем выявления существенных отклонения функционирования КФС от «нормального» профиля состояния системы.

В работе предложена классификация методов обнаружения аномалий, представленная на рис. 2.

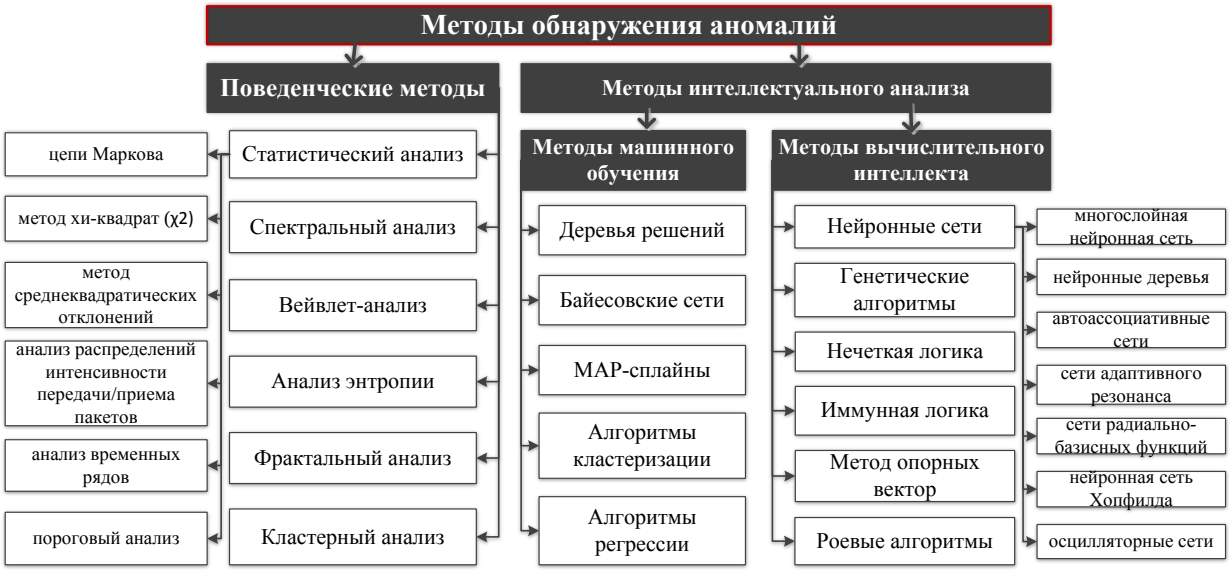



Рис. 2. Схема классификации методов обнаружения аномалий

В процессе исследования была изучена информация о применении данных методов для выявления аномалий, описанная в различных научных трудах.

При использовании поведенческих методов для построения модели нормального поведения используется набор контролируемых параметров системы, для которых может быть задан допустимый диапазон значений, построена матрица вероятности смены состояний, временной ряд или выбрано иное представление.

Методы интеллектуального анализа данных (ИАД) позволяют автоматически построить необходимую модель нормального поведения системы на основе некоторых обучающих данных, которые могут представлять собой набор правил поведения или вероятностные зависимости множества событий. В случае машинного обучения данный процесс проводится при помощи средств численных методов, методов оптимизации и различных техник работы с

данными в цифровой форме, вычислительного интеллекта – эвристических алгоритмов, используемых, например, в нечеткой логике, искусственных нейронных сетях. Процесс обнаружения аномалий представляет собой определение показателя неправильно предсказанных команд, т.е. фактически обнаруживается отличие в поведении объекта за счет поиска закономерностей в собранных данных и прогнозирования развития процессов [4].

Одними из основных требований, предъявляемых к данным решениям, являются обеспечение адаптивной и высоко масштабируемой аналитической обработки событий, обеспечивающей интеллектуальное управление большими объемами данных о безопасности в реальном или близком к реальному масштабу времени. Для анализа данных групп методов обнаружения аномалий в работе предлагается провести их сравнение по следующим характеристикам:

- однозначность выявления аномалии (ОВ);
- простота интерпретации результатов (И);
- адаптация к изменяющемуся поведению системы (А);
- необходимость большой выборки исходных данных для построения нормальной модели поведения (ВД);
- необходимость предварительного обучения для построения нормальной модели поведения (ПОб);
- возможность работы с большим объемом входных и выходных данных (БД).

Сравнительная характеристика поведенческих методов обнаружения аномалий приводится в таблице.

Таблица. Сравнительный анализ методов обнаружения аномалий

| Наименование метода | ОВ | И | А | ВД | ПОб | БД |
|---|---|---|---|---|---|---|
| Поведенческие методы | | | | | | |
| Статистический анализ | | | | | | |
| цепи Маркова | + | + | + | – | + | – |
| метод хи-квадрат ($\chi^2$) | + | + | – | + | + | – |
| среднеквадратические отклонения | + | + | + | + | + | – |
| анализ распределений интенсивности передачи/приема пакетов | – | + | – | + | – | – |
| анализ временных рядов | – | – | + | + | – | – |
| пороговый анализ | – | + | – | + | – | – |
| вейвлет-анализ | + | – | + | – | + | + |
| анализ энтропии | – | + | – | + | – | – |
| спектральный анализ | – | + | – | + | + | – |
| фрактальный анализ | + | – | – | + | + | – |
| кластерный анализ | + | – | – | + | + | – |
| Методы машинного обучения | | | | | | |
| Деревья решений | + | + | + | + | + | – |
| Байесовские сети | + | + | – | – | + | + |
| MAP-сплайны | + | – | – | + | + | + |
| Алгоритмы кластеризации и регрессии | + | + | – | + | + | + |
| Методы вычислительного интеллекта | | | | | | |
| Нейронные сети | + | – | + | + | + | + |
| Генетические алгоритмы | – | – | + | + | + | + |
| Нечеткая логика | – | – | + | + | + | – |
| Иммунные системы | + | – | + | + | + | + |
| Метод опорных векторов | – | + | – | – | + | + |
| Роевые алгоритмы | + | – | + | + | + | + |

Таким образом, преимуществами поведенческих методов являются простота интерпретации результатов анализа состояния системы, и как следствие, возможность проследить динамику процессов для выявления новых типов аномалий. Недостатками являются требования к наличию большого числа исходных данных для описания модели нормального поведения системы. Сложность описания данной модели становится причиной низкой достоверности обнаружения, так как важную роль играет правильный выбор данных параметров, в результате модель нормального поведения может оказаться неполной или избыточной, что приведет к пропуску атак или ложным срабатываниям.

Методы ИАД обладают большей адаптивностью к изменению поведения системы, за счет чего позволяют создавать и поддерживать системы обнаружения аномалий с меньшим вмешательством человека. Данные методы позволяют более эффективно выполнить оценку состояния наблюдаемых процессов, выявлять и ранжировать причины значимых изменений, прогнозировать и вырабатывать рекомендации. При использовании методов ИАД, аналогично поведенческим, возникает необходимость правильного выбора признаков нормального поведения системы, пригодных для обучения и проверки моделей анализа для минимизации пропусков аномалий и ложных срабатываний. Еще одним недостатком применения методов ИАД является относительная сложность интерпретации результатов в связи с динамикой изменения модели обнаружения.

Перспективными направлениями при проектировании систем выявления аномалий в настоящее время видится гибридизация подходов, которая позволила бы совмещать в себе преимущества различных методов и нивелировать их недостатки. Одним из вариантов такой гибридизации может являться использование методов ИАД для задания пороговых значений или преобразования входных параметров тестовых данных для построения модели нормального поведения системы.

**Заключение.** Результатом выполнения научно-исследовательской работы было выявление достоинств и недостатков существующих методов обнаружения аномалий для оценки их применения при разработке методик выявления аномалий в КФС. Выявлены особенности аномальной активности функционирования КФС. Проведен сравнительный анализ существующих методов обнаружения аномалий, по результатам которого определены основные преимущества и недостатки их применения в задачах обнаружения аномалий.

**Литература**

1. Henzinger T., Sifakis J. The Embedded Systems Design Challenge // Lecture Notes in Computer Science. – 2006. – V. 4085. – С. 1–15.
2. Katunzi B.R. Structure of Typical Iot Setup [Электронный ресурс]. – Режим доступа: http://www.theseus.fi/bitstream/handle/10024/119418/katunzi_bernard.pdf?sequence=1 (дата обращения: 17.12.2017).
3. Десницкий В.А., Котенко И.В., Ногин С.Б. Обнаружение аномалий в данных для мониторинга компонентов защиты Интернета вещей // XVIII Международная конференция по мягким вычислениям и измерениям (SCM'2015). Сборник докладов. – 2015. – Т. 2. – С. 17–22.
4. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. – 2016. – № 2(45). – С. 207–244.

**Давыдов Вадим Валерьевич**
Год рождения: 1997
Университет ИТМО, факультет безопасности информационных технологий, кафедра безопасности киберфизических систем, студент группы № N4159
Направление подготовки: 10.04.01 – Информационная безопасность
e-mail: davvad97@mail.ru

**УДК 004.716**

## ЗАЩИЩЕННЫЕ ПРОТОКОЛЫ В INTERNET OF VEHICLES ДЛЯ АУТЕНТИФИКАЦИИ ПО МЕСТОПОЛОЖЕНИЮ

**Давыдов В.В.**
**Научный руководитель – д.т.н., профессор Беззатеев С.В.**

Работа выполнена в рамках темы НИР № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность».

В современном мире, все больше и больше людей задумываются об использовании новых технологий, таких как сенсорные сети или Интернет вещей, в построении интеллектуальной дорожной инфраструктуры. Это развитие еще не получило широкого распространения из-за малого количества электромобилей, из-за их высокой цены и недоступности для большей части мирового населения. Очевидно, что в будущем, когда такая технология не станет новинкой, ее цена постепенно упадет, а количество владельцев увеличится, и все это будет сводиться к инфраструктуре, которая позволит автомобилям контролировать ситуацию на дорогах и решать часть проблем для того, чтобы сделать жизнь человека более удобной. В данной работе проведен анализ существующих методов позиционирования, а также описаны защищенные протоколы безопасности при передаче данных от автомобиля до базовой станции.
**Ключевые слова:** автомобиль, дорожная инфраструктура, информационная безопасность, протоколы безопасности, аутентификация по местоположению.

Проблема позиционирования транспортных средств на дороге стала очень важной в связи с развитием и желанием создать «самоуправляемые» автомобили, которые могут передвигаться по территории без какого-либо участия человека. В связи с этим одной из важнейших задач стоит безопасность использования таких технологий позиционирования. Аутентификация по местоположению в таком контексте играет значимую роль. При каких-либо инцидентах на дороге крайне важно правильно аутентифицировать виновника происшествия, узнать местоположение аварии. Прежде чем рассматривать аспекты безопасности, кратко опишем уже существующие методы позиционирования. Все методы локализации можно условно разделить на две группы: прямые и косвенные подходы [1].

Первый подход также известен как абсолютная локализация. Он использует сети Wireless Sensor Network (WSN). Каждый датчик оснащен приемником Global Positioning System (GPS). Этот метод эффективный, но дорогостоящий и громоздкий. Кроме того, экономически нецелесообразно оснащать каждый датчик приемником GPS, поскольку WSN развертываются с помощью сотен тысяч датчиков. Вторая проблема заключается в том, что GPS работает не везде. К примеру, на закрытых парковках или глубоких туннелях определение местоположения с помощью GPS не представляется возможным.

Второй подход является косвенным или, называя по-другому, относительной локализацией. Этот подход был разработан в первую очередь для исправления некоторых недостатков системы GPS, например, той же точности определения местоположения в труднодоступных местах.

Далее кратко опишем каждый из методов позиционирования.

1. Относительная локализация. Транспортные средства (ТС) условно можно разделить на две группы: оборудованные и необорудованные. Оборудованные ТС оснащены GPS-устройством, позволяющим им отслеживать свою географически-временную траекторию, а необорудованные – не имеют устройства GPS. Из-за большого разброса цен на рынке автомобилей, а также доходов населения, только часть ТС на дороге будет оснащена GPS-устройством. Данный метод позволяет необорудованным автомобилям узнавать их местоположение. Система работает следующим образом. Косвенный подход [2] реализует путь маршрутизации как последовательность подключенных узлов. Назовем каждый автомобиль узлом некоего графа. В такой системе только некоторые из узлов имеют приемник GPS, а остальные отправляют запросы на эти узлы с целью вычисления или получения примерного местоположения. В каждый момент времени в системе существует токен – автомобиль, к которому происходит подключение всех близлежащих необорудованных ТС. В какой-то момент времени, когда автомашина становится недоступна, или не выполняются условия, непосредственно описанные в алгоритме [2], такой токен передается другому оборудованному ТС. Подмножество узлов, которые имеют приемник, называют маяками, а другие, которые не имеют – общими. Используя передаваемый сигнал, содержащий некую информацию, общие узлы вычисляют местоположение, используя различные технологии. Этот метод очень полезен для труднодоступных мест, например, туннели или подземная парковка.
2. Локализация, ориентированная на человека. Данный тип подразумевает собой, что автомашина будет получать информацию с датчиков и устройств, которые при себе имеет человек. Например, одним из таких устройств может являться смартфон или планшет. Как только человек садится в автомобиль, его устройства автоматически соединяются с ТС и начинают передавать данные о местоположении и других показателях. Важно отметить, что, в данном случае автомобиль является инициатором протокола. Взаимодействие между человеком и автомобилем имеет свои плюсы и минусы. Говоря о позитивных аспектах, можно отметить высокую точность определения местоположения из-за наличия в гаджетах GSM-модулей, а также точность обусловлена количеством устройств, которые при себе имеет человек. С другой стороны, этот метод сильно зависит от наличия и заряда устройств, так как выключенный аппарат не сможет передавать информацию. Более того, используя этот метод, большое внимание должно быть уделено безопасности и конфиденциальности.
3. GPS. Сеть GPS – это технология, сеть и сервис, принадлежащие и обслуживаемые США. Служба GPS предоставляет конечным пользователям позиционирование, навигацию и синхронизацию сервисов. GPS состоит из космического, контрольного и пользовательского сегментов [3]. Космический сегмент состоит из созвездия 31 спутника (по состоянию на 17 октября 2017 года), не считая выведенные из эксплуатации, на орбите запасные части. GPS-спутники находятся на средней околоземной орбите на высоте приблизительно 20 200 км (12 550 миль). Каждый спутник облетает Землю два раза в день. Контрольный сегмент GPS состоит из глобальной сети наземных объектов, целью которых является отслеживание спутников, а также мониторинг их связи и передачи информации. Со спутниками связь происходит путем отправки команд и данных. Пользовательский сегмент состоит из конечных пользователей (гражданских и военных). Основным принципом использования всей системы является определение местоположения путем измерения времени приема синхронизированного сигнала от навигационных спутников антенны [3].
4. Локализация, основанная на мощности Wi-Fi сигналов. Данный метод полностью избавляет от необходимости оборудования автомобиля GPS или ГЛОНАСС. Работает он следующим образом. Существует база данных или карта сетей Wi-Fi. Гаджеты некоторых людей оснащены GPS-приемником или GSM. Раз в определенный промежуток времени

они подключаются к серверу и передают информацию о сигналах Wi-Fi вокруг, их мощностях, а также свое местоположение. Таким образом, данные на сервере сначала накапливаются, а потом обновляются в случае каких-либо изменений. Транспортному средству необходимо только лишь подключиться к серверу и отправить ему список сетей и их мощности, а в ответ они получат свое местоположение. Такой метод имеет ряд плюсов и минусов. Из положительных аспектов можно отметить независимость от GPS, низкое энергопотребление и повсеместное распространение. Главный минус – необходимость круглосуточного обеспечения работоспособности сервера и его защиты, а также отсутствие Wi-Fi сетей поблизости не позволит определить местоположение.

5. Триангуляция. Недавно исследователи предложили ряд методов позиционирования и оценки расстояния в [1, 4]. Данные методы основаны на придорожной инфраструктуре. На дороге расположены базовые станции (верификаторы), которые оборудованы устройствами передачи и получения информации. При передаче информации между ТС и базовыми станциями используются дистанционно-ограниченные протоколы, с помощью которых происходит подсчет расстояния между верификатором и ТС. Если верификаторы могут однозначно вычислить местоположение с использованием границ расстояния, и если это местоположение попадает в треугольную пирамиду, образованную между станциями, то они делают вывод, что местоположение ТС верно [5]. Эквивалентно только три верификатора необходимы для проверки местоположения транспортного средства в двух измерениях.

Передача информации между ТС и базовой станцией является ключевым моментом метода, поэтому очень важно обеспечить безопасность такой передачи. На рис. 1 представлен протокол передачи информации между базовой станцией и транспортным средством.

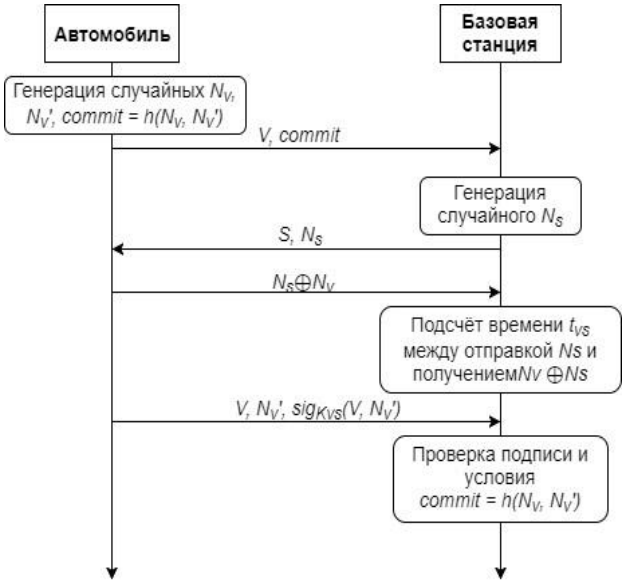



Рис. 1. Протокол передачи информации между базовой станцией и автомобилем

Во-первых, между ТС и базовой станцией должен быть разработан общий симметричный ключ для безопасного обмена информацией. Алгоритм генерации ключа зависит от вычислительных модулей, установленных в автомобиле и базовой станции. В настоящей работе протокол выработки ключа и создание безопасного канала не рассматриваются. Считается, что такой канал уже создан, и обмен данными между станцией и ТС осуществляется через такой канал.

Автомобиль является инициатором протокола. На стороне автомобиля генерируются два случайных значения *Nv* и *Nv′*, а также считается хэш от двух значений. Информация отправляется на базовую станцию, где, в свою очередь, генерируется случайное *Ns*, которое

отправляется автомобилю. Далее происходит ключевой момент протокола. В ответ на переданное *Ns*, отправляется *Ns*⊕*Nv*. Для определения расстояния на стороне станции считается время между отправкой *Ns* и получением *Nv*⊕*Ns*, а потом, на основе полученного времени и скорости передачи данных, считается расстояние [4]. Финальная часть протокола – проверка подлинности транспортного средства. Для этого автомобиль отправляет подписанное значение *Nv′*, а базовая станция проверяет подпись и значение хеш-функции.

Данный протокол был усовершенствован. На рис. 2 представлена обновленная версия протокола [1].

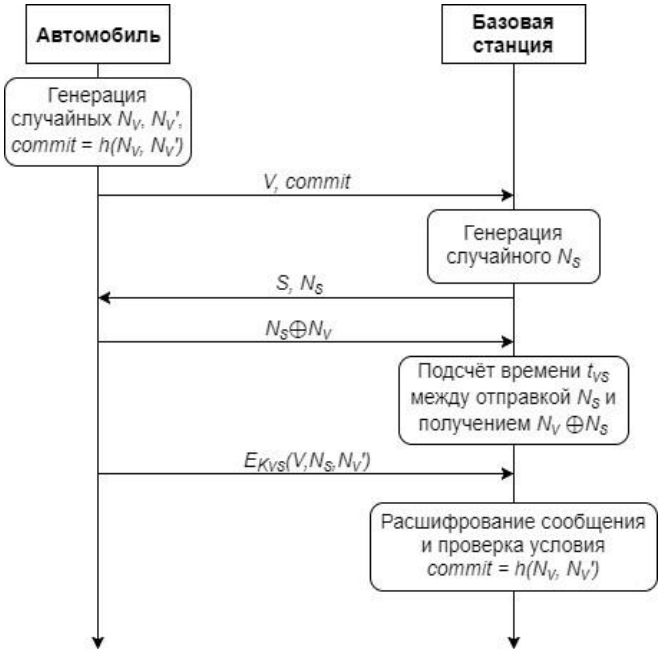



Рис. 2. Обновленная версия протокола (2006)

Представленный протокол отличается от предыдущего в финальной части: вместо отправки в открытом виде значения *Nv′* отправляется зашифрованное значение *Ns* и *Nv′*, что позволяет добиться максимальной безопасности при передаче данных. Данный протокол можно считать надежным и использовать при передаче данных между транспортным средством и базовой станцией.

**Литература**

1. Hubaux J.P., Capkun S., Luo J. The security and privacy of smart vehicles // IEEE Security & Privacy. – 2004. – V. 2. – № 3. – P. 49–55.
2. Capkun S. and Hubaux J.-P. Secure positioning of wireless devices with application to sensor networks [Электронный ресурс]. – Режим доступа: https://www.ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/system-security-group-dam/research/spot/secpos.pdf, своб.
3. Renfro B.A., Terry A. and Boeker N. An analysis of global positioning system (gps) standard positioning system (sps) performance for 2015 [Электронный ресурс]. – Режим доступа: https://www.gps.gov/systems/gps/performance/2015-GPS-SPS-performance-analysis.pdf, своб.
4. Raya M., Papadimitratos P., Hubaux J.P. Securing vehicular communications // IEEE wireless communications. – 2006. – V. 13. – № 5. – P. 8–15.
5. Zeng Y., Cao J., Hong J., Zhang S. and Xie L. Secure localization and location verification in wireless sensor networks: a survey // The Journal of Supercomputing. – 2013. – P. 1–17.

**Кулаков Артем Дмитриевич**
Год рождения: 1996
Университет ИТМО, факультет безопасности информационных технологий, кафедра безопасности киберфизических систем, студент группы № N4159
Направление подготовки: 10.04.01 – Информационная безопасность
e-mail: kulakov_add@mail.ru

**УДК 004.056**

# АНАЛИЗ ПОДХОДОВ К СОВМЕСТНОЙ ОЦЕНКЕ НАДЕЖНОСТИ И БЕЗОПАСНОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

**Кулаков А.Д.**
**Научный руководитель – к.т.н., доцент Волошина Н.В.**

Работа выполнена в рамках темы НИР № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность».

В работе рассмотрены методы совместной оценки безопасности и надежности сложных систем, существование которых обусловлено необходимостью учета проблем безопасности при оценке надежности систем, а также приведена классификация таких методов.
**Ключевые слова:** киберфизические системы, надежность, безопасность.

Существующие методы оценки надежности и безопасности по отдельности не учитывают взаимное влияние этих показателей друг на друга, поэтому для получения комплексного представления о безопасности и надежности системы следует использовать методы их совместной оценки.

В настоящей работе рассмотрены некоторые подходы к совместной оценке безопасности и защищенности систем, а также показана классификация этих методов, представленная в работе [1].

Надежность – свойство системы сохранять работоспособность, не наносить вред окружающей среде и людям. Безопасность – состояние системы, при котором действие внешних и внутренних факторов не приводит к нарушению в работе системы или к невозможности ее функционирования. Оценка этих двух параметров, учитывая их влияние друг на друга, – и есть цель методов совместной оценки.

Методы делятся на две большие группы: процессно-ориентированные и построенные на модели. Также методы можно разделить по их подходу к совместной оценке: направленные на унификацию, т.е. использование одной и той же методологии для оценки и надежности и безопасности; и направленные на интеграцию, другими словами, на определение требований надежности и безопасности по отдельности и последующий анализ и устранение конфликтов.

Методы классифицируются по этапу жизни системы, на котором они применяются: применяемые на этапе проектирования и применяемые уже к готовым системам на этапе их эксплуатации.

В качестве процессно-ориентированного подхода, направленного на унификацию, может быть приведен подход, описанный в работе [2]. Здесь предложены единые рамки для рисков и уязвимостей, учитывающие и надежность, и безопасность.

Применение метода состоит из следующих шагов:

– Шаг 1. Определение анализируемых технологических процессов;
– Шаг 2. Определение систем, ответственных за эти процессы;
– Шаг 3. Определение источников угроз;

– Шаг 4. Проведение анализа последствий реализации выявленных угроз;
– Шаг 5. Описание рисков, превышающих допустимый уровень;
– Шаг 6. Оценка рисков;
– Шаг 7. Определение возможных методов защиты и возврат к шагу 3.

Подход обеспечивает непрерывную оценку надежности и безопасности системы, поскольку цикл повторяется после возврата на шаг 3. В то же время шаги 1 и 2 выполняются лишь однажды, и возврат к ним невозможен. Подход рассматривает систему только на этапе ее эксплуатации, и при его применении будут рассматриваться одни и те же технологические процессы, определенные на шаге 1.

Один из подходов, направленных на интеграцию, представлен в работе [3], где его применение проиллюстрировано на примере умных зданий. Подход охватывает этапы проектирования системы и базируется на стандартах IEC 61508 и IEC 15408. Схема применения подхода показана на рисунке.

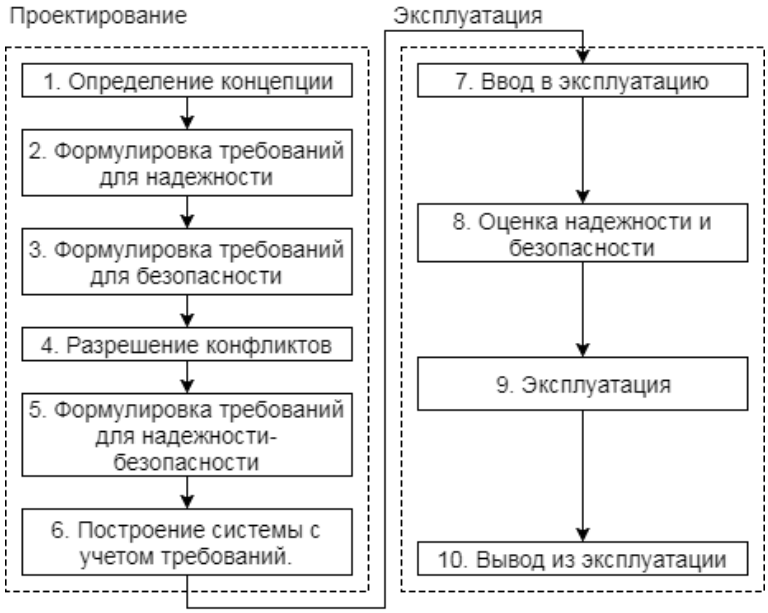



Рисунок. Схема применения подхода

Жизненный цикл системы начинается с определения физического расположения и сферы действия системы. После определения угроз, для надежности, вырабатываются требования. Затем происходит определение угроз безопасности, и вырабатываются требования по безопасности. Затем происходит разрешение возможных конфликтов между требованиями к безопасности и надежности, поскольку требования в одной сфере могут приводить к уязвимости в другой. После того, как конфликты разрешены, формируются общие требования. На следующем шаге происходит реализация требований и фаза, охватывающая проектирование системы, заканчивается. Далее происходит ввод в эксплуатацию, а затем собственно эксплуатация. Данный подход позволяет учитывать требования для надежности и безопасности уже на этапе проектирования, однако, как видно на рисунке, во время эксплуатации системы подход не задействуется.

Методы, основанные на модели, могут использовать как графические, так и неграфические модели. Методы, использующие графические модели, могут быть построены на основе деревьев отказов/атак, диаграмм состояний и т.д.

Метод, использующий расширенную версию дерева отказов, описан в работе [4]. Применение метода в этой работе показано на примере современной европейской системы автоматизированного управления движением железнодорожного транспорта (ERTMS). В стандартное дерево отказов включен «модуль безопасности», который содержит угрозы информационной безопасности. Этот подход наглядно иллюстрирует, что угрозы

безопасности напрямую влияют на надежность системы в целом. Этот подход учитывает события, связанные с отказом и ошибок компонентов системы или атак на эти компоненты. Однако этот подход не берет во внимание события надежности и безопасности, возникающие вследствие некорректного взаимодействия этих элементов.

В работе [5] показан подход (state/event fault trees (SEFTs)), использующий деревья отказов и диаграммы состояний для моделирования определенных состояний системы и поведения, приводящего к ошибкам. Временные зависимости между компонентами демонстрируются с помощью диаграммы состояний: события, вызывающие изменения состояния могут быть детерминированы или случайны. Временные взаимосвязи между событиями и моделируемыми состояниями показываются с помощью диаграммы состояний, в то время как связь компонентов отражается с помощью стандартного дерева отказов. Атаки изображаются как компоненты схемы, а этапы атаки – как субкомпоненты. Каждый этап атаки может быть изображен с помощью диаграммы состояний. В работе авторы проиллюстрировали свой подход применительно к системе контроля давления в автомобильных шинах, где изучили эффект компьютерных атак на элементы системы, обеспечивающие ее надежность. Этот метод, как и предыдущий, использует расширенную версию дерева отказов, но учитывает и состояние компонентов, и то, как происходит их взаимодействие.

В качестве примера неграфического метода может быть приведен подход STPA-sec, описанный в работе [6]. Данный подход основывается на методе STPA, который используется для оценки надежности систем. В основе метода лежит концепция STAMP, которая рассматривает систему как иерархическую структуру, в которой высокие уровни контролируют низкоуровневые процессы, а те, в свою очередь, подотчетны верхним уровням. Этот подход фокусируется на управляющих воздействиях. Каждое воздействие изучается в разных возможных условиях (например, корректное воздействие было оказано слишком рано или слишком поздно, или некорректное воздействие было оказано вовремя), и определяется, какие условия могут привести к опасному состоянию системы. После определения опасных состояний разрабатываются ограничения системы, направленные на избегание подобных состояний. Работа STPA-Sec построена также. Но после проведения анализа определяются управляющие воздействия, которые нарушают и надежность, и безопасность системы. Так как этот подход рассматривает систему с точки зрения контроля и управляющих воздействий, он не берет в расчет компонентный состав системы, а значит, надежность системы будет рассчитана только исходя из оценки адекватности контроля и своевременности оказания управляющих воздействий.

Необходимость применения методов совместной оценки надежности и безопасности вызвана, прежде всего, тем, что без учета проблем безопасности системы адекватная оценка ее надежности невозможна. Рассмотренные процессно-ориентированные методы позволяют обеспечить надежность и безопасность системы на этапах проектирования и эксплуатации, однако их применение осложнено тем, что ни один из них не охватывает оба эти этапа жизненного цикла системы. Для обеспечения надежности и безопасности системы на всех этапах может быть осуществлено совместное применение этих методов. Методы, построенные на модели, рассмотренные в данной работе, не зависят от этапов жизненного цикла системы и могут применяться на любом из них для получения актуальных данных о состоянии надежности и безопасности. Графические методы, использующие расширенную версию дерева отказов, подходят для оценки надежности и безопасности компонентного состава системы, так как рассматривают ее исходя из состояния компонентов и их взаимодействия. Для того чтобы учесть риски, не связанные с компонентным составом системы, в дополнение к этим методам может быть применен подход STPA-Sec, который направлен на выявление небезопасных и ненадежных управляющих воздействий.

Таким образом, существующие методы совместной оценки безопасности и надежности не позволяют осуществить комплексную оценку состояния системы, но их совместное применение дает возможность получить данные о состоянии всех ее элементов на всех этапах ее жизни. Отдельной задачей является построение методов учета подсистем информационной безопасности и их влияния на надежность работы компонентов.

**Литература**

1. Kriaa S. Joint safety and security modeling for risk assessment in cyber physical systems [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/profile/Siwar_Kriaa2/publication/302964728_Joint_Safety_and_Security_Modeling_for_Risk_Assessment_in_Cyber_Physical_Systems/links/5734682608aea45ee83aa398/Joint-Safety-and-Security-Modeling-for-Risk-Assessment-in-Cyber-Physical-Systems.pdf?origin=publication_detail, своб.
2. Aven T. A unified framework for risk and vulnerability analysis covering both safety and security // Reliab. Eng. Syst. Saf. – 2007. – V. 92. – № 6. – P. 745–754.
3. Novak T. and Gerstinger A. Safety- and Security-Critical Services in Building Automation and Control Systems // IEEE Trans. Ind. Electron. – 2010. – V. 57. – № 11. – P. 3614–3621.
4. Беззатеев С.В., Волошина Н.В., Санкин П.С. Методика расчета надежности сложных систем, учитывающая угрозы информационной безопасности // Информационно-управляющие системы. – 2014. – № 3(70). – С. 78–83.
5. Roth M. and Liggesmeyer P. Modeling and Analysis of Safety-Critical Cyber Physical Systems using State/Event Fault Trees // International Conference on Computer Safety, Reliability and Security. Workshops and Tutorials. – 2013. – P. 253–273.
6. Young W. and Leveson N.G. An integrated approach to safety and security based on systems theory // Commun. ACM. – 2014. – V. 57. – № 2. – P. 31–35.

**Лавринович Александр Андреевич**
Год рождения: 1994
Университет ИТМО, факультет безопасности информационных технологий, кафедра безопасности киберфизических систем, аспирант
Направление подготовки: 10.06.01 – Информационная безопасность
e-mail: lavrinovich.readit@gmail.com

**УДК 004.056**

# ПОДХОДЫ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ RFID-ТЕХНОЛОГИЙ

**Лавринович А.А.**
**Научный руководитель – к.т.н., доцент Волошина Н.В.**

В работе определены подходы к обеспечению информационной безопасности RFID-меток, применяемых в проекте по маркировке изделий из меха (товарная позиция 4403 ТН ВЭД ЕАЭС) в рамках государственного регулирования внешнеэкономической деятельности. В работе также рассмотрены основные угрозы информационной безопасности, актуальные для данного проекта на сегодняшний день, раскрыто их значение для таможенных органов и для участников внешнеэкономической деятельности.
**Ключевые слова:** RFID-технология, RFID-метка, маркировка товаров, контрольный идентификационный знак, информационная безопасность, внешнеэкономическая деятельность.

С 2016 года каждое изделие из меха, независимо от того произведено оно в России или ввезено из других стран, оснащается специальной биркой, на которой представлен серийный номер изделия и QR-код, а также Radio Frequency IDentification (RFID)-меткой, с помощью которого можно считать всю информацию о конкретном изделии. Участники рынка отчитываются в Федеральную налоговую службу (ФНС) обо всех перемещениях каждого изделия с момента производства или импорта на территорию Евразийского Союза и до момента продажи конечному покупателю. Эта информация позволяет контролировать весь оборот меховых изделий на рынке, она хранится в государственной базе данных [1, С. 229].

Тем не менее, несмотря на сложный организационный механизм обеспечения участников рынка контрольными идентификационными знаками (КиЗ) с конвертированными в них RFID-метками, актуальными являются вопросы обеспечения их информационной безопасности. Актуальность определяется экономической ценностью информации, хранящейся на RFID-метках, как для таможенных органов, как лиц, которые заинтересованы в получении достоверной информации с метки в целях осуществления таможенного контроля, так и для участников внешнеэкономической деятельности (ВЭД), для которых информация, записанная на метке, становится основой налоговой нагрузки при декларировании товаров из меха.

Цель работы – обозначить подходы к обеспечению информационной безопасности RFID-технологий, используемых в рамках контроля внешнеэкономической деятельности.

Практическое значение системы безопасности RFID-технологий в области ВЭД определяется следующими положениями.

Во-первых, безопасность информации, которую заключает в себе RFID-метка, необходима для осуществления таможенного контроля, а также иных видов государственного контроля (например, налогового).

Так, в RFID-метке маркированных изделий из меха содержится информация о стране происхождения товара [2]. В свою очередь, при уплате таможенных платежей крайне важна

страна происхождения товара – страна происхождения товара положена в основу единой системы преференций ЕАЭС. В случае если страной происхождения будет страна, указанная в перечне развивающихся или наименее развитых стран, то участник ВЭД имеет право на получение преференций по уплате таможенной пошлины. Если товар перемещается из страны, которая входит в перечень развивающихся стран, то ставка таможенной пошлины уплачивается в объеме 75% от ставки, указанной в ТН ВЭД ЕАЭС. Если товар перемещается из страны, которая входит в перечень наименее развитых стран, то ставка таможенной пошлины будет равна 0.

Иными словами, получение недостоверной информации о стране происхождения может занизить объем необходимых к уплате таможенных платежей, тем самым доходная часть федерального бюджета недополучит финансовые средства. Как известно, именно таможенные органы формируют значительную часть доходов бюджета страны.

Во-вторых, риски, так или иначе, присутствуют и для самих участников ВЭД.

Информация, которую получает таможенный орган об участнике ВЭД, о товарах, которые он перемещает через таможенную границу, является основой для формирования категории участника ВЭД в рамках системы категорирования. Одним из условий отнесения участника ВЭД к «зеленому» сектору является отсутствие нарушений таможенного законодательства. Поскольку требование о маркировке изделий из меха является обязательным, то отсутствие КИЗа будет определено, как административное правонарушение, за которое предусмотрена административная ответственность по статье 15.12 КоАП РФ. Таким образом, считывание информации, которая не соответствует действительности, или отсутствие информации может стать неблагоприятным фактором для участника ВЭД. В данном случае речь идет о несанкционированном изменении КИЗа, о котором участник ВЭД не знал, т.е. это было сделано без его ведома.

Основные угрозы информационной безопасности, актуальные для данной системы маркировки товаров:

1. уничтожение метки. Уничтожение RFID-метки – атака, направленная на прекращение существования и функционирования RFID-метки. При отсутствии сигнала метки, а также при отсутствии фактических форм таможенного контроля, товар может проникнуть на таможенную территорию без соблюдения требований законодательства. Наоборот, если фактические формы контроля будут проведены и будет обнаружена неработающая метка, это может привести к нежелательным последствиям для участника ВЭД, который не обеспечил должны уровень физической защиты КИЗа.

   По данной атаке следует принимать во внимание возможность «усыпления» или «убийства» чипа. Сделать это можно, поместив метку в сильное электромагнитное поле (RFID Zapper), «зашумить» диапазон считывателя маломощным передатчиком с малого расстояния, подавить работу считывателя «глушилкой» [3].

   Уничтожение RFID-метки также возможно с помощью пароля-убийцы (пароля, инициирующего «самоубийство» метки). Например, команда на самоуничтожение метки определена в стандарте EPC. Применение такой команды защищено паролем. Однако несанкционированное применение команды создает такие проблемы, как уничтожение информации. Проблемным также может быть вопрос качества пароля (сложность пароля зависит от мощности метки) [4];
2. создание дубликата КИЗа с RFID-меткой типа Read and Write взамен Read Only. Атака создания дубликата RFID-метки – атака, направленная на изготовление RFID-метки, которая в рамках атакуемой системы будет восприниматься как санкционированная. Сценарий атаки учитывает, что участник ВЭД получает КИЗ от уполномоченного органа, а при получении КИЗа участник ВЭД с помощью RFID-оборудования записывает на метку информацию о конкретном изделии, после чего информацию уже невозможно изменить (тип метки – Read Only). Однако в случае изготовления дубликата КИЗа с типом

RFID-метки Read and Write становится возможным изменение информации, а, значит, появляется возможность для манипулирования данными;

3. атаки типа «Человек посередине». Атака «человек-посередине» (man-in-the-middle) для RFID-метки – атака на RFID-метку, содержание которой заключается в том, что злоумышленник проникает в систему коммуникации RFID-метки и считывателя и передает информацию от имени RFID-метки считывателю.

Реализация данной атаки возможна в случае «заглушки» настоящей RFID-метки, при этом при прохождении таможенного контроля считывается информация с метки, которая считывателем таможенного органа воспринимается за исследуемую метку. Следовательно, передается информация, позволяющая получить необоснованные выгоды участнику ВЭД. Следует отметить, что данная атака возможна в случае отсутствия визуального контроля метки (считывание информации с помощью QR-кода);

4. DOS-атака. DOS-атака на RFID-систему – атака, цель которой вывести из строя RFID-систему, чтобы ее невозможно было использовать. Вектором DOS-атаки может быть, как сеть RFID-меток, так и сервера. Эти атаки обычно проявляются в виде физических атак, например, посредством заполнения системы шумовыми помехами, блокировкой радиосигналов или даже удалением или отключением RFID-меток [5].

Таким образом, обозначим подходы к обеспечению информационной безопасности RFID-меток. КИЗы, оснащенные RFID-метками, должны быть, во-первых, защищены от угроз уничтожения, во-вторых, – угрозы создания дубликата, в-третьих, – угроз «заглушения». В связи с этим актуально дальнейшее исследование вопроса.

Сегодня для типа метки, который используется для маркировки меха, возможна реализация таких атак, как несанкционированное копирование, уничтожение метки, «человек посередине», DOS-атака. Но с расширением практики применения RFID-технологии новые горизонты откроются и для злоумышленников, сегодня желающих снизить налоговую нагрузку или скомпрометировать других участников рынка, а завтра пытающихся проникнуть в государственные базы данных. В исследовании таких вопросов и заключаются перспективы дальнейшего исследования.

**Литература**

1. Маскальская А.Н. Анализ применения практики таможенной пошлины при ввозе меховых изделий на таможенную территорию ЕАЭС // Студент: наука, профессия, жизнь. Материалы IV Всероссийской студенческой научной конференции с международным участием: в 3 ч. – 2017. – С. 229–233.
2. Изделия из натурального меха [Электронный ресурс]. – Режим доступа: https://www.nalog.ru/rn77/taxation/labeling/mark/ своб.
3. Будзинский Д.Л., Кузьмин А.А., Уткин В.В. Безопасность в системах с RFID-идентификацией (по материалам интернет ресурсов) // Череповецкие научные чтения – 2012. Материалы Всероссийской научно-практической конференции. – 2013. – С. 35–38.
4. Xiao Q., Gibbons T. and Lebrun H. RFID Technology, Security Vulnerabilities, and Countermeasures [Электронный ресурс]. – Режим доступа: https://www.intechopen.com/books/supply_chain_the_way_to_flat_organisation/rfid_technology__security_vulnerabilities__and_countermeasures, своб.
5. RFID опять «взломан» – DoS атака с помощью дешевого радиопередатчика [Электронный ресурс]. – Режим доступа: https://www.ixbt.com/news/hard/index.shtml?05/94/01 своб.

**Мелешко Алексей Викторович**
Год рождения: 1995
Университет ИТМО, факультет безопасности информационных технологий, кафедра безопасности киберфизических систем, студент группы № N4159
Направление подготовки: 10.04.01 – Информационная безопасность
e-mail: lexa.0710@gmail.com

**Савков Сергей Витальевич**
Год рождения: 1988
Университет ИТМО, факультет безопасности информационных технологий, кафедра безопасности киберфизических систем, ассистент
e-mail: sergsavkov@gmail.com

**УДК 004.056**

# ОЦЕНКА РИСКОВ В КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ В УСЛОВИЯХ НЕПОЛНОТЫ ИСХОДНЫХ ДАННЫХ

**Мелешко А.В., Савков С.В.**
**Научный руководитель – к.т.н., доцент Волошина Н.В.**

Работа посвящена анализу различных методов оценки риска на предмет возможности использования их в киберфизических системах. В работе выявлены особенности оценки риска в киберфизических систем, проанализирована возможность использования существующих методик для анализа рисков в киберфизических системах. В результате анализа была предложена методика, представляющая собой синтез подхода, основанного на экспертном оценивании и измеряемых параметров киберфизической системы.
**Ключевые слова:** оценка риска, киберфизическая система, методы оценки риска.

В настоящее время киберфизические системы (КФС) получают активное распространение в различных сферах деятельности. Умный дом, системы управления водоснабжением, беспилотные летательные аппараты и автомобили, а также другие системы внедряются с целью облегчения деятельности человека. Однако такие системы могут быть подвержены различного рода атакам, последствия которых могут быть весьма значительными [1]. Например, атака на датчики беспилотного автомобиля может привести к ложным показаниям о скорости или расстоянии до препятствия, что, в свою очередь, может закончиться аварией. По этой причине проблема обеспечения безопасности КФС занимает далеко не последнее место. Для того что бы правильно разработать комплекс средств защиты от различных угроз, необходимо проанализировать риски их появления, а также возможные последствия. Для решения этой задачи могут быть использованы различные системы анализа риска.

Поскольку КФС получили распространение относительно недавно, то не все факторы риска можно однозначно оценить, а значит, появляется некая степень неопределенности. В работе [2] указано, что если есть неопределенность, нельзя исключать возможный вред, таким образом, для более полной оценки риска в КФС необходимо учитывать эту неопределенность. Также при оценке риска необходимо учитывать характеристики и параметры системы. В КФС параметры постоянно меняются, значит, для оценки риска

необходимо постоянно их обновлять. Следовательно, оценка риска в КФС имеет свои особенности и отличия от риск-анализа других систем.

Можно выделить следующие требования к оценке риска в КФС:
- достоверность результатов;
- учет всех возможных входных данных (в том числе нечисловых);
- методика оценки не вносит искажений в результаты оценки;
- объективное оценивание;
- работа в режиме реального времени;
- приоритет событий риска доступности над событиями риска конфиденциальности [3].

Далее в настоящей работе были рассмотрены некоторые подходы для оценки риска, которые могут быть применены в КФС.

Подход, основанный на экспертном оценивании, представляет собой комплекс логических и математических процедур, направленных на получение заключения эксперта по определенному кругу вопросов. Главным преимуществом этого метода является возможность использования для принятия оптимальных управленческих решений опыта и интуиции компетентного специалиста. В случае получения оценок несколькими экспертами прибегают к обобщению полученных оценок. Это может быть среднее значение или же более сложные способы.

Подход, основанный на накопленном опыте, базируется на том, что используются списки рисков, составленные ранее для предыдущих проектов. В рамках данного подхода анализируются прошлые происшествия, факторы рисков, последствия, которые они вызвали. Вся информация о происшествиях и факторах риска может быть найдена из различных источников, например из собственных архивных записей или же из сторонних источников. Однако возникает проблема определения качества источника, т.е. определения достоверности приведенной информации. Если используемые источники имеют рейтинги, то определить конечных список источников можно используя доверительный интервал, который можно рассчитать по формуле:

$$\bar{x} - t_{\alpha,n-1}\frac{\hat{\sigma}}{\sqrt{n}} < \mu < \bar{x} + t_{\alpha,n-1}\frac{\hat{\sigma}}{\sqrt{v}}, \quad (1)$$

где $\bar{x}$ – среднее арифметическое значение выборки; $t_{\alpha,n-1}$ – критическое значение $t$-статистики (распределения Стьюдента) с уровнем значимости α, числом степеней свободы $n-1$; $\hat{\sigma}$ – среднеквадратическое отклонение по выборке. В формуле (1) под выборкой понимается список рейтингов всех возможных источников.

После расчета доверительного интервала делаются выводы о возможности использования того или иного источника. Стоит заметить, что если источник не имеет никакого рейтинга, то определить его достоверность с помощью доверительного интервала невозможно.

Подход, основанный на имитационном моделировании, реализует, например, метод Монте-Карло. В данном методе в качестве входных параметров выступает статистическое распределение. Суть метода заключается в построении модели, состоящей из случайных величин, над которыми проводится серия экспериментов с целью выявления влияния исходных данных на зависящие от них величины.

В работе [4] изложена методика оценки риска, предлагаемая непосредственно для КФС. Оценивать риск предлагается по следующим формулам:

$$R(t) = \sum_{j=1}^{m} \omega_j \cdot R_j(t),$$

$$R_j(t) = \sum_{j=1}^{n} T_{ji}(t) \times P_{ji}(t) \times C_{ji},$$

где $R(t)$ – риск системы в момент времени $t$; $R_j(t)$ – риск атакуемого узла $j$ в момент времени $t$; $\omega_j$ – значение хоста $j$ в КФС. $T_{ji}(t), P_{ji}(t), C_{ji}$ – серьезность, вероятность успеха атаки и последствия атаки кибератаки $i$ на хосте $j$ в момент времени $t$; $m$ – количество хостов в КФС, а $n$ – типы кибератак.

RiskWatch – методология, разработанная одноименной компанией. В качестве оценки риска в методике выступают ожидаемые годовые потери (ALE), которые рассчитываются по формуле:

$$ALE = Asset\ Value \cdot Exposure\ Factor \cdot Frequency,$$

где $ALE$ – оценка ожидаемых годовых потерь для одного конкретного актива от реализации одной угрозы; $Asset\ Value$ – стоимость рассматриваемого актива; $Exposure\ Factor$ – коэффициент воздействия – показывает, какая часть (в процентах) от стоимости актива, подвергается риску; $Frequency$ – частота возникновения нежелательного события.

Каждый из рассмотренных подходов может быть применим для оценки риска в КФС, но они имеют свои недостатки, что, в свою очередь, ведет к неточной оценке риска.

Например, в подходе, основанном на экспертном оценивании, а также на накопленном опыте, нет возможности учесть текущие параметры КФС, а также итоговая оценка будет субъективной. В методе Монте-Карло сложно учесть все факторы риска в одной модели. В методе RiskWatch также нет возможности менять риск модель динамически. Метод из работы [2] позволяет производить оценку риска в реальном времени, однако оценка получается точечной, что не позволяет учесть неполные входные данные.

Опираясь на проведенный анализ можно предложить подход, объединяющий в себе несколько рассмотренных подходов, а именно, экспертное оценивание, метод Монте-Карло, а также текущие параметры системы. Схематично предлагаемый подход оценки риска представлен на рисунке.

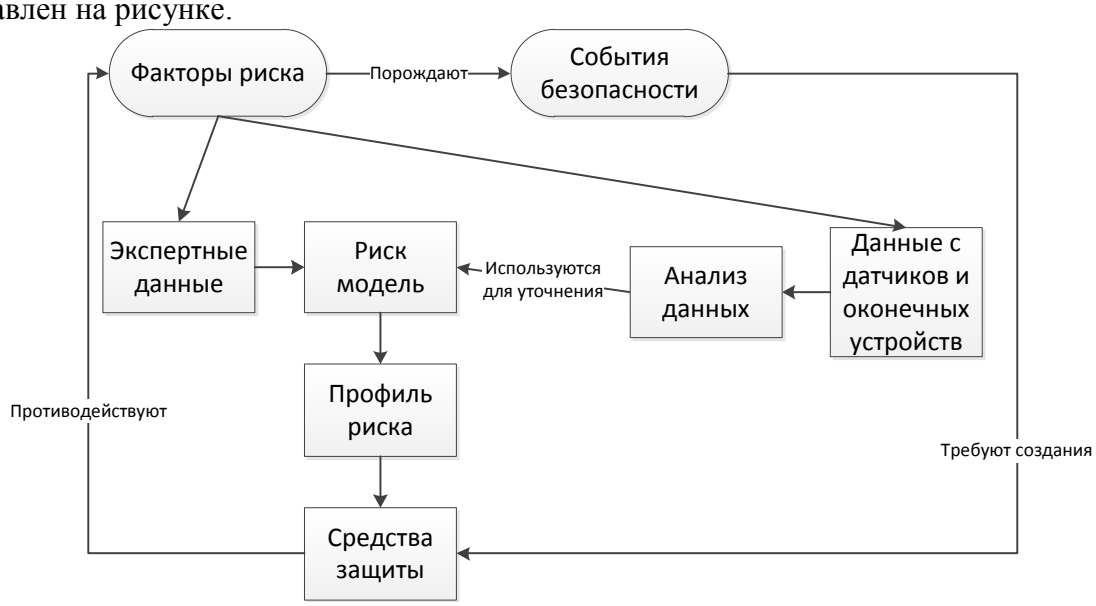



Рисунок. Синтез различных источников оценивания в рамках единой модели

В рамках предлагаемой модели под факторами риска рассматриваются как источники угроз, так и связанные с ними компоненты системы, и способы реализации угроз на компонентах системы. Под риск-моделью понимается объединение множества источников угроз, самих угроз, компонентов системы и связей между ними, представленное в виде направленного графа [5]. Профиль риска показывает плотность распределения оценок влияния каждого фактора риска на уровень безопасности системы. Экспертные данные являются входной информацией для оценивания, а данные с датчиков – информацией для уточнения параметров модели. Анализ данных подразумевает сбор статистических данных

работы датчиков с целью выявления изменения их показаний. На базе уточненной модели строится актуальный профиль риска, который передается на комплекс средств защиты для оптимизации его работы.

Для адекватного анализа данных, получаемых с датчиков, в рамках предложенного подхода необходимо использовать собственную статистику для определения аномалий в работе КФС.

Поскольку для расчета итогового профиля риска используются текущие параметры КФС, то итоговый профиль получается динамическим. Динамическая оценка позволяет оценивать текущий уровень безопасности КФС, что позволяет оперативно реагировать на события безопасности, неучтенные или некорректно оцененные при первоначальной экспертной оценке.

В дальнейшем в целях реализации предлагаемого подхода планируется разработать методы учета и анализа дополнительных данных, получаемых с датчиков, а также моделирование работы предлагаемого метода с использованием программной реализации.

**Литература**

1. Axelrod C.W. Managing the risks of cyber-physical systems // Systems, Applications and Technology Conference (LISAT). – 2013. – V. 9. – P. 1–6.
2. Cline P.B. The Merging of Risk Analysis and Adventure Education // Wilderness Risk Management. – 2015. – P. 43–45.
3. Peng Y., Lu T., Liu J., Gao Y., Guo X., Xie F. Cyber-Physical System Risk Assessment // Intelligent Information Hiding and Multimedia Signal Processing. – 2013. – V. 9. – P. 442–447.
4. Wu W., Kang R., Li Z. Risk assessment method for cyber security of cyber physical systems // Reliability Systems Engineering (ICRSE). – 2015. – V. 1. – P. 1618–1622.
5. Мелешко А.В. Разработка подсистемы стохастического моделирования экспертных данных для автоматизированной системы риск-анализа: выпускная работа бакалавра. – СПб.: Университет ИТМО, 2017.

**Минаева Тамара Александровна**
Год рождения: 1995
Университет ИТМО, факультет безопасности информационных технологий, кафедра безопасности киберфизических систем, студент группы № N4159
Направление подготовки: 10.04.01 – Информационная безопасность
e-mail: minaeva-toma-ya@yandex.ru

**Волошина Наталия Викторовна**
Год рождения: 1976
Университет ИТМО, факультет безопасности информационных технологий, кафедра безопасности киберфизических систем, к.т.н., доцент
e-mail: nataliv@yandex.ru

**УДК 004.056.55**

# ИССЛЕДОВАНИЕ МНОГОУРОВНЕВОГО ВСТРАИВАНИЯ В BMP-ИЗОБРАЖЕНИЯХ

**Минаева Т.А., Волошина Н.В.**
**Научный руководитель – к.т.н., доцент Волошина Н.В.**

Работа выполнена при финансовой поддержке Российского Фонда фундаментальных исследований в 2018 году (грант 17-07-00849-А) и в рамках темы НИР № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность».

Работа посвящена исследованию стеганографического встраивания информации в BMP-изображения (цифровых водяных знаков) в системах защиты авторских прав на цифровые объекты. Были реализованы и проанализированы, с помощью показателей визуального искажения на различные способы встраивания информации в изображение, два стеганографических метода: LSB-метод, при одноуровневой и многоуровневой реализации, и метод взвешенного многоуровневого LSB-встраивания (MLSB). Сравнив метод MLSB с обычным LSB-методом, были определены их недостатки и преимущества, а также выявлено, что MLSB-метод позволяет значительно уменьшить визуальное искажение изображения, путем комбинирования менее значимых бит (младших битовых плоскостей изображений) с целью оптимизации процесса встраивания информации в изображения.
**Ключевые слова:** стеганография, цифровые водяные знаки, наименее значимые биты, стеганоанализ, многоуровневое встраивание, стегановставка, взвешенный контейнер, LSB, MLSB, WF5.

В последнее время обмен данными в Интернете стал быстрым и удобным, вследствие чего использование цифровых ресурсов и управление ими становится наиболее востребовано. Проблема управления и обеспечение безопасности цифровых медиаресурсов становится актуальной задачей, для решения которой могут применяться стеганографические подходы. Сокрытие информации и ее выявление также является важной проблематикой в условиях быстро развивающихся инфраструктур сетевого обмена данными. В результате чего значительный объем передаваемых медиаресурсов часто сопровождается незаконным копированием и распространением, что может нарушать авторские права. Исходя из этого, возникает необходимость поиска способов внедрения авторской информации в передаваемые объекты и дальнейшего ее обнаружения в целях

защиты авторских прав на них. Одним из направлений для решения данной задачи является цифровая стеганография. Главной задачей стеганографии является организация скрытого канала связи с помощью особого внедрения информационного сообщения (например, авторская информация) в цифровые объекты (контейнеры), свободно распространяющиеся по сети. Также стеганографические методы могут применяться для построения системы защиты на базе незаметных цифровых водяных знаков. В качестве таких объектов (контейнеров) могу выступать цифровые изображения, аудио- и видеофайлы и т.д. Наиболее распространенным типом контейнера являются файлы изображения, часто файлы формата BMP. Положительной стороной в пользу выбора формата BMP выступает высокое качество изображения и простота формата. При этом разработчики стеганографических методов должны организовывать целостность передаваемых авторских данных, а также вносимые изменения в процессе встраивания в контейнере не должны привести к существенным потерям его качества (должны отсутствовать артефакты визуализации встраивания).

Существует много стеганографических методов встраивания информации в различные типы изображений и их области. В данной работе проводилось сравнительное исследование с целью выявления лучшего подхода к встраиванию при использовании многоуровневой модели изображения-контейнера (взвешенного контейнера [1]) BMP-изображения, сравнивая стеганографические методы: метод замены наименее значимых бит (LSB-метод) [2] и метод многоуровневого LSB -встраивания (метод MLSB) [1].

Для исследования в качестве контейнера рассматривается 24-битовое растровое изображение формата BMP в системе цветности RGB. Каждый пиксель представляет собой комбинацию значений яркости трех составляющих цвета – красного (R), зеленого (G) и синего (B), которые занимают каждый по 1 Б. Самым распространенным стеганогарфическим методом, позволяющим встроить информацию в пространственную область BMP-изображения, является LSB-метод. Суть метода заключается в том, что наименее значимые биты цветовых компонентов пикселя изображения заменяются битами передаваемой информации. Проведя исследования, было выявлено, что встраивать информацию можно не только в первые, наименее значимые биты [3], но и последующие три (в некоторых случаях 4), при этом не происходит сильного искажения изображения и показатель визуального искажения PSNR [4] не опускается ниже 30 дБ, как можно заметить в таблице, приведенной ниже. Если значения PSNR опускаются ниже 30 дБ, то такие искажения изображения становятся визуально обнаружимыми [5].

Таблица. Сравнение значений PSNR при встраивании информации в разные LSB

| | № бита | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 1&2 | 1&2&3 | 1&2&3&4 |
| PSNR (дБ) | 51,13 | 45,11 | 39,09 | 33,09 | 44,16 | 37,90 | 31,79 |

Классический метод встраивания LSB не требует дополнительных вычислений и позволяет скрывать в относительно небольших файлах объем авторской информации, не превышающей объем младшей битовой плоскости. При этом уровень вносимых искажений является достаточно существенным (около 50 дБ), хотя все еще обеспечивается их визуальная незаметность. Объем встраивания может быть увеличен за счет увеличения числа битовых плоскостей, используемых при встраивании. Однако при этом растет вероятность появления артефактов встраивания, следовательно, снижается его качество (уменьшение PSNR до уровня, близкого к 30 дБ). Кроме того, малейшее изменение изображения приводит к серьезным искажениям, вплоть до полной потери встроенной авторской информации.

Для решения задачи увеличения объема встраивания относительно классического LSB при уменьшении заметности вносимых искажений, был предложен метод многоуровневого

встраивания MLSB [1], использующий для встраивания помехоустойчивые коды. Для формирования рабочей области контейнера в этом методе также могут быть использованы различные комбинации наименее значимых бит цветовых компонентов пикселей BMP-изображения, а именно несколько младших битовых плоскостей.

В представленной работе проводилось исследование метода MLSB, реализованного на базе метода WF5 [1] на тестовых изображениях [6] различных типов: портрет, пейзаж, текст, натюрморт и т.д. В сформированный из трех младших битовых плоскостей взвешенный контейнер встраивалась псевдослучайная последовательность, так как предполагается, что авторская информация может быть зашифрована перед встраиванием. Сравнивая данный метод с применением LSB-встраивания, было выявлено, что при одинаковом объеме встраиваемой информации LSB-метод искажает изображение сильнее, чем метод MLSB, как можно заметить на рисунке, где значения PSNR при MLSB-методе значительно выше при разных способах формирования рабочей области. Это значит, что данный метод, по сравнению с обычным LSB-методом, позволяет комбинировать наименее значимые биты для лучшего распределения встраиваемой информации в контейнере, тем самым уменьшая визуальное искажение изображения.

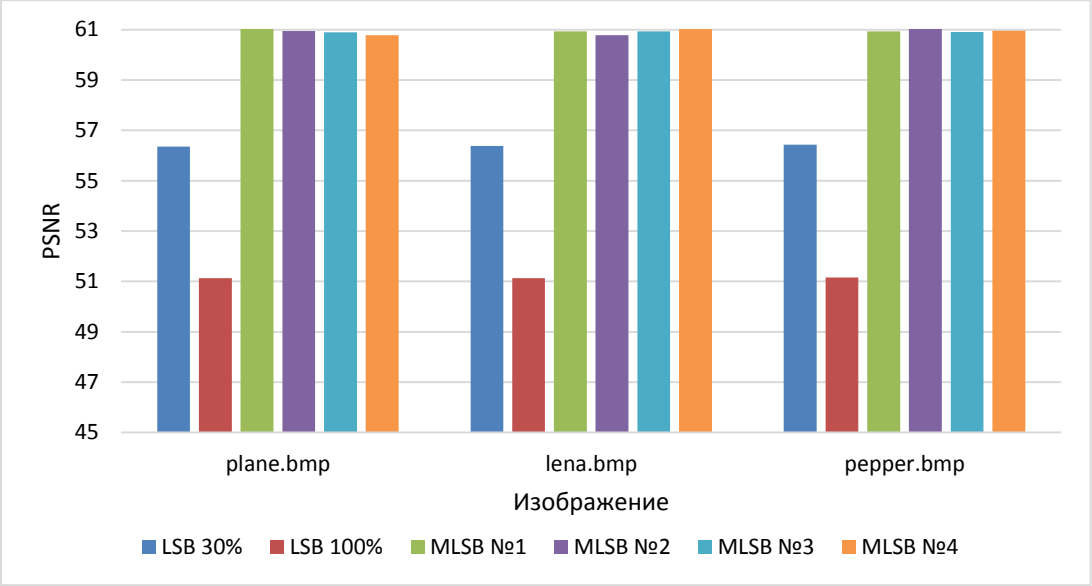



Рисунок. Гистограммы PSNR при встраивании LSB-методом и MLSB-методом

В результате исследования было выявлено, что при одинаковом объеме встраиваемой информации метод MLSB искажает изображение существенно меньше, чем обычный метод LSB. И даже при незначительном объеме встраивания у LSB-метода и при разных способах формирования рабочей области у метода MLSB, значения PSNR значительно выше при встраивании информации методом многоуровневого LSB-встраивания. Это означает, что для решения задачи увеличения объема встраивания в дальнейшем может рассматриваться метод WF5 с использованием других, более оптимальных с точки зрения объема встраивания, параметров помехоустойчивых кодов. Исследования проводились также при использовании разной встраиваемой информации: различные псевдослучайные последовательности; различные тестовые изображения: текст, портретное изображение, пейзаж и т.д. Результаты проведенного эксперимента по встраиванию также подтвердили преимущество метода MLSB над обычным LSB-методом.

**Литература**

1. Беззатеев С.В., Волошина Н.В., Жиданов К.А. Специальные классы кодов для стеганографических систем // Труды ТУСУР. – 2012. – № 1(25). – Ч. 2. – С. 112–118.

2. Минаева Т.А., Волошина Н.В., Беззатеев С.В. Анализ RS-метода стеганоанализа для BMP-изображений // Интеллектуальные и информационные технологии в формировании цифрового общества: сборник научных статей международной научной конференции. – 2017. – С. 10–15.
3. Khurana A., Mohit M.B. Comparison of LSB and MSB based Image Steganography // International Journal of Computer Science and technology. – 2012. – P. 870–871.
4. Fridrich J., Du R., Meng L. Steganalysis of LSB Encoding in Color Images // IEEE International Conference on Multimedia and Expo. – 2000. – P. 1279–1282.
5. Ammad U.I., Khalid F., Mohsin S., Khan Z., Toqeer M., Adnan K., Usman A., Muhammad N. An Improved Image Steganography Technique based on MSB using Bit Differencing // The Sixth International Conference on Innovative Computing Technology. – 2016. – P. 265–269.
6. USC-SIPI Image Database [Электронный ресурс]. – Режим доступа: http://sipi.usc.edu/database/ (дата обращения: 23.02.2018).

**Рудавин Николай Николаевич**
Год рождения: 1993
Университет ИТМО, факультет безопасности информационных технологий, кафедра безопасности киберфизических систем, студент группы № N4159
Направление подготовки: 10.04.01 – Информационная безопасность
e-mail: nikolay-rudavin@yandex.ru

**УДК 004.056.53**

# МЕТОДЫ АУТЕНТИФИКАЦИИ ПО ПОЧЕРКУ

**Рудавин Н.Н.**
**Научный руководитель – д.т.н., доцент Беззатеев С.В.**

Работа выполнена в рамках темы НИР № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность».

За последнее десятилетие в связи с увеличением доступности программно-аппаратных средств с помощью которых возможна организация несанкционированного доступа, казавшиеся ранее надежные средства аутентификации оказались очень уязвимы. В связи с этим остро встает вопрос поиска новых более эффективных методах аутентификации. Особенно актуальными решениями можно считать методы аутентификации, основанные на поведении субъекта, так как для организации доступа субъекту не требуется наличие дополнительных средств, а поведенческие данные невозможно повторить максимально достоверно, так как они основаны не только на физических особенностях субъекта, но и психологические особенности, которые в сочетании со знаниями субъекта о предоставляемой биометрической информации, дают максимально эффективный результат для защиты личных биометрических данных. В работе рассмотрены такие виды поведенческой аутентификации как клавиатурный и рукописный почерк, а также почерк управления мышью.
**Ключевые слова:** информационная безопасность, поведенческая аутентификация, рукописный почерк, клавиатурный почерк, акселерометр.

Важной особенностью задачи аутентификации пользователя по клавиатурному почерку является необходимость «обучения» программы, которая будет производить аутентификацию [1]. Под обучением понимается накопление информации, характеризующей особенности работы каждого пользователя с клавиатурой. Далее эта информация подвергается обработке.

Для обработки должны браться следующие факторы:

1. количество опечаток: субъект допускает типичные ошибки, связанные как с грамотностью, так и с промахами нажатия клавиш;
2. время удержания клавиш: от положения рук, и анатомических особенностей в сочетании с психологическими свойствами субъекта могут отличаться также и интервалы между нажатиями клавиш;
3. скорость набора текста, как в общем, так и отдельных слов [2];
4. степень аритмичности при наборе: разные сочетания символов субъект может писать с разной скоростью.

Метод может иметь следующие преимущества:

1. отсутствие требований к субъекту: человек выполняет привычные действия, а система их отслеживает;
2. отсутствие особых требований к аппаратной платформе, требуется обычная клавиатура и программное обеспечение, считывающее временные интервалы нажатия клавиш.

Существующие программные реализации подобных систем характеризуются недостаточной достоверностью аутентификации [3]. Актуальна разработка новых методов,

алгоритмов и их программно-аппаратных реализаций, повышающих эффективность систем идентификации и аутентификации.

Повышение достоверности аутентификации возможна при добавлении дополнительного фактора. Например, если использовать в момент аутентификации парольную фразу, то аутентификация становиться двухфакторной. Становясь основным фактором парольная фраза слабозащищена из-за возможности утери или хищения пароля, однако, фактор поведенческой аутентификации усложнит нарушителю задачу аутентификации, тем самым повышая надежность системы без снижения доступности (анализ клавиатурного почерка не усложняет задачу аутентификации для субъекта).

Касаемо методов аутентификации по рукописному почерку, в зависимости от вида способа получения подтверждения личности по личностным характеристикам субъекта, следует различать статические и динамические биометрические характеристики.

Для съема данных могут использоваться следующие принципы:

– устройство-позиционер: в данном случае помимо ручки требуется дополнительное устройство, которое оценивает местоположение и движение ручки через радиоканал или оптический либо инфракрасный порт;
– сенсорный экран: в данном случае ручка должна находиться на определенной поверхности, что может обеспечить высокую точность получения координат ручки, но устройство становится более громоздким и возможна обработка данных движения руки только непосредственно при контакте с поверхностью;
– встроенный акселерометр: ручка снимает данные перегрузок во время движения руки. Это гораздо удобнее с точки зрения компактности и простоты применения, также возможна обработка данных поведения не только во время подписи, но и в момент перемещения ручки для последующей постановки.

Все вышеуказанные принципы позволяют достоверно обработать текст, на рис. 1 показана проекция статической составляющей рукописного почерка на координатную плоскость двух субъектов.

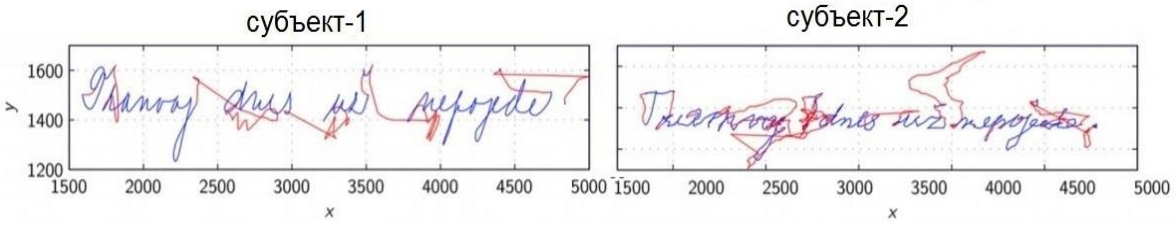



Рис. 1. Демонстрация рисунка почерка двух субъектов

При обработке динамических данных акселерометром записываются данные перегрузки, получаемые движением руки во время написания слов и перемещением руки.

Ниже приведены уникальные поведенческие свойства, которые необходимо выделять в ходе обработки рукописного почерка акселерометром:

1. число амплитуд сигнала перегрузок, характеризующих поворот ручки или ее резкое перемещение;
2. величина каждой амплитуды;
3. временные интервалы между амплитудами;
4. кривизна амплитуд сигнала акселерометра;
5. траектория перемещения ручки между словами.

По каждому из факторов можно назначить свои допустимые пределы для субъекта для системы принятий решения подтверждения личности.

Для исследования возможности корректной обработки динамической составляющей подписи был собран прототип (рис. 2), состоящий из микроакселерометра ADXL-335 и платы-контроллера Arduino Nano v3, обрабатывающей аналоговый сигнал, принимаемый с датчиков перегрузки.

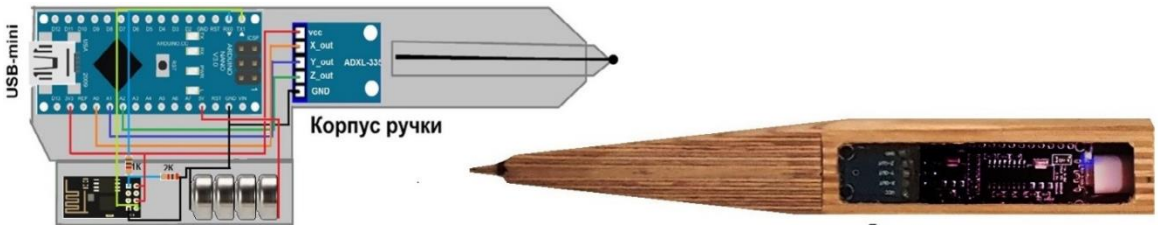



Рис. 2. Компоновочный эскиз (а) и фотография (б) рабочего прототипа

Движения человека во время подписи можно образно разделить на горизонтальную плоскость – непосредственно подпись – и вертикальную ось O:Z – постановка ручки в исходное положение и после завершения процедуры подписи.

На собранном прототипе, показанном выше, удалось собрать данные подписи и передать в программу вторичной обработки сигнала, основная задача которой была найти соответствие между эталонным сигналом и предоставляемым повторно. Для определения соответствия сигнала с эталонным применяется расчет значения коэффициент корреляции Пирсона. Данный критерий позволяет определить, есть ли линейная связь между изменениями значений двух переменных [4].

В программе вторичной обработки сигнала дополнительная синхронизация добавлена, и для проверки работоспособности метода были проведены тесты на проверку значений FRR и FAR – основных показателей надежности в системах биометрической аутентификации, где FRR (False Reject Rate) – ошибка первого рода [5]. Вероятность ошибочного отказа сотруднику аналогична термину «ложная тревога» в радиолокации, а FAR (False Acceptance Rate) – ошибка второго рода вероятности ошибочного пропуска злоумышленника, аналогична термину «пропуск цели».


Рис. 3. Примеры рисунков подписей, сделанных истинным субъектом (а) и ложными субъектами (б, в)

Для начала субъект предоставил свою подпись, сделав 100 попыток, далее выбран эталонный коэффициент корреляции, при котором значение FRR=1% (рис. 3, а). Далее двое ложных субъекта имея рисунок подписи, повторяют подпись по 50 попыток каждый, в конечном итоге из 100 попыток подделать подпись удалось пройти аутентификацию 3 раза (FAR=3%) (рис. 3, б, в).

Таким образом, доказана целесообразность исследования данного метода для разработки системы многофакторной аутентификации.

**Литература**

1. Лебедько Е.Г. Системы импульсной оптической локации. – СПб.: Лань, 2014. – 368 с.
2. Корпоративные информационные системы [Электронный ресурс]. – Режим доступа: http://pandia.ru/text/78/263/4531.php/, своб.
3. Ozan O., Ozarslan Y. Video lecture watching behaviors of learners in online courses // Educational Media International. – 2016. – V. 53. – P. 27–41.
4. Лысыч М.Н., Шабанов М.Л., Жадобкина В.В. Современные системы 3D сканирования // Молодой ученый. – 2014. – № 20. – С. 167–171.
5. Яблочников Е.И., Фомина Ю.Н., Грибовская А.А. Организация технологической подготовки производства в распределенной среде // Изв. вузов. Приборостроение. – 2010. – Т. 53. – № 6. – С. 12–15.

**Хакимова Эльвира Рустамовна**
Год рождения: 1995
Университет ИТМО, факультет безопасности информационных технологий, кафедра безопасности киберфизических систем, студент группы № N4159
Направление подготовки: 10.04.01 – Информационная безопасность
e-mail: elvirochka1995@mail.ru

**УДК 004.056**

# АНАЛИЗ ПОДХОДОВ К ПОСТРОЕНИЮ ИНТЕЛЛЕКТУАЛЬНЫХ КЛАССИФИКАТОРОВ ТЕКСТОВ, НАПИСАННЫХ НА РАЗНЫХ ЯЗЫКАХ

**Хакимова Э.Р.** (Университет ИТМО)
**Научный руководитель – к.т.н., вед.н.с. Чечулин А.А.**
(Санкт-Петербургский институт информатики и автоматизации РАН)

В работе рассмотрен анализ применения систем автоматического перевода текста для классификации веб-сайтов, содержащих текст на неизвестном языке, с целью повышения защищенности пользователя в сети Интернет от нежелательной или незаконной информации, а также проведен анализ подходов к классификации веб-сайтов и текстов.
**Ключевые слова:** Data Mining, анализ данных, защита от информации, категорирование веб-сайтов, автоматический перевод, системы машинного перевода.

В настоящее время происходит постоянный рост объема доступной информации в сети Интернет. Не вся информация, содержащаяся на веб-страницах, является желательной к распространению. В Российской Федерации имеется перечень информации, распространение которой на территории страны запрещено. Перечень такой информации представлен в статье 15.1 Федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [1].

Для защиты от этой нежелательной или запрещенной информации необходимо использовать эффективные механизмы, классифицирующие информацию и регулирующие доступ к ней. В первую очередь это важно для ограничения доступа к определенным видам информации по возрастным категориям, в частности, блокировки информации, запрещенной для просмотра детьми, а также защиты других пользователей от вредоносного контента. На сегодняшний день ограничение доступа достигается за счет ведения «черных» и «белых» списков, но данных подход не эффективен, так как количество сайтов растет с каждым днем, а базы запрещенных ресурсов не успевают за их темпом роста.

Общей целью исследования является защита пользователей в сети Интернет от нежелательной или незаконной информации.

Целью работы стал анализ возможности применения средств автоматического перевода текста для классификации веб-сайтов, содержащих текст на неизвестном языке.

Для достижения поставленной цели необходимо было решить следующие задачи:

1. провести анализ подходов к классификации веб-сайтов;
2. провести анализ подходов к классификации текстов на разных языках;
3. провести анализ существующих систем автоматического перевода.

Проблема недостаточной защищенности интернет-пользователей от нежелательной или запрещенной информации является актуальной в настоящее время. Успехи в данной области очень важны, например, для противодействия пропаганде экстремистской деятельности, борьбы с распространением нелицензионных материалов и ограждения несовершеннолетних от неприемлемого контента.

В данной области проводятся многочисленные исследования и разработка все более новых методов и подходов для решения проблемы защищенности Интернет-пользователей от вредоносного контента. Это применение «черных» и «белых» списков, использование систем родительского контроля, входящих в состав антивирусного программного обеспечения или же в виде самостоятельных решений, а также использование функции «безопасного поиска» в различных web-сервисах [2].

В данных системах блокировки нежелательного контента на первый план выходит необходимость минимизации количества ложных срабатываний, ведь если система будет систематически блокировать подозрительные на ее взгляд ресурсы, которые на самом деле не представляют никакой опасности, пользователь, скорее всего, просто отключит ее [3]. Для решения этой проблемы необходимо разработать алгоритмы, позволяющие успешно относить веб-сайты к определенным классам с необходимой точностью. Задача точной классификации содержимого веб-страниц усложняется тем, что классификатор, предназначенный для анализа страницы на одном языке, может некорректно работать со страницей на другом, тем самым, повышая риск получения пользователем нежелательного или запрещенного контента. В данной работе был предложен подход, основанный на использовании машинного перевода текста, содержащегося на веб-страницах, на язык, понятный классификатору.

В общем случае для определения тематического наполнения веб-страницы может использоваться следующая информация: текст, HTML-структура, URL-адрес, медиаконтент (изображения, видезаписи и т.д.).

Классификация веб-страниц по URL-адресу может быть осуществлена при условии, что адрес отражает тематику веб-сайта [4]. Достоинством данного подхода является то, что адрес сайта в большинстве случаев представляет собой набор (или элементы) английских слов, что позволяет унифицировать классификаторы. Главным недостатком является то, что смысловое содержание URL-адреса не всегда соответствует содержимому сайта.

Подход к классификации веб-сайтов, основанный на анализе структуры страниц (HTML-тегов), позволяет выделять из содержимого веб-страницы ключевые поля, такие как заголовки, названия разделов, подписи и др. Это позволяет не анализировать всю страницу целиком, а лишь наиболее важные ее части (например, заголовки, тексты ссылок, ключевые слова и т.д.), что существенно повышает качество работы классификатора по сравнению с анализом полного текста. Недостатком подхода является возможное отсутствие соответствующих тегов. Кроме того, структурные признаки веб-страниц позволяют выявить такие категории сайтов как чаты и блоги за счет схожей структуры страниц. Данный подход позволяет с высокой степенью точности отнести веб-страницу к классу, основанному на структурных признаках сайта, но не подходит для классификации, основанной на смысловых признаках.

Для классификации веб-страницы по признаку возрастной принадлежности, а также наличию нежелательной или запрещенной для распространения информации наиболее эффективным и широко используемым является анализ текстового содержания веб-страниц.

Классификация текстового содержимого может осуществляться полностью вручную, либо полуавтоматически с помощью созданного вручную набора правил, либо автоматически с применением методов машинного обучения. При этом, несмотря на высокую точность, ручная классификация дорога и неприменима в случаях, когда необходимо классифицировать большое количество веб-страниц с высокой скоростью.

Другой подход основан на формировании набора правил, по которым можно отнести текст к той или иной категории. Этот подход лучше предыдущего, поскольку процесс классификации автоматизируется и, следовательно, количество обрабатываемых документов практически не ограничено. Более того, построение правил вручную может дать лучшую

точность классификации. Однако создание и поддержание правил в актуальном состоянии требует постоянных усилий специалиста.

Основываясь на анализе описанных раннее недостатков, в настоящем исследовании был использован третий подход к классификации текстов, основанный на машинном обучении (Data Mining). В этом подходе «набор правил» или, как принято называть, критерий принятия решения текстового классификатора, вычисляется автоматически из обучающих данных (другими словами, производится обучение классификатора).

В настоящее время классификация сайтов по результатам анализа текста, содержащегося на веб-странице, производится с очень высокой степенью точности. Однако существуют веб-страницы на иностранных языках, к которым классификатор может быть не адаптирован. В подобных ситуациях переходят к другим методам классификации:

1. анализ объектов на странице, не связанных с текстом (например, медиаконтент);
2. создание нового классификатора с использованием обучающей выборки;
3. использование автоматического перевода иностранного текста.

Анализ изображений и другого контента, размещенного на веб-странице, безусловно, может сыграть очень важную роль в процессе выбора класса, которому принадлежит анализируемая страница, но далеко не всегда на веб-страницах размещенный контент соответствует ее содержанию, поэтому предлагаемый метод может использоваться лишь как дополнение к тестовому анализу.

Метод классификации с обучением классификатора с использованием обучающей выборки позволит адаптировать классификатор к иностранному языку и научить работать со страницами на анализируемом языке в дальнейшем, но обучение классификатора очень ресурсозатратно.

По этой причине в данной работе был использован метод автоматического (машинного) перевода иностранного текста на язык, понятный классификатору, и исследовалась зависимость точности его работы от перевода.

Системы автоматического (машинного) перевода – программы, осуществляющие полностью автоматизированный перевод. Главным критерием программы является качество перевода.

Так как необходимо использовать машинный перевод текста, размещенного на веб-сайте на язык, понятный классификатору, рассмотрим системы машинного перевода текста.

Примерами таких систем могут являться: Google Translate, Яндекс.Переводчик, PROMT, Bing, Webtran.

Выделим основные характеристики для сравнения систем машинного перевода.

1. Возможность автоматического определения языка. Так как текст, содержащийся на сайте, может быть написан на разных языках, необходимо, чтобы определение этого языка производилось автоматически.
2. Количество поддерживаемых языков. Так как сайты могут содержать информацию на различных языках, то чем больше языков поддерживает система машинного перевода, тем более вероятна успешная классификация сайта.
3. Возможность автоматического выбора стилистической направленности текста, что повысит качество перевода.
4. Возможность перевода устойчивых выражений (фразеологизмы, устойчивые словосочетания).
5. Возможность перевода больших объемов текста. Так как на сайтах может содержаться неограниченное количество текстовой информации, то необходимо, чтобы система машинного перевода могла обрабатывать большое количество текстовой информации [5].

Сравнительная характеристика выбранных систем машинного перевода по заданным критериям представлена в таблице.

Таблица. Сравнение систем машинного перевода

| Критерии | Системы | | | | |
|---|---|---|---|---|---|
| | Google Translate | Яндекс. Перевод | PROMT | Bing | Webtran |
| Автоматическое определение языка | + | + | + | + | – |
| Количество поддерживаемых языков | 103 | 95 | 17 | 62 | 102 |
| Выбор стиля текста | + | + | + | – | – |
| Перевод устойчивых выражений | + | + | + | – | + |
| Перевод больших объемов текста | + | + | – | + | + |

В результате анализа систем машинного перевода, была выбрана наилучшая система по параметрам, необходимым для перевода информации, содержащейся на сайтах: Google Translate.

В результате выполнения работы был проведен анализ имеющихся подходов к классификации веб-сайтов. Классификация веб-сайтов может быть основана на анализе URL-адресов, HTML-тегов и текстового содержимого. Так как первые два подхода не всегда характеризуют смысловое наполнение сайта, выбранным подходом является подход, основанный на анализе текстового содержимого сайта.

В связи с тем, что текстовая информация на иностранном языке, размещенная на сайте, может быть не понятна классификатору, необходимо использовать дополнительные методы классификации веб-сайта. Имеются также такие методы классификации веб-сайтов как по медиасодержимому, другим параметрам, не связанным с текстовым содержимым. Данные методы ресурсозатратны и не всегда позволяют определить категорию сайта. В связи с этим для обработки текстового содержимого сайтов, написанных на языках, неизвестных классификатору, необходимо использование автоматического перевода исходного текста на необходимый язык. Был проведен анализ существующих систем автоматического перевода. Рассмотрены современные системы машинного перевода, а также проведен сравнительный анализ по выбранным характеристикам.

**Литература**

1. Федеральный закон от 27.07.2006 г. № 149-ФЗ (ред. от 25.11.2017) «Об информации, информационных технологиях и о защите информации».
2. Новожилов Д.А., Чечулин А.А., Котенко И.В. Улучшение категорирования веб-сайтов для блокировки неприемлемого содержимого на основе анализа статистики HTML-тэгов // Информационно управляющие системы. – 2016. – № 6(85). – С. 65–73.
3. Антонов А.Ю., Чечулин А.А., Фаткиева Р.Р., Лебедева Т.Н. Программный модуль классификации веб-страниц на основе изображений в автоматизированной системе блокировки нежелательного контента: дипломная работа. – СПб.: Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина). – 2018. – 86 с.
4. Дюк В. Data Mining: учебный курс. – СПб.: Питер, 2001. – 368 с.
5. Сравнение онлайн-переводчиков [Электронный ресурс]. – Режим доступа: http://all-around-the-words.ru, своб.

**Борисенко Павел Сергеевич**
Год рождения: 1993
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, аспирант
Направление подготовки: 10.06.01 – Информационная безопасность
e-mail: borisenkopp@yandex.ru

**Мостовой Роман Александрович**
Год рождения: 1993
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, аспирант
Направление подготовки: 10.06.01 – Информационная безопасность
e-mail: rommostovoy@gmail.com

**Слепцова Дарья Максимовна**
Год рождения: 1993
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, аспирант
Направление подготовки: 10.06.01 – Информационная безопасность
e-mail:dsleptsova@corp.ifmo.ru

**Левина Алла Борисовна**
Год рождения: 1983
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, к.ф.-м.н., доцент
e-mail: levina@cit.ifmo.ru

**УДК 004.056.53**

## МОБИЛЬНЫЕ СОЦИАЛЬНЫЕ СЕТИ: АТАКИ ПО СТОРОННИМ КАНАЛАМ И ПРОТИВОДЕЙСТВИЕ ИМ

**Борисенко П.С., Мостовой Р.А., Слепцова Д.М.**
**Научный руководитель – к.ф.-м.н., доцент Левина А.Б.**

Мобильные социальные сети (MSN) – это сети, в которых люди со схожими интересами объединены между собой при помощи мобильных устройств. В последнее время область мобильных социальных сетей быстро развивается, в особенности благодаря появлению новых беспроводных технологий, позволяющих добиться более эффективной коммуникации и улучшенных сетевых показателей (например, уменьшение времени задержки, увеличенная скорость передачи данных и расширенное покрытие сети). Однако большинство пользователей MSN не осознают важность безопасности их мобильных устройств. В связи с этим множество атак, нацеленных на персональные данные и чувствительную информацию, представляют собой быстрорастущую угрозу на фоне не менее быстрорастущего прогресса в новых приложениях и сервисах MSN. Целью данной работы являлось изучение современного оборудования на предмет компрометации чувствительной пользовательской информации. Получить подобную информацию с мобильного устройства можно при помощи обычной недорогой аудиокарты. В работе авторы исследовали способы снятия сигнала по сторонним

каналам при помощи аудиокарты, влияние частоты дискретизации на качество записей утечек, а также предложили нейронные сети для улучшения качества извлечения информации.
**Ключевые слова:** мобильные социальные сети, безопасность информационных систем, атаки по сторонним каналам.

Быстро растущее число мобильных устройств, а также «социальные» мультимедийные приложения и услуги могут обеспечивать прямую связь между пользователями для разгрузки инфраструктуры сетевого оператора, что возможно во многих беспроводных технологиях [1]. Подобная гетерогенная связь стимулирует появление новой сетевой парадигмы, называемой мобильными социальными сетями (MSN), где модели взаимодействия и обмена данными между пользователями основаны на их социальных контактах и отношениях [2, 3]. Согласно отчету Sandvine Global Internet Phenomena, у MSN 22%-ная доля мобильного трафика в США, и эта цифра значительно выросла в последние десятилетия.

Одна из первых работ, посвященных MSN, с точки зрения сочетания функциональности обычных социальных сетей с особенностями мобильной связи, была обобщена в [4]. В данной работе авторы предложили пользователям использовать свои социальные контакты, чтобы повысить эффективность работы сети с точки зрения пользователя. Другая линия исследований по MSN рассматривает традиционные социальные сети с централизованным блоком управления, где данные могут быть получены непосредственно через мобильные устройства в случае отказа центрального узла [5]. В этих ситуациях устройства, находящиеся в непосредственной близости, могут взаимодействовать с использованием радиотехнологий ближнего действия [6–8].

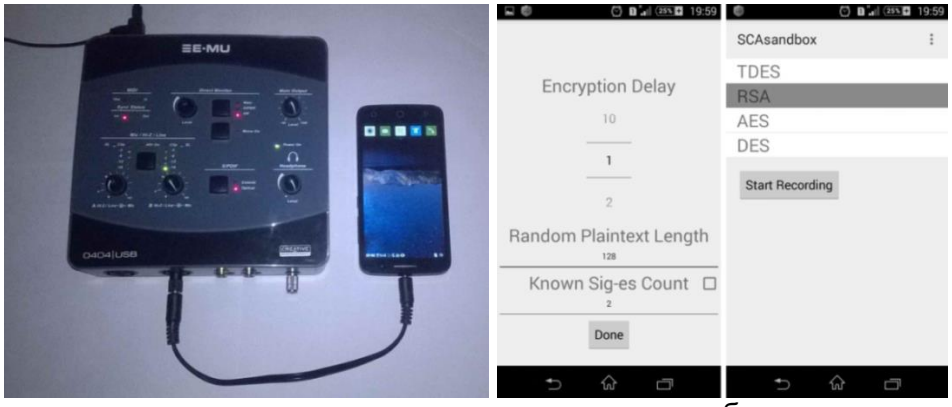
Современные MSN активно развиваются, чтобы удовлетворить компромисс между высокой скоростью передачи данных и низкой задержкой на основе реальных требований приложений. Однако передаваемые данные должны быть защищены независимо от сценария использования. В этой связи проблемы безопасности и конфиденциальности в средах MSN становятся очень важны. Существующие работы [9] дают ценные результаты в отношении конфиденциальности и безопасности, но они не учитывают надежность предлагаемых решений против атак, направленных на извлечение конфиденциальной информации с устройств пользователя, что являлось главной целью этой работы (рис. 1).


Рис. 1. Пример атаки по сторонним каналам в кафе (по аудиоканалу)

В повседневных приложениях работа криптографических алгоритмов сильно зависит от непосредственной среды исполнения. В среде физические и социальные взаимодействия могут контролироваться злоумышленниками, но и сами подслушиваемые данные могут использоваться в последующем криптоанализе для извлечения конфиденциальной информации. Действия, использующие утечки по физическому каналу, называются атаками на побочные каналы (SCA). Принимая во внимание улучшенное качество связи, предлагаемое MSN как на социальном, так и на сетевом уровне, злоумышленник может быть в первую очередь заинтересован в захвате авторизационных данных через SCA, чтобы затем захватить доступ к самим устройствам.

**Атаки по сторонним каналам на мобильные устройства.** В этом разделе описан основной сценарий атаки SCA. Очевидно, что, используя более сложное и, следовательно, дорогостоящее оборудование, атакующему будет легче провести успешную SCA. Однако полагаясь на допущение, что злоумышленник может воспользоваться только недорогим оборудованием для прослушивания, авторами приведен пример доступной SCA для получения записей сигнала со смартфона при помощи имеющейся на рынке внешней звуковой карты. Данный прототип для SCA представлен на рис. 2.

Из-за большого количества ограничений, связанных с SCA, было разработано специальное приложение, которое эффективно служит в качестве «песочницы» для соответствующих криптографических приложений. Кроме того, созданное приложение позволяет выполнять требуемые криптографические операции на высокой частоте для быстрого накопления достаточных данных для проведения дальнейших атак.




а б

Рис. 2. Прототип для атаки (а) и приложение для Android с функцией шифрования (б)

Как правило, модель атаки может быть представлена следующей последовательностью:

1. начальная подготовка: обучение – это процесс, выполняемый несколько раз, что делает расшифровку более вероятной;
2. сбор данных: оборудование атакующего пассивно выполняет мониторинг местоположения целевого мобильного телефона;
3. выполнение атаки: данные, полученные на этапе обучения, используются для расшифровки фактической информации на основе реального набора данных на этапе сбора данных. Этот шаг можно интегрировать с фазой сбора и динамически выполнять на ходу; или он может выполняться автономным статическим образом после того, как сбор данных завершен.

На начальном этапе обучения стоит генерировать несколько схожих криптографических операций (с тем же открытым текстом и ключевым материалом) перед обработкой случайных открытых текстов и (или) ключей. Цель состоит в том, чтобы обеспечить максимально возможную синхронизацию между атакующим инструментом и данными. Для этого если в трассировке имеется несколько равных записей, более вероятно обнаружение в зашифрованной последовательности стартовой и конечной точек утечки. Эта функциональность может быть применима для зашумленного оборудования внутри целевого устройства.

**Получение данных и анализ.** В этом разделе основное внимание уделялось сбору данных и возможностям его обработки во время SCA. Для реализации данной SCA авторы выбрали два устройства, предлагаемые разными производителями: Alcatel POP3 и Sony Xperia M2.

Во время начальной фазы обучения был выполнен чистый запуск данного приложения «песочница». На этом этапе большая часть фоновой активности целевого устройства была снижена. Наблюдения криптографической операции в режиме «песочницы» показывают относительно четкие следы, как показано на рис. 3. Например, первую операцию можно наблюдать из пункта 2:11,0 и до 2:12,5. Изучение операций в режиме «песочницы» позволяет

выполнить требования первоначального этапа обучения, дополняя набор криптографических отпечатков операции. Однако при анализе следов после фазы обучения для Xperia M2 отмечена резкая разница в определении данных – почти пустая трассировка. По-видимому, специфическая разница в оборудовании приводит к совершенно различным профилям утечек. Было решено сосредоточиться исключительно на анализе Alcatel POP3.

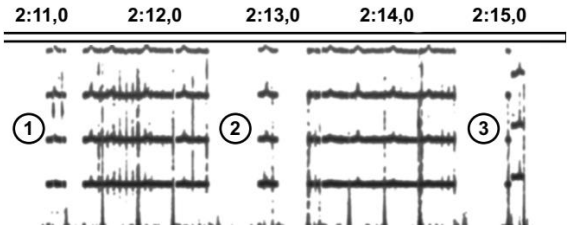
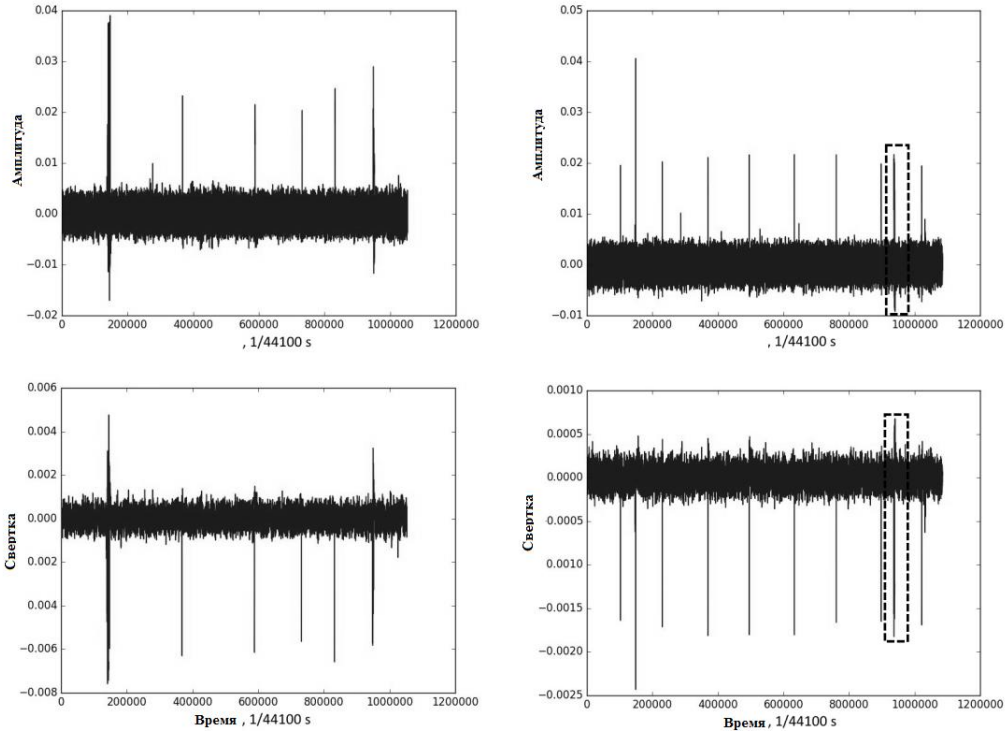



Рис. 3. Пример снятого сигнала для Alcatel POP3: каждая операция шифрования пронумерована

Следующим шагом SCA являлась предварительная обработка данных для последующего анализа нейронной сетью. Входные данные преобразовывались в векторный формат, где каждый вектор содержал запись сигнала во время криптографической операции. Затем выполнялась синхронизация записей, после чего разработанный авторами программный анализатор получал эти данные.




а б

Рис. 4. Обнаружение сигнатур: метод 1 (а); метод 2 (б)

Цель анализатора состоит в том, чтобы удалить шум от криптографических операций, а также экспортировать их для дальнейшей обработки нейронной сетью. В данном случае использовалось два различных метода (рис. 4):

1. функция свертки: программа рассматривала как запись сигнала, так и их сигнатуры как функции. Анализатор выполнял итерацию по всем гипотезам относительно первой сигнатуры и вычислял полученную функцию свертки между гипотезой и всем следом. Пики результирующих функций указывали на то, какие гипотезы являются наиболее вероятными и сколько сигнатур, соответствующих каждой конкретной гипотезе, присутствуют в следе;

2. функция свертки в окрестности: анализатор использовал набор периодов времени, прошедших между криптографическими операциями, как «решетку» для обнаружения сигнатуры. Функция свертки вычислялась между каждой гипотезой первой сигнатуры и соответствующими гипотезами других обнаруженных сигнатур на основе времени выполнения.

В заключение необходимо было отметить два интересных факта после выполнения операций предварительной обработки и синтаксического анализа:

- сигнатуры в основном не очень подробные из-за выборки звуковой карты. Следовательно, уровень детализации оказывает огромное влияние на предварительную обработку полученных данных;
- ошибка обнаружения, т.е. вероятность неправильного извлечения сигнатуры, вызванного шумом, отмечена пунктирной линией. Аналогичный результат был достигнут с использованием первого метода на том же трассе. Причина такой неточности может быть связана с низким качеством сигнала. Использование более дорогостоящего и надежного оборудования для сбора данных являлось решением обеих вышеупомянутых задач.

**Заключение.** Рост новых MSN создает серьезные проблемы для обеспечения информационной безопасности в мобильных устройствах. Распространение сервисов мобильных социальных сетей подвергает пользователя риску атаки его устройства. В работе авторы продемонстрировали, что использование недорогостоящего готового оборудования для атаки на побочный канал смартфонов возможно, и это является серьезной угрозой, ведь факт вторжения, по-прежнему, трудно обнаружить. Результаты показывают, что даже при использовании оборудования низкого класса злоумышленники могут обнаруживать сигналы криптографических вычислений соединенных сетью устройств. Лишь небольшое улучшение в инструментах позволит снимать более информативный сигнал и получать конфиденциальную информацию с большей точностью.

**Литература**

1. Lin L., Xu L., Zhou S. and Xiang Y. Trustworthiness-hypercubebased reliable communication in mobile social networks // Information Sciences. – 2016. – V. 369. – P. 34–50.
2. Hu X., Chu T.H., Leung V.C., Ngai E.C.-H., Kruchten P. and Chan H.C. A survey on mobile social networks: Applications,platforms, system architectures, and future research directions // IEEE Communications Surveys & Tutorials. – 2015. – V. 17. – № 3. – P. 1557–1581.
3. Su Z., Xu Q. and Qi Q. Big data in mobile social networks: A QoEoriented framework // IEEE Network. – 2016. – V. 30. – № 1. – P. 52–57.
4. Miluzzo E., Lane N.D., Fodor K., Peterson R., Lu H., Musolesi M., Eisenman S.B., Zheng X. and Campbell A.T. Sensing Meets Mobile Social Networks: The Design, Implementation and Evaluation of the CenceMe Application // Proc. of 6th ACM conference on Embedded network sensor systems. – 2008. – P. 337–350.
5. Kayastha N., Niyato D., Wang P. and Hossain E. Applications, architectures, and protocol design issues for mobile social networks: A survey // Proc. of the IEEE. – 2011. – V. 99. – № 12. – P. 2130–2158.
6. Bai B., Wang L., Han Z., Chen W. and Svensson T. Caching based socially-aware D2D communications in wireless content delivery networks: a hypergraph framework // IEEE Wireless Communications. – 2016. – V. 23. – № 4. – P. 74–81.
7. Vastardis N. and Yang K. Mobile social networks: Architectures, social properties, and key research challenges // IEEE Communications Surveys & Tutorials. – 2013. – V. 15. – № 3. – P. 1355–1371.
8. Ajami R., Qirim N.A. and Ramadan N. Privacy Issues in Mobile Social Networks // Procedia Computer Science. – 2012. – V. 10. – P. 672–679.
9. Liang X., Zhang K., Shen X. and Lin X. Security and privacy in mobile social networks: challenges and solutions // IEEE Wireless Communications. – 2014. – V. 21. – № 1. – P. 33–41.

**Варюхин Владимир Алексеевич**
Год рождения: 1995
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N4152
Направление подготовки: 10.04.01 – Информационная безопасность
e-mail: vladimirrus13@mail.ru

**Гоман Елена Вячеславовна**
Год рождения: 1995
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N4152
Направление подготовки: 10.04.01 – Информационная безопасность
e-mail: nen7995ka@mail.ru

**УДК 004**

# ОСОБЕННОСТИ ПРОВЕДЕНИЯ ВНУТРЕННЕГО АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МАЛЫХ ОРГАНИЗАЦИЯХ

**Варюхин В.А., Гоман Е.В.**
**Научный руководитель – д.т.н., профессор Гатчин Ю.А.**

В работе рассмотрены особенности проведения внутреннего аудита информационной безопасности в малых организациях. Данный процесс был рассмотрен в соответствии с циклической моделью Дёминга–Шухарта. Также были рассмотрены основные руководящие документы в области проведения аудита информационной безопасности.
**Ключевые слова:** аудит, информационная безопасность, организация, модель Дёминга–Шухарта, защита информации, сотрудник, анализ, угроза.

В век цифровых технологий информация представляет огромную ценность и имеет большое влияние, поэтому утечка информации конфиденциального характера может привести к невосполнимому ущербу. Для защиты данной информации уже действуют и постоянно разрабатываются новые законы и стандарты. Однако предложенные методы и средства по защите информации быстро устаревают, необходимо ежедневно отслеживать новые угрозы информационной безопасности (ИБ) и проверять работоспособность системы защиты в организациях. Эту функцию исполняет аудит ИБ, который является частью третьего этапа в циклической модели Дёминга–Шухарта, представленной на рисунке.

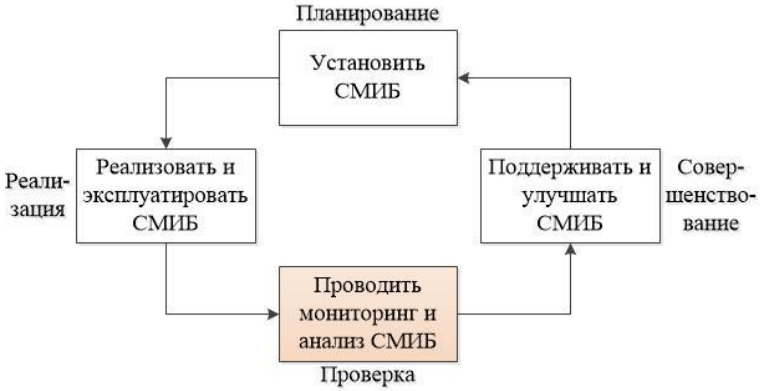



Рисунок. Модель Дёминга–Шухарта, где СМИБ – система менеджмента информационной безопасности

Целью работы являлось выявление особенностей при проведении внутреннего аудита информационной безопасности в малых организациях.

В ГОСТ Р 50922-2006 под «аудиторской проверкой информационной безопасности в организации» понимается периодический, независимый и документированный процесс получения свидетельств аудита и объективной оценки с целью, определить степень выполнения в организации установленных требований по обеспечению информационной безопасности [1]. Данное определение подразумевает внешний аудит, так как внутренний аудит – это постоянно функционирующая в организации система контроля.

Аудит проводится в целях установления степени защищенности информационных ресурсов, выявления уязвимостей в системе защиты, проверке на соответствие требованиям законодательству в области ИБ или для обоснованности инвестиций на развитие системы обеспечения ИБ компании.

В свою очередь, внутренним аудитом также называют текущий аудит, и его можно разделить на следующие типы:

- мониторинг состояния ИБ;
- регулярная проверка состояния ИБ.

Первый тип представляет собой автоматический и полуавтоматический непрерывный контроль систем и мер обеспечения ИБ. В целях данных работ использовались системы контроля и отчетности систем обеспечения ИБ и проводимые регламентные работы по мониторингу состояния ИБ.

Второй тип – аудит состояния ИБ, заключающийся в обследовании защищенности информационных систем объектов информатизации на периодической основе. Данный аудит включает в себя работы по инструментальному обследованию информационных систем, а также проверку соответствия состояния информационных систем требованиям, предъявляемым к обеспечению ИБ.

Обычно внутренний аудит осуществляется подразделением или должностным лицом организации.

Стандарт ISO/IEC 19011 описывает, что аудит должен проводиться беспристрастно, а результаты по окончанию проверки должны быть объективными. Также следует формировать группу аудиторов из числа таких специалистов, которые сами не являются разработчиками и администраторами используемых информационных систем и средств защиты информации и не имели отношения к их внедрению на данном предприятии [2].

Вышеперечисленное усложняет задачу поиска непредвзятого человека в малых организациях из-за небольшого штата сотрудников. По этой же причине аудиторов не проверяют на соответствие их квалификации требованиям программы аудита, но они должны обладать специальными знаниями и умениями, описанными в ISO 19011 в приложении А.

Одна из основных особенностей проведения внутреннего аудита ИБ в малых организациях – это ограниченное количество персонала, способного к проведению такого рода работ. Подобным компаниям свойственно, что сотрудники уже выполняют широкий круг обязанностей [3]. Таким образом, руководству фирмы необходимо назначить руководителя группы аудитора и определить состав аудиторской группы. В малой организации в силу небольшого контингента в группу будут входить сотрудники из отделов по информационной безопасности и информационных технологий, при этом выбираются наиболее опытные и грамотные сотрудники. Следствием этого будет отсутствие беспристрастного и объективного аудита, которое, в свою очередь, может добавить к уже существующим проблемам ИБ новые.

Следует учесть, что не всегда организация может проводить аудит своими силами, так как в силу дороговизны средств для инструментального анализа не все имеют возможность его приобрести.

Также следует упомянуть морально-этическую сторону вопроса, когда в малой организации практически все сотрудники знают друг друга и имеют налаженные социальные связи. При этом аудитор знает, что если он выявит нарушения, то к его коллеге могут применить санкции, и тогда он будет осуществлять проверку необъективно.

Выявленные особенности помогают сделать вывод, что для более эффективного внутреннего аудита ИБ в малых организациях, в которых циркулирует информация, подлежащая защите, следует заключить контракт на передачу функций внутреннего аудита с аутсорсинговой компанией, специализирующейся на данном виде деятельности. Это поможет проводить эффективный мониторинг функционирования системы защиты информации, так как к работе будут привлекаться незаинтересованные и независимые специалисты различных профилей.

**Литература**

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Введен 01.02.2008. – М.: Стандартинформ, 2008. – 8 с.
2. ISO/IEC 19011. Руководящие указания по аудиту систем менеджмента [Электронный ресурс]. – Режим доступа: http://pqm-online.com/assets/files/pubs/translations/std/iso-19011-2018-(rus).pdf, своб.
3. Малая организация «Словарь терминов» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_211197/#dst100140, своб.

**Дикий Дмитрий Игоревич**
Год рождения: 1994
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, аспирант
Направление подготовки: 10.06.01 – Информационная безопасность
e-mail: dimandikiy@mail.ru

**Артемьева Виктория Денисовна**
Год рождения: 1995
Балтийский федеральный университет имени Иммануила Канта, факультет медицинский институт
Направление подготовки: 31.05.01 – Лечебное дело
e-mail: vika_med2019@mail.ru

**УДК 007.51**

# МОДЕЛЬ БЕЗОПАСНОСТИ СРЕДЫ ИНТЕРНЕТ ВЕЩЕЙ

**Дикий Д.И.** (Университет ИТМО)**, Бурдаков А.А.** (Университет ИТМО)**, Метлушко А.И.** (Университет ИТМО)**, Трошин Д.Е.**(Университет ИТМО)**, Хорошев Р.Д.** (Университет ИТМО)**, Юшков Е.Ю.** (Университет ИТМО)**, Артемьева В.Д.** (Балтийский федеральный университет имени Иммануила Канта, Калининград)
**Научный руководитель – д.т.н., доцент Гришенцев А.Ю.** (Университет ИТМО)

Работа выполнена в рамках темы НИР № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность».

В работе рассмотрены современные проблемы безопасности Интернета вещей в виде трехуровневой модели. Описаны проблемы безопасности каждого конкретного слоя и приведены методы их решения.

**Ключевые слова:** Интернет вещей, безопасность, модель.

Интернет вещей (Internet of Things, IoT) играет все более и более важную роль в жизни человека с момента его появления. Он охватывает множество технологий, в том числе традиционное оборудование для общих бытовых нужд, такие как Radio Frequency IDentification (RFID)-метки и считыватели [1]. Учитывая большой потенциал Интернета вещей, также возникают множественные виды проблем, связанные с ним. В работе основное внимание уделяется проблемам безопасности. Эксперты выделяют три или четыре слоя с точки зрения безопасности Интернета вещей. Например, распространена такая модель [2]: слой восприятия, транспортный слой и прикладной слой. В данной работе отдельно проанализированы проблемы безопасности каждого слоя и предприняты попытки найти решения таковых.

С быстрым развитием Интернета вещей также быстро развиваются множество приложений Интернета вещей, которые способствуют нашей повседневной жизни. Они охватывают области от традиционного оборудования для общих бытовых предметов, которые помогают сделать жизнь человека лучше. Эта технология обладает большим потенциалом [3]. Между тем возникает ряд проблем на пути. Например, с точки зрения масштабируемости IoT-приложений, которые требуют большого количества устройств, зачастую, бывает трудно реализовать их из-за ограничений по времени, памяти, обработки и энергетических ограничений. Например, расчет суточных перепадов температуры по всей стране может требовать миллионы устройств и привести к неуправляемому объему данных.

Оборудования Интернета вещей от различных производителей часто имеют различные эксплуатационные характеристики, такие как частота дискретизации и распределение ошибок, между тем датчики и приводы компоненты Интернета вещей всегда очень сложны. Все эти факторы способствуют формированию гетерогенной сети Интернета вещей, в которой данные Интернета вещей будут глубоко неоднородны. Более того, потребуется передавать огромный объем необработанных данных в сложных и неоднородных сетях, даже с учетом сжатия и слияния данных, как способ уменьшения потока информации. Следовательно, одной из основных проблем в Интернете вещей на данный момент является стандартизация формирования и обработки данных для будущего Интернета вещей. Более того, не стоит забывать про внешних злоумышленников, авторов вредоносного программного обеспечения и вирусов, которые стремятся в процессе коммуникации нарушить целостность, доступность и конфиденциальность данных и информации. С развитием технологий Интернета вещей информационной безопасности будет непосредственно уделено огромное внимание.

В настоящее время Интернет вещей широко применяется в приложениях социальной жизни, таких как смарт-грид, умный транспорт, умный безопасности, умный дом [4]. Карточки доступа и некоторые другие малые применения также принадлежат к Интернету вещей. Применение Интернета вещей может принести людям удобство, но, если он не может обеспечить безопасность личной жизни, конфиденциальная информация может быть подвержена утечке в любой момент времени. Особенно остро стоит проблема в отношении медицины, когда устройства Интернета вещей обрабатывают информацию, содержащую сведения о состоянии здоровья, динамических и статических параметров человека. С широким распространением Интернета вещей риск раскрытия утечки информации будет увеличиваться, поэтому стоит уделять огромно внимание безопасности в среде Интернета вещей, учитывая возможные технологические продвижения в этой области, масштабируемость и существующую стандартизацию.

1. Слой восприятия. В этот слой включены исполнительные и сенсорные устройства, такие как: RFID-метки и считыватели, беспроводные сенсорные сети, GPS-устройства и комбинации этих технологий. В этом слое стоит уделять огромное внимание протоколам взаимодействия устройств дуг с другом. На данный момент нет единого протокола, учитывающего аспекты всех видов устройств. Сюда же относится физическая защита устройств. Это актуально, когда злоумышленник может иметь непосредственный доступ к устройствам или узлам сети. Другой проблемой этого слоя является криптографическая защита. Ввиду ограниченности вычислительных, энергетических мощностей на этом уровне трудно создать достаточно криптостойкий протокол, который не будет влиять на пропускную способность сети Интернета вещей. Аналогична ситуация относительно согласования ключей и ключевой информации. Для RFID-технологий также актуальна проблема коллизий, когда несколько меток находятся рядом с друг с другом. Здесь, во-первых, стоит проблема, как отличить одну метку от другой, а во-вторых, как ускорить процесс сканирования, в-третьих, как защитить метку от несанкционированного копирования. С другой стороны, как обозначается проблема, как обеспечить считывание информации, если несколько устройств посылают информацию на считыватель одновременно. Еще одной проблемой является управление доверием между устройствами. Особенно остро эта проблема стоит в моменты включения в сеть исполнительных устройств нового устройства.
2. Транспортный слой. Этот слой можно подразделить на несколько составляющих. Одна из самых основных – это доступ к сети. В качестве сети – это может быть выделенная сеть, сеть Wi-Fi точек, 3G- или LTE-сети мобильных устройств, а также ad hoc [5] – самоорганизующиеся сети (децентрализованная беспроводная сеть, не имеющая постоянной структуры, в которых клиентские устройства соединяются «на лету», образуя собой сеть). На этом уровне огромное внимание уделяется проблемам безопасности WiFi

– это атаки доступа, вредоносные фишинговые точки доступа и DDoS/Dos-атаки. Для того чтобы решить вопросы безопасности беспроводного доступа в Интернет, применяются контроль доступа и шифрование в сети. Контроль доступа означает, что доступ к сети Wi-Fi могут получить только авторизованные пользователи. Сетевое шифрование означает, что только получатель может правильно расшифровать содержимое данных. Контроль доступа и технологии шифрования сети включают WPA, шифрование, аутентификацию и т.д. Последнее время интенсивно развиваются одно ранговые ad hoc сети. Для них характерны следующие проблемы безопасности. Проблемы безопасности доступа к незаконному узлу: каждый узел должен иметь возможность подтвердить личность других узлов, которые взаимодействуют с узлом, в противном случае злоумышленник может легко захватить узел, тем самым предоставляя доступ к критическим ресурсам и информации, а также вмешиваться в работу других узлов связи. Авторизация и проверка подлинности может устранить эту проблему безопасности. Сертификация подтверждает, что узел является законным, а затем авторизация определяет, разрешено ли этому устройству выполнять определенные действия. Вопросы безопасности данных: беспроводная специальная сеть связи является неориентированной, следовательно, сенсорные данные, передаваемые по сети, могут быть легко компрометированы злоумышленником. Сети маршрутной информации также подвержены вредоносным идентификациям пользователей, и, таким образом, появляется возможность незаконно получить точное местоположение объекта. Механизм аутентификации и управления ключами, как правило, способны решить эту проблему безопасности.

3. Прикладной слой. Этот уровень охватывает приложения Интернета вещей и их поддержку. Основные вопросы безопасности включают в себя конфиденциальность информации при краже, незаконном подслушивании и так далее. DDoS-атаки на технологии сетевого уровня так же, как и атаки при передаче 3G, вызывают некоторые проблемы безопасности на прикладном уровне. Безопасность используемого приложения зависит от конкретного приложения. Вопросы безопасности не могут быть решены в других слоях. С различными приложениями возникают характерные им проблемы безопасности. Это в первую очередь связано с процессом разработки программного обеспечения и квалификации программистов, их ответственности и наличия технической поддержки.

**Заключение.** Рассмотрев многие аспекты технологии Интернета вещей, и проанализировав трехуровневую модель безопасности, можно сделать вывод о том, что с распространением данной технологии вопросы безопасности становятся с каждым днем все актуальнее. Построение модели безопасности способствует стандартизации и классификации уязвимостей технологии, а также позволяет уделять внимание конкретным ее элементам среды Интернета вещей и своевременно принимать все необходимые меры.

**Литература**

1. Thanapal P., Prabhu J., Jakhar M. A survey on barcode RFID and NFC [Электронный ресурс]. – Режим доступа: http://iopscience.iop.org/article/10.1088/1757-899X/263/4/042049/pdf, своб.
2. Jing Q., Vasilakos A.V., Wan J., Lu J., Qiu D. Security of the internet of things: Perspectives and challenges // Wireless Networks. – 2014. – V. 20(8). – P. 2481–2501.
3. Hachem S., Teixeira T. & Issarny V. Ontologies for the internet of things // ACM. – 2011. – P. 1–6.
4. Sundmaeker H., Guillemin P., Friess P. & Woelffle´ S. Vision and challenges for realising the internet of things [Электронный ресурс]. – Режим доступа: http://www.robvankranenburg.com/sites/default/files/Rob%20van%20Kranenburg/Clusterbook%202009_0.pdf, своб
5. Ahmed W., Elhadef M. Securing intelligent vehicular ad hoc networks: A survey // Lect Notes Electr Eng. – 2018. – V. 474. – P. 6–14.

**Добычина Анна Владимировна**
Год рождения: 1995
Университет ИТМО, факультет безопасных информационных технологий, кафедра проектирования и безопасности компьютерных технологий, студент группы № N4160
Направление подготовки: 11.04.03 – Конструирование и технология электронных средств
e-mail: anndobychina1@gmail.com

**Акимов Сергей Владимирович**
Год рождения: 1996
Университет ИТМО, факультет безопасных информационных технологий, кафедра проектирования и безопасности компьютерных технологий, студент группы № N4160
Направление подготовки: 11.04.03 – Конструирование и технология электронных средств
e-mail: sergeyakim12@mail.ru

**Хасанов Айнур Радикович**
Год рождения: 1993
Университет ИТМО, факультет безопасных информационных технологий, кафедра проектирования и безопасности компьютерных технологий, студент группы № N4160
Направление подготовки: 11.04.03 – Конструирование и технология электронных средств
e-mail: xacahob@bk.ru

**Кузнецов Александр Юрьевич**
Год рождения: 1989
Университет ИТМО, факультет безопасных информационных технологий, кафедра проектирования и безопасности компьютерных технологий, к.т.н., доцент
e-mail: alkuznetcov@corp.ifmo.ru

**УДК 004.72**

## ИССЛЕДОВАНИЕ ПРОТОКОЛОВ ПЕРЕДАЧИ ДАННЫХ В КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ

**Добычина А.В., Акимов С.В., Хасанов А.Р., Кузнецов А.Ю.**
**Научный руководитель – к.т.н., доцент Кузнецов А.Ю.**

Работа выполнена в рамках темы НИР № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность».

Настоящее исследование посвящено проблеме передачи данных в киберфизических системах. В работе проведен небольшой исторический экскурс в понятие киберфизических систем, определен генезис термина. Проведенный обзор протоколов передачи данных и сделанный на его основе сравнительный анализ позволили сделать вывод о том, что для успешного и безопасного функционирования киберфизических систем необходимо разработать абсолютно новый протокол передачи данных.
**Ключевые слова:** Интернет вещей, киберфизическая система, протокол передачи данных, сетевые протоколы, уязвимость сетевых протоколов.

Сегодня мы являемся свидетелями того, что интеллектуальные устройства все более усложняются, они имеют все больше возможностей, причем стоимость их при этом остается либо прежней, либо наблюдается даже удешевление. Безусловно, все это стало возможным, в том числе, и благодаря тому, что технологии сегодня стали самовоспроизводимыми, и отчасти быстрому росту числа самих информационных технологий. Не так давно производители высоких технологий явили миру интеграцию людей и вещей, назвав последнее Интернетом вещей (Internet of Things, IoT). Такая конвергенция дает возможность любому объекту извлекать информацию из окружающей среды для управления данными, чтобы в дальнейшем предоставить ее либо другим пользователям, либо же другим устройствам. Интернет вещей представляет собой динамически распределенную среду, которая обладает свойством связывать большое число интеллектуальных устройств, которые, в свою очередь, способны воспринимать саму окружающую среду и выполнять необходимые действия. Эти устройства собирают информацию о реальном мире, отслеживают состояние внешней среды, создают системы повсеместных вычислений и готовы взаимодействовать с другими устройствами, где бы они ни находились. Киберфизические системы (cyber-physical system) оказывают поддержку развития Интернета вещей. Благодаря киберфизическим системам достигается обеспечение совместной работы элементов физического и кибернетического пространств, объединяя при этом вычислительные ресурсы. И сами киберфизические системы, и Интернет вещей преследуют цель обрабатывания огромного числа разнородных данных, поступающих из окружающей среды. В связи с этим возникает вполне справедливый вопрос гармоничного взаимодействия всех устройств, интегрированных в единое информационное пространство. Исходя из этого, проблема исследования протоколов передачи данных в киберфизических системах достаточно актуальна. Для решения указанной проблемы необходимо решить ряд задач: определить генезис дефиниций киберфизическая система, протокол передачи данных; провести обзор существующих протоколов передачи данных; сделать сравнительный анализ протоколов передачи данных, на основании исследования предложить решение проблемы.

Несмотря на то, что концепции киферфизических систем и Интернета вещей переплетаются, все же между ними наблюдается некая демаркационная полоса. Сам термин «киберфизические системы» был впервые предложен в 2006 году Хелен Джилл (директор сектора Национального научного фонда в США) [1]. Киберфизические системы были достаточно быстро приняты со стороны государства. Очевидной для этого причиной послужило то обстоятельство, что киберфизические системы достаточно критичны для обеспечения национальной безопасности. Таким образом, подводя итог такому краткому экскурсу можно сказать, что киберфизическая система – это некая своего рода концепция, базирующаяся на информационно-технологических достижениях человечества, содержащая в своей основе интеграцию вычислительных ресурсов в процессы физического рода. Такая система объединяет оборудование, датчики, информационные системы на протяжении всей «жизни». Киберфизические системы относят к четвертой промышленной революции.

Не столь революционной, но все же достаточно важной и необходимой для любого взаимодействия, что касается информационных технологий, является дефиниция «протокол передачи данных».

Протокол передачи данных – это набор соглашений, который определяет обмен данных между различными программами [2]. С помощью протоколов определяют способы передачи сообщений и обработки ошибок в сети. Протоколы также дают возможность разработать стандарт, который не будет привязан к конкретной аппаратной платформе.

Взаимодействие киберфизических систем происходит за счет стандартных интернет-протоколов. Собственно говоря, каких-либо специализированных протоколов передачи данных в киберфизических системах на сегодняшний момент не существует. В связи с этим поведем наше дальнейшее исследование с позиции необходимости конкретного протокола

для киберфизической системы и, что самое главное, его уязвимости. Для наглядной визуализации представим протоколы передачи данных в виде схемы.

Передача данных – базовое направление киберфизических систем. Как было представлено выше, киберфизические системы не могут функционировать без глобальной сети. Более того, сами киберфизические системы достаточно громоздки, четкие границы их довольно сложно определить, а посему вопрос уязвимости этих систем достаточно существенен. Проведем сравнительную характеристику протоколов передачи данных на предмет их уязвимости (рисунок). А так как определяющим в киберфизических системах все же является сетевое взаимодействие, то сравнивать будем сетевые протоколы. Данные сведем в таблицу.


Рисунок. Общая классификация существующих протоколов передачи данных

Таблица. Сравнительная характеристика сетевых протоколов передачи данных

| Название протокола | Уровень уязвимости | Реальные и потенциальные опасности |
|---|---|---|
| Протокол HTTP | Высокий | Вредоносное ПО, файлы Cookies |
| Протокол HTTPS | Средний | Вредоносные файлы |
| FTP-протокол | Высокий | Вредоносное ПО (под видом сервера может выступить злоумышленник) |
| Протокол SMTP | Высокий | Вредоносная электронная почта |
| Протокол TCP | Средний | Вредоносное ПО |
| Протокол IP | Средний | Вредоносное ПО |

Как видно из результатов таблицы ни один из протоколов не обладает даже низким порогом уязвимости. Безусловно, в таблице представлены не все существующие протоколы, но ввиду ограниченности рамками объема работы, можно сказать, что и другие протоколы передачи данных не отвечают необходимому уровню безопасности.

Таким образом, в рамках настоящего исследования был рассмотрен феномен киберфизических систем и близкий ему феномен Интернета вещей. Определен генезис дефиниций киберфизическая система и протокол передачи данных. Проведен обзор

протоколов передачи данных, и представлена сравнительная характеристика сетевых протоколов, исходя из позиции уязвимости. В результате работы можно сделать следующий вывод: киберфизические системы остро нуждаются в разработке нового протокола передачи данных, отражающего все принципы безопасной работы этой системы в целом [3, 4].

**Литература**

1. Черняк Л. Интернет вещей: новые вызовы и новые технологии [Электронный ресурс]. – Режим доступа: http://www.osp.ru/os/2013/04/13035551 (дата обращения: 10.12.2017).
2. Протоколы передачи данных. Энциклопедия [Электронный ресурс]. – Режим доступа: https://dic.academic.ru/dic.nsf/ruwiki/461212 (дата обращения: 20.12.2017).
3. Берлин А.Н. Основные протоколы интернет. – М.: Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2008. – 504 с.
4. Черняк Л. Но пороге перемен: «большая семерка» ОС, версия 2014 [Электронный ресурс]. – Режим доступа: http://www.osp.ru/os/2013/10/13039062 (дата обращения: 17.12.2017).

**Ефимов Илья Анатольевич**
Год рождения: 1993
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N4255
Направление подготовки: 10.04.01 – Информационная безопасность
e-mail:efimov.i.3.3.3@gmail.com

**Седышева Валерия Дмитриевна**
Год рождения: 1967
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N4255
Направление подготовки: 10.04.01 – Информационная безопасность
e-mail: valeryvalmont@icloud.com

**Тимофеева Анна Алексеевна**
Год рождения: 1994
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N4255
Направление подготовки: 10.04.01 – Информационная безопасность
e-mail: anntim13@mail.ru

**Кузнецов Александр Юрьевич**
Год рождения: 1989
Университет ИТМО, факультет безопасных информационных технологий, кафедра проектирования и безопасности компьютерных технологий, к.т.н., доцент
e-mail: alkuznetcov@corp.ifmo.ru

**УДК 004.056**

## АНАЛИЗ МЕТОДОВ ПРОЕКТИРОВАНИЯ КОМПЛЕКСНЫХ СИСТЕМ БЕЗОПАСНОСТИ ДЛЯ ПРЕДПРИЯТИЙ НЕФТЕПЕРЕРАБАТЫВАЮЩЕЙ ПРОМЫШЛЕННОСТИ

**Ефимов И.А., Седышева В.Д., Тимофеева А.А.**
**Научный руководитель – к.т.н., доцент Кузнецов А.Ю.**

В работе описано развитие нормативно правовой базы в области обеспечения информационной безопасности техногенных объектов в России, производится сравнение с зарубежными аналогами нормативных документов. Выделены особенности нефтеперерабатывающей промышленности с точки зрения информационной безопасности, определены основные подсистемы обеспечения безопасности, а также, исходя из анализа нормативных документов, сформулирована методика проектирования информационной безопасности данного класса объектов.

**Ключевые слова:** метод проектирования ИБ, комплексные системы безопасности, информационная безопасность АСУ ТП, нефтеперерабатывающая промышленность, нормативная база ИБ техногенных объектов.

**Введение.** В Российской Федерации (РФ) действует большое количество нормативных документов, в той или иной степени касающихся темы защиты информации на предприятиях нефтеперерабатывающей промышленности и различного рода других техногенных объектов (ТО), включающих в себя использование автоматизированной системы управления технологическим процессом (АСУ ТП). Из них можно выделить следующие документы (гриф ДСП) в 2007 году положившие начало развития нормативной базы защиты информации на ТО с АСУ ТП: «Базовая модель угроз безопасности информации в ключевой системе информационной инфраструктуры (КСИИ)», «Методика определения актуальных угроз безопасности информации в КСИИ», «Общие требования по обеспечению безопасности информации в КСИИ», «Рекомендации по обеспечению безопасности информации в КСИИ».

Дальнейшие развитие нормативной базы послужило принятие Федерального закона № 256-ФЗ «О безопасности объектов ТЭК» [1] в 2011 году, в соответствии с которым субъекты отрасли должны использовать системы защиты информации и информационно-телекоммуникационных сетей от неправомерного доступа, а также персонал соответствующей квалификации и подготовки. Деятельность по обеспечению безопасности информации (ИБ) включает комплекс организационных и технических мер.

Следующая волна развития пришлась на 2014 г. – приказ ФСЭК России № 31 [2], представляющий требования к обеспечению защиты информации АСУ ТП на критически важных, потенциально опасных и представляющих собой повышенную опасность объектах.

Таким образом, у ИБ-специалистов промышленных предприятий имеется в распоряжении достаточно полная и применимая на практике база нормативных документов. Следование их требованиям вкупе со знанием лучших отраслевых практик, описанных в зарубежных документах, позволяет обеспечивать ИБ-защиту производственных и технологических процессов. Однако ни в одном из них так и не описаны методы построения комплексной защиты для нефтеперерабатывающей промышленности. В данной работе проведен анализ зарубежных и российских стандартов, изучена нормативная база РФ в области защиты техногенных объектов и представлен эшелонированный метод защиты.

**Западный и Российский подходы к защите АСУ ТП и проблематика с точки зрения ИБ.** Сравнив приказ № 31 ФСТЭК [3] и стандарт NIST SP 800-82 [4], очевидно, что при разработке приказа № 31 специалисты ФСТЭК изучали зарубежные стандарты и рекомендации по обеспечению безопасности АСУ, поэтому российский документ хорошо согласован с международной нормативной базой. Однако имеются и серьезные различия в подходах.

NIST SP 800-82 является набором рекомендаций по комплексному обеспечению безопасности индустриальных систем, содержащим методические наработки практиков. В свою очередь, Приказ ФСТЭК России № 31 – формальный документ. Он создан по аналогии с приказами ФСТЭК № 17 и № 21.

В приказе ФСТЭК № 31 обеспечение защиты информации АСУ ТП делится на пять больших этапов:

1. формирование требований (в том числе определение уровня значимости системы, необходимого класса защищенности, возможных угроз и требований к системе защиты);
2. разработка системы защиты на основе сформулированных требований;
3. ее внедрение;
4. обеспечение защиты в процессе эксплуатации системы;
5. обеспечение защиты при выводе системы из эксплуатации.

Стандарт NIST не выдвигает каких-либо формальных требований, а лишь предлагает набор методик и рекомендаций. Он содержит:

– предметные рекомендации, дающие представление о том, с чего следует начать и как наиболее эффективно построить систему защиты в целом;

– упрощенные модели злоумышленника и угроз АСУ ТП;
– большой раздел по типовым угрозам и уязвимостям АСУ ТП;
– рекомендации по созданию и реализации программы обеспечения безопасности АСУ ТП;
– подробное описание архитектуры АСУ ТП и общее описание подсистемы безопасности;
– всеобъемлющий раздел, посвященный всем классическим подсистемам информационной безопасности (контроль над доступом, идентификация и аутентификация, антивирусная защита, сети, аудиты, криптография и пр.).

Автором подчеркнуто, что NIST SP 800-82 и приказ ФСТЭК № 31 не противоречат друг другу. В России стало распространенной практикой одновременное использование этих документов и, соответственно, подходов.

При проектировании АСУ ТП подразумевалось, что они не будут изменяться в дальнейшем. Системы, созданные два десятка лет назад, до сих пор функционируют в своих первоначальных конфигурациях, многие из них зачастую не обновлялись. А производственная сеть создавалась отдельно от корпоративного контура.

Сегодня индустриальные сети либо напрямую связаны с другими информационными системами предприятий (интегрированы с системами SAP, с ERP-системами и т.п.), либо отделены от остальных контуров межсетевыми экранами и средствами обнаружения вторжений.

Принципиальное отличие АСУ ТП от привычных для специалистов по ИБ информационных систем заключается в том, что из триады «конфиденциальность – целостность – доступность» в данном случае наиболее критичной является доступность. В индустриальных системах в первую очередь важно, чтобы управляющий сигнал был вовремя принят и оказал необходимое воздействие.

Создание и работа подсистемы обеспечения безопасности нефтеперерабатывающих предприятий не должны мешать функционированию системы управления. Для обеспечения безопасности АСУ ТП крайне редко используются криптографические решения, поскольку они порождают избыточность вычислений и могут замедлить или вовсе остановить отправку и получение управляющего сигнала. Стандартным механизмом является периметровая защита – разделение (логическое или физическое) сетей на сегменты, которое позволяет выделить или изолировать индустриальные решения.

**ИБ-решения для предприятий нефтеперерабатывающей промышленности.** Перечислим подсистемы обеспечения информационной безопасности АСУ ТП:
– подсистема сетевой безопасности (в частности, межсетевое экранирование и обнаружения вторжений);
– подсистема двухфакторной (многофакторной) аутентификации;
– подсистема обеспечения целостности;
– подсистема быстрого восстановления конфигураций и данных;
– подсистема предотвращения утечек конфиденциальной информации;
– подсистема управления патчами;
– подсистема управления мобильными устройствами;
– подсистема управления неструктурированными данными;
– подсистема анализа защищенности;
– подсистема криптографической защиты.

Первые три подсистемы являются ключевыми, так как позволяют наиболее эффективно сохранять доступность АСУ. В большинстве случаев построение комплексной системы безопасности начинается с обеспечения целостности (регламентируются стандартами и руководствами NIST SP 800-12, 800-40 и 800-94).

Российский рынок решений для информационной защиты АСУ и индустриальных сетей находится в зачаточном состоянии. Каждый конкретный проект подразумевает сугубо индивидуальное решение. Кроме того, обеспечить безопасность АСУ ТП исключительно с

помощью серийных технических средств крайне сложно. Добиться максимального «эффекта» позволяет поиск уязвимостей путем построчного анализа кода.

Дело в том, что специфика АСУ ТП (приоритет доступности) не позволяет использовать ИБ-решения с большой интеллектуальной составляющей. Если для стандартной ИТ-системы приостановка какого-то процесса в случае подозрения на вредоносную активность является нормальной мерой, то в промышленных системах – это может стать причиной техногенной катастрофы.

Исходя из всего вышесказанного, проанализировав нормативно документацию и рассмотрев особенности нефтеперерабатывающей промышленности, определим методику построения комплексной системы ИБ АСУ ТП – эшелонированной защиты, которая включает в себя следующие уровни:

- физической безопасности (ограничение физического доступа к панелям управления, диспетчерским и другим помещениям, устройствам, кабелям);
- сетевой безопасности – сетевая инфраструктура (межсетевые экраны со встроенными сенсорами систем предотвращения вторжения) и средства защиты, интегрированные в сетевое оборудование (коммутаторы и маршрутизаторы);
- безопасности рабочих станций и серверов (управление обновлениями программного обеспечения (ПО), применение антивирусного ПО, удаление неиспользуемых приложений, протоколов и сервисов);
- безопасности приложений (аутентификация, авторизация и аудит при доступе к приложениям);
- безопасности устройств (контроль над изменениями и ограничение доступа).

Особое внимание следует уделять сетевому уровню. Многие компоненты АСУ ТП подключены к сетевой инфраструктуре IP/Ethernet, но для них не всегда возможна установка средств обеспечения ИБ, таких как антивирусы или системы предотвращения вторжений на уровне хоста.

**Заключение.** В работе рассмотрена Российская нормативная база в сравнении с зарубежными аналогами. Анализ материалов позволил выявить отсутствие как таковых методов проектирования комплексных систем безопасности и предложить свой метод – эшелонированной защиты.

**Литература**

1. Федеральный закон от 21.07.2011 № 256-ФЗ (ред. от 06.07.2016) «О безопасности объектов топливно-энергетического комплекса» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_117196/, своб.
2. «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (в ред. Приказа ФСТЭК России от 23.03.2017 № 49) [Электронный ресурс]. – Режим доступа:https://fstec.ru/component/attachments/download/715, своб.
3. NIST SP 800-82 [Электронный ресурс]. – Режим доступа: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf, своб.
4. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» в ред. Приказа ФСТЭК России от 15.02.2017 № 27 [Электронный ресурс]. – Режим доступа: https://fstec.ru/component/attachments/download/566, своб.

**Жакиш Мадина**
Год рождения: 1995
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N4150
Направление подготовки: 10.04.01 – Информационная безопасность
e-mail: zhakishmadina@gmail.com

**Федотова Виктория Валерьевна**
Год рождения: 1995
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N4150
Направление подготовки: 10.04.01 – Информационная безопасность
e-mail: fedvikoria95@mail.ru

**Созинова Екатерина Николаевна**
Год рождения:1986
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, к.т.н., доцент
e-mail: s.ekaterina-nik@mail.ru

**УДК 555.32**

## АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНТЕРНЕТА ВЕЩЕЙ

**Жакиш М., Федотова В.В., Созинова Е.Н.**
**Научный руководитель – к.т.н., доцент Созинова Е.Н.**

В работе выявлены и проанализированы угрозы информационной безопасности Интернета вещей. Особое внимание уделяется проблемам обеспечения правильной идентификации подлинности механизмов и обеспечение конфиденциальности данных Интернета вещей. Авторами рассмотрена триада безопасности, путем использования трех областей: конфиденциальность данных, целостность и доступность.

**Ключевые слова:** информационная безопасность, Интернет вещей, облачные технологии, угрозы облачных сервисов, IoT.

Интернет вещей (Internet of Things, IoT) – концепция вычислительной сети физических объектов («вещей»), оснащенных встроенными технологиями для взаимодействия друг с другом или с внешней средой, рассматривающая организацию таких сетей как явление, способное перестроить экономические и общественные процессы, исключающее из части действий и операций необходимость участия человека [1–4].

Актуальность IoT находит применение во множестве отраслей экономики, специализированных процессах, повседневной жизни. Вместе с тем ряд специалистов в области информационной безопасности (ИБ) отмечают, что распространение взаимодействия технических систем без участия человека несет в себе достаточно серьезные угрозы безопасности. С одной стороны, удаленное управление системами типа «Умный дом» позволяет с большим комфортом организовать свое жизненное пространство; а с другой,

датчики и элементы управления, системами жизнеобеспечения, оказавшись в руках злоумышленника, значительно увеличивают риски в области ИБ. Именно поэтому данная тема является актуальной.

Целью работы являлось проведение анализа угроз ИБ Интернета вещей. Основной целью безопасности IoT являются также обеспечение правильной идентификации подлинности механизмов и обеспечение конфиденциальности данных. Триада безопасности – выдающаяся модель для разработки механизмов безопасности путем использования трех областей: конфиденциальность данных, целостность и доступность.

Рынок безопасности Интернета вещей к 2021 году достигнет 37 млрд долл., согласно аналитическому отчету Marketsandmarkets.com. Где разрастается хаос в сфере кибербезопасности, там и тратятся большие деньги на обеспечение этой безопасности. Полный перечень угроз довольно большой, остановимся на самых основных моментах.

В рамках IoT-систем сбор данных идет в режиме реального времени. Например, данные о доступности дорогого промышленного оборудования, информация для контроля дорожного трафика, данные о состоянии здоровья человека, фотоматериалы, документы и пр. Устройства, передающие такого рода данные, могут иметь уязвимости, что, в свою очередь, может приводить к утечкам чувствительных данных. Также уязвимости могут быть на уровне протоколов взаимодействия элементов Интернета вещей. Это достаточно серьезная проблема, если лет 10–15 назад большинство устройств работали по клиент-серверной модели и представляли собой закрытые сети, то сейчас большинство устройств подключаются друг к другу напрямую, в обход центрального сервера, при этом облачная платформа используется для управления и сбора статистики. Это размывает периметр ИБ и заставляет организации пересматривать подходы к организации защиты на сетевом уровне.

С точки зрения прикладных протоколов сейчас все производители пытаются придумать что-то свое, какой-то общей стандартизации пока нет. Есть только ряд рекомендованных протоколов прикладного уровня, это, в частности, MQTT (Message Queue Telemetry Transport), Constrained Application Protocol (CoAP) и Advanced Message Queuing Protocol (AMQP). Однако многие производители IoT-устройств изначально были производителями электрооборудования, а не ИТ-компаниями, и, как следствие, когда они придумывают собственные протоколы и стандарты, то очень редко задумываются о безопасности.

Другая угроза – это взлом конечных устройств для организации атаки на инфраструктуру компании или предприятия через IoT-устройства. В качестве примера здесь можно привести случай, когда одна из модификаций ботнета Mirai заразила более 5 миллионов устройств, в том числе и IoT (веб-камеры и пр.) в 164 странах мира. Это, в частности, привело к тому, что у одного из немецких интернет-провайдеров были заражены практически все роутеры, что повлекло за собой серьезные потери репутации.

Еще одна угроза – это получение управления устройствами IoT и искажение поступающих от них данных. Например, если Интернет вещей используется в медицине, то врач может получать неправильные данные о состоянии пациента (от датчика) и назначить неправильное лечение.

По возможным угрозам имеются определенные решения. Обеспечение защиты конечных узлов при внедрении IoT включает в себя анализ прошивки с последующей сертификацией на отсутствие недокументированных возможностей, харденинг (усиление защиты) операционной системы, выявление уязвимостей в режиме реального времени, корректную настройку встроенного межсетевого экрана, предотвращение вторжений как на прикладном уровне, так и на уровне протоколов передачи данных, VPN, внедрение контроля целостности прошивки, создание единого центра сертификации либо децентрализованной доверенной системы аутентификации для общения между различными устройствами.

Требуется также обеспечить защиту облачной инфраструктуры, которая осуществляет управление и мониторинг, агрегирует и анализирует информацию, получаемую от IoT-устройств. После этого можно переходить к подбору межсетевых экранов, WAF, систем

предотвращения вторжений, VPN, средств защиты от DDoS и отслеживания поведения пользователей, SIEM. В каждом конкретном случае определяются дополнительные требования, специфичные для защиты IoT-устройств.

Если говорить про подход к защите IoT-систем в целом, то это нужно делать с одновременной проработкой требований ИБ, т.е. детально анализировать риски, появляющиеся с внедрением тех или иных технологий IoT, и выстраивать систему с учетом минимизации этих рисков. На сегодняшний день авторами было однозначно рекомендовано использовать IoT только для тех бизнес-процессов, нарушение функционирования которых не приводит к драматическим последствиям для бизнеса и здоровья людей.

11 октября 2016 года стало известно о планах Еврокомиссии – ввести обязательную сертификацию или другую аналогичную процедуру всех приборов, подключаемых к Интернету вещей.

Вывод. Наполнение концепции «Интернета Вещей» многообразным технологическим содержанием и внедрение практических решений для ее реализации, начиная с 2010 годов, считается восходящим трендом в информационных технологиях, прежде всего, благодаря повсеместному распространению беспроводных сетей, появлению облачных вычислений, развитию технологий межмашинного взаимодействия, началу активного перехода на IPv6 и освоению программно-конфигурируемых сетей.

Организации могут пытаться защищаться от хакеров, использующих IoT, ужесточая безопасность в сетях, содержащих IoT-устройства и т.д. Но все же меры по защите Интернета вещей от хакеров следует принимать именно на государственном уровне, поскольку в контроле нуждаются не только сами приборы, но и сети, к которым они подключены, а также облачные хранилища. Схема сертификации Интернета вещей сравнима с европейской системой маркировки энергопотребляющих товаров, принятой в 1992 году. Маркировка обязательна для автомобилей, бытовой техники и электрических ламп. Но производители техники считают систему подобной маркировки неэффективной для защиты от хакеров. Вместо этого они предпочли бы установить в приборы стандартный чип, который будет отвечать за безопасность подключения к Интернету.

**Литература**

1. Что такое Интернет вещей? [Электронный ресурс]. – Режим доступа: https://dynru.ru/question/what-is-internet-of-things/ (дата обращения: 14.01.2018).
2. Пять главных аспектов плохой безопасности интернета вещей [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/company/parallels/blog/332852/ (дата обращения: 18.01.2018).
3. Европа закручивает гайки интернету вещей [Электронный ресурс]. – Режим доступа: http://internetua.com/evropa-zakrucsivaet-gaiki-internetu-vesxei (дата обращения: 21.01.2018).
4. Бородин П.Н., Кучерявый А.Е. Интернет вещей как новая концепция развития сетей связи // Информационные технологии и телекоммуникации. – 2014. – Вып. 3. – С. 7–30.

**Ильченко Лидия Михайловна**
Год рождения: 1995
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N4151
Направление подготовки: 10.04.01 – Информационная безопасность
e-mail: Lidiya9510@yandex.ru

**Галлямова Миляуша Равильевна**
Год рождения: 1996
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N4151
Направление подготовки: 10.04.01 – Информационная безопасность
e-mail: Miljausha-18@mail.ru

**УДК 004.056**

# ПОСТРОЕНИЕ МОДЕЛИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННОГО ПРЕДПРИЯТИЯ

**Ильченко Л.М., Галлямова М.Р.**
**Научный руководитель – к.воен.н., доцент Юрин И.В.**

В работе рассмотрены угрозы информационной безопасности, направленные на основные и вспомогательные ценные активы телекоммуникационного предприятия, функционирующего на базе территориально распределенной информационной системы, с целью формирования модели угроз информационной безопасности.
**Ключевые слова:** модель угроз, модель нарушителя, информационная безопасность, телекоммуникационное предприятие, распределенная информационная система.

Территориально распределенные сети, рост числа пользователей, увеличение объемов информации, обрабатываемой в электронном виде, создает благоприятную среду для преднамеренных или непреднамеренных действий потенциального нарушителя.

Под угрозой информационной безопасности понимается совокупность условий и факторов, создающих реальную или потенциальную опасность нарушения безопасности информации – ГОСТ Р 50922-2006.

Угрозы информационной безопасности могут быть направлены на следующие ценные активы организации: бизнес-процессы, информация, аппаратные средства, носители данных, программное обеспечение, сеть, персонал, место функционирования организации [1].

В настоящей работе рассмотрена корпоративная распределенная многопользовательская информационная система (ИС), имеющая подключение к сетям общего пользования, обрабатывающая информацию разного уровня конфиденциальности, не содержащую сведения, составляющие государственную тайну.

Рассматриваемая ИС расположена в пределах трех контролируемых зон, территориально распределенных в пределах одного региона. Система состоит из менее, чем ста автоматизированных рабочих мест (АРМ), и одного сервера. Схематичный план физического расположения представлен на рис. 1.

По источнику возникновения угрозы можно разделить на внешние и внутренние, каждая из которых реализуется нарушителем с низким, средним или высоким потенциалом.

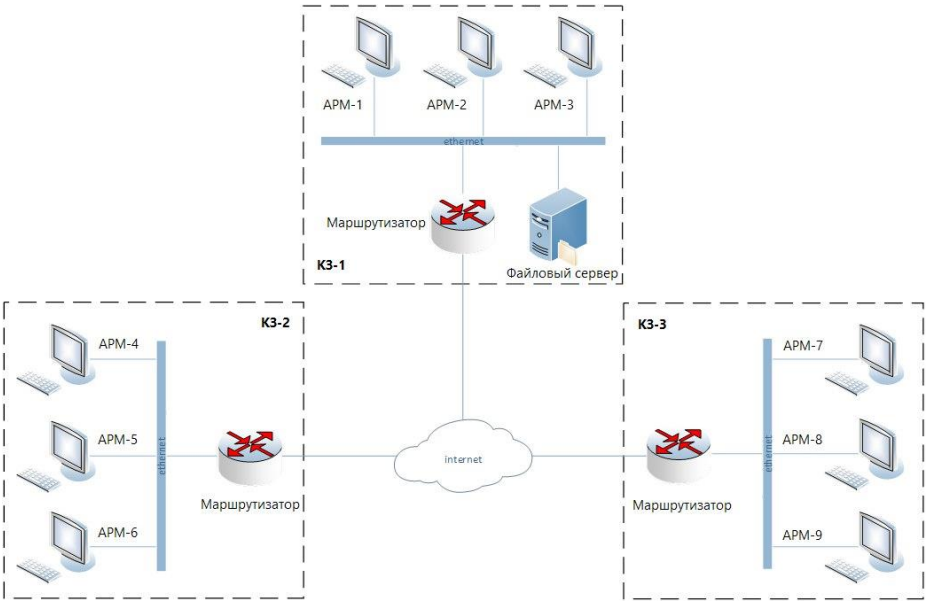



Рис. 1. Схематичное расположение распределенной информационной системы

Для рассматриваемой ИС актуальны следующие категории потенциальных нарушителей:

1. внутренний нарушитель с низким потенциалом: лицо, обеспечивающее функционирование ИС или обслуживающее инфраструктуру; имеет санкционированный доступ в контролируемую зону (КЗ), но не имеет доступа к информации; лица, привлекаемые для установки, монтажа, пусконаладочных работ; легитимный пользователь ИС;
2. внутренний нарушитель со средним потенциалом: администраторы ИС и администраторы безопасности;
3. внешний нарушитель с низким потенциалом: неустановленные внешние субъекты (физические лица); бывшие работники (пользователи);
4. внешний нарушитель со средним потенциалом: конкурирующие организации [2, 3].

В табл. 1 представлено соответствие ущерба свойствам основных активов организации, где К, Ц и Д – это конфиденциальность, целостность и доступность соответственно.

Таблица 1. Основные активы организации

| Источник угроз | Нарушитель | Направленность угрозы | Основные объекты защиты | | | |
|---|---|---|---|---|---|---|
| | | | Информация, необходимая для бизнес-процессов | Информация личного характера | Стратегическая информация | Информация, требующая продолжительного времени обработки и (или) связанная с затратами на ее приобретение |
| Антропогенные | Внутренний нарушитель с низким потенциалом | К | Низкий | Низкий | Низкий | Низкий |
| | | Ц | Средний | Средний | Средний | Средний |
| | | Д | Низкий | Низкий | Низкий | Низкий |
| | Внутренний нарушитель со средним потенциалом | К | Низкий | Низкий | Низкий | Низкий |
| | | Ц | Низкий | Низкий | Низкий | Низкий |
| | | Д | Средний | Средний | Средний | Средний |

| Источник угроз | Нарушитель | Направленность угрозы | Основные объекты защиты | | | |
|---|---|---|---|---|---|---|
| | | | Информация, необходимая для бизнес-процессов | Информация личного характера | Стратегическая информация | Информация, требующая продолжительного времени обработки и (или) связанная с затратами на ее приобретение |
| | Внешний нарушитель с низким потенциалом | К | Низкий | Низкий | Низкий | Низкий |
| | | Ц | Низкий | Низкий | Низкий | Низкий |
| | | Д | Средний | Средний | Средний | Средний |
| | Внешний нарушитель со средним потенциалом | К | Низкий | Низкий | Низкий | Низкий |
| | | Ц | Низкий | Низкий | Низкий | Низкий |
| | | Д | Средний | Средний | Средний | Средний |
| Техногенные | | К | Низкий | Низкий | Низкий | Низкий |
| | | Ц | Низкий | Низкий | Низкий | Низкий |
| | | Д | Низкий | Низкий | Низкий | Низкий |
| Стихийные | | К | Низкий | Низкий | Низкий | Низкий |
| | | Ц | Низкий | Низкий | Низкий | Низкий |
| | | Д | Низкий | Низкий | Низкий | Низкий |

В табл. 2 представлено соответствие ущерба вспомогательным активам рассматриваемой системы.

Таблица 2. Вспомогательные активы организации

| Источники угроз | Направленность угрозы | Вспомогательные объекты защиты |
|---|---|---|
| Антропогенные | Конфиденциальность | Низкий |
| | Целостность | Низкий |
| | Доступность | Средний |
| Техногенные | Конфиденциальность | Низкий |
| | Целостность | Низкий |
| | Доступность | Низкий |
| Стихийные | Конфиденциальность | Низкий |
| | Целостность | Низкий |
| | Доступность | Низкий |

Таблица 3. Перечень актуальных угроз ИБ в соответствии с банком данных угроз ФСТЭК

| Источник угрозы | Степень потенциального ущерба | Возможность реализации | | |
|---|---|---|---|---|
| | | Средняя | Высокая | Очень высокая |
| Внутренний нарушитель с низким потенциалом | Низкая | 15 | 71, 115, 179, | 67, 88, |
| | Средняя | 9, 12, 33, 45, 49, 51, 53, 72, 86, 87, 89, 90, 93, 100, 123, 145, 152, 153, 162, 167, 177, 178, 180, 185, 191, 192, | 18, 23, 30, 34, 91, 113, 140, 155, 182, 186 | 14, 22, 121, 156, 158, |
| | Высокая | | | |

| Источник угрозы | Степень потенциального ущерба | Возможность реализации | | |
|---|---|---|---|---|
| | | Средняя | Высокая | Очень высокая |
| Внутренний нарушитель со средним потенциалом | Низкая | | | |
| | Средняя | 25, 61, 63, 68, 94, 95, 102, 109, 114, 117, 118, 149, 150, 154, 163, 165, 166, 169, 187, 188 | 36, 122, 143, | |
| | Высокая | | | |
| Внешний нарушитель с низким потенциалом | Низкая | 15 | 4, 34, 71, 98, 99, 103, 115, 179, | 88, |
| | Средняя | 6, 49, 86, 89, 90, 93, 100, 145, 152, 153, 162, 168, 171, 178, 185, 191, 192, | 18, 91,113, 140, 155, 157, 160, 172 | 14, 22, 121, 158, 170, |
| | Высокая | | | |
| Внешний нарушитель со средним потенциалом | Низкая | 181, | 193 | |
| | Средняя | 33, 63, 68, 94, 95, 102, 109, 114, 117, 118, 127, 149, 154, 163, 180, 187, 190, | 30, 36, 122, 139, 143, 189, | |
| | Высокая | | | |

Модель угроз составлена в соответствии с банком данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю (ФСТЭК) и представлена в табл. 3, где каждая угроза выписана в соответствии с ее ID в банке [4].

Угрозы с низкой возможностью реализации отсутствуют.

Наиболее опасными угрозами являются те, чья вероятность реализации не ниже высокой, а степень ущерба – не ниже средней. Визуализация модели таких угроз представлена на рис. 2.

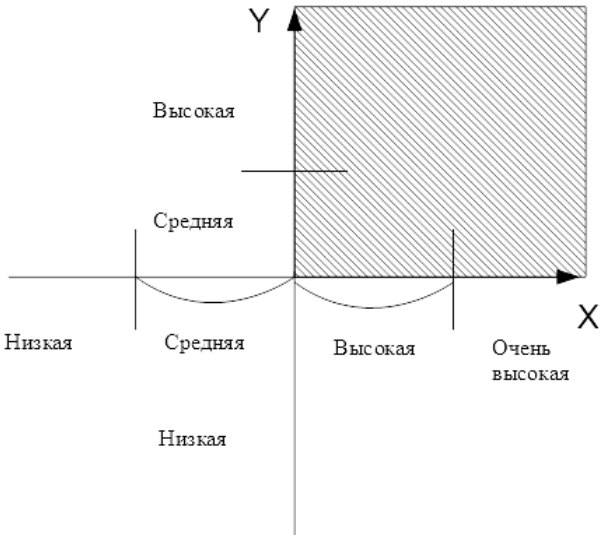



Рис. 2. Угрозы с высокой и очень высокой вероятностью реализации и средним и высоким потенциальным ущербом

Однако особенностью ИС телекоммуникационного предприятия является то, что наибольший ущерб для бизнес-процессов способны нанести угрозы, направленные на доступность информационных ресурсов, а не на их конфиденциальность [5].

В табл. 4 представлены такие угрозы.

Таблица 4. Перечень актуальных угроз для информационной системы телекоммуникационного предприятия

| Источник угрозы | Степень потенциального ущерба | Возможность реализации | | |
|---|---|---|---|---|
| | | Средняя | Высокая | Очень высокая |
| Внутренний нарушитель с низким потенциалом | Низкая | | | |
| | Средняя | 9, 12, 33, 45, 49, 51, 53, 72, 86, 87, 89, 90, 93, 100, 123, 145, 152, 153, 162, 177, 178, 180, 185, 191, 192, | 18, 23, 30, 91, 113, 140, 155, 182, 186 | 14, 22, 121, 156, 158 |
| | Высокая | | | |
| Внутренний нарушитель со средним потенциалом | Низкая | | | |
| | Средняя | 25, 61, 63, 94, 95, 102, 109, 114, 117, 118, 149, 150, 154, 165, 166, 169, 187, 188 | 36, 122, 143 | |
| | Высокая | | | |
| Внешний нарушитель с низким потенциалом | Низкая | | | |
| | Средняя | 6, 49, 86, 89, 90, 93, 100, 145, 152, 153, 162, 171, 178, 185, 191, 192 | 18, 91, 113, 140, 155, 157, 160, 172 | 14, 22, 121, 158, 170 |
| | Высокая | | | |
| Внешний нарушитель со средним потенциалом | Низкая | | | |
| | Средняя | 33, 63, 94, 95, 102, 109, 114, 117, 118, 127, 149, 154, 163, 180, 187, 190 | 30, 36, 122, 139, 143, 189 | |
| | Высокая | | | |

Угрозы с низкой возможностью реализации отсутствуют.

Исходя из вышесказанного, визуализация модели угроз может быть представлена следующим образом (рис. 3).

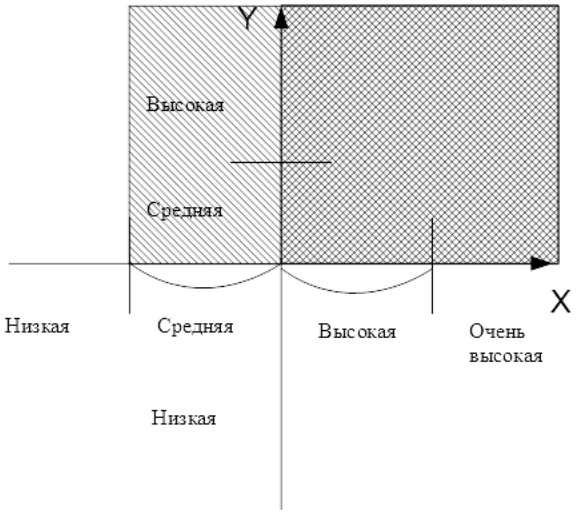


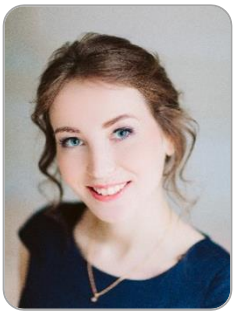

Рис. 3. Актуальные угрозы для ИС телекоммуникационного предприятия

**Заключение.** Таким образом, систему защиты предприятия необходимо создавать с учетом актуальных угроз информационной безопасности. В данном случае, речь идет не о том, что остальными актуальными (в соответствии с табл. 3) угрозами можно пренебречь, а о том, что угрозы, выделенные в табл. 4, должны стать приоритетными.

**Литература**

1. Хаммер М., Чампи Дж. Реинжениринг корпорации: Манифест революции в бизнесе / Пер. с англ. – СПб.: Изд-во С.-Петербургского университета, 1997. – 332 с.
2. Методика определения угроз безопасности информации в информационных системах: Проект Федеральной службы по техническому и экспортному контролю 2015 // [Электронный ресурс]. – Режим доступа: https://fstec.ru/component/attachments/download/812. (дата обращения: 20.01.2018).
3. Стефаров А.П., Жуков В.Г. Формирование типовой модели нарушителя правил разграничения доступа в автоматизированных системах // Изв. ЮФУ. Технические науки. – 2012. – № 12(137). – С. 45–54.
4. Коновалова Ю.Н. Построение модели угроз безопасности информации кредитной организации // Инновационная наука. – 2016. – № 5-2(17). – С. 125–128.
5. Дроботун Е.Б., Цветков О.В. Построение модели угроз безопасности информации в автоматизированной системе управления критически важными объектами на основе сценариев действий нарушителя // Программные продукты и системы. – 2016. – № 3(115). – С. 42–50.

**Калабишка Михаил Михайлович**
Год рождения: 1996
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N3401
Направление подготовки: 10.03.01 – Информационная безопасность
e-mail: kalabishkam@gmail.com



**Солдатова Елена Андреевна**
Год рождения: 1988
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, аспирант
Направление подготовки: 10.06.01 – Информационная безопасность
e-mail: Elena_SolD@bk.ru

**УДК 004.891.2**

# ИНТЕРНЕТ ВЕЩЕЙ КАК НОВАЯ СТУПЕНЬ РАЗВИТИЯ СМАРТ ТЕХНОЛОГИЙ

**Калабишка М.М., Солдатова Е.А.**
**Научный руководитель – д.т.н., доцент Беззатеев С.В.**

Работа выполнена в рамках темы НИР № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность».

В работе рассмотрен Интернет вещей, который обусловлен резким скачком Интернета, который достигается с помощью людей и их взаимодействия с большим объемом интернет-знаний. Интернет вещей получает все большую популярность, и решаются вопросы по стандартизации и протоколам в данной сфере.
**Ключевые слова:** Интернет вещей, безопасность, киберфизические системы.

Интернет вещей (Internet of Things, IoT) – это новый этап с долгоиграющим развитием в области вычислительной техники и коммуникаций. Его параметры, повсеместность и влияние на повседневную жизнь, бизнес, правительство, затмевает любой технический процесс, который был до этого. IoT – это термин, который относится к расширяющейся взаимосвязи умных устройств – от больших приборов (например, бытовая техника) до крошечных датчиков. Доминирующей темой является внедрение мобильных приемопередатчиков ближнего действия в широкий спектр гаджетов и повседневных предметов, позволяющих создавать новые формы общения между людьми и вещами, между вещами самих себя. Интернет поддерживает взаимосвязь между миллиардами промышленных и личных объектов, обычно через облачные сервисы. Объекты доставляют информацию о датчике, воздействуют на их среду и в некоторых случаях модифицируют себя, чтобы создать общее управление в более крупную систему, например, завод или город.

«Вещи» в IoT – это глубоко встраиваемые устройства, характеризующиеся узкой полосой пропускания, низким уровнем повторения данных, низким уровнем громкости использования данных. Эти «вещи» взаимодействуют друг с другом и обеспечивают обмен данных через пользовательские интерфейсы. Часть некоторых встроенных приборов в IoT, таких как видео с высоким разрешением, камеры безопасности, видео IP-телефонии (VoIP) телефонов и другие, требуют потоковой передачи с высокой пропускной способностью. Множество других бесчисленных продуктов просто требуют передачи пакетов данных, которые зависят от времени.

Быстро развивающийся Интернет включает миллионы, возможно даже миллиарды объектов, использующих стандарты связи архитектуры для предоставления услуг итоговым пользователям. Этот этап эволюции создает и совершенствует новые взаимодействия между физическим миром и цифровыми вычислениями, цифрового контента, анализа, приложений и услуг. Полученный IoT предоставляет беспрецедентные возможности для пользователей и поставщиков услуг в самых разных секторах мира. Области, в которых будут использоваться возможности сбора, анализа и автоматизации данных IoT, включают: здравоохранение, фитнес, домашний мониторинг и автоматизацию, энергосбережение и интеллектуальные сети, сельское хозяйство, транспорт, экологический мониторинг, инвентаризацию и управление продуктами, безопасность, наблюдение, образование и многие другие отрасли жизнедеятельности.

Развитие в сфере технологий происходит во многих областях. Неудивительно, что беспроводные сетевые исследования проводятся, и на самом деле были проведены, довольно давно, но имели другое название: мобильные вычисления, повсеместные вычисления, беспроволочный датчик сети и киберфизические системы.

Многие предложения и продукты были разработаны для маломощных протоколов, безопасности и конфиденциальности, адресации, недорогих радиостанций, энергосберегающих схем для длительного срока службы батарей и надежности сетей, составленных из ненадежных периодически спящих узлов. Эти беспроводные разработки имеют решающее значение для возрастания IoT. Развитие также связано с предоставлением IoT-устройств социальной сети – с использованием связи между машинами, хранением и обработкой больших объемов данных в реальном времени и приложений для предоставления конечным пользователям интеллектуальных и полезных интерфейсов к этим устройствам и данным.

Большинство имеют свое видение IoT. Например, по мнению Станковича [1], он предлагает личные достоинства, такие как оцифровка повседневной жизни деятельности; использование бионической кожи, чтобы общаться с окружающими смарт-пространствами для улучшения комфорта, здоровья и безопасности; умные часы и современные гаджеты для тела, которые оптимизируют доступ к городским услугам. Общегородские достоинства могут включать эффективный, бесперебойный транспорт без светофоров и 3D-транспортные средства. Умные здания могли не только управлять энергией и безопасностью, но также поддерживать здоровье и оздоровительные мероприятия. Таким же образом людям были предоставлены новые способы доступа в мир через смартфоны, IoT будет создавать новую парадигму таким образом, что мы имеем постоянный доступ к нужной информации.

Отдел стандартов электросвязи Международного союза электросвязи (МСЭ-телекоммуникации) опубликовал Рекомендацию Y. 2060, названную «Обзор Интернета вещей» [2]. Документ содержит следующие определения, которые предполагают сферу применения IoT: Интернет вещей (IoT): глобальная инфраструктура для информации общества, предоставления расширенных услуг, путем соединения (физического и виртуального) вещей, основанных на существующих и развивающихся, взаимодействующих информационных и коммуникационных технологий. Вещь: в Интернете вещей, это объект физического мира (физические вещи) или информационного мира (виртуальные вещи), который способен идентифицировать и интегрировать в коммуникационные сети. Устройство: это часть оборудования с обязательными возможностями связи и дополнительными возможностями считывания, активации, сбора данных, данных хранения и обработки данных.

Большинство литературы рассматривает IoT, как включающую взаимосвязанные интеллектуальные объекты. Рекомендация Y.2060 расширяет эту концепцию, включив в нее виртуальные вещи, а затем исследуемую тему. Рекомендация Y.2060 характеризует IoT путем добавления измерения «Коммуникация между любыми вещами» к информационным и

коммуникационным технологиям, которые уже предоставляют связь «в любое время» и «в любом месте».

В книге «Проектирование Интернета вещей» [3] элементы IoT сводятся к простому уравнению: Физические объекты + контроллеры, датчики, приводы + Internet = IoT.

Данное уравнение аккуратно отражает суть Интернета вещей. Экземпляр IoT состоит из набора физических объектов, каждый из которых: содержит микроконтроллер, обеспечивающий интеллект; содержит датчик, который измеряет некоторые физические параметры и (или) исполнительный механизм, который воздействует на какой-либо физический параметр; предоставляет средства для общения через Интернет или в какой-либо другой сети.

Один элемент, не вошедший в уравнение и упомянутый в определении Y.2060, является средством идентификации отдельной вещи, обычно называемой тегом.

Фраза «Интернет вещей» всегда используется в литературе, но более точно будет назвать «Интернетом вещей» или «Сети вещей». Например, установка на основе «Умного дома» состоит из множества вещей в доме, которые связаны между собой через Wi-Fi или Bluetooth с некоторым центральным контроллером. На заводе или ферме сеть вещей может позволить корпоративным приложениям взаимодействовать с окружающей средой и запускать приложения для использования сети вещей. В этих примерах удаленный доступ через Интернет обычный, но не всегда доступен. Независимо от того, доступно ли такое интернет-соединение, сбор интеллектуальных объектов на сайте, а также любые другие локальные вычислительные и запоминающие устройства могут быть охарактеризованы, как сеть или интернет вещей.

В ближайшей перспективе разрозненных решений, скорее всего, опережают развертывание совместимых на основе стандартов решений для IoT. Эта ситуация распространена, когда появляются новые технологии или области применения. Например, Sutaria и Govindachari [4] отмечают, что две характеристики сетевых устройств IoT, которые создают проблемы – это наличие устройств с малой мощностью (которые должны функционировать в течение нескольких месяцев или лет без перезарядки) и частых данных обмены по сетям с потерями. Существующие стандартные протоколы Интернета в этом контексте не оптимальны. В более широком смысле существует несоответствие между огромным количеством устройств, которые быстро генерируют данные по распределенной области и используют множество сетевых технологий и облачных систем, которые хранят огромное количество данных в небольшом количестве местоположений с относительно медленной скоростью обновления данных. Интеграция этих двух классов систем для удовлетворения потребностей пользователей требует определенных возможностей протокола по всей архитектуре сети/протокола, от физического до промежуточного уровня, до уровня приложений.

Для решения этих проблем работают несколько отраслевых организаций и форумов по стандартизации, над расширением или принятием интернет-протоколов к устройствам IoT. Чтобы обеспечить общую систему отсчета и классифицировать необходимые функции и их местоположение в стеке протоколов, некоторые из этих групп также решают проблему формальной архитектуры для IoT. Хотя существующие стандарты и Интернет делают IoT возможным, набор широко ожидаемых новых стандартов, которые адаптируют или дополняют существующие для IoT, скорее всего, невозможны в ближайшей перспективе. Как и многие другие события, сделанные в Интернет, IoT будет развиваться и стремительно быстро, и проходить через дарвинистские процессы, и разумные технологии и механизмы протокола постепенно станут видимыми [5–7].

**Литература**

1. Stankovic J. Research Directions for the Internet of Things // Internet of Things Journal. – 2014. – V. 1. – № 1. – P. 3–9.

2. Overview of the Internet of Things // Recommendation Y.2060 [Электронный ресурс]. – Режим доступа: https://www.itu.int/rec/dologin_pub.asp?lang=f&id=T-REC-Y.2060-201206-I!!PDF-E&type=items, своб.
3. McEwen A. and Cassimally H. Designing the Internet of Things. – Wiley, 2014. – 338 p.
4. Sutaria R. and Raghunath G. Making sense of interoperability: Protocols and Standardization initiatives in IoT [Электронный ресурс]. – Режим доступа: http://www.cymbet.com/pdfs/Low_power_IoT_ComNet_2013_Mindtree.pdf, своб.
5. Параманов А.И. Разработка и исследование комплекса моделей трафика для сетей связи общего пользования: дис. ... канд. техн. наук: 05.12.13. – СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2014. – 325 с.
6. Ferguson J. and Redish A. Wireless Communication with Implanted Medical Devices Using the Conductive Properties of the Body // Expert Review of Medical Devices. – 2011. – V. 6. – № 4. – P. 427–433.
7. Common Requirements and Capabilities of a Gateway for Internet of Things Applications // Recommendation Y.2067 [Электронный ресурс]. – Режим доступа: https://www.google.ru/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjg-MDWjObdAhXFJSwKHTv-ArsQFjAAegQICRAC&url=https%3A%2F%2Fwww.itu.int%2Frec%2Fdologin_pub.asp%3Flang%3De%26id%3DT-REC-Y.4101-201710-I!!PDF-E%26type%3Ditems&usg=AOvVaw0hiVd41T2ra0qMOVeCc1dJ, своб.

**Калинкина Мария Евгеньевна**
Год рождения: 1991
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, аспирант
Направление подготовки: 09.06.01 – Информатика и вычислительная техника
e-mail: mariia_kalinkina@mail.ru

**Козлов Алексей Сергеевич**
Год рождения: 1984
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, аспирант
Направление подготовки: 09.06.01 – Информатика и вычислительная техника
e-mail: zz.kozlov@gmail.com

**Лабковская Римма Яновна**
Год рождения: 1988
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, к.т.н.
e-mail: labkovskaya@mail.ifmo.ru

**Пирожникова Ольга Игоревна**
Год рождения: 1989
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, к.т.н.
e-mail: cheezecake@mail.ru

**Ткалич Вера Леонидовна**
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, д.т.н., профессор
e-mail: vera_leonidovna_tkalich@mail.ru

**УДК 531.768**

## ПЕРСПЕКТИВЫ РАЗВИТИЯ МИКРОАКСЕЛЕРОМЕТРОВ

**Калинкина М.Е., Козлов А.С., Лабковская Р.Я., Пирожникова О.И., Ткалич В.Л.**
**Научный руководитель – к.ф.-м.н., доцент Сидорова Е.И.**

Работа выполнена в рамках темы НИР № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность».

Микромеханические датчики инерциальных систем навигации и управления находят все более широкое применение на подвижных объектах различных видов применения. Успехи в разработке методов и средств производства изделий микроэлектроники позволили обеспечить необходимую базу для разработки и массового производства микроакселерометров.
**Ключевые слова:** микроакселерометр, акселерометр, микромеханические датчики, МЕМС, микроэлектроника.

Развитие данной области науки и техники началось в 1960-х гг., однако вопросы теоретического и практического характера остаются нерешенными и, становятся все более сложными из-за растущих требований к системам автоматического контроля и мониторинга.

Качество и динамические свойства акселерометров, которые широко используются в различных отраслях промышленности, во многом определяются качеством чувствительного элемента в системах стабилизации и навигации.

Для разработки и усложнения процессов управления подвижными объектами требуется постоянное увеличение точности измерений параметров движения, включая ускорение, а также обработку информации. Принципы проектирования микромеханических систем, методы анализа и синтеза их свойств требуют постоянного улучшения. Факторы, упомянутые выше, и определяют актуальность темы исследования.

**Область применения.** Изобретение относится к измерительной технике. Акселерометры являются на сегодняшний момент одними из наиболее перспективных приборов для использования в приборах компенсационного типа с дискретным выходом в системах стабилизации, навигации и наведения. Оно может найти применение в приборах для измерения механических величин компенсационного типа.

Разработки ориентированы на такие направления как:
- повышение точности измерения акселерометра [1–9];
- увеличение малой полосы пропускания [2, 7, 8, 10];
- повышение стабильности коэффициента преобразования [11];
- повышение надежности [12].

**Имеющиеся проблемы.** Из анализа существующих конструкций чувствительных элементов (ЧЭ) интегральных акселерометров следует, что у всего множества разработанных подвижных узлов микросистемных датчиков измерения ускорений с электростатической обратной связью, обеспечивающей наиболее компактную конструктивную схему, имеются следующие недостатки:
- неудовлетворительная погрешность измерений [1, 3, 4];
- малая полоса пропускания [2, 7];
- низкая точность измерения [2, 8, 9, 13];
- постоянство разрешающей способности [11];
- большие массогабариты [5];
- динамическая погрешность [10].

Это является препятствием для увеличения диапазона измерений.

Перечисленные проблемы в целом затрудняют измерение ускорения, и для их устранения предлагаются следующие решения, которые выполняются за счет того, что:
- на подвижной части первой пластины выполнены прорези [1];
- прорези выполнены со стороны каждой подставки [1];
- длины прорезей выполнены равными [1];
- в генератор введена местная отрицательная обратная связь [2];
- введены балластный резистор, первый и второй компараторы, логическое устройство ИЛИ, реле [11];
- на стойку установлена втулка из инвара [3];

- подвижный элемент, первый, второй, третий и четвертый неподвижные электроды выполнены прямоугольными по форме [12];
- первый, второй, третий и четвертый неподвижные электроды выполнены равными по площади [12];
- на второй пластине выполнены первый и второй неподвижные электроды дифференциального емкостного преобразователя, на третьей пластине выполнены третий и четвертый неподвижные электроды [12];
- первый и второй резисторы выполнены в одной микросборке с генератором высокой частоты, первым и вторым усилителями переменного тока, суммирующим усилителем, демодулятором и усилителем постоянного тока на одной подложке [4];
- первая пластина выполнена из монокристаллического кремния [4];
- каждая из основных плоскостей внутренней неподвижной части пластины расположена на расстоянии, не меньшем величины максимального хода внешней подвижной части пластины [5];
- выводы компенсационной катушки, токоподводы и места соединения токоподводов с выводами компенсационной катушки расположены в плоскости, проходящей через ось подвеса и нейтральную ось магнита [5];
- грузы выполнены из электропроводного материала и расположены в рабочем зазоре силового преобразователя [5];
- внешняя подвижная часть пластины, упругие перемычки и внутренняя неподвижная часть с указанным расстоянием ее основных плоскостей от основных плоскостей внешней подвижной части выполнены единым элементом методом анизотропного травления кремния [5];
- введен в отрицательную обратную связь блок управления динамической ошибкой, вход которого соединен с выходом фазового детектора отрицательной обратной связи через сглаживающий фильтр, а выход блока управления динамической ошибкой соединен с одним из входов сумматора через преобразователь напряжение-ток, причем выход [6];
- введен дифференциальный усилитель постоянного тока [7];
- подвижная часть, неподвижная часть и плоские перемычки чувствительного элемента выполнены в одной первой пластине из монокристаллического кремния [14];
- плоские перемычки выполнены так, что одна из поверхностей каждой плоской перемычки совмещена с одной и той же поверхностью подвижной части первой пластины [14];
- выходы первого и второго усилителей переменного тока подключены к разнополярным входам суммирующего усилителя [14];
- первая пластина установлена так, что совмещенные с одной из поверхностей подвижной части первой пластины поверхности плоских перемычек расположены со стороны третьей пластины [14];
- введен интегратор, а на вход компаратора – первый дифференцирующий фильтр и сумматор [13];
- введена аналоговая, интегрирующая и дискретная интегрирующая отрицательные обратные связи [10];
- введена местная положительная обратная связь и фильтр верхних частот, местная отрицательная обратная связь с выхода усилителя на вход второго преобразователя напряжение-ток через фазовый детектор отрицательной обратной связи, а также компаратор, интегрирующий усилитель, реверсивный двоичный счетчик, генератор опорного напряжения, введена интегрирующая отрицательная обратная связь, второй сумматор, интегрирующий усилитель [8];
- введен фильтр верхних частот и преобразователь напряжение-ток [9];
- содержит корпус, первую пластину из монокристаллического кремния дифференциальный емкостный преобразователь положения, третью пластину на другой

стороне неподвижной части первой пластины, магнитоэлектрический силовой преобразователь с постоянным магнитом [9].

**Заключение.** Проанализировав всю информацию, можно сказать, что рынок глобальных компенсационных акселерометров в настоящее время является растущим рынком в секторе измерительной техники. Компенсационные акселерометры обнаружили быстрое развитие в нынешние и прошлые годы и, вероятно, будут продолжать развиваться в предстоящие годы.

**Литература**

1. Пат. RU 2545469 (C1), МПК7 G 01P 15/13. Компенсационный акселерометр // Августов Л.И. (RU), Баженов В.И. (RU), Горбачев Н.А. (RU) и др.; заявитель и патентообладатель ОАО «Раменское приборостроительное конструкторское бюро» (ОАО «РПКБ») (RU). – № 2013152824/28; заявл. 27.11.2013; опубл. 20.08.14. – 2 с. – 0,04 п.л.
2. Пат. RU 2513667 (C1), МПК7 G 01P 15/13. Компенсационный акселерометр // Кулешов В.В. (RU), Савельев В.В. (RU), Кулешов Д.В. (RU); заявитель и патентообладатель «Тульский государственный университет» (ТулГУ) (RU). – № 2012148111/28; заявл. 12.11.2012; опубл. 20.04.2014. – 2 с. – 0,04 п.л.
3. Пат. RU 2514151 (C1), МПК7 G 01P 15/13. Компенсационный акселерометр // Горбачев Н.А. (RU), Масленников А.В. (RU), Соловьев В.М. (RU), и др.; заявитель и патентообладатель ОАО «Раменское приборостроительное конструкторское бюро» (ОАО «РПКБ») (RU). – № 2012150512/28; заявл. 26.11.2012; опубл. 27.04.2014. – 2 с. – 0,04 п.л.
4. Пат. RU 2249221 (C1), МПК7 G 01 P15/13. Компенсационный акселерометр // Баженов В.И. (RU), Горбатенков Н.И. (RU), Загибина Т.П. (RU), и др; заявитель и патентообладатель ОАО «Раменское приборостроительное конструкторское бюро» (ОАО «РПКБ») (RU). – № 2003123629/28; заявл. 31.07.2003; опубл. 27.03.2005. – 2 с. – 0,04 п.л.
5. Пат. RU 2028000 (C1), МПК7 G01 P15/08, МПК7 G01 P15/13. Компенсационный акселерометр // Баженов В.И., Брищук Е.С., Вдовенко И.В., и др; заявитель и патентообладатель ОАО «Раменское приборостроительное конструкторское бюро» (RU). – № 93004341/10; заявл. 29.01.1993; опубл. 27.01.1995. – 2 с. – 0,04 п.л.
6. Пат. RU 2614205 (C1), МПК7 G01 P15/13. Компенсационный акселерометр // Кулешов В.В. (RU); заявитель и патентообладатель «Тульский государственный университет» (ТулГУ) (RU). – № 2016101301; заявл. 18.01.2016; опубл. 23.03.2017. – 2 с. – 0,04 п.л.
7. Пат. RU 2096785 (C1), МПК7 G01 P15/13. Компенсационный акселерометр // Баженов В.И., Вдовенко И.В., Горбатенков Н.И., и др.; заявитель и патентообладатель ОАО «Раменское приборостроительное конструкторское бюро». – № 96114940/28; заявл. 23.07.1996; опубл. 20.11.1997. – 2 с. – 0,04 п.л.
8. Пат. RU 2363957 (C1), МПК7 G01 P15/13. Компенсационный акселерометр // Кулешов В.В. (RU); заявитель и патентообладатель «Тульский государственный университет» (ТулГУ) (RU). – № 2008109640/28; заявл. 11.03.2008; опубл. 10.08.2009. – 2 с. – 0,04 п.л.
9. Пат. RU 2359277 (C1), МПК7 G01 P15/13. Компенсационный акселерометр // Кулешов В.В. (RU), Кулешов Д.В. (RU), Кулешов А.В. (RU) и др.; заявитель и патентообладатель «Тульский государственный университет» (ТулГУ) (RU). – № 2008104439/28; заявл. 05.02.2008; опубл. 20.06.2009. – 2 с. – 0,04 п.л.
10. Пат. RU 2541720 (C1), МПК7 G01 P15/13. Компенсационный акселерометр // Савельев В.В. (RU), Кулешов В.В. (RU), Кулешов В.Д. (RU); заявитель и

патентообладатель «Тульский государственный университет» (ТулГУ) (RU). – № 2013143638/28; заявл. 26.09.2013; опубл. 20.02.2015. – 2 с. – 0,04 п.л.

11. Пат. RU 2155965 (C1), МПК7 G 01P 15/13. Компенсационный акселерометр // Баженов В.И., Бражник В.М., Краснов В.В.; заявитель и патентообладатель ОАО «Раменское приборостроительное конструкторское бюро». – № 99115633/28; заявл. 19.07.1999; опубл. 10.09.2000. – 2 с. – 0,04 п.л.
12. Пат. RU 2186401 (C1), МПК7 G 01 P15/13. Компенсационный акселерометр // Баженов В.И., Ларин П.В., Минаев Ю.А., и др.; заявитель и патентообладатель ОАО «Раменское приборостроительное конструкторское бюро» (ОАО «РПКБ») (RU). – № 2001107913/28; заявл. 27.03.2001; опубл. 27.07.2002. – 2 с. – 0,04 п.л.
13. Пат. RU 2539826 (C2), МПК7 G01 P15/00. Компенсационный акселерометр // Савельев В.В. (RU), Кулешов В.В. (RU), Кулешов В.Д. (RU); заявитель и патентообладатель «Тульский государственный университет» (ТулГУ) (RU). – № 2013108330/28; заявл. 25.02.2013; опубл. 27.01.2015. – 2 с. – 0,04 п.л.
14. Пат. RU 17733 (U1), МПК7 G01 P15/13, МПК7 G01 P15/08. Компенсационный акселерометр // Баженов В.И., Будкин В.Л., Вдовенко И.В. и др.; заявитель и патентообладатель ОАО «Раменское приборостроительное конструкторское бюро». – № 2000125811/20; заявл. 17.10.2000; опубл. 20.04.2001. – 2 с. – 0,04 п.л.

**Кашицин Николай Олегович**
Год рождения: 1994
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N4255
Направление подготовки: 10.04.01 – Информационная безопасность
e-mail: nick.kashitsin@gmail.com

**Самойленко Александр Владимирович**
Год рождения: 1995
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N4255
Направление подготовки: 10.04.01 – Информационная безопасность
e-mail: aronornone@gmail.com

**УДК 004**

# ИССЛЕДОВАНИЕ МЕТОДОВ ОЦЕНКИ СРЕДСТВ ФИЗИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

**Кашицин Н.О., Самойленко А.В.**
**Научный руководитель – ассистент Попов И.Ю.**

В работе рассмотрена проблема оценки эффективности средств физической защиты. Раскрывается содержание существующих методов оценки эффективности средств физической защиты, а также выделяются положительные и отрицательные стороны. На основе проведенного исследования рассматривается применение методов оценки на примере.
**Ключевые слова:** методы оценки, информационная безопасность, СФЗ, исследование методов оценки СФЗ.

Надеяться на случайное достижение желаемого исхода событий в вопросах обеспечения безопасности недопустимо, особенно если приходится противодействовать осознанной планируемой деятельности хорошо подготовленного нарушителя [1].

Анализ средств физической защиты (СФЗ) показывает то, из чего формировалась система, помогает определить ценность имущества, находящегося во владении, и выделить угрозы безопасности, а также рассчитать экономическую сторону аспекта. Целей для проведения анализа на предприятии может быть множество – начиная от новшеств в сфере СФЗ, так и в особенностях деятельности самого предприятия, связанных с течением информационных потоков, ценных вещей и др. Только проводя оценку эффективности системы безопасности можно увидеть изменения, которые происходят в системе безопасности [2].

Путь нарушителя – упорядоченная последовательность действий против предприятия, которая при успешном завершении приведет к краже, диверсии или другому враждебному акту. В таблице приведен пример пути нарушителя, пытающегося взломать насос.

Таблица. Пути, используемые нарушителем безопасности

| Действия нарушителя | Элемент задержки | Элемент обнаружения |
|---|---|---|
| Преодолеть забор | Материал забора | Датчик на заборе |
| Пройти наружную дверь | Прочность двери | Датчики на двери |
| Преодолеть стену | Прочность стены | Охрана |

| Действия нарушителя | Элемент задержки | Элемент обнаружения |
|---|---|---|
| Пройти внутреннюю дверь | Прочность двери | Датчики двери |
| Сломать насос | Время, нужное для поломки насоса | Поломка насоса |

Весь анализ базируется на основании того, что существует возможность просчитать путь нарушителя. Как и было сказано ранее, разработка системы осуществляется с определения целей и угроз СФЗ – критического имущества. Все остальные элементы защиты соответственно выбираются исходя из особенностей предприятия. Рабочие характеристики, используемые для анализа пути нарушителя – вероятность обнаружения, время задержки, надежность связи и время реакции охраны. За счет того, что путей проникновения может быть просто огромное множество, то для их расчета используются компьютерные модели, например, модель EASY.

Задачей нарушителя является достижение объекта с наименьшей вероятностью быть остановленным СФЗ или же, по-другому говоря, с максимальной вероятностью успешного завершения нападения. Для решения этой задачи нарушитель должен стараться уменьшить время прохождения пути, однако не всегда можно придерживаться данного типа атаки, бывает и другой. Иногда можно пожертвовать этим временем и преодолеть барьеры защиты максимально, быстро не считаясь с вероятностью обнаружения, поэтому можно выделить две разновидности атаки: скрытое нападение и силовая атака. Имея в виду эти две крайности, можно найти меры для оценки эффективности работы системы. Первая их них – это сравнение общего времени прохождения пути со временем реакции охраны. Для эффективной СФЗ характерно обеспечивать достаточный уровень задержки, чтобы охрана могла среагировать на попытку проникновения. Время реакции охраны должно быть меньше минимального времени прохождения рубежей защиты, поэтому чтобы повысить эффективность, необходимо уменьшать время реакции охраны или добавлять элементы защиты для увеличения минимального времени прохождения рубежей защиты. Недостатком этого метода является то, что не учитывается обнаружение, а задержка без предварительного обнаружение не имеет смысла, так как для того, чтобы прервать действие нарушителя необходимо его обнаружить и оповестить силы реагирования.

Другой мерой эффективности является суммарная вероятность. Для эффективной системы эта вероятность должна иметь приемлемую величину. Недостатком является то, что отсутствует учет задержки. Обнаружение без задержки может быть не эффективным.

Чтобы рассчитать вероятность обнаружения нарушителя, например, на сигнализационном рубеже необходимо, чтобы были выполнены сразу три условных события: средство обнаружения (СО) должно находиться в работоспособном состоянии, процесс обнаружения должен закончиться формированием сигнала тревоги, сигнал тревоги не должен быть ложным.

В связи этим дадим обозначения всем вышеперечисленным событиям:

- вероятность безотказной работы $R$;
- вероятность обнаружения $P_{\text{об.ном}}$;
- вероятность правильного не обнаружения $P_{\text{ном}}$.

Все эти вероятности стоит перемножить, так как вероятность наступления результирующего события определяется как произведение вероятностей наступления каждого из событий.

Теперь, чтобы осуществить такой расчет, необходимо определить паспортные значения характеристик СО в вероятностном виде.

Вероятности ложной тревоги и отказа определяются в соответствии с выражениями:

$$P_{\text{лт}}(t) = 1 - e^{-t/T_{\text{лт}}}; \quad (1)$$

$$Q(t) = 1 - e^{-\frac{t}{T_0}}(2), \quad (2)$$

где $T_{\text{лт}}$ (ложной тревоги) и $T_0$ – параметры датчика, связанные со временем; $t$ – интервал времени, а $Q$ – вероятность отказа. Но для того, чтобы рассчитать данные вероятности

необходимо задать интервал времени наблюдения $t$. Логично, что с увеличением времени интервала будет увеличиваться вероятность появления ложной тревоги и вероятность отказа, в то время как вероятность появления нарушителя, наоборот, будет понижаться, кроме того необходимо использовать события прямо противоположные выше указанным формулам – т.е. вероятность правильного не обнаружения и вероятность безотказной работы. Следовательно, конечная формула будет следующей:

$P_{\text{ноб}}(t) = 1 - P_{\text{лт}}(t) = e^{-\frac{t}{T_{\text{лт}}}}$.

А вероятность безотказной работы:

$R(t) = 1 - Q(t) = e^{-\frac{t}{T_{\text{лт}}}}$.

Что, в конечном итоге, выливается в следующую формулу, определяющую человека-нарушителя:

$P_{\text{чн}} = P_{\text{об.ном}} \times P_{\text{ноб}}(t) \times R(t) = P_{\text{об.}} \times e^{-\frac{t}{T_{\text{лт}}}} \times e^{-\frac{t}{T_{\text{о}}}}$.

Ни время задержки, ни вероятность обнаружения нельзя взять по-отдельности, потому чтобы использовать правильную меру эффективности необходимо включить своевременное обнаружение всех трех вышеперечисленных компонентов. Согласно принципу своевременного обнаружения, эффективная система определяется по суммарной вероятности обнаружения нарушителя в момент, когда у сил реагирования еще достаточно времени для его перехвата.

Для расчета вероятности будем считать, что нарушитель до критической точки обнаружения (КТО) будет стремиться уменьшить обнаружения, а после КТО уменьшить величину задержки. Вначале осторожно, потом быстро, так как после обнаружения уже не будет смысла беспокоиться о времени реакции охраны. Чтобы достичь своей цели нарушитель может прибегнуть к совместному использованию силы, скрытности и обмана. Вот почему для эффективности системы так важно четко сформулировать основную угрозу. Нарушитель может и вовсе не иметь никакой тактики. Но обычно предполагается, что после КТО он будет двигаться с максимальной скоростью. Естественно, что если он не будет пользоваться такой тактикой, то эффективность системы возрастает, поэтому важно помнить об эшелонированной защите.

Когда один из элементов последствия потери данных незначительны, т.е. когда он может быть восполняемым или же его потеря несущественна – то на замену приходит качественный анализ, так как детальный анализ рассматривает и задействует все рубежи обороны, чтобы предотвратить любые потери имущества. При этом анализе вероятностям присваиваются не числовые, а описательные характеристики (например, низкая, высокая). В данном случае в основном используются не экспериментальные решения, а оценки.

Существуют два метода:

1. простой метод – заключается в сравнении субъективно предсказанного времени задержки после обнаружения со временем реакции сил реагирования. Если время задержки существенно превышает время реакции – высокая вероятность;
2. сложный метод добавляет на ось времени КТО. Далее аналитик берет точки до КТО, оценивает из них и берет максимальную. Действуя по этой методике аналитик предсказывает, где находится КТО. Данный анализ очень зависим от профессиональной ориентации аналитика.

**Литература**

1. Гарсия М.Л. Проектирование и оценка систем физической защиты. Системы безопасности. – Бёрлингтон, 2001. – 336 с.
2. Бакланов В.В., Духан Е.И., Шамонин Е.Д. Оценка эффективности систем физической защиты. – Екатеринбург: УМЦ УПИ, 2015. – 229 с.

**Ким Юлия Вячеславовна**
Год рождения: 1997
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N3351
Направление подготовки: 10.03.01 – Информационная безопасность
e-mail: yulia1344@gmail.com

**Матвеева Анастасия Андреевна**
Год рождения: 1998
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N3351
Направление подготовки: 10.03.01 – Информационная безопасность
e-mail: anastasiamatveevaitmo@gmail.com

**УДК 004.932.1**

# МЕТОДЫ РАСПОЗНАВАНИЯ ОБРАЗОВ ПРИ НАРУШЕНИЯХ СЕМАНТИЧЕСКОЙ ЦЕЛОСТНОСТИ ВИЗУАЛЬНОЙ ИНФОРМАЦИИ

**Ким Ю.В., Матвеева А.А.**
**Научный руководитель – Викснин И.И.**

В работе рассмотрены методы, применимые в компьютерном зрении и способствующие улучшению качества распознавания образов, в частности, сохранению семантической целостности визуальной информации.
**Ключевые слова:** машинное обучение, компьютерное зрение, семантическая целостность, визуальная информация, распознавание образов.

В течение последних нескольких десятков лет широкое распространение получило машинное обучение. В работе освещен раздел компьютерного зрения, а именно методы повышения качества распознавания образов. Компьютерное зрение – это широкий пласт теоретических изысканий и технических методик по распознаванию, отслеживанию и классификации объектов. Авторы различных научных работ сходятся во мнении, что одной из основных целей в области компьютерного зрения является снижение процента ошибки распознавания образов. Ошибкой распознавания образов в данной работе считается ситуация, когда нужный объект на изображении не обнаруживается, либо обнаруживается некорректно [1–10].

На основе изученных источников авторами была поставлена цель исследования – поиск эффективных методов для распознавания образов в случае вероятности возникновения нарушения семантической целостности. Реализация цели потребовала решения следующих задач:

1. рассмотрение целостности информации на основе ее концептуальных составляющих, а именно синтаксической, семантической и прагматической целостности;
2. освещение этапов процесса распознавания образов.

Существует множество методов улучшения качества распознавания образов, но в большинстве случаев они предлагаются отдельно друг от друга. Авторы хотели предложить последовательность методов, которые возможно будет использовать на протяжении всего процесса анализа изображения. Исходя из этого, третьей задачей является:

3. поиск методов сохранения семантической целостности визуальной информации относительно каждого этапа распознавания образов.

Целостность информации можно подразделить на три составляющие: прагматическая, синтаксическая и семантическая. Прагматическая целостность – это аспект целостности информации, при котором излагаются факты, основанные на достоверных и полных свидетельствах. Синтаксическая целостность – категория целостности информации, при которой обеспечивается донесение информации с использованием корректных конструкций и структур. Семантическая целостность – категория, при которой не происходит нарушения смыслового контекста информации. В процессе распознавания образов на изображении существует вероятность, что объект будет распознан неверно, поэтому семантическая целостность в области компьютерного зрения играет наиболее существенную роль.

Процесс распознавания образов состоит из трех основных этапов:

1. подготовка изображения к анализу;
2. обработка визуальной информации;
3. классификация объектов на изображении.

Нарушение семантической целостности визуальной информации может произойти по следующим причинам:

– наличие шумов на изображении;
– размытие изображения;
– неверно подобранная обучающая выборка для классификатора;
– недостаточность обучающей выборки для классификатора.

На начальном этапе анализа изображения авторами предлагалось нормировать изображение. Нормирование позволяет сделать изображение нечувствительным к изменениям освещенности и осуществляется согласно формуле:

$$[r', g', b'] = \left[ \frac{r}{\sqrt{r^2 + g^2 + b^2}}, \frac{g}{\sqrt{r^2 + g^2 + b^2}}, \frac{b}{\sqrt{r^2 + g^2 + b^2}} \right],$$

где $r$, $g$, $b$ – исходные составляющие RGB-вектора пикселя; $r'$, $g'$, $b'$ – нормированные составляющие RGB вектора пикселя.

Применение нормирования изображения, представленного на рис. 1, а, иллюстрирует рис. 1, б.

а б

Рис. 1. Исходное изображение (а); нормированное изображение (б)

Для минимизации ошибок распознавания считается целесообразным использовать кластеризацию. Однако большинство существующих методов кластеризации однозначно не обеспечивают сохранение семантической целостности информации, так как обладают следующими недостатками:

– чувствительность к выбросам;
– необходимость предварительного указания пользователем количества кластеров;
– необходимость определения пользователем параметров кластеризации.

С учетом перечисленных недостатков был разработан новый способ кластеризации. Он объединяет в себе элементы метода роя частиц, который предполагает движение группы частиц с целью нахождения лучшего решения в данной области, и метода *k*-средних, который разделяет изображение на заранее заданное число кластеров с определенными центроидами и распределяет пиксели посредством вычисления минимального значения их функции расстояния относительно каждого центроида. Из

каждого метода были отобраны операции, обеспечивающие автоматическое вычисление всех параметров без необходимости вмешательства пользователя. Из метода роя частиц были заимствованы следующие действия: движение группы частиц (попиксельное прохождение по изображению), поиск лучшего решения для роя в целом (нахождение в заданной области пикселя с максимальным значением средней интенсивности). Относительно алгоритма кластерного анализа *k*-средних были улучшены следующие его составляющие: исчезла необходимость предварительного установления числа кластеров пользователем; помимо минимизации функции расстояния была добавлена дополнительная операция по минимизации функции цвета. Данный аспект вносит наибольший вклад в обеспечение семантической целостности, ведь отдельный объект изображения (в некоторых случаях – часть объекта) характеризуется относительной однородностью цвета и отсутствием резких перепадов, т.е. если функция расстояния $d$ для пикселей $a$ и $b$ одного объекта стремится к минимуму, то и функция цвета $f$ будет стремиться к минимуму. Результат кластеризации на основе метода роя частиц представлен на рис. 2, а.

а б

Рис. 2. Кластеризованное изображение (а); результат работы классификатора Хаара (б)

Для этапа классификации авторами использовались каскады Хаара. Данный метод базируется на признаках Хаара. Каждый такой признак состоит из смежных прямоугольных областей. Они позиционируются на изображении, далее суммируются интенсивности пикселей в областях, после чего вычисляется разность между суммами – значение признака Хаара. Признаки Хаара организованы в каскадный классификатор. Работа с ним подразумевает два шага. Первый шаг заключается в настройке классификатора с использованием обучающей выборки изображений (дополнительно было решено нормировать обучающие изображения с целью повышения достоверности распознавания). Второй шаг заключается в использовании настроенного классификатора. При работе с каскадами Хаара изображение представляется в виде матрицы согласно формуле:

$$II(x,y) = \sum_{i=0,\, j=0}^{i \le x,\, j \le y} I(i,j),$$

где $I$ – интенсивность пикселя входного изображения. Каждый элемент матрицы представляет собой сумму пикселей в прямоугольнике от точки (0,0) до точки $(x, y)$. Процедура обучения проходит за $T$ итераций, в результате которых получается каскад из $T$ слабых классификаторов. Работа обученного классификатора происходит следующим образом: на вход алгоритму поступает изображение размером $W \times H$. Алгоритм сканирует изображение на 11 масштабах: размер окна 24×24 пикселя, и при этом каждый следующий уровень в 1,25 раза больше предыдущего. Результат работы классификатора Хаара по распознаванию автомобиля представлен на рис. 2, б.

Таким образом, путем выполнения поставленных задач, была достигнута цель исследования. Авторами были отобраны методы, снижающие вероятность возникновения

нарушения семантической целостности. Относительно первого этапа распознавания образов: бинаризация и нормирование; относительно второго этапа: кластеризация с учетом функции расстояния и функции цвета; относительно третьего этапа: каскады Хаара с нормированной обучающей выборкой. Рис. 3, а, иллюстрирует, как указанная последовательность действий улучшает качество распознавания автомобиля по сравнению с рис. 3, б, где применялся только классификатор Хаара с ненормированной обучающей выборкой.

а б

Рис. 3. Результат распознавания автомобиля при использовании только классификатора Хаара с ненормированной обучающей выборкой (а); результат распознавания автомобиля при использовании предложенного алгоритма анализа изображений (б)

**Литература**

1. Hammons T.J. Artificial intelligence in power system engineering: Actual and potential applications of expert systems, knowledge-based systems, and artificial neural networks // IEEE Power Engineering Review. – 1994. – P. 11–16.
2. Vernon D. Machine Vision in the Electronics and PCB Inspection Industry. The Current Position and Future Directions [Электронный ресурс]. – Режим доступа: https://homepages.inf.ed.ac.uk/rbf/CVonline/LOCAL_COPIES/ECVNET/electronics.inspection.html, своб.
3. Mathieu R.G., Woodard R.L. Data integrity and the Internet: implications for management // Internet Research. – 1995. – P. 3–7.
4. Ibrahim H. A strategy for semantic integrity checking in distributed databases // Ninth International Conference on Parallel and Distributed Systems. – 2002. – P. 139–144.
5. Udagepola K.P., Xiang L., Wijeratne A.W., Xiaozong Y. Semantic integrity constraint violations check for spatial database updating [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/publication/258881722_Semantic_Integrity_Constraint_Violations_Check_for_Spatial_Database_Updating, своб.
6. Aly A.A., Deris S.B., Zaki N. Research review for digital image segmentation techniques // International Journal of Computer Science & Information Technology. – 2011. – V. 3. – № 5. – P. 99–106.
7. Xiang Y., Chung A.C.S. and Ye J. A new active contour method based on elastic interaction // IEEE Computer Society Conference on Computer Vision and Pattern Recognition. – 2005. – P. 452–457.
8. Choudhury S., Chattopadhyay S.P., Hazra T.K. Vehicle detection and counting using haar feature-based classifier // 8th Annual Industrial Automation and Electromechanical Engineering Conference. – 2017. – P. 106–109.
9. Xie L., Tian Q., Zhang B. Feature normalization for part-based image classification // IEEE International Conference on Image Processing. – 2013. – P. 2607–2611.
10. Viksnin I.I., Drannik A.L., Iureva R.A., Komarov I.I. Flocking factors' assessment in case of destructive impact on swarm robotic systems // 18th Conference of Open Innovations Association and Seminar on Information Security and Protection of Information Technology. – 2016. – P. 357–363.

**Кляус Татьяна Константиновна**
Год рождения: 1993
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, аспирант
Направление подготовки: 10.06.01 – Информационная безопасность
e-mail: t_klyaus@corp.ifmo.ru

**УДК 004.056**

# ВЫБОР СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ В СИСТЕМЕ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА, МЕТОДОМ ОПРЕДЕЛЕНИЯ ОПТИМАЛЬНОЙ СТРАТЕГИИ ИГРОКА В АНТАГОНИСТИЧЕСКОЙ ИГРЕ С НУЛЕВОЙ СУММОЙ

**Кляус Т.К.**
**Научный руководитель – д.т.н., профессор Гатчин Ю.А.**

Задача защиты системы электронного документооборота сводится к задаче классической защиты информационной системы, что подразумевает применение механизмов контроля целостности используемого программного обеспечения, регистрации событий, криптографической защиты, межсетевого экранирования, антивирусной защиты и т.д. В работе задача защиты системы электронного документооборота от атак канального, сетевого и транспортного уровней решена с помощью определения оптимальной стратегии игрока (защитника информационной системы) путем нахождения седловой точки. В качестве элементов матрицы игры взяты коэффициенты эффективности средств защиты информации из графиков оценки безопасности (Security Value Maps) NSS Labs.

**Ключевые слова:** информационная безопасность, атака, антагонистическая игра, средства защиты информации, межсетевой экран, средство предотвращения вторжений.

Внедрение систем электронного документооборота (СЭД) охватывает организации и предприятия различных отраслей деятельности. Информация, циркулирующая в системах данного типа, как правило, содержит конфиденциальную информацию (персональные данные, коммерческую или служебную тайну и т.д.). Содержащаяся в электронных документах информация требует защиты от ее утечки.

К задаче защиты СЭД необходимо подходить с точки зрения классической защиты информационной системы (ИС). Необходимо использовать механизмы, обеспечивающие:

1. контроль целостности используемого программного обеспечения;
2. регистрацию событий в ИС;
3. криптографическую защиту;
4. межсетевое экранирование;
5. виртуальные частные сети;
6. антивирусную защиту;
7. аудит информационной безопасности [1].

Существуют различные подходы к выбору средств защиты ИС. В том числе для решения данной задачи могут применяться методы теории игр [2].

Для атаки СЭД и нарушения конфиденциальности циркулирующих в ней электронных документов злоумышленник может использовать уязвимости протоколов канального, сетевого, транспортного уровней, а также уровня приложений модели OSI. Межсетевые экраны (МЭ) и системы предотвращения вторжений (СПВ) являются наиболее распространенными средствами защиты информации (СЗИ) в корпоративных сетях.

МЭ позволяет контролировать отправляемый и принимаемый трафик посредством фильтрации пакетов в соответствии с заданными правилами (политикой безопасности). В настоящее время в корпоративных информационных системах применяются МЭ «нового поколения» – Next Generation Firewalls (NGFW). В отличие от традиционных МЭ, МЭ «нового поколения» осведомлены о запущенных в системе приложениях, способны отслеживать передаваемый и принимаемый трафик на 2–7 уровнях модели OSI (традиционные МЭ отслеживают трафик на 2–4 уровнях), имеют возможность настраивать правила политики безопасности МЭ для конкретного пользователя, поддерживают работу устройства как в режиме моста, так и в режиме маршрутизации. Кроме того, МЭ «нового поколения» имеют интегрированную СПВ, которая обнаруживает атаки с помощью их сигнатур и эвристических методов [3].

Предположим, что у администратора безопасности на выбор есть следующие аппаратные МЭ «нового поколения» с интегрированными СПВ: FortiNet FortiGate 600D v.5.4.5, Palo Alto Networks PA-5250, Checkpoint Software Technologies 15600. Выберем наиболее оптимальный вариант МЭ с помощью методов теории игр на основе данных исследований, проведенных независимой лабораторией NSS Labs [4]. В таблице приведены данные об эффективности безопасности (Security Effectiveness) МЭ и СПВ из графиков оценки безопасности (Security Value Maps) NSS Labs.

Взаимодействие между злоумышленником и защитником ИС может быть представлено как антагонистическая игра с нулевой суммой. Эффективность безопасности СЗИ может быть интерпретирована как вероятность того, что атака не будет реализована злоумышленником, т.е. приведенные значения являются выигрышами защитника системы. Стратегиями игрока I (защитника системы) является применение одного из вышеперечисленных СЗИ, а стратегиями игрока II (злоумышленника) – реализация атак, обнаруживаемых СПВ (например, атаки канального уровня), или атак, обнаруживаемых МЭ (атаки сетевого и транспортного уровней) [5].

Таблица. Выбор СЗИ с помощью нахождения седловой точки

| № п/п | Средства защиты информации | Эффективность безопасности | | $\alpha_i = \min_k a_{ik}$ |
|---|---|---|---|---|
| | | СПВ | МЭ | |
| 1 | FortiNet FortiGate 600D v.5.4.5 | 0,79 | 1 | 0,79 |
| 2 | Palo Alto Networks PA-5250 | 0,4 | 0,94 | 0,4 |
| 3 | Checkpoint Software Technologies 15600 | 0,9 | 0,94 | 0,9 |
| | $\beta_k = \max_i a_{ik}$ | 0,9 | 1 | |

Приведенная таблица представляет собой матрицу выигрышей:

$H = \{a_{ik}\}_{m,n}$, $i$=1…$m$, $k$=1…$n$;

$A = \{a_1, a_2, ..., a_m\}$ – множество стратегий игрока I (защитника СЭД);

$B = \{b_1, b_2, ..., b_n\}$ – множество стратегий игрока II (злоумышленника).

Для определения оптимальной стратегии игрока необходимо найти седловую точку, которая представляет собой ситуацию равновесия и является лучшим откликом на стратегии другого игрока.

Для построения стратегии игрока I используется принцип максимина, основанный на максимизации минимальных выигрышей. Для этого в каждой строке таблицы находится минимальный элемент

$\alpha_i = \min_k a_{ik}$, $i$=1, 2, 3.

Затем выбирается максимальное число

$\alpha = \max_i \min_k a_{ik}$.

В данном случае, α=0,9.

Для построения стратегии игрока II используется принцип минимакса, основанный на минимизации максимальных потерь. Для этого в каждом столбце таблицы ищется максимальный элемент

$\beta_k = \max_i a_{ik}$, $k$=1, 2.

Затем выбирается минимальное число

$\beta = \min_k \max_i a_{ik}$.

В данном случае β=0,9.

Найденная ситуация является равновесной:

$\max_i \min_k a_{ik} = \min_k \max_i a_{ik}$.

Оптимальной стратегией защитника ИС является установка Checkpoint Software Technologies 15600.

Безусловно, подобный подход к определению наилучшего СЗИ для СЭД имеет ряд ограничений – для его применения необходимо точно знать вероятность обнаружения программным или аппаратным средством той или иной атаки, что на практике возможно не всегда. Однако в данном случае, при наличии рассчитанного на основании методики коэффициента эффективности безопасности СЗИ, определение оптимальной стратегии защитника системы является возможным.

**Литература**

1. Сабанов А.Г. Некоторые аспекты защиты электронного документооборота [Электронный ресурс]. – Режим доступа: https://ecm-journal.ru/post/Nekotorye-aspekty-zashhity-ehlektronnogo-dokumentooborota.aspx/, своб.
2. Заркумова Р.Н. Применение методов теории игр при выборе средства эффективной защиты // Сборник научных трудов НГТУ. – 2009. – № 4(58). – С. 41–46.
3. A Guide to Choosing a Next-Generation Firewall [Электронный ресурс]. – Режим доступа: http://www.tomsitpro.com/articles/next-generation-firewall-vendors,2-847.html/, своб.
4. NSS Labs [Электронный ресурс]. – Режим доступа: https://www.nsslabs.com/, своб.
5. Стратегические игры [Электронный ресурс]. – Режим доступа: http://dit.isuct.ru/IVT/sitanov/Literatura/POM/Chapter10/index.html, своб.

**Мариненков Егор Денисович**
Год рождения: 1998
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N3252
Направление подготовки: 10.03.01 – Информационная безопасность
e-mail: egormarinenkov@gmail.com

**Жукова Юлия Александровна**
Год рождения: 1998
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N3252
Направление подготовки: 10.03.01 – Информационная безопасность
e-mail: zhukova1998@gmail.com

**Шуваев Александр Константинович**
Год рождения: 1998
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N3252
Направление подготовки: 10.03.01 – Информационная безопасность
e-mail: arcshev@gmail.com

**УДК 004.75**

# ЗАЩИЩЕННОЕ ГРУППОВОЕ УПРАВЛЕНИЕ БЕСПИЛОТНЫМИ ЛЕТАТЕЛЬНЫМИ АППАРАТАМИ

**Мариненков Е.Д., Жукова Ю.А., Шуваев А.К.**
**Научный руководитель – к.ф.-м.н., доцент Комаров И.И.**

В работе авторами рассмотрена группа беспилотных летательных аппаратов, как самоорганизующаяся система, основанная на мультиагентном подходе. Рассмотрены методы группового управления для применения в контексте группы беспилотных летательных аппаратов. Формализовано информационное взаимодействие элементов группы, выявлены уязвимости возникновения деструктивного информационного воздействия, предложены контрмеры, основанные на классических подходах к обеспечению информационной безопасности.
**Ключевые слова:** мультиагентные системы, робототехнические системы, беспилотные летательные аппараты, информационное взаимодействие, деструктивное информационное воздействие, информационная безопасность.

В настоящее время в различных сферах деятельности ставятся задачи, которые могут быть решены с помочью использования беспилотных летательных аппаратов. В основном такие задачи имеют гражданское назначение. Беспилотные летательные аппараты (БПЛА) отлично подходят для воздушного мониторинга, создания карт местности, поисковых работ. В России активно разрабатываются БПЛА для внедрения в области экологической и сельскохозяйственной деятельности [1]. В работе [1] описаны перспективы применения БПЛА, но не акцентируется внимание на организации коллективного управления БПЛА.

При разработке робототехнической системы (РТС) необходимо учитывать такой фактор как информационная безопасность (ИБ). Как правило, на всех этапах разработки

этому фактору уделяется недостаточное внимание, в связи с чем такая система подвержена различным информационным угрозам [2].

Авторами настоящей работы рассмотрено применение БПЛА как самоорганизующейся группы, способной решать задачи, нехарактерные для любого участника данной группы в частности. Данная тематика стала развитием парадигмы применения мобильных робототехнических систем в пространстве, а не в плоскости [3].

Одной из главных задач разработки самоорганизующейся коллаборации БПЛА является обеспечение ИБ при взаимодействии агентов между собой. Поскольку децентрализованные методы коллективного управления базируются на мультиагентном подходе, возможна адаптация и применение их в контексте групп БПЛА.

Проанализировав работу [4], была выбрана децентрализованная коллективная стратегия, в связи с ее преимуществами:

- время принятия решения линейно зависит от количества объектов в группе;
- в связи с отсутствием центрального управляющего устройства повышается отказоустойчивость системы;
- наличие общего канала информации позволяет реализовать взаимодействие между объектами коллаборации, что обеспечивает нахождение оптимального алгоритма для реализации поставленной авторами цели.

Каждый агент группы получает необходимую информацию из окружающей среды и от иных агентов. Данные процессы получения и обмена информацией можно описать как внутреннее и внешнее информационное взаимодействие (ИВ). К внутреннему ИВ относится совокупность данных, получаемая исключительно от встроенных устройств агента. Данную информацию можно подразделить на информацию о положении в пространстве (устройство определения положения в пространстве), объектов его системы (устройства сканирования окружающей среды) и препятствий данной среды (устройства сканирования окружающей среды). Данная информация обрабатывается процессорным устройством (ПУ), после чего передается в виде команд устройствам регулирования положения в пространстве и дополнительным устройствам, необходимым для выполнения поставленных задач. К внешнему ИВ относятся данные, получаемые агентом от других агентов, такие как местоположение, техническое состояние и информация о препятствиях других агентов. В свою очередь, агент передает другим агентам ту же информацию, после чего группа коллективно выявляет задачи, распределяя их между агентами, и пути их решения.

В ходе анализа определенного ИВ, были выявлены уязвимости для деструктивного информационного воздействия (ДИВ). Для обеспечения ИБ внутреннего ИВ вводится аудит технического состояния, который позволяет выявить устройства с нарушением функционирования, которые, в свою очередь, передают негативную информацию другим устройствам. Аудит оповещает другие устройства о неисправных, после чего информация от данных устройств не используется для обработки. Данный метод «блокирования» позволяет исключать негативную информацию из ИВ, сохраняя функционирование устройств.

Для обеспечения ИБ внешнего ИВ авторами были проанализированы классические подходы обеспечения ИБ, такие как метод классификации информации, мобильная криптография, «товарищеская» модель, Police Office Model (POM). Для разработки системы аутентификации был модернизирован классический подход POM внедрением мобильной криптографии и оптимизацией данного подхода для использования в децентрализовано организованной группе. Таким образом, с начала функционирования группы в каждый определенный дискретный момент времени любой агент может быть назначен Police Officer (PO) – устройством, отвечающим за безопасности своей области. При миграции агента в область, контролируемую PO, PO отправляет агенту программу, содержащую зашифрованную функцию, и которую необходимо выполнить агенту, используя «секретную» информацию. Результат, полученный после выполнения, отправляется PO, после чего происходит процесс дешифрации, и PO сравнивает полученный результат с необходимым

результатом. Таким образом, РО выявляет доверенность агента и, в случае несовпадения результатов, оповещает всех других агентов о недоверенном. Исключение недоверенного агента из ИВ позволяет защитить других агентов от ДИВ. Для ликвидации уязвимостей в процессе обмена информацией предлагается использование криптосистемы с открытым ключом, что позволяет обеспечить конфиденциальность, целостность и доступность информации, в связи с возможностью отправлять информационные сообщения (ИС) любому агенту и исключением возможности «прочтения» ИС не адресатом.

Введенные контрмеры позволяют говорить о разработанной модели защищенного ИВ в группе БПЛА. В дальнейшем авторы планируют определить риски возникновения ДИВ в разработанной модели, после чего улучшить модель с целью понижения рисков. Также планируется разработка алгоритма перемещения коллаборации БПЛА в пространстве на основе разработанной модели и впоследствии реализация автономной самоорганизующейся группы БПЛА в симуляторе пространства, с целью эмпирической проверки разработанных моделей и алгоритмов.

**Литература**

1. Трубников Г.В. Применение беспилотных летательных аппаратов в гражданских целях // UAV. RU. Беспилотная авиация [Электронный ресурс]. – Режим доступа: http://www.uav.ru/articles/civil_uav_th.pdf, своб.
2. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. – М.: Горячая линия-Телеком. – 2004. – 280 с.
3. Михайлов Б.Б., Назарова А.В., Ющенко А.С. Автономные мобильные роботы – навигация и управление // Изв. ЮФУ. Технические науки. – 2016. – № 2(175). – С. 48–67.
4. Каляев И.А., Гайдук А.Р., Капустян С.Г. Модели и алгоритмы коллективного управления в группах роботов. – М.: ФИЗМАТЛИТ, 2009. – 280 с.

**Матвеева Анастасия Андреевна**
Год рождения: 1998
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N3351
Направление подготовки: 10.03.01 – Информационная безопасность
e-mail: anastasiamatveevaitmo@gmail.com

**Ким Юлия Вячеславовна**
Год рождения: 1997
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N3351
Направление подготовки: 10.03.01 – Информационная безопасность
e-mail: yulia1344@gmail.com

**УДК 004.896**

# МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОММУНИКАЦИОННЫХ КАНАЛОВ НА ПРИМЕРЕ ГРУППЫ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

**Матвеева А.А., Ким Ю.В.**
**Научный руководитель – Викснин И.И.**

В работе рассмотрены механизмы обеспечения целостности информации в группах беспилотных летательных аппаратов. Большее внимание уделяется прагматической целостности. В целях ее обеспечения предлагается дополнение к механизму построения доверия и репутации агентов на основе теории кредита.
**Ключевые слова:** беспилотные летательные аппараты, децентрализованное коллективное управление, мультиагентные системы, теория кредита, прагматическая целостность информации.

В XXI веке мультиагентные робототехнические системы являются неотъемлемой частью повседневной жизни. Они помогают автоматизировать такие процессы, как, например: отслеживание посевных комплексов, патрулирование территории с целью выявления фактов нарушения природоохранного режима, проведение хирургических операций, мониторинг чрезвычайных ситуаций, составление карт мест крушения самолетов и восстановление картины происшествия, управление транспортными средствами и многие другие. При этом робототехнические системы гораздо продуктивнее человеческого персонала. Этому способствует ряд причин: быстрота реализации выполнения работы; повышенная устойчивость к условиям работы, независимость от психологических и физиологических аспектов; высокая точность выполняемых действий [1–6].

Стратегии группового управления роботами делятся на две группы: централизованные и децентрализованные. В свою очередь, централизованное управление бывает единоначальным и иерархическим. Централизованное единоначальное управление: в группе имеется центральное устройство управления (ЦУУ) (командир), на которого возлагаются задачи планирования и контроля действий всех членов группы. Централизованное иерархическое управление заключается в том, что командир управляет рядом подчиненных, каждый из которых, в свою очередь, управляет определенной подгруппой роботов из данной группы.

Преимуществом централизованного управления является простота его реализации. Однако все системы группового управления, использующие централизованные стратегии, имеют следующие существенные недостатки:

– низкая отказоустойчивость – выход из строя одного центрального устройства управления приводит к выходу из строя системы в целом либо значительной ее части;
– длительное время принятия решений – центральный узел управления должен решать сложную задачу оптимизации действий всех членов группы или подгруппы.

Этих недостатков лишены группы, применяющие стратегии децентрализованного управления. Отсутствие ЦУУ минимизирует временные затраты на принятие решений, и отказ одного или нескольких участников значительно не повлияет на работоспособность группы.

Стратегия децентрализованного управления делится на два вида: коллективная и стайная. При децентрализованном коллективном управлении роботы группы имеют общий канал обмена информацией друг с другом. В случае децентрализованного стайного управления члены группы не имеют канала связи и принимают решения на основе косвенной информации об изменениях окружающей среды, вызванных действиями других роботов.

Авторы отдают предпочтение стратегии коллективного управления, поскольку наличие общего канала связи обеспечивает общение роботов с целью нахождения оптимального алгоритма достижения поставленных целей. Однако в таком случае возникает необходимость обеспечения безопасности передачи информации по коммуникационным каналам.

Общая постановка задачи звучит следующим образом: имеется группа, состоящая из $N$ агентов; у них имеется общий канал связи, с помощью которого они обмениваются информацией для достижения общей цели в течение периода $T$; требуется найти методы, которые позволят минимизировать вероятность деструктивного информационного воздействия на группу.

Исходя из этого, целью исследования являлся поиск эффективных методов, обеспечивающих сохранение целостности передаваемой по каналу связи информации. Децентрализованное коллективное управление освещалось на основе беспилотных летательных аппаратов (БПЛА). В частности, рассмотрены мультироторные летательные аппараты, а именно квадрокоптеры.

Достижение цели потребовало выполнение нижеперечисленных задач:
– изучить механизмы «жесткой» и «мягкой» безопасности;
– осветить аспект прагматической целостности информации;
– рассмотреть механизм обеспечения сохранения прагматической целостности на основе теории кредита.

На данный момент механизмы обеспечения информационной безопасности в мультиагентных робототехнических системах подразделяют на два основных вида: механизмы обеспечения «жесткой» безопасности и механизмы обеспечения «мягкой» безопасности. К первому виду данных механизмов относятся шифрование каналов связи с открытым ключом, использование мобильной криптографии, авторизация агентов.

Примером механизмов «мягкой» безопасности является модель доверия и репутации к объектам. Можно считать, что одной из уязвимостей данной модели является случай, когда диверсанты в группе роботов составляют половину или большинство: тогда они могут выставлять друг другу высокие оценки доверия, дискредитируя при этом остальных агентов. В качестве метода решения помимо доверия было предложено измерять репутацию агента в течение времени взаимодействия.

Однако перечисленные выше способы ориентированы в основном на сохранение семантической целостности – смысловой составляющей. В данной работе большое внимание уделено прагматической целостности информации – категории, заключающейся в достоверности и полноте знаний, на основе которых передается информация. Следует учитывать, что чтобы не подрывать доверие к себе ложной информацией, БПЛА могут не предоставлять ее другим в полном виде. В таком случае происходит нарушение прагматической целостности. Для его предотвращения в качестве дополнительных параметров для вычисления доверия и репутации авторами предлагается способ, основанный на теории кредита. Под кредитом зачастую понимают доверие, которое кредитор оказывает должнику при выдаче ссуды, что является наиболее подходящим для механизма «мягкой»

безопасности. Капиталотворческая теория кредита гласит, что кредитование способствует росту благосостояния населения. В контексте информационной безопасности кредит ведет к улучшению общего уровня безопасности.

Каждому БПЛА группы в начале работы будет выдаваться «кредит» на информацию, который определяется временем взаимодействия; длиной промежутка времени, за который должна произойти отдельная выплата; размером передаваемой информации за один промежуток времени. Это выражено в формуле:

$$CREDIT = f(t, Size, T),$$

где $t$ – промежуток времени, за который должна произойти отдельная «выплата»; $Size$ – размер отдельной «выплаты»; $T$ – период, за который должен быть выплачен весь «кредит».

В течение каждого заданного промежутка времени для погашения кредита БПЛА должен передавать фиксированное количество данных о своем местоположении, состоянии окружающей среды и т.д. В случае если БПЛА удержит какую-либо информацию, он нарушает фиксированный «платеж», и в качестве санкции налагается штраф, снижающий ценность «выплат» этого БПЛА. Механизм определения штрафа представлен в формуле:

$$FINE = f(payment_{lie}),$$

где $payment_{lie}$ – «платеж», при котором произошло удержание информации.

По итогам заданного периода будут подсчитываться «задолженности» каждого БПЛА по выданному «кредиту», и агенты с большей «задолженностью» будут иметь меньший показатель доверия, а следовательно, и репутации. Проверка выплат будет осуществляться в группе регулярно переизбираемым случайным образом ответственным агентом. Функция определения доверия выражена в формуле:

$$TRUST_i = f(\sum_{j=1}^{j=T} payment_{ij}),$$

где $TRUST_i$ – доверие к $i$-му агенту; $t_j$ – промежуток времени, за который должна произойти отдельная «выплата»; $T$ – период, за который должен быть выплачен весь «кредит»; $payment_{ij}$ – выплата $i$-го агента за $j$-промежуток времени.

Таким образом, авторами были выполнены поставленные задачи и достигнута цель исследования. Были описаны существующие способы обеспечения безопасности коммуникационных каналов БПЛА. В частности, было уделено особое внимание прагматической целостности информации и предложен способ ее сохранения, основанный на теории кредита.

**Литература**

1. Зикратов И.А., Зикратова Т.В., Лебедев И.С., Гуртов А.В. Построение модели доверия и репутации к объектам мультиагентных робототехнических систем с децентрализованным управлением // Научно-технический вестник информационных технологий, механики и оптики. – 2014. – № 3(91). – С. 30–38.
2. Комаров И.И., Дранник А.Л., Юрьева Р.А. Моделирование проблем информационной безопасности мультиагентных систем // В мире научных открытий. – 2014. – № 4(52). – С. 61–70.
3. Ramchurn S.D., Huynh D., Jennings N.R. Trust in multi-agent systems // Knowledge Engineering Review. – 2004. – V. 19. – № 1. – P. 1–25.
4. Бешта А.А., Кирпо М.А. Построение модели доверия к объектам автоматизированной информационной системы для предотвращения деструктивных воздействий на систему // Изв. ТПУ. – 2013. – Т. 322. – № 5. – С. 104–108.
5. Лаврушин О.И. Базовые основы теории кредита и его использование в современной экономике // Вопросы регулирования экономики. – 2017. – V. 8. – № 2. – P. 6–15.
6. Евтух А.Т. Теория кредита: социально-экономический аспект // Финансы и кредит. – 2005. – № 25(193). – С. 21–27.

**Менщиков Александр Алексеевич**
Год рождения: 1991
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, аспирант
Направление подготовки: 10.06.01 – Информационная безопасность
e-mail: menshikov@corp.ifmo.ru

**Комарова Антонина Владиславовна**
Год рождения: 1993
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, аспирант
Направление подготовки: 10.06.01 – Информационная безопасность
e-mail: piter-ton@mail.ru

**УДК 004.056**

# СПОСОБ ПОСТРОЕНИЯ ЗАЩИЩЕННОГО ВЕБ-РЕСУРСА С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ HONEYPOT И ДИНАМИЧЕСКОЙ ГЕНЕРАЦИЕЙ КОНТЕНТА

**Менщиков А.А., Комарова А.В.**
**Научный руководитель – д.т.н., профессор Гатчин Ю.А.**

Работа выполнена в рамках темы НИР № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность».

Современные информационные системы содержат огромное количество информации: коммерческой и личной. Любая информация подвержена утечкам по незащищенным каналам. Во всемирной сети существуют специальные программные средства, веб-роботы, которые несанкционированно собирают разного рода информацию. Владельцам веб-сайтов необходимо применять меры защиты от кражи своей информации. В работе рассмотрен подход по построению защищенного ресурса в сети Интернет. Непосредственно защита осуществлялась путем использования технологии Honeypot и динамической генерации контента сайта.
**Ключевые слова:** информационная безопасность, защита информации, веб-роботы, парсинг, сбор информации, технология Honeypot, обнаружение веб-роботов, динамическая генерация контента.

Любой веб-ресурс, даже не использующийся людьми в данный промежуток времени, каждый день посещается большим количеством веб-роботов (парсеров, краулеров) [1]. Эти роботы могут быть легитимными (они могут анализировать контент веб-ресурса, индексировать сайты для улучшения работы в поисковых системах и т.д.) и нелегитимными – т.е. роботами-злоумышленниками. Цель последних – эксплуатация уязвимостей сайта. Вредоносные парсеры рассылают рекламу, спам, совершают покупки, крадут информацию о товарах на сайте и многое другое [2]. Такие злонамеренные действия, в конечном счете, ведут к финансовым потерям владельца сайта: к проблемам доступа у легитимных пользователей, к уменьшению пропускной способности ресурса, увеличению траффика за единицу времени [3]. Трудность состоит в том, что парсеров не просто вычислить, так как они скрывают свое присутствие, маскируются под реальных людей, и могут иметь распределенную архитектуру. Но и краулеры имеют свои слабые стороны: их создатели стремятся держать баланс между стоимостью разработки и степенью защиты своего робота. Большинство парсеров имеют «универсальную» архитектуру, подходящую для большинства сайтов, но не для всех. Столкнувшись с «защищенным» ресурсом, веб-роботы могут не

только украсть заведомо подложную информацию, но и могут быть засечены, что в дальнейшем может привести к раскрытию своего «хозяина». Также, краулеры имеют слабую рефлексию результатов, т.е. в случае сбора очевидно ложной информации, «хозяин» может далеко не сразу зафиксировать этот факт и внести исправления. Несмотря на все вышесказанное, с каждым годом можно наблюдать увеличение объема парсинга на несколько процентов [4]. По этой причине создание способа построения защищенного веб-ресурса становится актуальной задачей.

В аналогичном направлении исследований работают и другие ученые, в том числе и несколько зарубежных коллективов, особенно стоит отметить исследователей из Wright State University [5].

Среди характеристик поведения пользователей веб-ресурса авторы выделяют временные, структурные, поведенческие, основанные на ошибках, и основанные на типе контента. Анализ этих категорий позволяет выявлять признаки, характерные для средств автоматизированного сбора информации (парсеров, краулеров). Обнаружение достигается за счет использования технических методов обнаружения, сигнатурных правил обнаружения и расчета статистических метрик поведения.

Для того чтобы выявить робота-злоумышленника, авторами предлагается использовать технологию Honeypot, что в переводе с английского «горшок с медом» или другими словами – приманка. Как следует из названия, Honeypot – это ресурс безопасности, предназначение которого – попасться злоумышленнику, навлечь на себя атаку [5]. Данный ресурс может являться и имитируемым сервисом, и полноценной операционной системой, может представлять собой как специальный выделенный сервер, так и один сетевой сервис, главной целью ресурса остается привлечение внимания взломщиков. После нападения владелец Honeypot может исследовать поведение парсера, изучить стратегию его поведения и таким образом определить, как могут быть нанесены удары по реально существующим объектам безопасности.

В качестве способов первичного обнаружения краулера могут использоваться скрытые для человеческого глаза разделы ресурса (ссылки или файлы), которые робот заполнит, а человек – нет; анализ структуры запроса, если запрос нехарактерен для легитимного пользователя; некоторые технические методы (анализ источников запросов, анализ правильности обработки активного содержимого и т.д.) [3].

Совокупность различных подходов к обнаружению позволяет осуществить точную корректировку обнаружения и управлять соотношением точности и полноты обнаружения, а также частотой ложных срабатываний.

Для изучения поведения краулера на веб-ресурсе, в него был встроен модуль динамической генерации правдоподобного контента на уровне рендеринга шаблонов списков и единиц данных. Для генерации использовались методы цепей Маркова и LSA с рандомизацией. Генерация производилась на основе корпуса существующих текстов из веб-ресурса, что позволило создавать тексты, мало отличимые от оригинала. Мы проанализировали разные выборки из текстов и различные параметры алгоритмов, но это не повлияло существенным образом на поведение веб-роботов на ресурсе, они продолжали свою активность даже будучи внутри Honeypot, что позволило изучить их действия, модифицируя структуру сайта и объем получаемых ими данных.

В связи с все большим ростом количества и активности веб-роботов, тема исследования на сегодняшний день является актуальной. Рассматриваемый в работе способ построения веб-ресурса показал свою эффективность и хорошие результаты по обнаружению и противодействию автоматизированному сбору информации. В дальнейшем авторами планируется увеличить выборку и создать универсальную библиотеку данных, которые могли бы использоваться и в других проектах. Работа в данном направлении будет способствовать дальнейшему развитию области, и может послужить хорошим базисом для будущих исследований.

**Литература**

1. Менщиков А.А., Комарова А.В., Гатчин Ю.А. Автоматизированное извлечение адресов из неструктурированных текстов // Интернет и современное общество: сборник тезисов докладов [Электронный ресурс]. – Режим доступа: http://ojs.ifmo.ru/index.php/IMS/issue/view/19, своб.
2. Menshchikov A., Komarova A., Gatchin Y.A., Korobeynikov A.G., Tishukova N. A Study of Different Web-Crawler Behaviour // Proceedings of the 20th Conference of Open Innovations Association FRUCT. – 2017. – P. 268–274.
3. Менщиков А.А., Комарова А.В., Гатчин Ю.А. Изучение поведения средств автоматизированного сбора информации с веб-ресурсов // Вопросы кибербезопасности. – 2017. – № 3(21). – С. 49–54.
4. Менщиков А.А., Гатчин Ю.А. Построение системы обнаружения автоматизированного сбора информации с веб-ресурсов // Инженерные кадры – будущее инновационной экономики России: Материалы Всероссийской студенческой конференции: в 8 ч. – 2015. – Т. 4. – С. 58–61.
5. Сайт Web and Complex Systems Lab [Электронный ресурс]. – Режим доступа: https://wsu-wacs.github.io/ (дата обращения: 10.03.2018).

**Мишина Надежда Сергеевна**
Год рождения: 1995
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N4160
Направление подготовки: 11.04.03 – Конструирование и технология электронных средств
e-mail: mishina_ns3108@mail.ru

**Мишин Ярослав Дмитриевич**
Год рождения: 1996
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N4160
Направление подготовки: 11.04.03 – Конструирование и технология электронных средств
e-mail: mishinyd@mail.ru

**Бондаренко Игорь Борисович**
Год рождения: 1972
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, к.т.н., доцент
e-mail: igorlitmo@rambler.ru

**УДК 004.032**

## ПРОБЛЕМЫ ПРИНЯТИЯ РЕШЕНИЙ В ИЕРАРХИЧЕСКИХ СИСТЕМАХ

**Мишина Н.С., Мишин Я.Д.**
**Научный руководитель – к.т.н., доцент Бондаренко И.Б.**

В работе рассмотрена теория иерархических многоуровневых систем, на основе которой строится математическая модель двухуровневой системы принятия решений. Рассмотрены основные признаки, присущие построенной модели, приведены проблемы, связанные с принятием решений в подобных иерархических системах.
**Ключевые слова:** иерархическая система, многоэшелонная структура, интеллектуальные агенты, математическая модель, проблемы принятия решений.

Каждый человек ежедневно сталкивается с ситуациями, когда от него требуется принятие какого-либо решения, при этом в тех случаях, когда принимаемое решение не связано с каким-либо материальным или социальным ущербом, в его основу ложится интуиция и опыт осуществляющего выбор субъекта [1]. Однако довольно распространен иной класс принятия решений, которые можно назвать ответственными, и которые влияют на дальнейшее развитие той или иной социальной, экономической или технической системы. В этом случае решение лица должно основываться не только на множестве критериев качества, но и на решениях других групп и субъектов иерархической системы, совокупная деятельность которой может активизировать определенный процесс и привести к требуемому результату.

Практически каждая современная система представляет собой иерархическую структуру, в которой у каждого ее элемента имеется своя цель, однако в совокупности они

способствуют функционированию единого процесса. Согласно теории иерархических многоуровневых систем М. Месаровича, структуры подобного типа называются многоэшелонными и представляются в виде относительно независимых, взаимодействующих между собой подсистем, некоторые (или все) из которых имеют право на принятие решений, а их иерархия определяется тем, что некоторыми подсистемами влияют или управляют вышестоящие из них [2].

Основной отличительной особенностью таких систем является предоставление подсистемам всех уровней определенной свободы в принятии решений, при этом возможно отличие этих решений от решений вышестоящих подсистем, что способствует росту эффективности ее функционирования в целом. Поскольку каждая подсистема обладает определенной свободой в выборе целей, такую иерархическую структуру называют также многоцелевой.

Можно выделить следующие общие черты, характерные для любой многоуровневой иерархической системы [3]:

1. прямая зависимость аспектов деятельности подсистемы от ее уровня;
2. прямая зависимость времени принятия решений от уровня подсистемы;
3. наличие более медленных аспектов поведения системы на более высоких ее уровнях.

Наиболее простой иерархической системой является такая, где все элементы низшего уровня находятся в подчинении единого органа высшего управления. В качестве примера рассмотрим двухуровневую многоцелевую систему принятия решений $C$ (рисунок), осуществляющую управление процессом $P$ и состоящую из одного вышестоящего (координирующего) элемента $C_0$ и $n$ подчиненных ему элементов $C_1$, $C_2$, …, $C_n$ [3]. Исследование подобных систем представляет интерес для теории многоуровневых систем по следующим причинам [4]:

1. система является простейшей для своего класса, при этом в ней прослеживаются все существенные особенности, характерные для многоуровневой системы;
2. система является базовым элементом при построении более сложных многоуровневых систем.

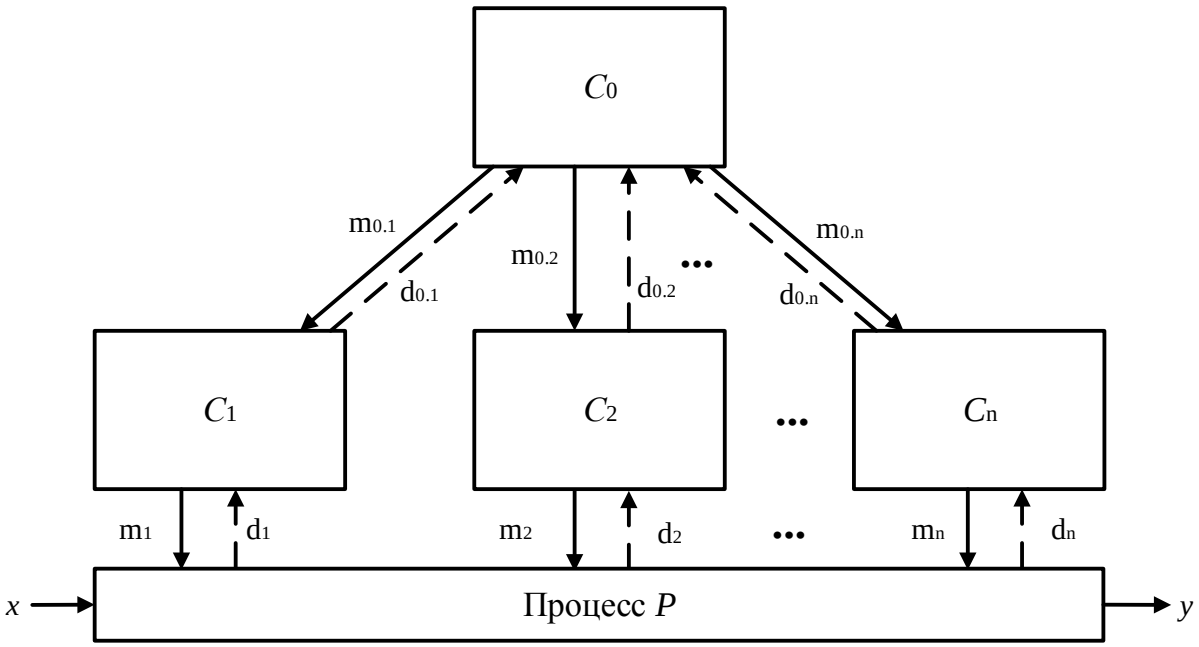



Рисунок. Модель двухуровневой многоцелевой иерархической системы

Процесс $P$ является управляемой подсистемой, на которую оказывают воздействия $m_1$, $m_2$, …, $m_n$ управляющие подсистемы $C_1$, $C_2$, …, $C_n$, а также возмущения $x$ из внешней среды. Эти управляющие подсистемы $C_1$, $C_2$, …, $C_n$ функционируют согласно координирующему сигналу $m_{0,1}$, $m_{0,2}$, …, $m_{0,n}$ от вышестоящей управляющей системы $C_0$.

Пунктирными линиями $d_{0,1}$, $d_{0,2}$, …, $d_{0,n}$ и $d_1$, $d_2$, …, $d_n$ на рисунке отражена существующая в системе отрицательная обратная связь, подразумевающая передачу информационных сигналов управляющей системе $C_0$ и системам $C_1$, $C_2$, …, $C_n$ соответственно. Выход $y$ процесса $P$ подразумевает выполнение некоторой общей цели, существующей в системе. Предположим, что непосредственная связь между $C_1$, $C_2$, …, $C_n$ отсутствует, а $C_0$ не имеет прямой связи с $P$.

Исследуемая иерархическая система обладает следующими видами целей:

1. цели управляемых/управляющих подсистем $C_1$, $C_2$, …, $C_n$;
2. цели координирующего органа $C_0$;
3. общая цель двухуровневой системы.

Проблемой принятия решений в подобной структурированной системе является то, что сама их природа хотя и подразумевает некоторую целенаправленную деятельность всех подсистем $C_1$, $C_2$, …, $C_n$, однако, при этом способствует предоставлению некоторой свободы в выборе их собственных решений, которые могут как соответствовать, так и не соответствовать решениям верхнего уровня $C_0$. В подобных иерархических структурах имеется вероятность формирования противоречащих друг другу («конфликтных») целей и решений, что, с одной стороны, препятствует непосредственному управлению ими, а, с другой, способствует росту эффективности функционирования системы при условии правильного сочетания имеющихся ограничений с поставленными целями и принятыми решениями. Разрешением подобных конфликтов занимается координирующий орган $C_0$, который, также преследуя собственные цели, посылает координационные сигналы подсистемам $C_1$, $C_2$, …, $C_n$, при этом содержание подобных сигналов формируется на основании информационных сигналов $d_{0,1}$, $d_{0,2}$, …, $d_0$, поступающих от подсистем $C_1$, $C_2$, …, $C_n$ и содержащих данные о проделанной ими работе. Поскольку прямое взаимодействие с процессом $P$ осуществляется только органами $C_1$, $C_2$, …, $C_n$, то достижение общей цели возможно только в случае совместимости всех задач, решаемых двухуровневой иерархической системой, что реализуется именно благодаря наличию некоторой свободы действий в принятии собственных решений, т.е. отсутствует жесткое управление координирующим органом $C_0$ действиями подсистем $C_1$, $C_2$, …, $C_n$.

Особенностью взаимодействия $C_0$ и $C_1$, $C_2$, …, $C_n$ является тот факт, что принимаемые решения последних зависят именно от решений координирующего органа, т.е. проблемы, которые решают элементы нижестоящего уровня $C_1$, $C_2$, …, $C_n$, зависят от того, какое действие предпринял вышестоящий элемент $C_0$. Одновременно с этим проблема, которую решает вышестоящий элемент $C_0$, зависит от действий, предпринимаемых элементами нижестоящего уровня $C_1$, $C_2$, …, $C_n$, что в совокупности с предыдущим утверждением составляет замкнутый круг, выход из которого осуществляется за счет введения приоритета действий для вышестоящего элемента $C_0$. Подобный приоритет позволяет не только указать нижестоящим элементам $C_1$, $C_2$, …, $C_n$ спектр их возможных действий, но и, в случае необходимости, побудить их к смене собственного решения [4].

Что касается влияния элементов нижестоящего уровня $C_1$, $C_2$, …, $C_n$ на координирующий орган $C_0$, оно может быть представлено либо непосредственно, либо косвенно, однако имеется всегда, поскольку достижение конечной общей цели $y$ системы в целом и цели $C_0$, в частности, зависит от действий, предпринимаемых нижестоящим уровнем $C_1$, $C_2$, …, $C_n$. В процессе информационного обмена, который осуществляется до принятия $C_0$ очередного решения $m_{0,i}$ ($m_{0,i} \in \{m_{0,1}, m_{0,2}, \ldots, m_{0,n}\}$), вышестоящий элемент обладает превосходством над управляемым элементом $C_i$ ($C_i \in \{C_1, C_2, \ldots, C_n\}$) и имеет возможность требовать от него информацию $d_{0,i}$ ($d_{0,i} \in \{d_{0,1}, d_{0,2}, \ldots, d_{0,n}\}$) нужного ему вида. Как правило, информация содержит решение, которое собирается принять $C_i$, что позволяет координатору $C_0$ оценить процесс принятия решения подсистемой $C_i$, которая, в свою очередь, может использовать $d_{0,i}$ в качестве дополнительной переменной,

определяющей принятое решение $m_i$ ($m_i \in \{m_1, m_2, \ldots, m_n\}$), что позволит обеспечить для себя более выгодные условия [4].

Одна из главных проблем принятия решений в подобной многоцелевой иерархической системе заключается в выборе того набора ограничений $\{l_{i,1}, l_{i,2}, \ldots, l_{i,n}\}$, которые необходимо наложить на каждую нижестоящую подсистему $C_i$ с целью обеспечения выполнения поставленных для системы $C$ задач. Отсюда прослеживается очевидный недостаток многоуровневой системы, выраженный наличием трудностей в анализе ее функционирования и управления ею, что в совокупности усложняет внешнее воздействие на нее.

Другой не менее значимой трудностью является начало работы («запуск») системы $C$, поскольку для этого необходимо, чтобы орган $C_0$ принял решение о функционировании нижестоящих органов, которое, по сути, не будет иметь под собой информационной базы $d_{0,1}, d_{0,2}, \ldots, d_{0,n}$ от $C_1, C_2, \ldots, C_n$. Получается, первая «волна» координирующих действий $m_{0,1}, m_{0,2}, \ldots, m_{0,n}$ будет основываться только на личных умозаключениях $C_0$, последующая корректировка которых будет осуществляться уже в процессе функционирования системы, а значит, важно то, насколько правильными являются принятые органом $C_0$ решения, и как быстро после «запуска» система скорректирует свои последующие действия для стабилизации своей работы.

В заключение стоит отметить, что, несмотря на ряд недостатков, многоцелевая иерархическая система является одной из самых распространенных и успешно функционирующих на сегодняшний день, ее реализацию можно наблюдать в организации как многих социальных (государство, предприятие и т.д.), так и физических систем (технические устройства). В настоящее время основными задачами в этой области являются совершенствование иерархической системы и автоматизация ее функционирования.

**Литература**

1. Андрейчикова О.Н., Джабер Ф.Ф., Андрейчикова А.В. Автоматизированное принятие решений в иерархических системах // Программные продукты и системы. – 1993. – № 3. – С. 23–29.
2. Месарович М., Мако Д., Такахара И. Теория иерархических многоуровневых систем. – М.: Мир, 1973. – 345 с.
3. Светлосанов В.А. Применение системного анализа в исследованиях природных систем. – М.: 11-й формат, 2009. – 99 с.
4. Гулякина Н.А. Общая теория систем. – Минск: Белорусский государственный университет информатики и радиоэлектроники, 2007. – 208 с.

**Бондарева Анастасия Дмитриевна**
Год рождения: 1995
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N4154
Направление подготовки: 10.04.01 – Информационная безопасность
e-mail: Bondareva.AD@yandex.ru

**Созинова Екатерина Николаевна**
Год рождения:1986
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, к.т.н., доцент
e-mail: s.ekaterina-nik@mail.ru

**УДК 004.056**

# МОДЕЛЬ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМАХ ТИПА «УМНЫЙ ДОМ»

**Бондарева А.Д., Созинова Е.Н.**
**Научный руководитель – к.т.н., доцент Созинова Е.Н.**

Работа выполнена в рамках темы НИР № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность».

В работе были исследованы существующие методики разработки модели нарушителя. Классифицированы нарушители информационной безопасности систем типа «Умный дом». Предложена модель нарушителя для таких систем.
**Ключевые слова:** автоматизированная система управления зданием, «Умный дом», защита информации, нарушитель информационной безопасности, угрозы безопасности информации.

При обеспечении информационной безопасности (ИБ) любой автоматизированной системы необходимо исследовать все возможные источники угроз ИБ, как главной составляющей возможных каналов воздействия на защищаемую информацию или ее перехвата. Наиболее опасными из них являются антропогенные источники, а именно люди, которые могут реализовать угрозы безопасности информации (БИ) как умышленно, так и случайно.

Так как на данный момент отсутствует общий регламент по защите информации (ЗИ) в решениях задач в системах типа «Умный дом» (УД), то в целях создания единого обобщенного подхода к обеспечению ИБ УД очевидна постановка задачи разработки модели нарушителя ИБ конкретно для системы УД.

Для решения поставленной задачи было проведено исследование законодательной и нормативно-правовой базы Российской Федерации (РФ) в области информационной безопасности, проведен анализ научной литературы и методических рекомендаций ФСТЭК и ФСБ России по составлению моделей нарушителя. На основе результатов исследования, представленных в табл. 1, был определен структурный базис модели нарушителя УД.

Таблица 1. Сравнение структур модели нарушителя

<table>
<tr><td>СТО БР ИББС-1.0-2014 Обеспечение ИБ организаций БС РФ [1]</td><td>Методика определения УБИ в информационных системах (ИС) [2]</td><td colspan="2">Модель угроз и нарушителя безопасности персональных данных (ПДн), обрабатываемых в типовых ИСПДн отрасли [3]</td><td>Методические рекомендации ФСБ [4]</td></tr>
<tr><td rowspan="3">Описание и классификация нарушителей ИБ</td><td>Типы нарушителей</td><td rowspan="3">Описание нарушителей ИБ</td><td>Категории нарушителей</td><td rowspan="3">Описание нарушителей (субъектов атак)</td></tr>
<tr><td>Виды нарушителей</td><td></td></tr>
<tr><td>Потенциал нарушителей</td><td>Возможности нарушителей</td></tr>
<tr><td>Возможная мотивация действий</td><td>Мотивация</td><td colspan="2" rowspan="3"></td><td>Цель атаки</td></tr>
<tr><td>Опыт</td><td rowspan="2">Компетентность</td><td></td></tr>
<tr><td>Знания</td><td>Имеющаяся информация об объекте атаки</td></tr>
<tr><td>Доступные ресурсы, необходимые для реализации угрозы</td><td>Ресурсы, требуемые для реализации угроз БИ</td><td colspan="2">Имеющиеся у нарушителя средства атак</td><td>Имеющиеся у нарушителя средства атак</td></tr>
<tr><td>Способ реализации угроз ИБ со стороны указанных нарушителей</td><td>Способы реализации угроз БИ</td><td colspan="2">Описание каналов атак</td><td>Описание каналов атак</td></tr>
<tr><td></td><td></td><td colspan="2">Тип нарушителя при использовании криптографических средств защиты информации (СКЗИ)</td><td>Объект атаки</td></tr>
</table>

Таким образом, представляется целесообразным разработать модель нарушителя УД по общим пунктам исследованных документов. Также следует принять во внимание модель автоматизированной системы управления зданием (АСУЗ) «Умный дом» [5], а именно исследовать нарушителей на каждом уровне системы.

При составлении обобщенной модели нарушителя, представленной в табл. 2, нарушители были подразделены на внешних и внутренних. Однако при составлении актуальной модели нарушителя для конкретной системы УД следует учитывать и комбинированного нарушителя, как совместные или согласованные действия внутреннего и внешнего, обладающего всеми их знаниями, возможностями и ресурсами. Также в соответствии с [5] объектами атаки являются защищаемая информация, оборудование, на котором она хранится, а также устройства системы УД.

Таблица 2. Модель нарушителя для систем типа УД

<table>
<tr><td>Уровень</td><td>Операторского управления</td><td>Автоматического управления</td><td>Исполнительных устройств</td></tr>
<tr><td colspan="4">Виды нарушителей</td></tr>
<tr><td rowspan="3">Внутренний</td><td colspan="3">Пользователи УД</td></tr>
<tr><td colspan="3">Посетители и обслуживающий персонал помещения (здания)</td></tr>
<tr><td colspan="3">Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ, обеспечивающих функционирование АСУЗ</td></tr>
<tr><td rowspan="5">Внешний</td><td colspan="3">Разработчики, производители, поставщики программных, технических и программно-технических средств (ПТС)</td></tr>
<tr><td>Террористические, экстремистские группировки</td><td rowspan="3"></td><td rowspan="4">Криминальные элементы, представители преступных организаций</td></tr>
<tr><td>Лица, организующие DoS-атаки</td></tr>
<tr><td>Криминальные элементы</td></tr>
<tr><td colspan="2">Лица, разрабатывающие или распространяющие вирусы и другие вредоносные программные коды</td></tr>
<tr><td colspan="4">Посторонние лица, пытающиеся получить доступ к защищаемой информации в инициативном порядке</td></tr>
<tr><td colspan="4">Потенциал нарушителей</td></tr>
<tr><td>Внутренний</td><td>Низкий</td><td colspan="2">Средний</td></tr>
<tr><td>Внешний</td><td>Низкий</td><td>Высокий</td><td>Средний</td></tr>
<tr><td colspan="4">Возможности нарушителей</td></tr>
<tr><td rowspan="3">Внутренний</td><td colspan="3">Возможность проводить атаки в пределах контролируемой зоны (КЗ), с физическим доступом к средствам вычислительной техники (СВТ), линиям связи, системам электропитания и заземления</td></tr>
<tr><td colspan="3">Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты УД</td></tr>
<tr><td colspan="3">Возможность изменять конфигурацию технических средств обработки информации (ТСОИ), вносить программно-аппаратные закладки в ПТС УД и обеспечивать съем информации, используя непосредственное подключение к ТСОИ</td></tr>
<tr><td rowspan="5">Внешний</td><td colspan="3">Возможность внесения недекларированных возможностей (НДВ), программных закладок, вредоносных программ в программное обеспечение (ПО) УД на стадии его разработки, внедрения и сопровождения</td></tr>
<tr><td>Возможность несанкционированного доступа (НСД) из общественных сетей связи</td><td></td><td rowspan="2"></td></tr>
<tr><td colspan="2">Возможность создания и применения специальных технических средств (ТС) для добывания или воздействия на информацию или ТС, распространяющейся в виде физических полей или явлений</td></tr>
<tr><td colspan="3">Возможность создавать способы атак, осуществлять их подготовку и проведение за пределами КЗ</td></tr>
<tr><td colspan="3">Возможность привлекать специалистов, имеющих опыт разработки и анализа оборудования УД</td></tr>
<tr><td colspan="2">Возможность доступа к проводным каналам или к зоне устойчивого перехвата радиосигналов сети</td><td></td></tr>
</table>

<table>
<tr><td>Уровень</td><td>Операторского управления</td><td>Автоматического управления</td><td>Исполнительных устройств</td></tr>
<tr><td colspan="4">Мотивация</td></tr>
<tr><td rowspan="2">Внутренний</td><td colspan="3">Причинение имущественного ущерба путем обмана или злоупотребления доверием</td></tr>
<tr><td colspan="3">Непреднамеренные, неосторожные или неквалифицированные действия</td></tr>
<tr><td rowspan="4">Внешний</td><td>Совершение террористических актов</td><td rowspan="3"></td><td rowspan="3">Причинение имущественного ущерба путем мошенничества или иным преступным путем</td></tr>
<tr><td>Идеологические или политические мотивы</td></tr>
<tr><td>Причинение имущественного ущерба путем мошенничества или иным преступным путем</td></tr>
<tr><td colspan="3">Выявление уязвимостей с целью их продажи и получения финансовой выгоды</td></tr>
<tr><td colspan="4">Любопытство или желание самореализации</td></tr>
<tr><td colspan="4">Опыт</td></tr>
<tr><td rowspan="2">Внутренний</td><td colspan="3">Для непреднамеренных воздействий (НПВ) специфический опыт не требуется</td></tr>
<tr><td rowspan="2">Опыт работы в области применения информационных технологий или в области ЗИ</td><td rowspan="2">Опыт настройки и работы с оборудованием УД (логическими контроллерами, датчиками и т.д.)</td></tr>
<tr><td>Внешний</td></tr>
<tr><td colspan="4">Знания</td></tr>
<tr><td rowspan="5">Внутренний</td><td colspan="3">Сведения о мерах ЗИ, применяемых в информационной системе данного типа</td></tr>
<tr><td colspan="3">Сведения о структурно-функциональных характеристиках и особенностях функционирования УД</td></tr>
<tr><td>Легальное имя доступа</td><td rowspan="3">Сведения в конструкторской документации на аппаратные и программные компоненты УД</td></tr>
<tr><td>Защищаемая информация</td></tr>
<tr><td>Сведения о физических мерах защиты АСУЗ</td></tr>
<tr><td rowspan="3">Внешний</td><td colspan="3">Общедоступная информация об уязвимостях отдельных компонент АСУЗ</td></tr>
<tr><td colspan="3">Сведения о мерах ЗИ, применяемых в информационной системе данного типа</td></tr>
<tr><td>Информация о возможных способах атак</td><td></td><td></td></tr>
<tr><td colspan="4">Доступные ресурсы, необходимые для реализации угрозы</td></tr>
<tr><td rowspan="2">Внутренний</td><td colspan="3">Штатные средства АСУЗ</td></tr>
<tr><td colspan="3" rowspan="2">Доступные в свободной продаже аппаратные средства и ПО, в том числе программные и аппаратные компоненты СКЗИ</td></tr>
<tr><td rowspan="3">Внешний</td></tr>
<tr><td colspan="3">Специально разработанные ТС и ПО</td></tr>
<tr><td colspan="2">Средства перехвата и анализа информационных потоков в каналах связи</td><td rowspan="2"></td></tr>
<tr><td colspan="2">Специальные ТС перехвата информации по ТКУИ</td></tr>
<tr><td colspan="4">Способ реализации угроз ИБ со стороны указанных нарушителей</td></tr>
<tr><td rowspan="3">Внутренний</td><td colspan="3">НПВ на информацию</td></tr>
<tr><td colspan="2">НСД к панели оператора или управляющему устройству</td><td></td></tr>
<tr><td colspan="3">Преднамеренные воздействия (ПНВ) на защищаемую информацию, носители информации, датчики, логические устройства и электроприборы</td></tr>
<tr><td rowspan="2">Внешний</td><td colspan="3">ПНВ на информацию и средства, НСД через незащищенные каналы связи</td></tr>
<tr><td>Перехват информативных сигналов по техническим каналам утечки информации (ТКУИ)</td><td></td><td>ПНВ на средства, расположенные за пределами КЗ</td></tr>
</table>

| Уровень | Операторского управления | Автоматического управления | Исполнительных устройств |
|---|---|---|---|
| | | | Атаки на сигнальные цепи, цепи электропитания и заземления |
| | Атаки, основанные на использовании уязвимостей и НДВ средств зашиты, внесенные в процессе создания, перевозки, внедрения, наладки этих средств | | |

Таким образом, можно сделать вывод о том, что более всего для нарушителя интересен уровень операторского управления, так как именно на данном уровне нарушитель имеет больше всего возможностей, ресурсов и знаний, обладает высоким потенциалом для реализации угроз БИ.

**Заключение.** В результате данной работы:
1. разработана обобщенная модель нарушителя ИБ систем типа «Умный дом»;
2. исследованы возможные нарушители для каждого уровня АСУЗ «Умный дом»;
3. полученные результаты предлагается использовать для актуализации модели угроз при создании системы защиты информации УД.

**Литература**

1. Стандарт банка России СТО БР ИББС-1.0-2014. Обеспечение информационной безопасности организации банковской системы Российской Федерации. Общие положения [Электронный ресурс]. – Режим доступа: https://www.cbr.ru/credit/Gubzi_docs/st-10-14.pdf, своб.
2. Методика определения угроз безопасности информации в информационных системах. Проект [Электронный ресурс]. – Режим доступа: https://fstec.ru/component/attachments/download/812, своб.
3. Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли [Электронный ресурс]. – Режим доступа: http://minsvyaz.ru/common/upload/publication/1410084of.pdf, своб.
4. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_126992/, своб.
5. Бондарева А.Д., Созинова Е.Н., Фаязов К.А. Модель защищаемой информации в системах типа «Умный дом» // Научно-технический вестник Поволжья. – 2017. – № 6. – С. 173–175.

**Мухамеджанов Данияр Давлетович**
Год рождения: 1992
Университет ИТМО, факультет безопасных информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N4250
Направление подготовки: 10.04.01 – Информационная безопасность
e-mail: mdonic92@gmail.com

**Ряскин Глеб Александрович**
Год рождения: 1995
Университет ИТМО, факультет безопасных информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N4154
Направление подготовки: 10.04.01 – Информационная безопасность
e-mail: ryaskingleb20@gmail.com

**Таранов Сергей Владимирович**
Год рождения: 1991
Университет ИТМО, факультет безопасных информационных технологий, кафедра проектирования и безопасности компьютерных систем, аспирант
Направление подготовки: 10.06.01 – Информационная безопасность
e-mail: serg.tvc@mail.ru

**УДК 004.052.42+ 004.056.2**

# ПРИМЕНЕНИЕ СПЛАЙН-ВЕЙВЛЕТОВ ВТОРОГО ПОРЯДКА НА СЕТКЕ, ГЕНЕРИРУЕМОЙ КЛЕТОЧНЫМИ АВТОМАТАМИ

**Мухамеджанов Д.Д., Ряскин Г.А., Таранов С.В.**
**Научный руководитель – к.ф.-м.н., доцент Левина А.Б.**

Работа выполнена в рамках темы НИР № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность».

Вейвлетные преобразования находят широкое применение для сжатия, фильтрации и анализа сигналов. В работе проанализировано влияние метода генерации сетки для сплайн-вейвлетных разложений второго порядка на параметры сжатия исходного сигнала. Предложен метод создания сетки на основе клеточных автоматов, дающий лучшие показатели сжатия для сплайн-вейвлетных преобразований второго порядка.
**Ключевые слова:** вейвлет-преобразование, сплайны, клеточные автоматы, сжатие, обработка сигналов.

Одной из основных проблем киберфизических систем является обработка больших объемов данных, поэтому разработка новых и эффективных алгоритмов сжатия сигналов различной природы является актуальной задачей. В связи с этим последние десятилетия отмечены возрождением интереса к локальной аппроксимации и, в частности, к сплайнам и вейвлетам [1–3]. Это объясняется широким применением последних при обработке больших объемов информации, сжатии информации и фильтрации [4, 5]. Основная задача обработки с помощью – сокращение объема числового потока за счет выявления и отбрасывания несущественных (с той или иной точки зрения) частей [6]. Основная идея вейвлетного

разложения заключается в том, что информационный поток можно разделить на составляющие таким образом, чтобы можно было выделить основной информационный поток и уточняющий поток. Первый поток обычно называется основным, а второй – дополнительным.

Вейвлетное разложение потока на составляющие может осуществляться более одного раза. На втором шаге/уровне вейвлетного разложения основной поток по аналогии с исходной последовательностью, разделяется на две составляющие. В итоге результатом второго уровня разложения является основной поток и два вейвлетных потока, которые могут при необходимости отбрасываться либо наоборот уточнять основной поток. Процесс перехода от исходного информационного потока к двум его составляющим называется декомпозицией, а соответствующие формулы – формулами декомпозиции. Для сплайн-вейвлетного преобразования помимо самого информационного потока необходима сетка равной длины, состоящая из элементов того же поля, что и исходный поток. К тому же нужно определить номера элементов изначального информационного потока, которые будут из него выбрасываться.

При сплайн-вейвлетном преобразовании из начального информационного потока выбрасывается элемент (или блок элементов), поэтому последовательность, получившаяся после подобного преобразования, представляет собой измененную версию исходного потока. Поток, получившийся в результате подобного изменения, является основным потоком. Результатом процесса декомпозиции является элемент дополнительного или вейвлетного потока. Для сплайн-вейвлетного преобразования необходима сетка элементов, которая вместе с исходным потоком модифицируется путем выбрасывания из нее блока элементов.

Таким образом, для формулы декомпозиции второго порядка необходимо дополнительно определить сетку, которая будет оказывать влияние на параметры возможного сжатия, фильтрации, уточнения исходного сигнала. В данной работе сетка для вейвлет-преобразования задавалась с помощью клеточных автоматов. Клеточный автомат представляет собой динамическую систему с дискретными изменениями состояний в каждый момент времени.

Клеточный автомат обладает следующими свойствами.

1. Можно рассматривать как множество конечных автоматов.
2. Каждая клетка (ячейка) может находиться в одном из состояний в конечном множестве.
3. Изменение состояния каждой клетки зависит от состояния ее соседей и состояния самой клетки на данный момент времени. Множество соседей называют окружением клетки.
4. Переходы состояний могут описываться «правилами».

Простейшим клеточным автоматом будет одномерный клеточный автомат с двумя возможными состояниями, а соседями клетки будут смежные с ней клетки. Такие автоматы называются элементарными. Три клетки (центральная, ее соседи) порождают 8 комбинаций состояний этих трех клеток. Далее на основе анализа текущего состояния тройки принимается решение о том, будет ли центральная клетка 1 или 0 на следующем шаге. Всего существует 256 возможных правил, которые кодируются в соответствии с кодом Вольфрама.

Например, правило 30 можно представить, как последовательность логических операций или в виде таблицы состояний (табл. 1).

Таблица 1. Правило 30 для клеточного автомата

| 111 | 110 | 101 | 100 | 011 | 010 | 001 | 000 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 |

Для эксперимента были построены программные модели простейших клеточных автоматов. Неравномерная сетка для сплайн-вейвлетного разложения второго порядка генерировалась правилами 22 и 193. В качестве сетки использовались с 100 по 220 уровни эволюции автомата. На каждом уровне первые 4 бита задают элемент сетки в 16 системе счисления. Последующие 4 бита задают количество выбрасываемых элементов на одном

этапе разложения. Всего в эксперименте было задано 120 элементов исходного потока и для данного потока, используя клеточные автоматы, была сгенерирована сетка по вышепредставленному алгоритму.

В табл. 2 представлено сравнение существующих методов выбора сетки и предложенного в работе метода на основе клеточных автоматов.

Таблица 2. Сравнение методов генерации сетки

| Метод задания сетки и выбрасывания элементов | Количество сохраняемых элементов исходного потока | Шаг сетки | Количество единовременно выбрасываемых узлов | Коэффициент сжатия $Q$ после 3 уровня разложения |
|---|---|---|---|---|
| Метод с оценкой априорной информации | <8 | 4, 5, 6 | $2\times N$ | 0,8743 |
| Равномерная сетка с фиксированным шагом | <8 | 4, 5, 6 | 8 | 0,8623 |
| Сетка на основе клеточного автомата правило 193 | <8 | 4 | 1–16 | 0,8273 |
| Сетка на основе клеточного автомата правило 22 | <8 | 4 | 1–16 | 0,8426 |

В табл. 2 переменная $N$ обозначает уровень разложения в формуле сплайн-вейвлетного преобразования. В отличие от существующих методов сетка и выбрасываемые элементы зависят от исходного потока, что позволяет подстроиться под конкретные значения исходного потока. Если в других методах элементы выбрасываются независимо от исходных значений, в результате чего может быть потеряна информация в исходном потоке, либо каким-то образом искажена (смазанные участки на изображении, усредненные значения в экспериментальных данных), то в предложенном методе сетка коррелирует с исходными значениями, что позволяет добиться лучшего показателя сжатия.

Алгоритмы задания сеток в сплайн-вейвлетных разложениях оказывают прямое влияние на параметры алгоритмов сжатия данных, таких как соотношение сжатия и качества восстанавливаемого сигнала. Сплайн-вейвлетные разложения являются крайне полезными при работе с большими массивами данных, а также при обработке экспериментальных данных (очистка от шумов, выделение областей интереса), вейвлет-преобразование дает наиболее наглядную и информативную картину результатов эксперимента, позволяет очистить исходные данные от шумов и случайных искажений, и даже выделить некоторые особенности анализируемых данных.

В результате данной работы:

1. был разработан метод генерации сетки на основе клеточных автоматов для сплайн-вейвлетных разложений второго порядка;
2. исследованы характеристики разработанной конструкции и проведено сравнение с аналогичными методами;
3. предложены области применения разработанного метода.

**Литература**

1. Демьянович Ю.К., Ходаковский В.А. Введение в теорию вейвлетов. Курс лекций. – СПб.: Изд-во ПГУПС, 2007. – С. 49.
2. Демьянович Ю.К., Косогоров О.М. О параллельном вэйвлетно-сплайновом адаптивном сжатии // Процессы управления и устойчивость. Труды 38-й международной научной конференции аспирантов и студентов. – 2007. – С. 152–155.

3. Демьянович Ю.К., Косогоров О.М. Алгоритмы параллельного вейвлетно-сплайного адаптивного сжатия. Высокопроизводительные параллельные вычисления на кластерных системах // Материалы шестого Международного научно-практического семинара. – 2007. – Т. 1. – С. 169–175.
4. Левина А.Б. О вэйвлетных разложениях линейных пространств над произвольным полем и о некоторых приложениях // Журнал Математическое моделирование. – 2008. – Т. 20. – С. 104–108.
5. Добеши И. Десять лекций по вейвлетам. – Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001. – 464 с.
6. Левина А.Б., Сплайн-вэйвлеты и их некоторые применения: дис. на соиск. учен. степ. канд. физ.-мат. наук. – М., 2009. – 215 с.


**Позволенко Виталий Александрович**
Год рождения: 1995
Университет ИТМО, факультет безопасных информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N4151
Направление подготовки: 10.04.01 – Информационная безопасность
e-mail: frozensculpture@gmail.com

**Воробьева Алиса Андреевна**
Год рождения: 1986
Университет ИТМО, факультет безопасных информационных технологий, кафедра проектирования и безопасности компьютерных систем, к.т.н., доцент
e-mail: alice_w@mail.ru

**УДК 004.85**

# АНАЛИЗ УТЕЧЕК ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ DLP И МЕТОДОВ ЛИНГВИСТИЧЕСКОЙ ИДЕНТИФИКАЦИИ

**Позволенко В.А.**
**Научный руководитель – к.т.н., доцент Воробьева А.А.**

Работа выполнена в рамках темы НИР № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность».

В работе рассмотрены существующие методы расследования компьютерных преступлений, указаны их недостатки, проанализирована возможность использования методов лингвистической идентификации в расследовании с применением DLP-систем и разработан метод расследования утечек конфиденциальной информации.
**Ключевые слова:** информационная безопасность, DLP, киберинцидент, утечка данных, лингвистическая идентификация.

С течением времени количество компьютерных преступлений интенсивно растет, появляются все новые и новые методы защиты информации. Одним из видов киберинцидентов является утечка конфиденциальной информации, следовательно, возникает необходимость разработки методов их расследования с целью нахождения источника утечки и применения санкций по отношению к нему.

Потенциальным источником утечки конфиденциальной информации в организации является любой сотрудник, вне зависимости от его должности и предоставленных ему прав доступа к информации конфиденциального характера.

Целью исследования являлась разработка метода проведения постинцидентного анализа утечек информации конфиденциального характера. В ходе исследования были поставлены следующие задачи:

- анализ существующих методов расследования утечек;
- анализ возможности использования методов лингвистической идентификации в связке с существующими методами;
- разработка метода проведения постинцидентного анализа;
- сбор данных для эксперимента и получения результатов;
- оценка итоговых результатов применения методов лингвистической идентификации при расследовании.

В качестве методов расследования были кратко рассмотрены SIEM-системы, DLP-системы и «Мониторинг СМИ и социальных сетей» [1, 2]. Основным недостатком SIEM и DLP является то, что они не действуют вне периметра организации. Также особенностью DLP является то, что система предотвращает утечки и не позволяет полноценно работать с уже произошедшими инцидентами. Исходя из этого, можно с уверенностью сказать, что утечка конфиденциальной информации способна произойти за пределами организации с использованием личных мобильных телефонов и компьютерной техники. Лингвистическая идентификация автора по его сообщениям способна компенсировать этот недостаток путем установления источника утечки, но в данной работе она имеет смысл после того, как утечка уже произошла.

В ходе работы был разработан пошаговый метод проведения постинцидентного анализа, для которого необходимо:

1. собрать сообщения $M$ от пользователей $U$;
2. извлечь лингвистические признаки $F$ [3] из $M$;
3. извлечь $F$ из сообщения с конфиденциальной информацией $m_{conf}$;
4. определить автора $m_{conf}$;
5. проанализировать получившиеся результаты.

На первом этапе было собрано множество сообщений от множества пользователей, посредством DLP-системы контура информационной безопасности (КИБ) SearchInform, а именно с помощью модулей: MailSniffer, FTPSniffer, HTTPSniffer. Перехваченные данные были в текстовом виде.

На втором и третьем этапах было произведено извлечение лингвистических признаков, алгоритм показан на рис. 1.

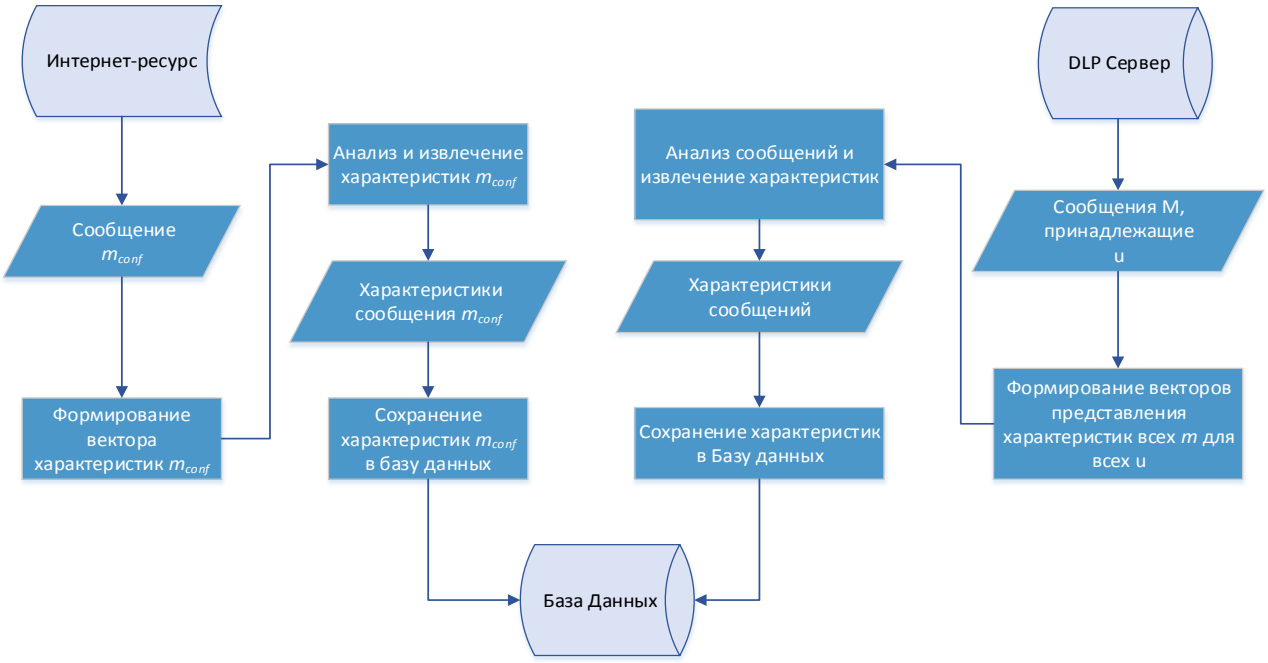



Рис. 1. Извлечение лингвистических признаков

Четвертым этапом являлось определение источника утечки. Из компьютерной системы получен список пользователей и их сообщений. Затем произведено извлечение характеристик их сообщений, после чего произведено разделение данных на обучающую и тестовую выборки. На этих данных построен алгоритм модели классификации, который проходил тестирование. После этого тестирования получен классификатор, на вход которого подавалось сообщение с конфиденциальной информацией, а на выходе получен список вероятных авторов сообщения с информацией конфиденциального характера.

Этап анализ и оценки происходил по следующему алгоритму, показанному на рис. 2.

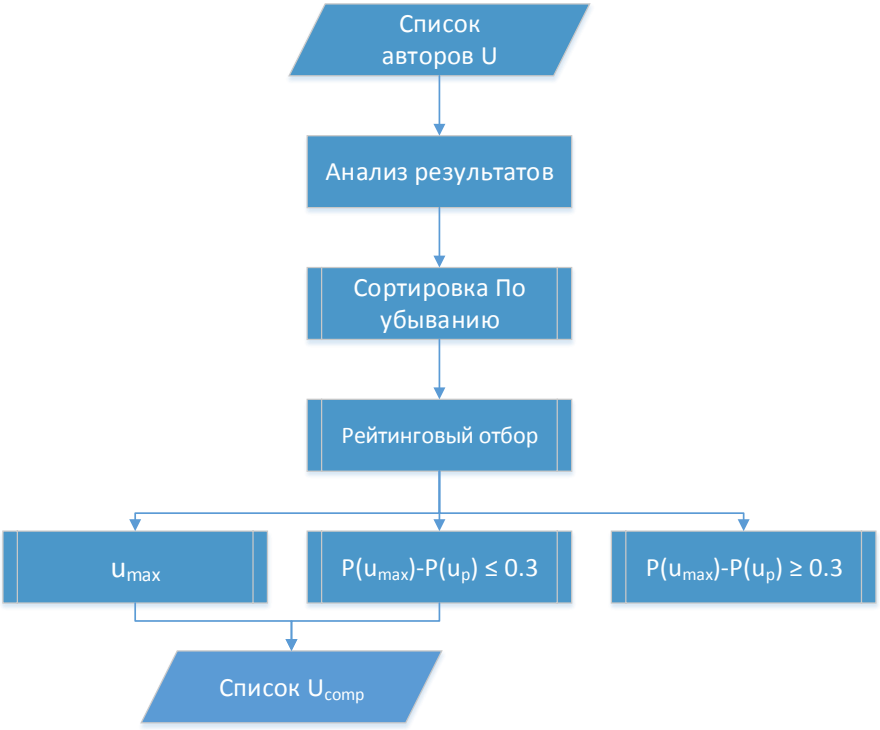



Рис. 2. Анализ и оценка результатов

В результате работы удалось установить точность идентификации верно определенных источников утечки – 75,69%. Количество пользователей на один набор сообщений было равно 10, среднее количество сообщений на один набор – 231, а среднее количество символов в одном сообщении составляло 1200.

Дальнейшие планы по исследованию предполагают рассмотреть возможность выявления методов стеганографии, а также определить влияние этих методов на лингвистические характеристики автора сообщения.

**Литература**

1. Расследование утечки: капля за каплей [Электронный ресурс]. – Режим доступа: https://www.osp.ru/cio/2013/11/13038649/ (дата обращения: 05.12.2017).
2. Федотов Н.Н. Расследование инцидентов ИБ: Как расследовать разглашение конфиденциальной информации в блогах и форумах? [Электронный ресурс]. – Режим доступа: http://forensics.ru/investigation_blogs.html (дата обращения: 04.12.2017).
3. Воробьева А.А. Идентификация автора анонимных сообщений Интернет-порталов на русском языке: отчет о НИР. – СПб.: Университет ИТМО, 2015. – 44 с.

**Садикова Анастасия Александровна**
Год рождения: 1997
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N3456
Направление подготовки: 10.03.01 – Информационная безопасность
e-mail: nastya.sadkoo@mail.ru

**Двойникова Анастасия Александровна**
Год рождения: 1996
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N3455
Направление подготовки: 10.03.01 – Информационная безопасность
e-mail: titova.yulishna@mail.ru

**Титова Юлия Алексеевна**
Год рождения: 1996
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N3456
Направление подготовки: 10.03.01 – Информационная безопасность
e-mail: titova.yulishna@mail.ru

**УДК 004.49**

# АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ПОСТРОЕНИИ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ ДЛЯ УЧРЕЖДЕНИЙ ИСПОЛНИТЕЛЬНЫХ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ

**Садикова А.А., Двойникова А.А., Титова Ю.А.**
**Научный руководитель – к.т.н., доцент Кузнецов А.Ю.**

Безопасность информации в автоматизированной системе базируется на способности этой системы сохранять конфиденциальность при обработке, передаче, хранении данных, а также на способности противостоять их разрушению, хищению. К автоматизированной системе в защищенном исполнении также предъявляется требование доступности циркулирующей в ней информации. В работе проанализированы методы защиты информации при проектировании различных автоматизированных систем в защищенном исполнении для учреждений органов государственной власти.
**Ключевые слова:** автоматизированная система в защищенном исполнении, защита информации, ФСТЭК, ИСПДн, АСУ ТП, ГИС.

Для обработки информации, необходимость защиты которой определяется законодательством Российской Федерации (РФ) или решением ее обладателя, должны создаваться автоматизированные системы в защищенном исполнении (АСЗИ), в которых реализованы в соответствии с действующими нормативными правовыми актами требования о защите информации (ЗИ) [1].

Проблема защиты информации в автоматизированных системах является актуальным с начала использования средств вычислительной техники для обработки информации. Реальность угроз информации в автоматизированных системах (АС) и высокая мера их

опасности, как показывает практика, остается и в настоящее время. Существует большое количество каналов для несанкционированного проникновения к информации и способов использования этих каналов [2].

Цель работы – проанализировать методы ЗИ при проектировании различных АСЗИ для учреждений органов государственной власти.

Процесс создания АСЗИ подразумевает выполнение комплекса мероприятий, которые направлены на разработку и применение информационной технологии, занимающиеся ЗИ, установленные в соответствии с требованиями стандартов и (или) нормативных документов по ЗИ как во вновь создаваемых, так и в действующих автоматизированных системах.

При создании (модернизации) АСЗИ необходимо руководствоваться следующими общими требованиями:

- система ЗИ АСЗИ должна обеспечивать комплексное решение задач по ЗИ от несанкционированного доступа (НСД), от утечки защищаемой информации по техническим каналам, от несанкционированных и непреднамеренных воздействий на информацию (на носители информации) применительно к конкретной АСЗИ;
- система ЗИ АСЗИ должна разрабатываться (проектироваться) с учетом возможности реализации требований о защите обрабатываемой информации при использовании в АСЗИ методов и программно-аппаратных средств организации сетевого взаимодействия;
- система ЗИ АСЗИ должна создаваться с учетом обеспечения возможности формирования различных вариантов ее построения, а также расширения возможностей ее составных частей (сегментов) в зависимости от условий функционирования АСЗИ и требований о ЗИ;
- ЗИ должна обеспечиваться во всех составных частях (сегментах) АСЗИ, используемых в обработке защищаемой информации;
- входящие в состав АСЗИ средства ЗИ и контроля эффективности ЗИ не должны препятствовать нормальному функционированию АСЗИ;
- программное обеспечение системы ЗИ должно быть совместимым с программным обеспечением других составных частей (сегментов) АСЗИ и не должно снижать требуемый уровень защищенности информации в АСЗИ;
- программно-технические средства, используемые для построения системы ЗИ, должны быть совместимы между собой (корректно работать совместно) и не должны снижать уровень защищенности информации в АСЗИ [1].

В работе рассмотрена ЗИ в таких автоматизированных системах, как: информационная система персональных данных (ИСПДн), автоматизированная система управления технологическими процессами (АСУ ТП), государственная информационная система (ГИС).

Вопросы выполнения требований по защите персональных данных (ПДн) не теряют своей актуальности. На основе Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (ПП № 1119) был разработан приказ ФСТЭК от 18 февраля 2013 г. № 21 (приказ № 21), в котором описаны состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн. Данный приказ позволяет операторам ПДн отказываться от базовых мер в сторону компенсирующих, учитывая их экономическую целесообразность. Требования к классам сертифицированных средств защиты информации (СЗИ) приведены к уровням защищенности (УЗ) [3]. УЗ ИСПДн определяется согласно ПП № 1119. Для каждого из четырех УЗ ПДн предполагаются соответствующие им способы, обеспечивающие безопасность ПДн. В приказе № 21 обозначено 109 мер защиты, которые классифицированы в 15 групп, из которых 40 мер являются компенсирующими. После определения списка мер и

проверки нейтрализации ими актуальных угроз, оператор должен добавить к текущему списку меры, предусмотренные другими нормативными актами (например, ПП № 1119, Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»). В итоге получается окончательный список мер, необходимых к выполнению.

Приказ ФСТЭК от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (приказ № 31) разработан во исполнение поручения Президента РФ. Он должен подкреплять Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», который вступил в силу с 01 января 2018 г. ФСТЭК признает, что в АСУ ТП возможно применение СЗИ, сертифицированных в ФСТЭК, либо прошедших оценку соответствия по Федеральному закон от 27.12.2002 № 184-ФЗ «О техническом регулировании». Также в документе указано, что для АСУ ТП не обязательна аттестация. Для каждого класса защищенности (КЗ), которых в данном нормативном акте три, предполагаются соответствующие меры ЗИ. В данном приказе обозначено 167 мер защиты, классифицированных в 21 группу, из которых 41 мера является компенсирующей. Для снижения рисков угроз безопасности следует опираться на следующие нормативные акты и ресурсы:

- приказ № 31;
- ГОСТ Р ИСО/МЭК 27034-1. Безопасность приложений;
- ГОСТ Р 56939-2016. Разработка безопасного программного обеспечения;
- методические рекомендации по обновлению сертифицированных средств защиты информации;
- также создан и развивается Банк данных угроз безопасности информации.

К защите информации, содержащейся в ГИС, предъявляются законодательные требования, определяемые Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». Для ЗИ, содержащейся в ГИС, необходимо для начала определить перечень защищаемой информации и КЗ. Для каждого КЗ, количество которых аналогично количеству в приказе № 31, предполагаются соответствующие меры ЗИ. В данном приказе обозначено 113 мер защиты, систематизированных в 13 групп, из которых 30 мер являются компенсирующими. Для защиты информации разрабатывается модель угроз безопасности информации и классификация. После составляется перечень мер защиты для нейтрализации актуальных угроз. На основании данного перечня реализуется техническое проектирование и внедрение проектных решений. Далее следует аттестация и техническое сопровождение аттестованной системы ЗИ. В случае, когда защищаемая ГИС содержит ПДн, мероприятия по ЗИ рассматриваются в комплексе.

В настоящее время законодательная база РФ в области информационной безопасности постоянно изменяется и расширяется. При оптимизации АС следует особое внимание уделять системе безопасности обработки данных, поскольку качество технологии обработки значительно зависит от системы ее защиты. Таким образом, защита информации, обрабатываемой и поступающей в АС, является интегральной, т.е. представляет из себя комплекс методов и средств, которые обеспечивают конфиденциальность, целостность, доступность защищаемой информации, а также аутентичность (обеспечение истинности источника информации) и неотказуемость (гарантирует невозможность отказа от авторства или факта получения информации).

**Литература**

1. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. – Введен 01.09.2014. – М.: Стандартинформ, 2014. – 15 с.
2. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. – М.:Горячая линия-Телеком, 2001. – 3 с.
3. Prozorov A. Защита ПДн по новому стилю: Минюст утвердил приказ ФСТЭК № 21 (SOISO) [Электронный ресурс]. – Режим доступа: https://www.securitylab.ru/blog/personal/80na20/29858.php (дата обращения: 26.03.2018).

**Сергеев Сергей Сергеевич**
Год рождения: 1994
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N4255
Направление подготовки: 10.04.01 – Информационная безопасность
e-mail: me@sergeysergeev.ru

**Горошков Вячеслав Александрович**
Год рождения: 1995
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N4255
Направление подготовки: 10.04.01 – Информационная безопасность
e-mail: gorosvia@ya.ru

**УДК 004.428.4**

# СКАНИРОВАНИЕ РЕСУРСОВ ЛОКАЛЬНОЙ СЕТИ СРЕДСТВАМИ WEB-БРАУЗЕРА

**Сергеев С.С., Горошков В.А.**
**Научный руководитель – к.т.н., доцент Кузнецов А.Ю.**

Работа посвящена исследованию возможности реализации сканирования локальной сети удаленного пользователя посредством web-технологий. Выполнен анализ возможностей современных web-браузеров, предложены и реализованы алгоритмы сбора информации об окружении пользователя и сканировании сети. Дана оценка возможности дальнейшего применения полученных результатов.
**Ключевые слова:** JavaScript, HTML, web, сети, браузер.

Рассмотрим следующую задачу: существует некоторая сетевая инфраструктура (рис. 1), которую требуется исследовать, но сканирование адреса сети результатов не даст, так как устройство находится за NAT, и из внутренней сети порты во внешнюю сеть не транслируются. Но у нас есть возможность заставить пользователя атакуемого устройства осуществить переход по произвольной ссылке на веб-ресурс, которую мы можем передать.

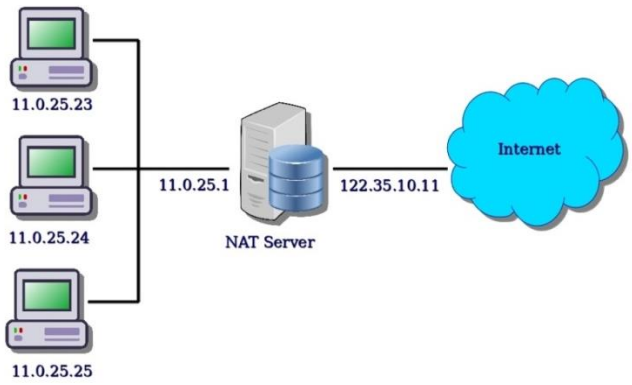



Рис. 1. Структура сети с использование NAT

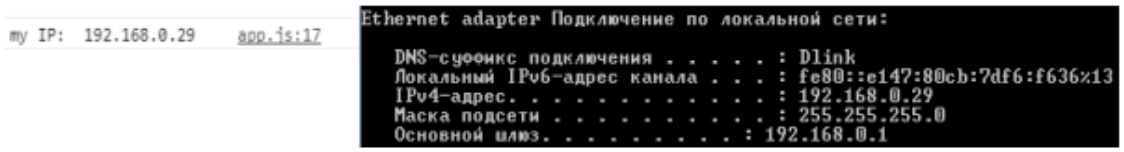
Исходя из задачи, следует реализовать web-приложение, позволяющее осуществить атаку через браузер пользователя, исполняющий скрипт на языке JavaScript в браузере, на стороне ЭВМ пользователя.

Для начала требуется определить локальный IP-адрес компьютера во внутренней сети. Для этого воспользуемся интерфейсом RTCPeerConnection, представляющим коллекцию

WebRTC-протоколов, позволяющих организовать передачу данных между браузерами пользователей и другими приложениями по технологии peer-to-peer [1].

Алгоритм получения IP представляется следующим образом:

– создается и инициализируется объект RTCPeerConnection;
– задается callback функция для обработчика onicecandidate, который срабатывает, когда ICE агенту требуется доставить сообщение через сервер;
– в callback функции проверить на существование переданного объекта «кандидата», произвести считывает свойства и парсинг IP.



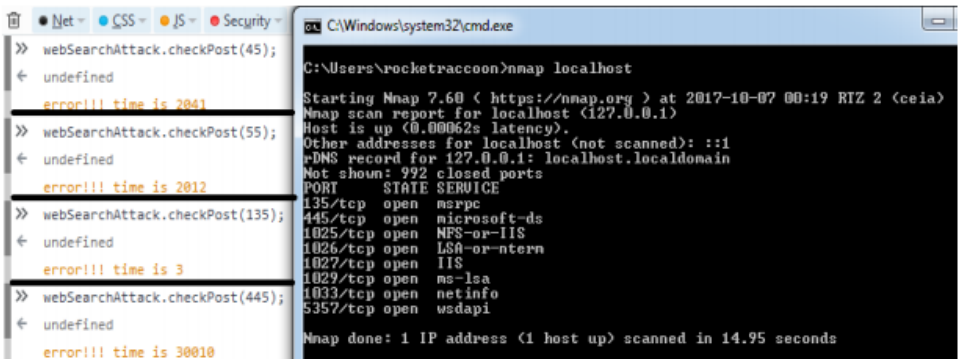

а б

Рис. 2. Сравнение полученного IP с реальным

На рис. 2, а, представлены результат работы скрипта из приложения 1, выведенный в консоль разработчика, и параметры адаптера, полученные в консоли windows с помощью команды ipconfig (рис. 2, б).

Посредством чистого JavaScript невозможно получить маску подсети, предположим, что в Интранете используется класс сети C, так как это наиболее частое явление. Следовательно, маску подсети принимаем за 255.255.255.0.

Далее рассмотрим подходы для сканирования портов локальной машины и других хостов в локальной сети. Один из способов – отправка ajax запросов на исследуемые сокеты. Однако возникает две существенных проблемы. Первая проблема заключается в наложении ограничений с помощью CORS политики, используемой современными браузерами, что решается правильной конфигурацией сервера «отдающего» запрашиваемую страницу с «правильным» HTTP-заголовком. Вторая – возможность обнаружения только веб-сервисов, так как технология ajax способна работать только с протоколом HTTP. Добиться обнаружения различных сервисов на хосте можно довольно интересным способом: осуществить добавление в DOM страницы объекта изображения с атрибутом src, принимающем в себе следующий формат адреса ftp://ip:port , где IP – IP сканируемого хоста, port – сканируемый порт. Суть метода основывается на замере времени между началом загрузки изображения по указанному адресу и возникновением ошибки, которая должна отслеживаться в callback-функцией, переданной объекту с помощью атрибута onerror. Пример работы метода представлен на рис. 3, а, на котором представлен вывод консоли разработчика браузера Mozilla Firefox, в которую был произведен вывод временных промежутков запроса сокетов. На рис. 3, б – вывод сканирования локального хоста на наличие открытых tcp портов.




а б

Рис. 3. Тестирование функции сканирования портов

По результатам вызова метода сканирования портов можно утверждать, что запрос на закрытый порт требует в среднем около двух секунд времени, в то время как запрос на открытый порт может происходить как несколько миллисекунд (запрос на 135 tcp порт – 3 мс), так и довольно долго – порядка 30 с. В ходе эксперимента с портами 1025 и 1026, засечь время вопроса за адекватное время не удалось. Таким образом, можно прийти к выводу, что подобный метод можно использовать для сканирования Интранета.

Исходя из особенности реализации функции определения локального IP-адреса, следует отметить, возможность применения данного метода для браузеров Mozilla Firefox и Google Chrome.

Также требуется обратить внимание на информацию о блокировании в браузере Google Chrome запросов по протоколу ftp в связи с угрозой, которая реализуется в данной работе [2]. Следовательно, можно сделать вывод о применимости описанных методов исключительно к браузеру Mozilla Firefox, который по состоянию на 2017 год занимает 5,96% рынка [3]. Таким образом, можно сделать вывод, о потребности более глубокого погружения в решаемую проблему в дальнейших исследованиях по данной тематике.

**Литература**

1. RTCPeerConnection [Электронный ресурс]. – Режим доступа: https://developer.mozilla.org/enUS/docs/Web/API/RTCPeerConnection (дата обращения: 06.10.2017).
2. Drop support for subresources with legacy protocols. (removed) [Электронный ресурс]. – Режим доступа: https://www.chromestatus.com/feature/5709390967472128 (дата обращения: 06.10.2017).
3. Browser Market Share Worldwide [Электронный ресурс]. – Режим доступа: http://gs.statcounter.com/ (дата обращения: 06.10.2017).

**Сергеев Сергей Сергеевич**
Год рождения: 1994
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N4255
Направление подготовки: 10.04.01 – Информационная безопасность
e-mail: me@sergeysergeev.ru

**Лихачева Татьяна Сергеевна**
Год рождения:1994
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, аспирант
Направление подготовки: 09.06.01 – Информатика и вычислительная техника
e-mail: lihtanse@mail.ru

**Кузнецова Ольга Валерьевна**
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, к.т.н., доцент
e-mail: olunchik_1989@mail.ru

**Кузнецов Александр Юрьевич**
Год рождения: 1989
Университет ИТМО, факультет безопасных информационных технологий, кафедра проектирования и безопасности компьютерных технологий, к.т.н., доцент
e-mail: al.ur.kouznetsov@gmail.com

**УДК 004.428.4**

## АНАЛИЗ МАССИВОВ ДАННЫХ ПРИ ПРОЕКТИРОВАНИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ УПРАВЛЕНИЯ СТАНКАМИ С ЧИСЛОВЫМ ПРОГРАММНЫМ УПРАВЛЕНИЕМ ДЛЯ ИЗГОТОВЛЕНИЯ ПЕЧАТНЫХ ПЛАТ

**Сергеев С.С., Лихачева Т.С., Кузнецова О.В., Кузнецов А.Ю.**
**Научный руководитель – к.т.н., доцент Кузнецов А.Ю.**

Работа выполнена в рамках темы НИР № 416037 «Разработка комплекса автоматизации проектирования и прототипирования электронных средств».

Работа посвящена вопросам импортирования и визуализации трехмерных моделей с помощью библиотеки OpenCASCADE. Рассмотрены различные форматы хранения трехмерных моделей, а также выявлены некоторые проблемы при их обработке, и предложены алгоритмы их решения.
**Ключевые слова:** OpenCASCADE, визуализация, разработка, 3D, IDF.

В рамках работы была поставлена задача разработать программное обеспечение, способное импортировать, визуализировать трехмерные модели различных форматов, а также преобразовывать их в команды на языке G-code, для дальнейшего запуска программ на разрабатываемом станке с числовым управлением.

В качестве импортируемых программой данных были выбраны следующие, популярные в системах автоматизированного проектирования, форматы:

– STEP – формат данных, определенный международным стандартом ISO 10303, для описания и обмена данными в САПР;
– IGES – формат векторной 2D/3D-графики, основанный на спецификации Initial Graphics Exchange. Используется многими программами автоматизированного проектирования в качестве стандартного, основанного на тексте ASCII-формата, предназначенного для хранения и экспорта векторных данных. Может хранить модели каркаса, поверхности представляемых твердых объектов, диаграммы и другие объекты;
– IDF – содержит информацию о форме платы, положении и размере отверстий с металлизацией и отверстий без металлизации, а также о размещении и основной форме компонентов;
– STL – формат 3D-графики, хранящий информацию об объекте как список треугольных граней, которые описывают его поверхность, и их нормалей. STL-файл может быть текстовым (ASCII) или двоичным.

Таким образом, первоочередной задачей являлось исследование методов импорта данных форматов.

В качестве основы для реализации задач по импорту и визуализации 3D-объектов была выбрана библиотека OpenCASCADE, являющаяся одной из самых популярных библиотек для реализации систем автоматизированного проектирования. Исходный код библиотеки Open CASCADE доступен и распространяется бесплатно по лицензии Open CASCADE Technology Public License [1], являющейся производной от GNU LGPl. Сторонние разработчики могут использовать код Open CASCADE в своих продуктах (в том числе коммерческих), однако обязаны, в соответствии с LGPL, отсылать любые изменения в исходных текстах Open CASCADE ее оригинальному разработчику – Open CASCADE S.A.S [2].

Реализация библиотеки Open CASCADE основана на принципах объектно-ориентированного программирования и уже содержит готовые реализации импорта и обработки форматов STEP, IGES и STL. Для этого были использованы экземпляры соответствующих классов: STEPControl_Reader, IGESControl_Reader и StlAPI_Reader.

Для импорта из формата STEP (IGES) во внутренний объект фигуры класса TopoDS_Shape требуется реализовать следующий алгоритм:

1. иинициализировать экземпляр reader класса STEPControl_Reader для формата STEP (или IGESControl_Reader для формата IGES);
2. вызвать метод ReadFile объекта reader с переданной в качестве аргумента строкой, содержащей путь до открываемого файла соответствующего формата;
3. проверить – возвратил ли метод в предыдущем шаге значение IFSelect_RetDone; если возвращено отличное значение, то можно считать, что импорт завершился с ошибкой, иначе следует переходить к следующему шагу;
4. вызвать метод TransferRoots у объекта reader для получения всех сущностей модели;
5. последним шагом является вызов метода OneShape, который должен возвратить экземпляр объекта TopoDS_Shape, содержащий 3D-модель.

STL-формат можно импортировать следующим образом: объявить экземпляр reader класса StlAPI_Reader и вызвать метод Read у объекта reader с аргументами экземпляра класса TopoDS_Shape и строкой, содержащей адрес файла.

В результате изучения возможностей библиотеки Open CASCADE было обнаружено отсутствие возможности импорта объекта в формате IDF. В данном случае было принято

решение о реализации собственного алгоритма импорта подложки модели печатной платы на основе спецификации IDF версии 3.0. В результате анализа стандарта были выявлены следующие особенности формата:

– формат разделен на несколько блоков информации;
– некоторые блоки информации не несут информации для решения поставленной задачи, поэтому могут быть проигнорированы во время чтения файла;
– согласно спецификации формат описывается в виде последовательности символов ASCII.

Для импортирования подложки печатной платы были использованы следующие секции данных:

– секция заголовка – HEADER, несущая в себе помимо метаинформации, важные данные о единицах (миллиметры или мил – тысячные доли дюйма), измерениями в которых описаны параметры модели;
– секция внешней границы – BOARD_OUTLINE, в первой строке которой указана толщина подложки, а каждая последующая строка описывается согласно таблице.
– секция дриллирования – DRILLED_HOLES, описывающая диаметр отверстия и координаты его расположения [3].

Таблица. Формат данных секции BOARD_OUTLINE

| № | Описание | Тип | Значение |
|---|---|---|---|
| 1 | Метка цикла | Целый int | 0 – означает внешнюю границу<br>1 – означает вырез<br>*n* – означает дополнительный вырез |
| 2 | *X* координата | Дробный float | Любое значение |
| 3 | *Y* координата | Дробный float | Любое значение |
| 4 | Угол | Дробный float | 0 – означает прямую линию между точками<br>≠ 0 – означает дугу между точками.<br>При положительном значении дуга против часовой стрелки.<br>360 – означает окружность с центром в предыдущей точке |

Таким образом, был разработан на языке C++ класс CPIdf_Reader, осуществляющий чтение файла, обработку вышеописанных секций и построение конечной трехмерной модели подложки печатной платы на основе примитивов, предусмотренных библиотекой Open CASCADE. Конечным результатом работы методов класса является трехмерная модель объекта в качестве экземпляра класса TopoDS_Shape.

**Литература**

1. Open CASCADE Technology version 6.7.0 and later are governed by GNU Lesser General Public License (LGPL) version 2.1 with additional exception [Электронный ресурс]. – Режим доступа: https://www.opencascade.com/content/licensing (дата обращения: 15.03.2018).
2. Колдыркаев Н. Каскад из CAD'ов // Linux Format. – 2009. – № 7. – С. 30–32.
3. Intermediate Data Format. Mechanical Data Exchange Specification for the Design and Analysis of Printed Wiring Assemblies [Электронный ресурс]. – Режим доступа: http://www.simplifiedsolutionsinc.com/images/idf_v30_spec.pdf, своб.

**Тимофеев Виталий Владимирович**
Год рождения: 1998
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N3255
Направление подготовки: 10.03.01 – Информационная безопасность
e-mail: invitt98@gmail.com

**Мараев Антон Андреевич**
Год рождения: 1987
Университет ИТМО, факультет лазерной и световой инженерии, кафедра оптико-электронных приборов и систем, к.т.н.
e-mail: aamaraev@corp.ifmo.ru

**Тимофеев Александр Николаевич**
Год рождения: 1945
Университет ИТМО, факультет лазерной и световой инженерии, кафедра оптико-электронных приборов и систем, к.т.н., ст.н.с.
e-mail: timofeev@corp.ifmo.ru

**УДК 681.78**

# РАЗРАБОТКА ПРОГРАММЫ РАСЧЕТА ЯРКОСТИ ПОЛУПРОВОДНИКОВЫХ ИСТОЧНИКОВ ОПТИЧЕСКОГО ИЗЛУЧЕНИЯ

**Тимофеев В.В., Мараев А.А., Тимофеев А.Н.**
**Научный руководитель – к.т.н. Мараев А.А.**

Предложена методика машинного расчета яркости полупроводниковых излучающих диодов и структура, интерфейсы разработанной компьютерной программы расчета яркости и выбора по определенному набору параметров из серийно выпускаемых диодов наиболее эффективных излучателей.
**Ключевые слова:** яркость полупроводниковых излучающих диодов, методика для машинного расчета, интерфейс программы, коэффициент формы диаграммы направленности, база данных.

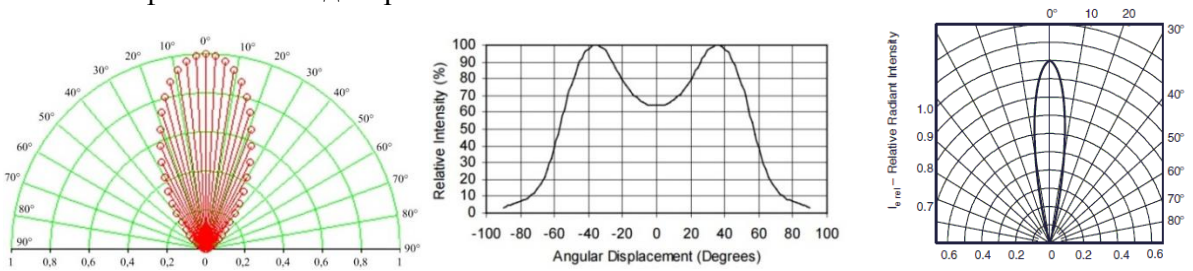
В настоящее время в различных автоматических оптико-электронных системах и комплексах контроля и управления (ОЭСКУ) широко используются полупроводниковые излучающие диоды (ПИД) [1, 2]. При проектировании таких ОЭСКУ по определенным требованиям необходимо осуществлять выборку ПИД из большого количества серийно выпускаемых моделей и типов.

Одной из основных характеристик, определяющих структуру оптической системы и качество работы ОЭСКУ, является пространственная характеристика яркости ПИД. В этой связи целью настоящей работы являлось создание компьютерной программы расчета яркости серийно выпускаемых ПИД, а затем, и выбор наиболее эффективных излучателей по определенному набору параметров.

**Особенности расчета яркости ПИД при реализации компьютерной программы.** Для решения поставленной цели осуществлялось определение основных параметров ПИД для формирования их базы, разработка алгоритма расчета яркости ПИД, определение структуры компьютерной программы выбора ПИД для различных классов ОЭСКУ.

Такие параметры ПИД как максимальная длина волны излучения, ширина спектрального диапазона, мощность излучения, полуширина диаграммы излучения излучающего диода и габаритные размеры обычно нормируются техническими условиями ПИД, в то время как при проектировании ОЭСКУ значение яркости приходится рассчитывать.

Диаграммы серийных излучающих диодов сильно отличаются друг от друга (рис. 1) даже для одного и того же типа ПИД [3], поэтому при создании базы параметров ПИД целесообразно проводить расчет яркости и коэффициента формы диаграммы направленности $K$ по точкам фактической диаграммы.




а б в

Рис. 1. Типовые графики относительного распределения силы излучения для ПИД: Kingbright L132XHT (а); Luxeon LXHL-BD01 (б); Vishay TSAL5100 (в)

Параметр яркости ПИД рассчитывается по известной формуле [4], при этом параметр $K$ зависит от формы диаграммы излучения

$$L_e = \frac{4KP_e}{(\pi d_{\text{ИИ}} \sin \theta_{1/2})^2}, \quad (1)$$

где $P_e$ – поток излучения ПИД; $\theta_{1/2}$ – значение угла половинной яркости; $d_{\text{ИИ}}$ – размер излучающей поверхности ПИД; $K$ – коэффициент формы диаграммы направленности.

Чтобы перейти к расчету интегральной яркости ПИД с помощью компьютерной программы, основываясь на определении яркости, разобьем все поле яркости ПИД на $n$ кольцевых зон, в которых яркость $L_i$ будет приниматься постоянной и равной [5]

$$L_i = J_i / (S \cos Q_i), \quad (2)$$

где $S$ – площадь излучающей площадки ПИД; $J_i$ – сила излучения в направлении $Q_i$; $Q_i$ – центральный угол (рис. 2), определяемый

$$Q_i = i\, Q_{1/2} / (n+1),\ i = 0,1,...,n. \quad (3)$$

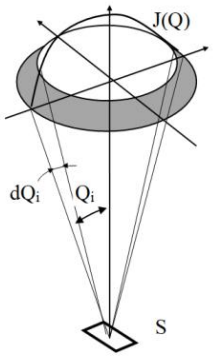



Рис. 2. К расчету яркости элементарной зоны в программе расчета

Тогда среднегабаритная яркость источника определится конечной суммой

$$L_{\Sigma} = [\sum_{i=0}^{n} (J_i \Big/ S \cos Q_i)]/(n+1), \quad (4)$$

и коэффициент формы, с учетом формул (1) и (4), будет находиться из выражения

$$K = \frac{L_{\Sigma} (\pi d_{\text{ИИ}} \sin \theta_{1/2})^2}{4P_e}. \quad (5)$$

**Элементы разработанной компьютерной программы для отбора из серии полупроводниковых излучающих диодов.** При создании компьютерной программы отбора из серии выпускаемых ПИД – наиболее эффективных излучателей по определенному набору параметров (например, максимальной яркости при минимальной потребляемой энергии) – предлагается структура (рис. 3), состоящая из следующих модулей:

– редактируемой базы данных;
– расчета параметра яркости;
– выбора ПИД по параметрам, задаваемым разработчиком ОЭСКУ.


Рис. 3. Структура разрабатываемой компьютерной программы

Для работы компьютерной программы из указанных параметров формируется база данных, интерфейс которой (рис. 4) состоит из четырех полей ввода паспортных значений и блока с 5-ю значениями силы света, которые определяются по точкам диаграммы рассчитываемого светодиода.

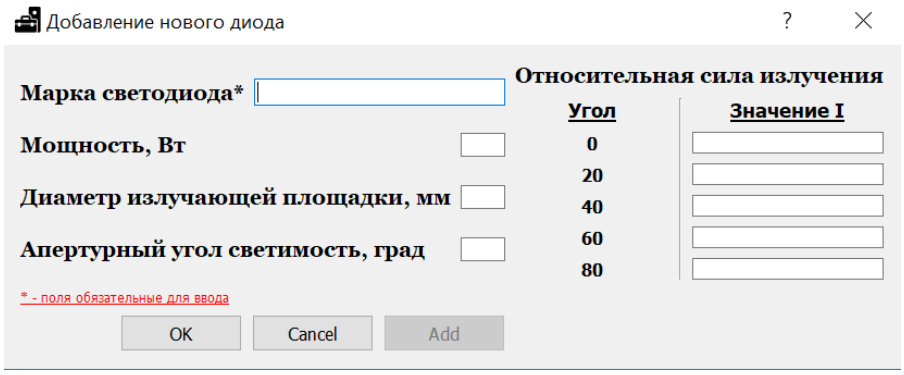



Рис. 4. Интерфейс программы добавления нового диода в базу данных

Полученные с помощью программы коэффициенты К для расчета энергетической яркости наиболее часто применимых в ОЭСКУ полупроводниковых излучающих диодов приведены в таблице.

Таблица. Полученные коэффициенты *K* для расчета энергетической яркости ПИД по формуле (1)

| ПИД | λ, нм | Δλ, нм | *P*, мВт | $2\theta_{1/2}$, ..° | *K* |
|---|---|---|---|---|---|
| TSAL5100 | 940 | 50 | 35 | 20 | 0,58 |
| SFH 485 P | 880 | 80 | 200 | 80 | 0,82 |
| L132XHC | 700 | 45 | 100 | 50 | 0,74 |
| LXHL-BD01GT | 625 | 20 | 27 | 60 | 0,68 |
| ARL-5613UBD | 465 | 30 | 100 | 50 | 0,6 |
| ARL-5013URBC/3L | 625 | 30 | 90 | 40 | 0,65 |
| B5-FC-T5000-40 | 640 | 30 | 80 | 40 | 0,68 |

**Заключение.** В результате работы:
- создана компьютерная программа расчета яркости серийно выпускаемых полупроводниковых излучающих диодов;
- получены коэффициенты *K* для расчета энергетической яркости наиболее часто применимых в ОЭСКУ полупроводниковых излучающих диодов;
- определена структура и параметры выбора из серийно-выпускаемых полупроводниковых излучающих диодов наиболее эффективных излучателей.

В дальнейшем планируется повысить точность вычислений значений яркости ПИД за счет улучшенного алгоритма нахождения яркости по диаграмме излучения с применением аппроксимаций.

**Литература**

1. Якушенков Ю.Г. Основы оптико-электронного приборостроения: учебник. – 2-е изд., перераб. и доп. – М.: Логос, 2013. – 376 с.
2. Коротаев В.В., Мараев А.А., Тимофеев А.Н. Телеориентирование в луче с оптической равносигнальной зоной. Монография. – СПб.: Университет ИТМО, 2015. – 339 с.
3. Горбунова Е.В. Исследование пространственных характеристик излучающих диодов и их зависимости от возможных производственных дефектов // Актуальные теоретические и практические вопросы современного оптико-электронного приборостроения. Сборник трудов молодых ученых. – СПб.: НИУ ИТМО, 2012. – 128 с.
4. Ишанин Г.Г., Козлов В.В. Источники оптического излучения. – СПб.: Политехника, 2009. – 412 с.
5. Великотный М.А. Структура поля излучения светодиодов полусферической конструкции // Труды ЛИТМО. – 1975. – Вып. 81. – С. 44–49.

**Титова Юлия Алексеевна**
Год рождения: 1996
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N3456
Направление подготовки: 10.03.01 – Информационная безопасность
e-mail: titova.yulishna@mail.ru

**Садикова Анастасия Александровна**
Год рождения: 1997
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N3456
Направление подготовки: 10.03.01 – Информационная безопасность
e-mail: nastya.sadkoo@mail.ru

**УДК 004.75**

# УЯЗВИМОСТИ ТЕХНОЛОГИИ РАСПРЕДЕЛЕННЫХ СЕТЕЙ WAN

**Титова Ю.А., Садикова А.А.**
**Научный руководитель – ассистент Попов И.Ю.**

Все распределенные сети в своей основе имеют схожую конструкцию и строятся на одинаковых принципах, поэтому и уязвимости у сетей WAN имеют схожий характер. Зная основные типы угроз, можно максимально защитить корпоративную сеть, что значительно уменьшает риски нарушения конфиденциальности, целостности и доступности. В работе рассмотрены наиболее распространенные уязвимости и основанные на них типы угроз.
**Ключевые слова:** распределенная сеть, корпоративная сеть, уязвимости сети, информационная безопасность, Wide Area Network (WAN).

Для современных корпоративных сетей все чаще используют Интернет в качестве физической основы, и поэтому сеть имеет интерфейсы, выходящие во внешнюю среду. Такая топология сети приводит к появлению дополнительных уязвимостей, которыми может воспользоваться атакующий, цель которых использовать уязвимости бизнес-приложений и получения скрытого доступа к конфиденциальным данным. Корпоративным сетям всех форм, размеров и отраслей промышленности требуется действенная защита от угроз извне.

В работе рассмотрены типовые угрозы распределенной сети Wide Area Network (WAN):

1. анализ сетевого трафика;
2. подмена доверенного объекта или субъекта;
3. ложный объект [1].

Анализ сетевого трафика. Сеть WAN обладает некоторыми особенностями, главная особенность заключается в том, что местоположение элементов имеет распределенный характер. Исходя из этого, управляющие, информационные, командные и прочие сообщения передаются между объектами сети WAN в виде пакетов на весьма большие расстояния, зачастую проходя через сеть Интернет. Из-за данной особенности возникает характерная уязвимость. Атакующий может, находясь во внешней сети, просматривать передаваемые пакеты [2]. Такая угроза имеет название «анализ сетевого трафика» (sniffing), или «сетевой анализ».

Реализация угрозы «сетевой анализ» дает возможность в первую очередь выявить соответствие между отправляемыми командами и выполняемыми в системе действиями. Это

достигается с помощью перехвата и анализа передаваемых пакетов. А уже знание команд распределенной сети дает возможность на практике смоделировать и реализовать типовую удаленную атаку. Во-вторых, с помощью такой атаки злоумышленник имеет возможность не только просматривать и анализировать трафик, но и перехватывать пакеты, которые передаются между элементами распределенной сети. Таким образом, атака типа «анализ сетевого трафика» заключается в обладании несанкционированным доступом к конфиденциальной информации, циркулирующей между сетевыми элементами [1]. Отметим, что на практике при использовании этой уязвимости нельзя модифицировать или подменять пакеты, а сам анализ допустим только внутри одного сегмента сети. Самым распространенным примером может служить перехват логина и пароля, передаваемых без криптозащиты.

Подмена доверенного объекта или субъекта. Одной из основных уязвимостей сети WAN является проблема однозначного определения отправителя сообщения. С этой проблемой борются путем создания виртуального канала, т.е. перед установлением контакта объекты обмениваются контрольными пакетами, которые аутентифицируют их в сети. Это действие называется handshake (рукопожатие). Однако зачастую для передачи коротких одиночных сообщений, такой канал не создается [3], что особо опасно, поскольку служебные сообщения практически всегда передаются способом, не требующим подтверждения.

Для пересылки пакета по сети применяется уникальный идентификатор (на канальном уровне модели OSI – это адрес аппарата – сетевого адаптера, на сетевом уровне адрес представляется, к примеру, IP-адресом). Сетевой адрес помимо этого может применяться для установления идентификации объектов и субъектов распределенной сети, но это способ распознавания не должен быть единственным, так как его довольно просто подделать. Если в сети используются слабые алгоритмы идентификации, то возможно осуществление атаки, когда злоумышленник подменяет поле адреса из пересылаемого пакета на адрес системного элемента. Существуют два вида такой атаки:

1. атака при установленном виртуальном канале;
2. атака без установленного виртуального канала.

При условии создания виртуального соединения, уязвимость заключается в следующем: атакующий подменяет свой идентификатор на идентификатор адресата. В этом случае переданный адресату пакет будет воспринят системой, как пакет, полученный от доверенного источника. Для реализации данной атаки нужно справиться с системой идентификации и аутентификации пакетов, которая зачастую использует контрольную сумму, вычисляемую при помощи открытого ключа, вырабатываемого динамически при поднятии канала. Однако на деле часто для идентификации сообщений используется два счетчика: номер канала и номер пакета [4].

Как уже было отмечено, для сообщений, в которых передаются команды, в распределенных сетях используется передача, не требующая установления виртуального канала, следовательно, созданное соединения является необязательным. Атака без создания защищенного соединения заключается в том, что при передаче служебных сообщений от имени сетевых управляющих устройств, к примеру, от имени роутеров. В данной ситуации для установления объекта, отправившего пакет, могут быть использованы только заранее определенные ключи, что приводит к неудобствам. Однако иначе идентификация таких сообщений без создания виртуального канала осуществима только по сетевому адресу отправителя, который можно подделать [3]. Таким образом, злоумышленник, посылая пакеты от имени внутреннего объекта, может причинить вред работе сети, к примеру, изменив настройки маршрутизатора.

Ложный объект. Если в сети WAN не закреплены правила определения достоверных сетевых управляющих устройств, то подобная распределенная сеть подвержена типовой удаленной атаке, которая связана с модификацией маршрутных таблиц и введением в сеть

ложного объекта. Таким образом, отметим еще одну уязвимость, которая служит появлению типовой угрозы типа «ложный объект» [3].

Практически каждое сетевое устройство имеет свою таблицу маршрутизации, в которой указывается оптимальный маршрут, что позволяет связать все устройства и сетевые сегменты в единую систему. В настоящее время эти таблицы строятся автоматически с помощь различных протоколов управления сетью. Так протоколы RIP (Routing Internet Protocol) и OSPF (Open Shortest Path First) позволяют роутерам обмениваться маршрутной информацией, протокол ICMP (Internet Control Message Protocol) – сообщить хостам о перестройке маршрутов, а протокол SNMP (Simple Network Management Protocol) дает возможность удаленно управлять роутерами.

Маршрутизация выполняет одну из самых важных функций при работе сети, а это значит, что изменение злоумышленником настроек маршрутизации может привести к серьезным последствиям. Так, типовой атакой является атака, связанная с навязыванием ложного маршрута – злоумышленник перестраивает таблицу маршрутизации так, чтобы новый маршрут пролегал через ложный объект – хост атакующего.

Таким образом, ввести ложный объект злоумышленник может несанкционированно используя ранее отмеченные протоколы, управляющие сетью. Для изменения маршрутных таблиц атакующий отправляет по сети пакет со служебным сообщением, подменив свой адрес на адрес управляющего маршрутизатора [4]. В результате проведенной атаки злоумышленник получает возможность перехватывать, перенаправлять и даже подделывать потоки информации.

В работе приведены самые распространенные типовые угрозы. Зная их можно грамотно организовать защиту, что поможет в разы снизить вероятность взлома распределенной сети.

**Литература**

1. Макаренко С.И. Информационная безопасность: учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М.А. Шолохова, 2009. – 371 с.
2. Яблочников Е.И., Фомина Ю.Н., Грибовская А.А. Организация технологической подготовки производства в распределенной среде // Изв. вузов. Приборостроение. – 2010. – Т. 53. – № 6. – С. 12–15.
3. Замятина О.М. Вычислительные системы, сети и телекоммуникации. Моделирование сетей: учебное пособие. – Люберцы: Юрайт, 2016. – 159 с.
4. Дейтел Х.М., Дейтел П.Д., Чофнес Д.Р. Операционные системы. Т. 2. Распределенные системы, сети, безопасность / Пер. с англ. С.М. Молявко. – М.: БИНОМ, 2013. – 704 с.

**Бондаренко Игорь Борисович**
Год рождения: 1972
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, к.т.н., доцент
e-mail: igorlitmo@rambler.ru

**Шиманчук Сергей Николаевич**
Год рождения: 1994
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, студент группы № N4255
Направление подготовки: 10.04.01 – Информационная безопасность
e-mail: shimanchuk.s@gmail.com

**УДК 004.021**

# РАЗРАБОТКА МОДЕЛИ ЭВОЛЮЦИИ НА ПРИМЕРЕ УПРАВЛЕНИЯ РАБОТОЙ ГЕНЕТИЧЕСКОГО АЛГОРИТМА ПРИ ОПТИМИЗАЦИИ МНОГОПАРАМЕТРИЧЕСКОЙ ФУНКЦИИ

**Бондаренко И.Б., Шиманчук С.Н.**
**Научный руководитель – к.т.н., доцент Бондаренко И.Б.**

В работе рассмотрены преимущества теории эволюционного моделирования сложных систем перед традиционными подходами. Исследован и описан принцип работы генетического алгоритма, и предложены варианты улучшения его работы путем управления коррекцией вероятности мутации, по экспериментальным результатам которых представлены графики эволюции хромосом.
**Ключевые слова:** эволюционное моделирование, генетический алгоритм, многопараметрическая функция, процесс эволюции, вероятность мутации, частота успеха мутаций.

Существуют традиционные подходы к моделированию сложных систем, которые реализуют последовательную технологию многоуровневой декомпозиции, усреднения и упрощения, выделения ряда существенных характеристик, выявления основных законов и зависимостей. На их основе и строятся модели для управления, мониторинга, прогнозирования. Однако такой подход эффективен только для описания поведения формализованных, жестких, динамически неизменяемых, механистических систем в ограниченном пространстве. При усложнении систем, их динамическом изменении теряется адекватность поведения модели.

В отличие от традиционных подходов в теории эволюционного моделирования предметной области ставится в соответствие единое описание элементов и их взаимодействий. Теория эволюционного моделирования, в отличие от других подходов, строит единую виртуальную модель. Моделирование в предлагаемой теории осуществляется на основе фиксированного набора базовых классов, замены итерационного проектирования модели на эволюционный, и усовершенствованного диаграммного представления [1].

Генетический алгоритм – это один из основных эволюционных алгоритмов, предназначенный для решения задач оптимизации и моделирования путем случайного подбора, рекомбинирования искомых параметров с использованием механизмов, аналогичных естественному отбору в природе, а именно, таких механизмов, как наследование, мутация, отбор и скрещивание.

По сравнению с обычными оптимизационными методами, генетический алгоритм (ГА) имеет ряд особенностей, например, таких как параллельный поиск, случайные мутации и рекомбинации уже найденных хороших решений.

Принцип работы рассматриваемого алгоритма строится следующим образом. Вначале генерируется, случайным образом и в определенных пределах, начальная популяция решений – набор параметров, выступающий начальным решением поставленной задачи. Для каждого параметра решения рассчитываются значения функции приспособленности. После чего, в зависимости от рассчитанной на предыдущем этапе функции приспособленности, формируется новое поколение: выбираются родители по правилу – чем больше у особи (параметра) приспособленность, тем больше она должна участвовать в скрещивании; и при помощи генетических операторов создаются потомки нового поколения. К созданным потомкам применяется мутация, т.е. операция, которая случайным образом с определенной вероятностью меняет фрагмент особи, что обеспечивает разнообразие параметров решений. После чего происходит обновление текущей популяции новыми потомками.

В конце указывается критерий завершения работы ГА. Критерии могут быть разными и зависят от преследуемых целей, например:

– достигнуто определенное количество поколений;
– найдено оптимальное решение;
– ограничение по времени работы алгоритма;
– достигнута заданная точность.

Изменение поколений не улучшает результат, что показано на рис. 1 в виде прямой линии.

$$N = F\left(Q(X), \{S_{\text{отб}}, S_{\text{скр}}, S_{\text{мут}}\}, p_{\text{мут}}, e, N_{\text{хр}}\right),$$

где $Q(X)$ – вид (сложность) исследуемой функции; {…} – кортеж, содержащий типы операторов отбора ($S_{\text{отб}}$), скрещивания ($S_{\text{скр}}$) и мутации ($S_{\text{мут}}$); $p_{\text{мут}}$ – вероятность мутации; $e$ – точность; $N_{\text{хр}}$ – количество хромосом в популяции.

Исследование зависимости $N=f(N_{\text{хр}})$ показало, что между размером популяции и количеством поколений выявлена отрицательная корреляция.

По мнению большинства исследователей $p_{\text{мут}}$ выбирается из диапазона 0,5–1%. Точное значение этого параметра определить невозможно, так как при небольших значениях ($p_{\text{мут}}$<0,5%) сходимость ГА будет слишком медленной, а при $p_{\text{мут}}$>1% движение к оптимуму происходит скачкообразно, а варианты решений, близкие к оптимуму, могут быть разрушены, что также замедлит сходимость. Остальные параметры в соотношении в процессе работы ГА неизменны [2].

В результате проведения экспериментов выявлено, что наилучшая хромосома эволюционирует так, как показано на рис. 1 для функции типа:

$$Q(X) = \sum_{i=1}^{n} (x_i - A\sin\omega t)^2,$$

где $n$=9, $e$=0,1, $N$<50 000 с вещественным кодированием хромосом и пропорциональным отбором при различных размерах популяции на отрезке поиска. Аналогичные зависимости получены и в работе.

Из рис. 1 видно, что при количестве поколений 50 000 оптимум с требуемой точностью не достигается из-за «стагнации» алгоритма и ступенчатого характера сходимости, исследуемого ГА. Причем количество ступенек зависит от размера популяции. Такие же результаты получаются исследователями ГА при управлении начальной популяцией и использовании метамоделей для оптимизируемых функций.

Исходя из этого, целью исследований в нашей работе являлось ускорение сходимости при:

$$N_{\text{хр}} \to \min, \quad N \to \min.$$

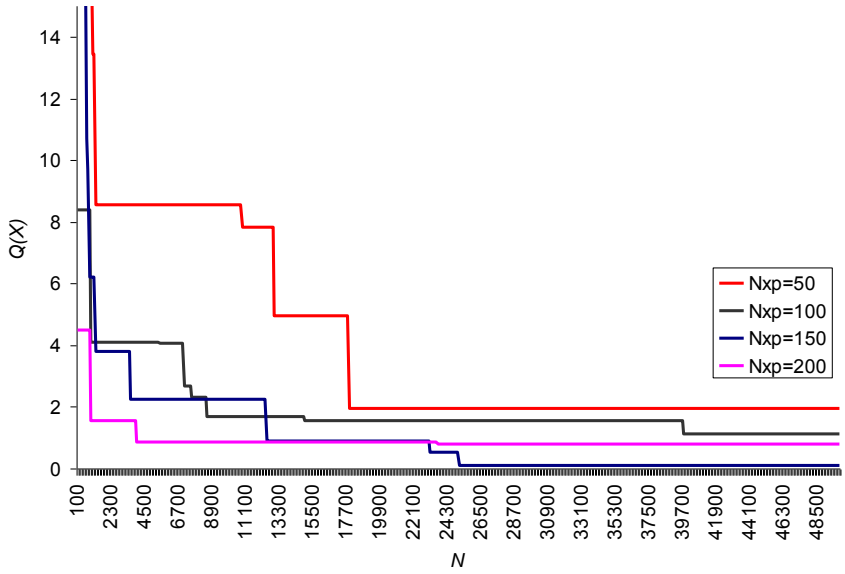



Рис. 1. Эволюция наилучшей хромосомы

Несмотря на предложенные исследователями многочисленные подходы: использование штрафов; введение в ГА дополнительных операторов мутации; гибридизация ГА – добавление в колонию хромосомы, работающей по особому алгоритму, например, «жадному»; элитизм – сохранение и переход наилучших хромосом в следующее поколение без изменений; уменьшение $p_{мут}$ при успешном движении к оптимуму и другие, – управление работой ГА усложняется, а выигрыш в сходимости достигается незначительный и лишь на определенных интервалах $N$.

В связи с этим для выполнения цели исследования представлялось интересным разработка и исследование процедур: коррекции $p_{мут}$ и интенсивного отбора наилучших хромосом при «стагнации» сходимости ГА, а также сравнение их эффективности.

Закон прогресса изменяется по закону:

$$G = G_0 \exp(\alpha t), \quad (1)$$

где $G_0$ – состояние эволюции в начальный момент времени; α – коэффициент, определяющий скорость и характер развития прогресса.

Рассматривая метод управления мутациями, можно периодически оценивать частоту успеха мутаций на $i$-ой итерации по соотношению:

$$\frac{n_{успех}}{n_{мут}} = \frac{n_{успех}}{N_{хр} N} > \frac{1}{5}, \quad (2)$$

где $n_{успех}$ – количество успешных мутаций; $n_{мут}$ – общее число мутаций.

При выполнении соотношения (2), т.е. при 20% успешности попыток мутаций, ход эволюции решений ГА считается успешным. Тем не менее, универсального правила управления мутациями в зависимости от вида функции исследователями не выработано.

Исследователи этого вопроса, сопоставив длины более 100 генетических деревьев нуклеотидных последовательностей ДНК, пришли к выводу, что отношение периодов интенсивного развития и скачкообразных преобразований к долгим и постепенным составляет в среднем 22% к 78% [3].

Для проведения имитационного эксперимента на персональном компьютере сделаны следующие преобразования.

Соотношение (1) преобразовано для удобства к виду:

$$G(N) = a - b \cdot \ln(N), \quad (3)$$

где $a$ и $b$ – коэффициенты.

Условие расхождения процесса поиска с законом (3) на промежутке длиной $k–i$ поколений запишем

$$\left|\frac{G(N_i)-G(N_k)}{Q(X^{(i)})-Q(X^{(k)})}\right| > 0{,}28,\ \ i<k\,. \qquad (4)$$

Значения $a$, $b$ и $k–i$ подбирались экспериментально. При выполнении условия (4) значение $p_{мут}$ увеличивалось с шагом 0,001 [4].

Результаты имитационных экспериментов управления мутациями представлены на рис. 2.

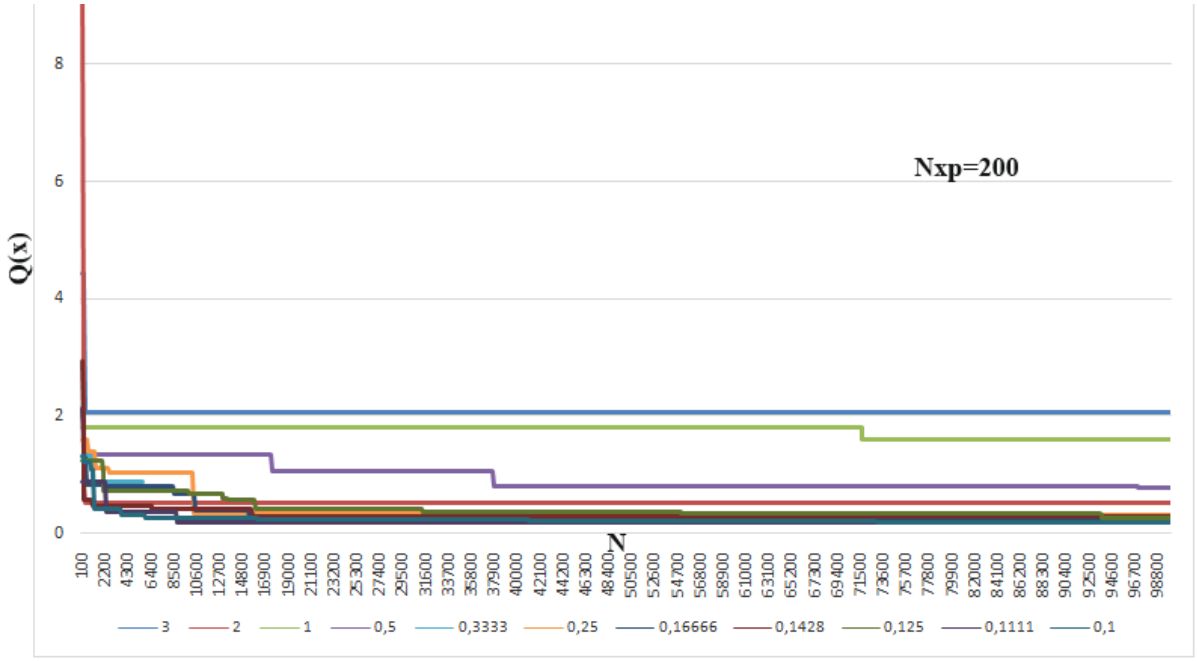



Рис. 2. Результаты имитационных экспериментов

Управление величиной мутации позволило ускорить сходимость ГА при оптимальном количестве хромосом и поколений.

В дальнейшем планируется исследование процедуры интенсивного отбора наилучших хромосом при «замирании» сходимости ГА и сравнение эффективности исследуемых методов ускорения сходимости ГА.

Используя полученные результаты можно будет переходить непосредственно к самой разработке модели эволюции управления работой ГА.

**Литература**

1. Гудилов В.В. Эволюционное проектирвоание аппаратных средств // Информатика, вычислительная техника и инженерное образование. – 2011. – № 5(7). – С. 11–34.
2. Бондаренко И.Б., Каляева Е.А., Кокшаров Д.Н. Адаптация параметров генетического алгоритма для оптимизации сложных функций // Изв. вузов. Приборостроение. – 2011. – № 9(54). – С. 5–9.
3. Кошев А.Н., Салмин В.В., Генералова А.А., Бычков Д.С. Разработка генетического алгоритма с адаптивными мутациями для определения глобального экстремума функции n-переменных [Электронный ресурс]. – Режим доступа: http://naukovedenie.ru/PDF/32TVN616.pdf, своб.
4. Pagel M., Venditti C., Meade A. Large Punctuational Contribution of Speciation to Evolutionary Divergence at the Molecular Level // Science. – 2006. – V. 314. – P. 119–121.

**Югансон Андрей Николаевич**
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, аспирант
Направление подготовки: 10.06.01 – Информационная безопасность
e-mail: a_yougunson@corp.ifmo.ru

**Заколдаев Данил Анатольевич**
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, к.т.н., доцент
e-mail: d.zakoldaev@mail.ru

**УДК 004.054**

# ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ МАШИННОГО ОБУЧЕНИЯ ДЛЯ АНАЛИЗА ТЕХНОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ПРОГРАММНЫХ СРЕДСТВ

**Югансон А.Н., Заколдаев Д.А.**
**Научный руководитель – к.т.н., доцент Заколдаев Д.А.**

Работа выполнена в рамках темы НИР № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность».

В работе рассмотрены вопросы анализа технологической безопасности программных средств. Предложено использование технологии Big Code для повышения качества оценивания надежности программного обеспечения. Данная технология находится на стыке машинного обучения, программной инженерии, языков программирования и обработки естественных языков. Приведены достоинства и недостатки использования технологии Big Code на ранних этапах разработки программного обеспечения. Описаны перспективы применения машинного обучения.
**Ключевые слова:** Big Code, структурированные и неструктурированные данные, технологическая безопасность программных средств, надежность программного обеспечения, анализ исходных кодов.

Современные стандарты по разработке промышленного программного обеспечения (ПО) подразумевают главенствование вопроса обеспечения надежности функционирования ПО над оценкой надежности. Парадокс заключается в том, что для должного обеспечения уровня надежности функционирования разработанного ПО, необходимо однозначно определять этот уровень. На сегодняшний день в отрасли не принят единый стандарт по оценке надежности.

Проблема обеспечения надежности программных продуктов стала одним из важнейших приоритетов мирового экономического развития, эффективным средством решения социальных задач. В цивилизованных государствах сложилась развитая система технического законодательства, не просто устанавливающая конкретные обязательные требования к качеству ПО, но нацеленная на то, чтобы эти требования были финансово и экономически обоснованы [1].

Оценка надежности программных средств представляет собой совокупность операций, включающих выбор номенклатуры показателей надежности оцениваемого программного средства, определение значений этих показателей и сравнение их с базовыми значениями.

Здесь и далее, под технологической безопасностью программных средств будет пониматься способность программных средств сохранять заданный уровень пригодности в заданных условиях в течение заданного интервала времени, где в качестве ограничения уровня пригодности рассматриваются дефекты безопасности и уязвимости [2]. В свою очередь, машинное обучение – это методы и алгоритмы, предназначенные для частичной или полной автоматизации решения сложных профессиональных задач в самых разных областях человеческой деятельности.

По информации аналитической компании Gartner (сведения за июль 2017 года) машинное обучение находится на пике завышенных ожиданий (рис. 1). Это значит, что данную технологию пытаются применять практически в каждой области, начиная от приложений в офисной автоматизации и заканчивая приложениями в медицине и биоинформатике.

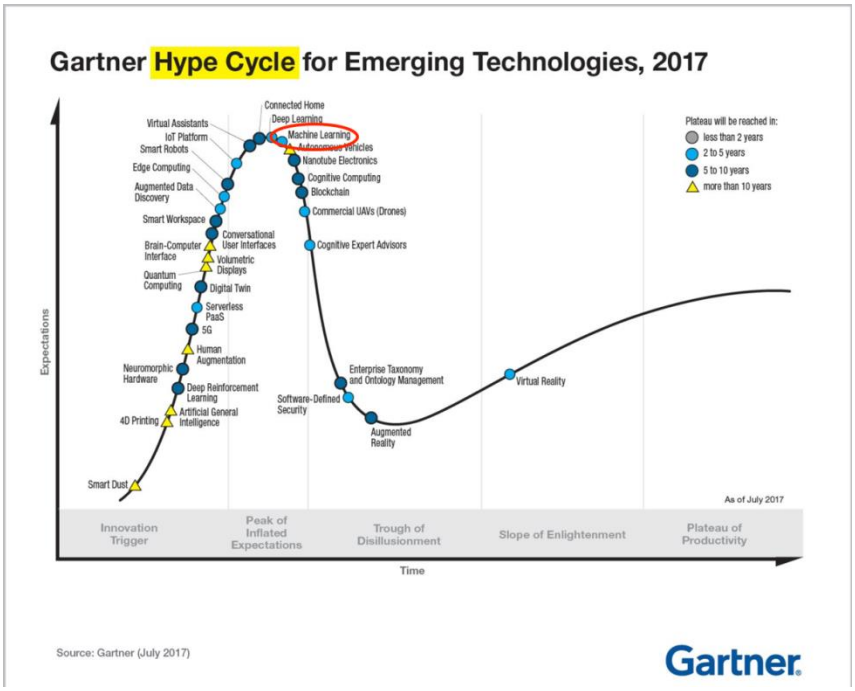


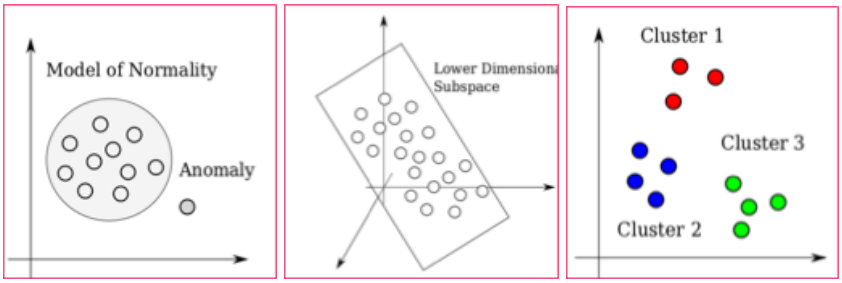

Рис. 1. Исследовательский отчет фирмы Gartner

На сегодняшний день некоторые специалисты уже проявляют скепсис относительно перспектив применения методов и алгоритмов машинного обучения. Данная работа описывает некоторые практические аспекты применения машинного обучения в контексте информационной безопасности, и, в частности, при анализе технологической безопасности программных средств.

Можно выделить следующие основные типы задач, решаемые с помощью машинного обучения [3], для анализа технологической безопасности программных средств:

1. задача обнаружения аномалий (outliers detection) – обнаружение в обучающей выборке небольшого числа нетипичных объектов. В некоторых приложениях их поиск является самоцелью (например, обнаружение мошенничества) (рис. 2, а);
2. задача сокращения размерности заключается в том, чтобы по исходным признакам с помощью некоторых функций преобразования перейти к наименьшему числу новых признаков, не потеряв при этом никакой существенной информации об объектах выборки. В классе линейных преобразований наиболее известным примером является метод главных компонент (рис. 2, в);
3. задача кластеризации (clustering) заключается в том, чтобы сгруппировать объекты в кластеры, используя данные о попарном сходстве объектов. Функционалы качества могут

определяться по-разному, например, как отношение средних межкластерных и внутрикластерных расстояний (рис. 2, в).




а б в

Рис. 2. Обнаружение аномалий (а); сокращение размерности (б); кластеризация (в)

Рассмотрим метод обнаружения уязвимостей с помощью выявления аномалий (рис. 3).

На первом этапе происходит синтаксический анализ исходного кода, благодаря которому выделяются так называемые API symbols – типовые функции и типы данных.

На втором этапе происходит построение векторного пространства, где каждой символу API соответствует свое измерение.

Далее происходит определение основных паттернов API с помощью метода определения главных компонент (Principal Component Analysis, PCA). Данный метод аппроксимирует облако наблюдений до эллипсоида, сохраняя наибольшее количество информации.

Наконец, каждая функция выражается через смесь доминирующих паттернов API. Такое представление позволяет идентифицировать похожие функции, использующие схожие паттерны API, и, соответственно, содержащие похожие уязвимости.

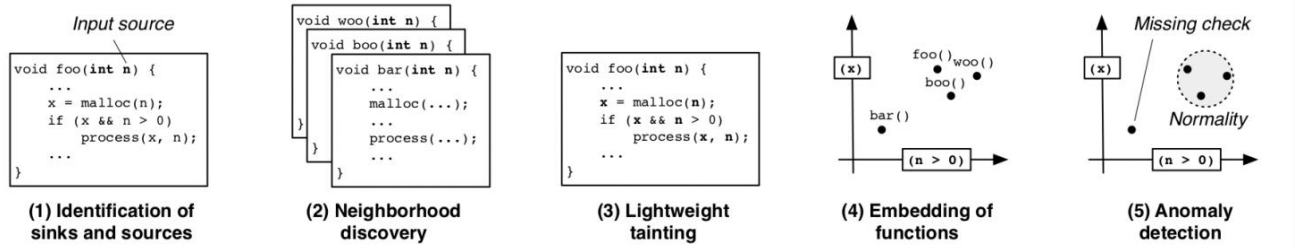



Рис. 3. Метод обнаружения уязвимостей с помощью выявления аномалий

Следующий метод обнаружения уязвимостей основан на сокращении размерности (рис. 4).

Рассмотрим данный метод на примере проверки условий:

1. определяются для исследуемой функции все входные и выходные параметры;
2. происходит группировка схожих по содержанию функций;
3. определяются основные условия, выполнение которых обязательно для корректной работы функций из выбранной группы;
4. группы функций представляются в виде векторов, содержащих проверку этих условий;
5. формируется эталонная модель функции для группы функций. Благодаря сформированной эталонной модели происходит выявление аномальных функций (например, функций, в которых отсутствует проверка какого-либо условия).

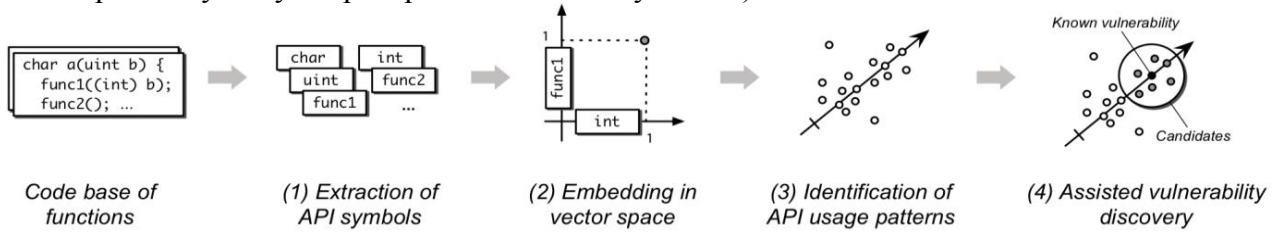



Рис. 4. Метод обнаружения уязвимостей, основанный на сокращении размерности

Еще одним примером практического применения методов машинного обучения является метод обнаружения уязвимостей при помощи решения задачи кластеризации (рис. 5).

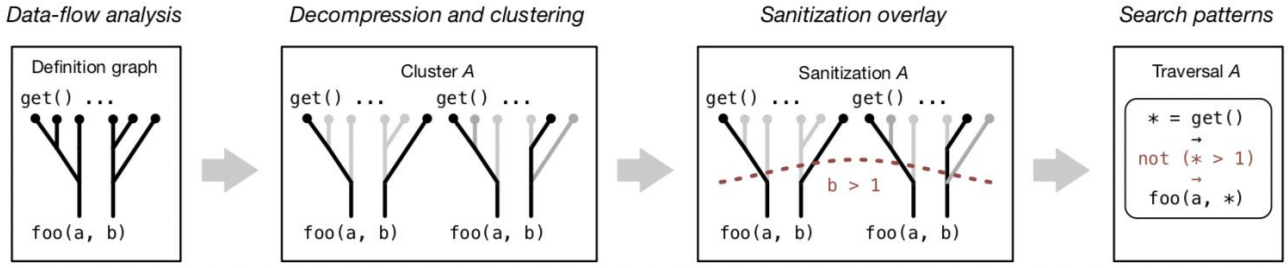



Рис. 5. Метод обнаружения уязвимостей при помощи решения задачи кластеризации

Данный метод заключается в следующем.

1. Определяются все вызовы выбранной функции, и строится соответствующий граф определения. Данный граф показывает, как входные данные инициализируются и экранируются в конкретной функции.
2. Далее, графы определения раскладываются для перечисления отдельных вызовов функций. Затем вызовы функций группируются для определения наборов вызовов с аналогичными инициализируемыми аргументами.
3. Для каждого сформированного кластера определяется некоторый предел для экранирования аргументов, т.е. определяются условия, проверка которых должна выполняться после инициализации и перед вызовом.
4. В результате генерируются поисковые шаблоны, содержащие условия проверки, для обхода всех графов вызовов функций.

Принимая во внимание все вышесказанное, можно усовершенствовать методику для расчета оценки технологической безопасности программных средств, предложенную в работе [4] следующим образом.

– На первом этапе происходит вычисление расчетных метрик. Данный этап подразумевает определение таких метрик, как показатель устойчивости к искажающим воздействиям, вероятность безотказной работы, оценка по среднему времени восстановления, оценка по продолжительности преобразования входного набора данных в выходной.
– На втором этапе дается оценка метрикам с помощью экспертного опроса.
– Третий этап включает в себя использование технологии Big Code. В рамках данного этапа происходит следующее: строится вероятностная модель на основе большого объема исходных кодов. Затем данная модель используется для проверки метрик исследуемого исходного кода.
– Четвертый этап – сравнение полученных метрик с соответствующими значениями аналога или программного средства, принимаемого за эталонный образец. В качестве аналогов выбираются реально существующие программные средства того же функционального назначения, что и сравниваемое программное обеспечение, с такими же основными параметрами, подобной структурой и применяемые в схожих условиях эксплуатации.

Таким образом, в ходе исследования была предложена принципиально новая технология, позволяющая повысить качество оценки надежности программных средств.

Предложенная методика сложна в применении, так как требует знаний таких характеристик ПО, которые можно вычислить только после длительной эксплуатации. Основываясь на данной работе, можно сделать вывод: отсутствует общее решение проблемы расчета оценки надежности ПО, и существуют множество частных решений, которые не учитывают такие факторы как интенсивность внесения и устранения ошибок в программе [5].

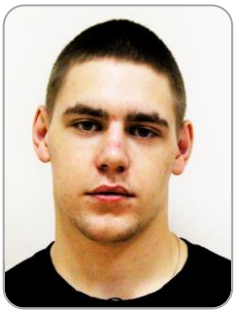
Важным вопросом практического применения методики является подготовка исходных данных. Эта задача особенно актуальна при оценке на ранних этапах жизненного цикла. Исходные данные (общее количество ошибок и временные характеристики процессов их поиска и устранения) могут быть получены с использованием объектно-ориентированных метрик сложности и статистики, собранной при разработке похожих программных проектов, в том числе с помощью использования технологии Big Code.

Тем не менее, использование представленной методики позволит повысить уровень качества автоматизированных систем управления различного назначения, а также минимизировать риски, связанные с отказом программного обеспечения на ранних стадиях эксплуатации. Данная методика будет использована при разработке научных и программных решений для расчета надежности программных средств.

**Литература**

1. Нагорный С.И., Донцов В.В. О подходах к определению требований, предъявляемых к средствам вычислительной техники, выполненной в защищенном исполнении // Спецтехника и связь. – 2010. – № 1. – С. 46–54.
2. Марков А.С. Немонотонные модели оценки надежности и безопасности функционирования программных средств на ранних этапах испытаний // Вопросы кибербезопасности. – 2014. – № 2(3). – С. 10–17.
3. Yamaguchi F., Lindner F., Rieck K. Vulnerability extrapolation: assisted discovery of vulnerabilities using machine learning // Proceedings of the 5th USENIX conference on Offensive technologies. – 2011. – P. 13–13.
4. Югансон А.Н., Заколдаев Д.А. Разработка методики для расчета оценки технологической безопасности программных средств // Вестник УрФО. Безопасность в информационной сфере. – 2017. – № 1(23). – С. 20–23.
5. Хунов Т.Х. Анализ моделей прогнозирования надежности программных средств // Новые информационные технологии в автоматизированных системах. – 2016. – № 19. – С. 219–223.

**Зенин Михаил Максимович**
Год рождения: 1996
Университет ИТМО, факультет информационной безопасности и компьютерных технологий, кафедра проектирование и безопасности компьютерных систем, студент группы № N3455
Направление подготовки: 10.03.01 – Информационная безопасность
e-mail: mix.zenin.ifmo@yandex.ru



**Боровик Владимир Сергеевич**
Год рождения: 1996
Университет ИТМО, факультет информационной безопасности и компьютерных технологий, кафедра проектирование и безопасности компьютерных систем, студент группы № N3455
Направление подготовки: 10.03.01 – Информационная безопасность
e-mail: bobahbdb@gmail.com

**Югансон Андрей Николаевич**
Университет ИТМО, факультет безопасности информационных технологий, кафедра проектирования и безопасности компьютерных систем, аспирант
Направление подготовки: 10.06.01 – Информационная безопасность
e-mail: a_yougunson@corp.ifmo.ru

**УДК 004.056.5**

# СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СМАРТ-КОНТРАКТОВ

**Югансон А.Н., Боровик В.С., Зенин М.М.**
**Научный руководитель – аспирант Югансон А.Н.**

В работе приведен обзор средств обеспечения информационной безопасности смарт-контрактов для платформы Ethereum. Рассмотрены базовые принципы работы технологии блокчейн и смарт-контрактов. Дана характеристика способам обеспечения безопасности смарт-контрактов для платформы Ethereum.
**Ключевые слова:** блокчейн, уязвимости программного обеспечения, смарт-контракты, язык программирования Solidity.

Блокчейн – распределенный цифровой реестр, обеспечивающий принцип неизменности данных, представляющий из себя постоянно растущую последовательность блоков, которая распространяется между участниками с помощью пиринговых сетей [1].

Блокчейн работает по следующим правилам:

- новые транзакции рассылаются всем узлам;
- каждый узел объединяет пришедшие транзакции в блок [2];
- каждый узел пытается подобрать хэш блока, удовлетворяющий текущей сложности;
- как только такой хэш найден, этот блок отправляется в сеть;
- узлы принимают этот блок, только если все транзакции в нем корректны и не используют уже потраченные средства;
- свое согласие с новыми данными узлы выражают, начиная работу над следующим блоком и используя хэш предыдущего в качестве новых исходных данных (рис. 1).

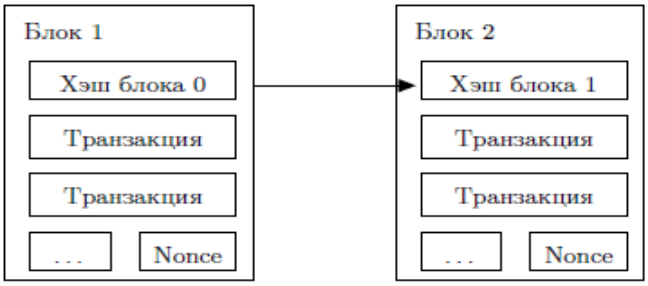



Рис. 1. Формирование цепи блоков

Bitcoin является ярким примером применения технологии блокчейн в финансовой сфере, но также существует множество других традиционных областей, в которых применение блокчейн может решить существующие проблемы.

Создание блокчейна является сложной инженерной задачей, которая требует высокой квалификации программистов, а также для полноценной работы сети необходимо достаточное количество узлов, обеспечивающих подтверждение транзакций. В настоящее время для решения таких задач существуют публичные блокчейн-платформы, основной задачей которых является предоставление инструментов разработки для создания децентрализованных приложений на их основе. Самой популярной из таких платформ на данный момент является Ethereum. Ethereum представляет собой блокчейн со встроенным тьюринг-полным языком программирования Solidity, позволяющим любому желающему писать смарт-контракты, децентрализованные приложения, а также создавать свои протоколы.

Смарт-контракт – это программный код, который хранится в блокчейне. Выполнение смарт-контракта происходит при поступлении новой транзакции, имеющей вызов функций из контракта. Код контракта пишется на специальном языке программирования Solidity. Перед публикацией кода в блокчейн он компилируется до байт-кода для виртуальной машины Ethereum (EVM).

За вызов функций смарт-контракта пользователь должен заплатить определенное количество внутренней валюты – газа. Стоимость зависит от сложности и количества производимых смарт-контрактом вычислений, а также от цены на газ. Цена за единицу газа определяется относительно к ETH. Узел, подтвердивший транзакцию, получает комиссию в размере количество газа умноженного на его цену.

Частный случай смарт-контрактов – мультиподпись. Мультиподпись – это подпись схема реализации электронной подписи, которая для своей достоверности требует наличия согласия $M$ из $N$ участников, где $1<M<=N$.

Алгоритм мультиподписи заключается в следующем:

– один из владельцев кошелька формирует транзакцию;
– транзакция записывается в смарт-контракт, встает в очередь и находится там до тех пор, пока ее не подпишут нужное, для ее исполнения, количество владельцев;
– после сбора необходимого количества подписей, она может быть исполнена (рис. 2).

Мультиподпись – значимая часть экосистемы Ethereum, на ней основан наиболее распространенный кошелек – Parity, который был взломан из-за ошибки проектирования смарт-контракта.

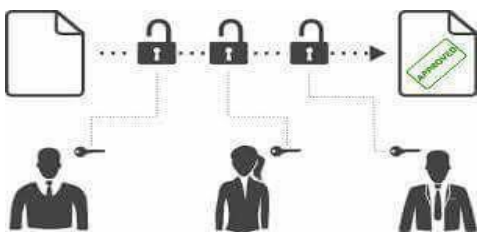


Рис. 2. Принцип работы мультиподписи

Децентрализованные приложения обязаны быть максимально надежными с точки зрения информационной безопасности, так как наличие уязвимостей в них может повлечь огромные финансовые и репутационные потери [3, 4].

**Аудит смарт-контрактов.** Одним из способов обеспечения информационной безопасности является аудит кода контракта экспертами в области безопасности. В данный момент одним из таких признанных экспертов является компания Zeppelin, которая разработала отраслевые стандарты безопасности для внедрения и проектирования смарт-контрактов. Компания предоставляет безопасные шаблоны для типовых контрактов, такие как токен ERC-20, Crowdsale и другие.

**Статические анализаторы.** Еще одним инструментом для анализа безопасности кода контрактов являются статические анализаторы. Анализатор сканирует код и на основе заданных правил ищет потенциально опасные места в программе. Как правило, статические анализаторы имеют интеграцию со средой разработки, что позволяет обнаруживать и устранять уязвимости на самых ранних этапах разработки.

**Выполнение в тестовой сети.** Для Ethereum существуют несколько тестовых сетей, которые позволяют протестировать приложение в условиях, максимально приближенных к реальной сети, без опасности потерять средства. Тестовые сети максимально идентичны главной сети, за исключением того, что токен, который находится в обращении данной сети ничего не стоит, его можно получить бесплатно. Это значит, что после загрузки контракта в тестовую сеть можно проводить полноценный аудит безопасности и тестирование на проникновение, не боясь за средства, хранимые на контракте.

Естественно, не один из вышеперечисленных методов не дает полноценной гарантии отсутствия уязвимостей в коде контракта. Для максимальной защиты рекомендуется использовать все перечисленные средства обеспечения безопасности.

**Литература**

1. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [Электронный ресурс]. – Режим доступа: https://bitcoin.org/bitcoin.pdf, своб.
2. Becker G. Merkle signature schemes, merkle trees and their cryptanalysis [Электронный ресурс]. – Режим доступа: http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/becker_1.pdf, своб.
3. Atzei N., Bartoletti M., Cimoli T. A survey of attacks on Ethereum smart contracts (SoK) // International Conference on Principles of Security and Trust. – 2017. – P. 164–186.
4. Банк данных угроз безопасности информации [Электронный ресурс]. – Режим доступа: http://bdu.fstec.ru, своб.

**Кремнев Иван Александрович**
Год рождения: 1994
Университет ИТМО, факультет систем управления и робототехники, кафедра высшей математики, студент группы № Р4295
Направление подготовки: 01.04.02 – Прикладная математика и информатика
e-mail: juankremnev@gmail.com

**УДК 004.85**

# КОМПЬЮТЕРНОЕ ЗРЕНИЕ В РОБОТОТЕХНИКЕ

**Кремнев И.А.**
**Научный руководитель – к.ф.-м.н., доцент Фильченков А.А.**

Работа выполнена в рамках темы НИР № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность».

В работе рассмотрены подходы к построению трехмерных карт вероятности нахождения ключевых точек объекта. Инструментом решения задачи выбраны глубокие нейронные сети. Исследованы различные архитектуры сетей, учитывающие высокую размерность целевой функции, а также особенности синтетических данных для обучения. Генеративные подходы используются для моделирования распределения на скрытые переменные, описывающие положение объекта в пространстве.
**Ключевые слова:** компьютерное зрение, глубокое обучение, объемное представление.

Задача предсказания ключевых точек объекта по изображениям с камеры возникает в процессе автоматизации производства. Традиционно предсказание ключевых точек объекта с целью определения его положения в пространстве связано с такими задачами, как определение позы человека. В подобных задачах набор ключевых точек всегда известен, поэтому зачастую формально рассматривается задача регрессии координат ключевых точек в плоскости изображения или в пространстве сцены [1]. В настоящей задаче, однако, модели объектов в сцене могут быть разными, а также часть ключевых точек может быть скрыта от камеры. Исходя из этого, формально требуется ставить задачу предсказания вероятностного распределения ключевых точек по изображениям с одной или двух камер [2].

Популярным инструментом решения задачи компьютерного зрения являются нейронные сети. В данной работе производится сравнительный анализ различных нейросетевых моделей, в частности, сверточных кодировщиков, а также генеративной модели вариационного автокодировщика, как возможных инструментов для вычисления требуемых вероятностей. Использование генеративных моделей повышает способность сети предсказывать скрытые ключевые точки за счет выделения скрытых переменных, отвечающих, в частности, за форму и положение объекта [3].

Чтобы решить проблему высокой размерности целевой функции, приходится проводить обучение нейросетевой модели в несколько этапов, вводя при этом промежуточные цели, такие как предсказание распределения ключевых точек на плоскости изображения, а также предсказание матрицы поворота модели. Также возможен подход с постепенным увеличением разрешения по третьему измерению при помощи множественных целей, чтобы обучение проходило наиболее гладко [2].

Данные для обучения используются синтетические. С одной стороны, этот подход обеспечивает почти безграничный набор данных, что существенно при обучении нейронных сетей, а также точные метки. С другой, приходится сталкиваться с проблемой низкой

обобщающей способности обученных моделей на реальные данные. Последняя проблема должна решаться как улучшением используемых в синтезе текстур, так и выбором архитектур сетей, наиболее способных к обобщению.

В ходе исследования рассмотрены следующие варианты нейросетевых архитектур.

1. Последовательность сверточных кодировщиков, каждый из которых улучшает объемные предсказания распределения ключевых точек предыдущего на основе его карт активации с предпоследнего слоя. Такая архитектура была успешно использована в задаче предсказания положение тела человека [2]. Результаты текущих исследований показали, что такая система обучается распознавать видимые ключевые точки, но не справляется с точками, скрытыми от камеры.
2. Вариационный автокодировщик. Это генеративная модель для оценки правдоподобия предсказываемых значений ключевых точек, принцип работы которой заключается в моделировании распределения на пространстве скрытых переменных, отвечающих за ключевые особенности объектов на изображении. Приближение распределения на предсказываемых данных достигается алгоритмом оптимизации нижней границы на обоснованность (ELBO). Теория и вариации такой архитектуры подробно описаны в работе [3]. Вариационный автокодировщик позволил захватить информацию о скрытых точках, но его генеративная природа не позволила достигнуть достаточной точности при определении их пространственного положения.
3. Комбинация сверточной сети с вариационным кодировщиком. Учитывая преимущества и проблемы двух рассмотренных до этого архитектур, естественным шагом является их комбинация с правильным распределением задач. В связи с этим в ходе исследования разработана модель глубокой нейронной сети, получающей на вход изображения с камер, и обрабатывающей эти данные в непоследовательном графе вычислений. Сначала вариационный кодировщик моделирует распределение скрытых переменных для оценки матрицы аффинного преобразования пространства, включающей информацию о повороте и сдвиге объекта в пространстве. Кроме того, кодировщик предсказывает структуру группы ключевых точек для данного объекта, отвечающую его геометрической форме. Данные, предсказываемые кодировщиком, подаются на вход сверточной сети вместе с исходными изображениями. Она использует изображения для уточнения предсказания положения ключевых точек, полученного кодировщиком.
4. Интерес представляет использование капсульной сети, сильной стороной которой является внимание к пространственному положению детектируемых особенностей на изображении. Хотя на данный момент инструмент капсульных сетей недостаточно развит, в конце 2017 года был предложен эффективный метод обучения таких сетей. Использование данной архитектуры можно рассматривать как дальнейшее направление исследования.

Все предложенные архитектуры включают в себя общепринятые методы регуляризации, такие как батч-нормализация или дропаут. Без использования этих техник сети склонны к переобучению.

Предложенные архитектуры разрабатываются и обучаются с использованием фреймворков Tensorflow и Keras. В качестве функций потерь используются дивергенция Кульбака–Лейблера, при обучении вариационного кодировщика в пространстве скрытых переменных, и среднеквадратичное отклонение, при обучении объемных предсказаний.

Дальнейшее исследование должно двигаться в направлении обобщения распознавательной способности на модели различных геометрических форм. Кроме того, требуется повышать надежность системы на случай наличия лишь одной камеры. Бинокулярное зрение может играть существенную роль в качестве модели. В таком сценарии должна возрасти роль предсказываемой вариационным кодировщиком матрицы аффинного преобразования.

**Литература**

1. Park S., Hwang J., Kwak J. 3D human pose estimation using convolutional neural networks with 2D pose information // In ECCVW. – 2016. – P. 156–169.
2. Pavlakos G., Zhou X., Derpanis K.G., Daniilidis K. Coarse-to-Fine Volumetric Prediction for Single-Image 3D Human Pose [Электронный ресурс]. – Режим доступа: https://arxiv.org/pdf/1611.07828.pdf, своб.
3. Doresch C. Tutorial on Variational Autoencoders [Электронный ресурс]. – Режим доступа: https://arxiv.org/pdf/1606.05908.pdf, своб.

**Воронов Александр Сергеевич**
Год рождения: 1991
Университет ИТМО, факультет систем управления и робототехники, кафедра информационно-навигационных систем, аспирант,
Направление подготовки: 12.06.01 – Фотоника, приборостроение, оптические и биотехнические системы и технологии
АО «Концерн «ЦНИИ «Электроприбор», м.н.с.
e-mail: al-s-voronov@yandex.ru

**Кондрашкин Геннадий Евгеньевич**
Год рождения: 1995
Университет ИТМО, факультет систем управления и робототехники, кафедра информационно-навигационных систем,
студент группы № Р4130
Направление подготовки: 24.04.02 – Системы управления движением и навигация
e-mail: gena-kondrashkin@mail.ru

**УДК 629.5.054**

# ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ КОМПОЗИЦИОННЫХ МАТЕРИАЛОВ В ПРИБОРАХ НАВИГАЦИИ

**Воронов А.С., Кондрашкин Г.Е.**
**Научный руководитель – д.т.н., доцент Евстифеев М.И.**

Рассмотрены преимущества применения композиционных материалов в приборах навигации. Показана эффективность применения композитов для приборов судостроения. Приведено сравнение основных свойств композиционных материалов с классическими конструкционными. Представлены примеры использования композитов в приборах навигации. Описана перспектива применения композитов в аддитивных технологиях 3D-печати.
**Ключевые слова:** композиционный материал, механические свойства, аддитивные технологии, магнитная проницаемость, приборы навигации.

В настоящее время благодаря наборам специфических свойств и развитию технологий производства, композиционные материалы (КМ) находят применение в различных сферах деятельности, таких как машино-, авиа-, судостроение и т.д., причем сферы их использования постоянно расширяются. Применение КМ открывает возможности для разработки новых конструкций или модернизации уже существующих.

Целью работы являлось определение возможности применения композиционных материалов в элементах конструкции приборов навигации.

Композиционный материал – материал, состоящий из двух и более компонентов (фаз). Обязательными фазами являются матрица и наполнитель. Помимо этого в состав композита могут вводиться различные компоненты для улучшения его свойств, такие как ускоритель, упрочнитель, отвердитель и т.д. [1]. В зависимости от типов и соотношений этих компонентов, можно управлять свойствами композита, такими как прочность, плотность, упругость, жаропрочность, коррозионная стойкость и т.д. В отличие от КМ, традиционные конструкционные материалы (сталь, титан) не обладают широким диапазоном значения свойств.

В таблице представлено сравнение значений основных характеристик сталей и некоторых композиционных материалов.

Таблица. Сравнительная характеристика материалов

| Характеристика | Пено-пласт | Синтак-тик | Сферо-пластик | Угле-пластик | Стекло-пластик | Сталь | Титан |
|---|---|---|---|---|---|---|---|
| Плотность, кг/м$^3$ | 30–400 | 400–650 | 570–720 | 1450–2000 | 1600–2000 | 7640–8800 | 4120–4540 |
| Модуль упругости при сжатии, МПа | 20–600 | 1000–3000 | 130–1300 | 120000–130000 | 18000–40000 | 200000–210000 | 112000–120000 |
| Предел прочности, МПа | 0,7–15 | 25–46 | 90–120 | 490–600 | 400–440 | 330–600 | 300–450 |
| Коэффициент температурного расширения, $(1/К)\cdot10^{-6}$ | 5–10 | 8 | 45–65 | 1–2 | 5–14 | 13 | 7,7–10,4 |
| Диэлектрическая проницаемость, $10^6$ Гц | 1,0-1,3 | 1,2–2,0 | 1,3–1,5 | 2–4 | 4–5 | – | – |
| Акустическая прозрачность | 0,05–0,5 | 0,3–0,45 | 0,3–0,45 | 0,2 | 0,02 | 0,001–0,01 | 0,02–0,1 |

В последнее время КМ все чаще применяются при изготовлении корпусов как надводных судов, так и подводных аппаратов, в частности, автономных необитаемых. Такие композиционные материалы должны обеспечивать достаточную прочность конструкции и способность предотвратить повреждение компонентов подводного аппарата в случае столкновения с какими-либо объектами [2]. Одними из наиболее перспективных КМ для создания корпусов автономных необитаемых подводных аппаратов (АНПА) являются сферопластики, стеклопластики, углепластики. Основными их преимуществами являются прочность, возможность работы в агрессивных средах без коррозии, а также сохранение стабильности размеров при смене температуры. Очевидно, такие композиты нашли свое применение в приборах навигации [1].

В АО «Концерн «ЦНИИ «Электроприбор», одном из ведущих предприятий в области разработке и производстве навигационных систем, КМ используются в различных приборах. Одними из примеров использования композиционных материалов является аварийно-спасательный буй (рис. 1, а). Буй устанавливается на подводные лодки и в случае аварийной ситуации отдается и всплывает на поверхность для подачи сигнала [3]. Корпус данного устройства изготовлен из сферопластика. Одним из преимуществ этого композита является малая плотность и высокая прочность, что позволяет снизить массу и увеличить плавучесть.

а б

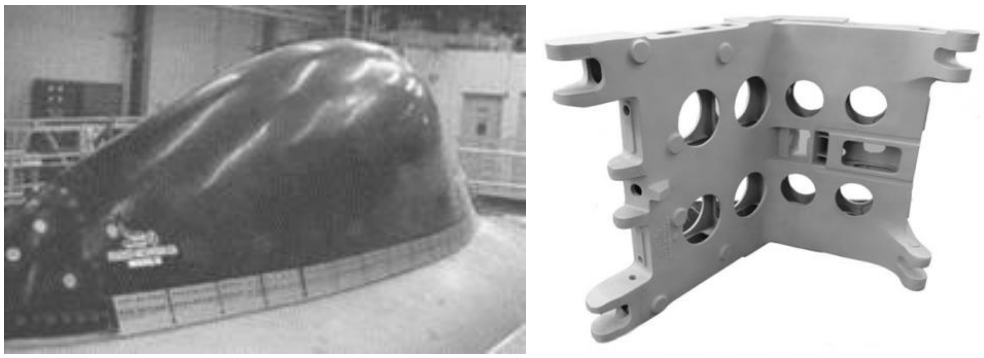
Рис. 1. Аварийно-спасательный буй (а); датчик индукционного лага (б)

В приборе УПИ (устройство приемное индукционное) – датчике индукционного лага (рис. 1, б) используется заливочный КМ – компаунд, основная задача которого состоит в герметизации электроники и контактов. Компаунд защищает блок электроники от внешних механических воздействий и гидростатических нагрузок. Применение титанового армирующего элемента и корпуса позволяет увеличить прочность датчика и расширить сферу его использования [4].

В приборах навигации возможно применение композитов для антенн радиопеленгатора, гирокомпасов и других приборов (обтекатели акустических антенн подводной лодки, обтекатели выдвижных устройств). Отличительной особенностью применения стеклопластиков в данных устройствах является его акустическая прозрачность.

Перспективным направлением композиционных материалов является их использование на судах автономных систем в качестве гребных винтов из углепластика подводной лодки. В сравнении с традиционным материалом гребного винта (марганцево-бронзовый сплав), углепластик обладает виброакустическими и прочностными характеристиками [5].

В судостроении КМ, а именно стеклопластики, используются в качестве носового обтекателя ограждения выдвижных устройств (ОВУ) (рис. 2, а), устройства роботизированной коробки передач, решеток забортных отверстий. Основная причина применения композиционных материалов в данных устройствах обусловлена рядом их преимуществ перед традиционным материалом – статью: повышенная коррозионная стойкость, меньшая масса, приводящая к облегчению всей конструкции устройства, пониженная горючесть, а также стойкость к солнечной и ультрафиолетовой радиации [5].



а б

Рис. 2. Физическая модель ОВУ (а); изделие из композитного материала, изготовленное с помощью аддитивных технологий (б)

Все чаще для производства деталей различной сложности применяются аддитивные технологии. Одним из перспективных направлений данных технологий является 3D-печать различных деталей и заготовок. Использование трехмерной печати обусловлено рядом преимуществ: существенное уменьшение подготовки к изготовлению и временных затрат на создание детали, снижение финансовых затрат и отходов производства. Недостатками данной технологии является дороговизна самих устройств и материалов для печати. На рис. 2, б представлено изделие, выполненное с помощью аддитивных технологий [6].

Эксплуатационные требования, предъявляемые к деталям, обуславливают выбор материала, используемого для 3D-печати. На сегодняшний день известно большое количество материалов для создания 3D-моделей: пластик, фотополимерные материалы, металлические и композитные порошки. Основными отличительными особенностями для пластика является его высокая прочность, гибкость, износостойкость; для фотополимерных материалов – высокая точность и детализация, гладкая поверхность готовых изделий, низкая температура размягчения; для металлических порошков – большой выбор металлов и их сплавов, повышенная прочность, любая геометрия; для композитных порошков – возможность создания полноцветных объектов, низкая себестоимость. Очевидно, КМ нашли применение для 3D-печати в приборах навигации [6]. Одними из примеров таких приборов

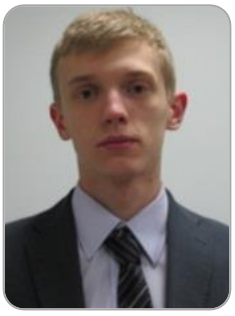
является гиростабилизированный гравиметр, микромеханический гироскоп RR-типа и гироскопический прибор с карданновым подвесом. В дальнейшем при развитии аддитивной технологии возможно создание приборов на основе металлических порошков.

**Результаты.** В связи с расширением использования композиционных материалов в судостроении и возможностью их применения в приборах навигации, они представляют собой актуальную задачу исследования. Применение композитов открывает возможности для решения новых задач, а также позволяет добиться требуемых свойств конструкции, что невозможно при использовании традиционных конструкционных материалов. Широко развивающееся направление изготовления деталей из композиционных материалов с помощью аддитивных технологий актуально как для судостроительной отрасли, так и для проектирования приборов навигации.

**Литература**

1. Кербер М.Л., Виноградов В.М., Головкин Г.С. и др. Полимерные композиционные материалы: структура, свойства, технология: учебное пособие / Под ред. А.А. Берлина. – СПб.: Профессия, 2008. – 560 с.
2. Гуменюк Н.С., Грушин С.С. Применение композитных материалов в судостроении // Современные наукоемкие технологии. – 2013. – № 8(1). – С. 116–117.
3. Новак А. РИА новости [Электронный ресурс]. – Режим доступа: https://ria.ru/science/20041101/722358.html (дата обращения: 20.02.2018).
4. Аванесов Ю.Л., Воронов А.С., Евстифеев М.И. Компьютерное моделирование прочностных характеристик датчика индукционного лага // Научно-технический вестник информационных технологий, механики и оптики. – 2016. – Т. 16. – № 4. – С. 738–744.
5. Никитин В.С., Половинкин В.Н. Применение композитных материалов в зарубежном подводном кораблестроении [Электронный ресурс]. – Режим доступа: http://www.proatom.ru/modules.php?name=News&file=article&sid=7479 (дата обращения: 24.02.2018).
6. 3D-оборудование для профессионалов. Основы 3D печати [Электронный ресурс]. – Режим доступа: http://3d.globatek.ru/world3d/osnovy_3D_pechati/ (дата обращения: 05.03.2018).

**Гаврилова Марина Владимировна**
Год рождения: 1996
Университет ИТМО, факультет систем управления и робототехники,
кафедра информационно-навигационных систем,
студент группы № Р3430
Направление подготовки: 24.03.02 – Системы управления движением и навигация
e-mail: marinagavrilova2012@yandex.ru



**Ефремов Роман Сергеевич**
Год рождения: 1990
АО «Концерн «Электроприбор»
e-mail: rsefremov@gmail.com

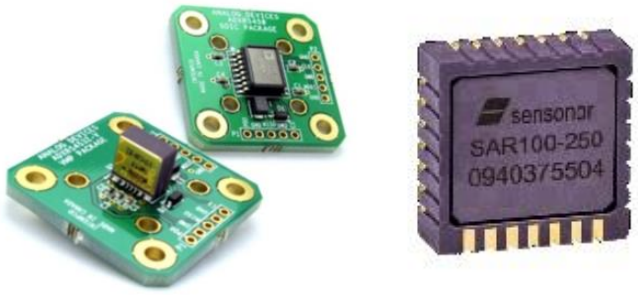
**УДК 681.51**

# РАЗРАБОТКА И ИЗГОТОВЛЕНИЕ ЭКСПЕРИМЕНТАЛЬНОГО ОБРАЗЦА МИКРОМЕХАНИЧЕСКОГО ГИРОСКОПА С ВЕРТИКАЛЬНОЙ ОСЬЮ ЧУВСТВИТЕЛЬНОСТИ

**Гаврилова М.В.** (Университет ИТМО)**, Ефремов Р.С.** (АО «Концерн «ЦНИИ «Электроприбор»)
**Научный руководитель – к.т.н. Ковалёв А.С.** (АО «Концерн «ЦНИИ «Электроприбор»)

Работа посвящена разработке и изготовлению микромеханического гироскопа в новом корпусе, обеспечивающем возможность монтажа на боковую грань. По результатам испытаний в горизонтальном положении подтверждена работоспособность микромеханического гироскопа в новом корпусе. С учетом новой электрической принципиальной схемы разработан экспериментальный образец микромеханического гироскопа с вертикальной осью чувствительности. Проведены испытания экспериментального образца.
**Ключевые слова:** датчик, микромеханика, микромеханический гироскоп, микроэлектроника, навигация.

В настоящее время микромеханические датчики (ММД) применяются при решении широкого спектра задач: от определения положения мобильного телефона в руках пользователя до построения на их основе высокоточных систем ориентации и навигации. На зарубежном рынке ММД такими фирмами как Analog Devices, STMicroelectronics, Sensonor, представлена номенклатура микромеханического гироскопа (ММГ), отвечающая различным требованиям потребителей к целому ряду параметров: количество осей чувствительности, диапазон измерения, точностные характеристики, а также конструктивные особенности [1–3]. Среди представленных ММГ можно выделить датчики, поставляемые в корпусах, позволяющих монтировать их на печатные платы в двух положениях: горизонтальном и вертикальном. Примером таких ММГ могут служить ADXRS453 фирмы Analog Devices (рис. 1, а) и SAR100 фирмы Sensonor (рис. 1, б).




а б

Рис. 1. Гироскоп ADXRS453 (а); гироскоп SAR100 (б)

В табл. 1 приведены характеристики гироскопов ADXRS450, ADXRS453, SAR100, а также гироскопа ММГ-ЭП1, разработанного в АО «Концерн «ЦНИИ «Электроприбор» [4].

Таблица 1. Характеристики зарубежных и отечественного ММГ

| | Диапазон измерения, °/с | Плотность мощности шума, °/с/√Гц | Нелинейность градуировочной характеристики, % | Полоса пропускания, Гц |
|---|---|---|---|---|
| ADXRS450 | ±400 | 0,015 | 0,05 | 80 |
| ADXRS453 | ±400 | 0,015 | 0,05 | 77,5 |
| SAR100 | ±400 | 0,03 | 0,1 | 50 |
| ММГ-ЭП1 | ±450 | 0,005 | 0,5 | 200 |

Из табл. 1 видно, что характеристики изделия ММГ-ЭП1 сопоставимы с характеристиками зарубежных аналогов. Предполагается, что с использованием чувствительного элемента (ЧЭ), применяемого в ММГ-ЭП1, и нового корпуса можно разработать ММГ с вертикальной осью чувствительности и аналогичными характеристиками.

В настоящей работе было необходимо оценить возможность применения корпуса с дополнительными контактными площадками для создания гироскопа с вертикальной осью чувствительности. На рис. 2 показана трехмерная модель применяемого корпуса.

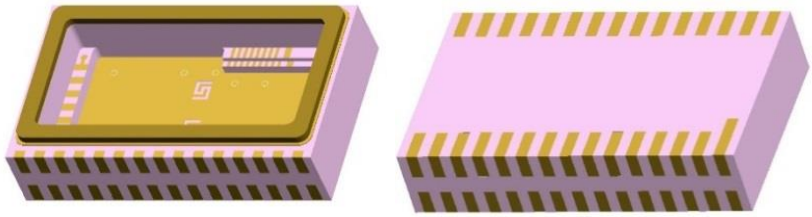


Рис. 2. Модель корпуса с выводами на ребро

При разработке и изготовлении ММГ в новом корпусе был взят за основу типовой технологический процесс сборки ММГ, который условно можно разделить на три части:

1. монтаж интегральной микросхемы и ЧЭ в корпус;
2. проволочная микросварка;
3. герметизация.

Для проверки работоспособности ММГ в новом корпусе были проведены испытания в горизонтальном положении. Испытания проводились для определения коэффициента преобразования, плотности мощности шума и нестабильности нулевого сигнала. Результаты испытаний представлены в табл. 2.

Для включения экспериментального ММГ в вертикальном положении был разработан специальный макет. Особенностью ММГ в новом корпусе и принципиальной электрической схемы для его включения является неизменный состав электрорадиоизделия (ЭРИ) и электрических цепей, но и отличное расположение выводов на корпусе. С учетом этой

особенности, разработанный макет включал в себя имеющуюся тестовую плату с ЭРИ, применяемую для проведения испытаний в горизонтальном положении, к которой была подсоединена макетная печатная плата. Описанная конструкция, включающая в себя тестовую и макетную печатную плату, а также напаянный ММГ, приведена на рис. 3.

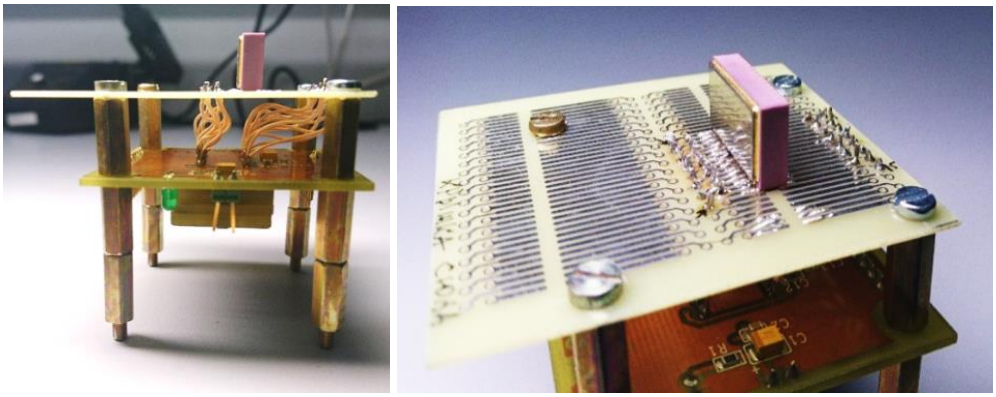


Рис. 3. Экспериментальный макет

Результаты испытаний для двух положений представлены в табл. 2.

Таблица 2. Результаты испытаний

| | Коэффициент преобразования, ед. | Плотность мощности шума, °/с/√Гц | Нестабильность нулевого сигнала, °/час |
|---|---|---|---|
| Горизонтальное положение | –0,209 | 0,0149 | 18,75 |
| Вертикальное положение | –0,194 | 0,0047 | 6,93 |

Исходя из полученных результатов испытаний, можно сделать вывод, что новый корпус не вносит значительных изменений в работу ММГ, а характеристики при вертикальном монтаже сравнимы с характеристиками в горизонтальном положении. Результаты работы могут быть использованы для создания нового исполнения ММГ с вертикальной осью чувствительности.

**Литература**

1. Analog Devices [Электронный ресурс]. – Режим доступа: http://www.analog.com, своб.
2. STMicroelectronics [Электронный ресурс]. – Режим доступа: http://www.st.com, своб.
3. Sensonor [Электронный ресурс]. – Режим доступа: http://www.sensonor.com, своб.
4. Пешехонов В.Г. и др. Результаты испытаний установочной партии микромеханических гироскопов RR-типа // Гироскопия и навигация. – 2011. – № 1(72). – С. 37–48.

**Гопанков Даниил Николаевич**
Год рождения: 1995
Университет ИТМО, факультет систем управления и робототехники,
кафедра информационно-навигационных систем,
студент группы № Р4130
Направление подготовки: 24.04.02 – Системы управления движением и навигация
e-mail: gopankov_d@mail.ru

**Степанов Алексей Петрович**
Год рождения: 1981
Университет ИТМО, факультет систем управления и робототехники,
кафедра информационно-навигационных систем, д.т.н., доцент
АО «Концерн «ЦНИИ «Электроприбор», ст.н.с.
e-mail: apstepanow@mail.ru

**УДК 621.371.361.1**

# АНАЛИЗ ПОГРЕШНОСТЕЙ ИНЕРЦИАЛЬНО-СПУТНИКОВОЙ СИСТЕМЫ НА МИКРОМЕХАНИЧЕСКИХ ИНЕРЦИАЛЬНЫХ ДАТЧИКАХ, АНТЕННЫЙ МОДУЛЬ КОТОРОЙ ИМЕЕТ РАСПРЕДЕЛЕННЫЙ В ПРОСТРАНСТВЕ ФАЗОВЫЙ ЦЕНТР

**Гопанков Д.Н.**
**Научный руководитель – д.т.н., доцент Степанов А.П.**

Проведен аналитический обзор существующих на сегодняшний день особенностей спутниковых навигационных систем. Представлены возможные варианты повышения точности и методы борьбы с многолучевостью посредством информации от инерциального измерительного модуля. Анализируя текущее состояние СНС-компасов, предложена схема построения СНС-компаса, позволяющая повысить его точность при сохранении требуемых массогабаритных характеристик.
**Ключевые слова:** навигационная система, фазовые измерения, СНС-компас, многолучевость, фазовый центр.

Ужесточение требований в области обеспечения безопасности судовождения, стабилизации комплексов различных технических средств, освоение северных районов Мирового океана обуславливают создание новых подходов к информационному обеспечению подвижных объектов. В связи с этим массовое применение находят информационные системы, базирующиеся на технологиях глобальных спутниковых навигационных систем (СНС). Одной из таких систем, широко применяемых для навигационного обеспечения подвижных объектов, является так называемый «СНС-компас».

Современные спутниковые компасы – это системы, представляющие собой многоантенную спутниковую приемную аппаратуру, основной задачей которой является определение с высокой точностью не только линейной скорости и координат места, но также и параметров ориентации объекта, включая истинный курс. Исходной информацией в данных системах служат фазовые измерения на несущей частоте спутникового сигнала [1].

Рассмотрим основные проблемы СНС-компасов. На данный момент в существующих СНС-компасах, основные подходы построения которых уже стали классическими, проблемы повышения точности и устранения многолучевости являются наиболее трудоемкими для решения. Известна проблема устранения неоднозначности фазовых измерений.

Точность определения параметров ориентации зависит от длины базы, т.е. от расстояния между фазовыми центрами антенн, и с увеличением длины базы растет и

точность. Однако повышение точности за счет увеличения размеров базы представляется неприемлемым, так как размещение громоздких СНС-компасов возможно далеко не на всех суднах. В то же время, небольшие габариты компаса повышают угловую жесткость системы.

В СНС-компасах точность во многом определяется взаимным положением антенной базы и навигационного спутника (НС). Например, наиболее выгодным положением является окологоризонтное (на высотах порядка от 5 до 45 градусов) с взаимно ортогональным расположением линий НС-ведущая антенна и антенная база. Такое взаимное положением возможно, по аналогии с решением задачи навигации в приемной аппаратуре СНС, охарактеризовать геометрическим фактором взаимного положения базы и НС. Особенно актуальной проблема геометрического фактора становится при резком снижении количества НС, участвующих в решении.

Рассмотрим известные методы борьбы с вышеописанными проблемами при использовании в СНС-компасе только информации от СНС, т.е. без интеграции в него инерциального измерительного модуля.

Использование фазовых измерений позволяет достичь высокой точности показаний спутниковых навигационных систем лишь после определения целого числа длин волн, укладывающихся в измеряемом расстоянии от спутника до приемника. Задача определения этих периодов известна как задача исключения неоднозначности. Необходимость ее решения возникает на начальном этапе обработки фазовых измерений, при появлении новых спутников, или после перерывов в приеме спутниковых сигналов.

Перечислим известные методы борьбы с неоднозначностью в СНС-компасах [2]:

1. изменение положение спутников;
2. измерения от избыточного количества спутников;
3. двухчастотные измерения;
4. дополнительные антенны на коротких базах;
5. вращение объекта;
6. вращение измерительного модуля.

Не будем подробно останавливаться на каждом из методов. Первые пять методов и раньше повсеместно использовались для исключения неоднозначности в СНС-компасах. Шестой метод был впервые использован в СНС-компасе ОРИОН разработки АО «ЦНИИ «Электроприбор» и доказал свою эффективность с точки зрения возможности осуществления калибровки в условиях объекта гироскопов, акселерометров, погрешностей фазы несущей, лучшего значения геометрического фактора многоантенной системы, в связи с чем достигается высокая точность определения ориентации.

Далее перейдем к описанию следующей немалозначимой проблемы – устранение многолучевости. Для смягчения эффектов многолучевого распространения существует два метода:

1. алгоритмический: метод обработки сигналов;
2. аппаратный: многолучевые дроссельные кольца.

Метод обработки сигналов. В этом методе анализируются данные для разделения прямого сигнала от косвенного сигнала (сигналов). Если косвенный путь значительно длиннее прямого пути, тогда с легкостью возможно отличить их друг от друга. Но если разница мала, и отраженный сигнал близок к прямому сигналу, то различить их будет проблематично. При использовании сигналов СНС метод обработки сигналов неэффективен, если разница между прямым путем и косвенным путем составляет менее нескольких метров. Удаление многолучевого сигнала происходит за счет удаления части прямого сигнала, что, в свою очередь, увеличивает уровень шума. В связи с этим можно сделать вывод, что метод обработки сигналов подходит для сигналов, разница в длине пути которых более 10 м [3].

Многолучевые дроссельные кольца. Эта техника работает только для многолучевых сигналов, отраженных от объектов, находящихся главным образом ниже антенны. Отраженный сигнал, который попадает на нижнюю сторону антенны, может быть устранен.

Недостатком данного метода является невозможность устранения отраженных сигналов сверху, т.е. источник отраженного сигнала расположен над антенной, например, отраженный сигнал от высотного здания [4].

При использовании сразу двух этих методов можно уменьшить влияние как близкорасположенных отраженных сигналов, так и удаленных.

Также в борьбе с многолучевостью стоит отметить антенны с правой круговой поляризацией. При отражении сигнала от сильно отражающей поверхности его круговая поляризация изменяется с правосторонней на левостороннюю, и антенны, спроектированные для сигналов с правосторонней поляризацией, будут ослаблять сигналы с противоположной поляризацией.

На сегодняшний день компании по производству СНС-компасов стремятся минимизировать массогабаритные характеристики, однако это негативно сказывается на точности выдачи навигационных параметров. Также одним из недостатков современных СНС-компасов стоит выделить проблему необходимости как минимум четырех спутников для решения задачи навигации и значительное время готовности к работе.

Погрешность выработки курса для существующих СНС-компасов можно описать зависимостью $0,6^{\circ} \cdot 1/L(3\sigma)$, где $L$ – межантенное расстояние [5].

В последующей работе будет разрабатываться схема СНС-компаса как интегрированной системы на микромеханических инерциальных датчиках, антенный модуль которой имеет распределенный в пространстве фазовый центр, обеспечивающей определение параметров ориентации, в том числе истинного курса, при наблюдении лишь одного навигационного спутника. Предполагается, что в системе будет осуществляться сканирующее движение фазового центра антенной системы для решения проблемы неоднозначности фазовых измерений, возможности работы только с одним спутником и борьбы с явлением многолучевости.

Данная схема будет строиться на основе уже существующего СНС-компаса ОРИОН, принцип действия которого основан на механическом вращении измерительного модуля.

Планируемый СНС-компас вращаться не будет, однако новизной планируемой работы будет то, что вращение системы будет имитироваться программно путем управления фазовым центром антенной системы. Для проверки основных положений в работе предполагается проведение полунатурных экспериментов.

**Заключение.** Использование многоантенного СНС-компаса с распределенным в пространстве фазовым центром позволит решить задачу сохранения высокой точности показаний при уменьшении массогабаритных характеристик. К тому же данная схема построения сокращает количество необходимых спутников для решения задачи навигации до одного.

**Литература**

1. Антонович К.М. Использование спутниковых радионавигационных систем в геодезии: монография В 2-х т. Т.1. – М.: ФГУП «Картгеоцентр», 2005. – 334 с.
2. Степанов О.А., Кошаев Д.А. Исследование методов решения задачи ориентации с использованием спутниковых систем // Гироскопия и навигация. – 1999. – № 2. – С. 30–54.
3. Емельянцев Г.И. О результатах обработки данных навигационных спутников ГЛОНАСС в GPS-компасе с антенной базой на уровне длины волны несущей // XXII Межд. конф. по интег. навигационным системам. – 2015. – С. 9–20.
4. Mohinder S., Grewal L.R. Global Positioning Systems, Inertial Navigation, and Integration. – John Wiley & Sons, 2004. – 554 p.
5. Емельянцев Г.И., Степанов А.П. Интегрированные инерциально-спутниковые системы ориентации и навигации. – СПб.: ГНЦ РФ АО «Концерн «ЦНИИ «Электроприбор», 2016. – 394 с.

**Иванов Дмитрий Павлович**
Год рождения: 1994
Университет ИТМО, факультет систем управления и робототехники,
кафедра информационно-навигационных систем,
студент группы № Р4230
Направление подготовки: 24.04.02 – Системы управления движением и навигация
e-mail: iPostDima@ya.ru

**УДК 531.383.001.4**

# ИДЕНТИФИКАЦИЯ ПАРАМЕТРОВ ТЕМПЕРАТУРНОЙ МОДЕЛИ ПОГРЕШНОСТИ ГИРОСКОПА

**Иванов Д.П.**
**Научный руководитель – к.т.н., доцент Литвиненко Ю.А.**

Работа выполнена в рамках темы НИР № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность».

Проблема идентификации неизвестных параметров модели ухода гироскопа рассмотрена в постановке нелинейной задачи фильтрации, предполагающей наличие нелинейностей в модели динамики. Предложен подход, построенный на базе фильтра калмановского типа, и его сравнение с алгоритмом идентификации на основе метода наименьших квадратов.
**Ключевые слова:** модель погрешности, фильтрация, идентификация.

**Введение.** В настоящее время в системах инерциальной навигации и стабилизации для обработки информации активно применяют алгоритмы калмановской фильтрации [1–3]. Бесспорным преимуществом такого подхода является легкость реализации рекуррентных процедур для выработки навигационных параметров, однако, такие процедуры требуют достаточно точного описания поведения динамической системы и процесса измерений.

Для решения задачи идентификации параметров моделей чувствительных элементов, используемых для настройки фильтров калмановского типа, предложены различные методы, [4, 5], в частности, субоптимальные алгоритмы обработки информации на базе метода наименьших квадратов (МНК) [4] и полиномиальной фильтрации [5]. Следует отметить, что удобный и экономичный с вычислительной точки зрения подход, рассмотренный в [4], не допускает его использования при идентификации суммы составляющих погрешностей чувствительных элементов, что ограничивает его применение. В этой связи в данной работе рассмотрена возможность решения задачи идентификации при нелинейности в уравнениях динамики, описывающих поведение погрешностей чувствительных элементов, с использованием подхода, связанного с линеаризацией уравнений динамики с последующим использованием фильтров калмановского типа. Основным предметом исследования являлось рассмотрение особенностей реализации фильтров калмановского типа, связанных с выбором точки линеаризации уравнений динамики, и оценка эффективности таких алгоритмов путем сравнения с результатами, приведенными в [4]. Для идентификации неизвестных параметров предложено использовать:

– линеаризованный фильтр Калмана (ФК);
– обобщенный фильтр Калмана (ОФК).

Объектом исследований явились погрешности двухстепенного поплавкового гироскопа в составе инерциальной навигационной системы среднего класса точности.

**Описание модели.** В целях сравнения с результатами, приведенными в [4], будем полагать, что уход гироскопа описывается марковским процессом первого порядка:

$$\dot{\varepsilon}(t) = -\alpha\varepsilon(t) + \sqrt{2\alpha\sigma_\varepsilon^2}\xi(t)\ ,\ \varepsilon(0) \in N\{0, \sigma_\varepsilon^2\}, \quad (1)$$

где $\xi(t)$ – гауссовский белый шум единичной интенсивности, распределенный по нормальному закону с дисперсией $\sigma_\varepsilon$; $\alpha$ – неизвестный параметр корреляции, подлежащий идентификации.

При этом задача идентификации решается по измерениям, проведенным в дискретные моменты времени *k*:

$$Y(k) = \varepsilon(k) + \nu(k),\ \nu(k) \in N\{0, R\}. \quad (2)$$

Предполагается, что параметр $\alpha$ не меняется во времени, и, следовательно, может быть описан как $\dot{\alpha} = 0$.

Рассмотрим ряд алгоритмов определения параметра $\alpha$, основанных на разложении нелинейных функций в ряд Тейлора в некоторых точках линеаризации $\varepsilon_0, \alpha_0$. Вводя обозначения:

$$\varepsilon(t) = \varepsilon_0(t) + \Delta\varepsilon(t),\ \alpha = \alpha_0 + \Delta\alpha\ , \quad (3)$$

модель (1) можно записать в виде суммы:

$$\dot{\varepsilon}_0(t) + \Delta\dot{\varepsilon}(t) = -(\alpha_0 + \Delta\alpha)(\varepsilon_0(t) + \Delta\varepsilon(t)) + \sqrt{2(\alpha_0 + \Delta\alpha)\sigma_\varepsilon^2}\xi(t)\ . \quad (4)$$

Из которого может быть получено следующее выражение с точностью до членов второго порядка малости для описания поведения $\Delta\varepsilon(t)$ и $\varepsilon_0(t)$:

$$\Delta\dot{\varepsilon}(t) \cong -\alpha_0\Delta\varepsilon(t) - \Delta\alpha\varepsilon_0(t) + \sqrt{2\alpha_0\sigma_\varepsilon^2}\xi(t),\ \dot{\varepsilon}_0(t) = -\alpha_0\varepsilon_0(t)\ . \quad (5)$$

В силу постоянства описания параметра корреляции α, вводя вектор состояния $\Delta X_P(t) = |\Delta\varepsilon, \Delta\alpha|^T$, его поведение может быть описано следующим приближенным линеаризованным уравнением:

$$\dot{X}_P(t) = F_P(t)X_P(t) + G_P(t)\xi_P(t) = \begin{vmatrix}\Delta\dot{\varepsilon}(t)\\ \Delta\dot{\alpha}(t)\end{vmatrix} \approx \begin{vmatrix}-\alpha_0 & -\varepsilon_0(t)\\ 0 & 0\end{vmatrix}\begin{vmatrix}\Delta\varepsilon(t)\\ \Delta\alpha(t)\end{vmatrix} + \begin{vmatrix}\sqrt{2\sigma_\varepsilon^2\alpha_0}\xi(t)\\ 0\end{vmatrix}. \quad (6)$$

При этом модель псевдоизмерений может быть описана как:

$$Y'(k) = Y(k) - X_0(k) = \Delta X(k) + \nu(k) = H_P X_P(k) + \nu(k), \quad (7)$$

где $H_P = [1\ \ 0]$.

Используя стандартные процедуры перехода к дискретному времени можно получить два алгоритма оценивания на базе фильтров калмановского типа: линеаризованный фильтр, когда точка линеаризации $\alpha_0$ постоянна, а точка $\varepsilon_0(t)$ меняется в соответствии с (4), и обобщенный фильтр, особенностью которого является уточнение точек линеаризации на величину выработанных по измерениям поправок. Изложенный подход может быть легко обобщен на случай описания поведения чувствительных элементов комбинацией нескольких случайных процессов.

**Результаты.** Для оценки качества алгоритмов предлагается, в качестве измерений, использовать тестовую реализацию процесса (1) с различными значениями дисперсии $\sigma_\varepsilon$. Результаты идентификации неизвестного параметра $\alpha$ на основе трех алгоритмов, варьируя $\alpha_0$, приведены в таблице.

Таблица. Ошибка оценки параметра $\alpha$ с использованием МНК, ФК и ОФК

| Значение $\sigma_\varepsilon$, °/ч | Относительная погрешность, % | | | | | | |
|---|---|---|---|---|---|---|---|
| | МНК | ФК | | | ОФК | | |
| | | $\alpha_0 = 1$ | $\alpha_0 = 0{,}1$ | $\alpha_0 = 0{,}001$ | $\alpha_0 = 1$ | $\alpha_0 = 0{,}1$ | $\alpha_0 = 0{,}001$ |
| 0,01 | 0,28 | 18,42 | 0,71 | 1,42 | 0,48 | 1,14 | 1,85 |
| 0,1 | 2,85 | 12,78 | 7,15 | 6,98 | 0,72 | 0,72 | 0,72 |
| 1 | 39,77 | 71,00 | 71,00 | 71,00 | 7,51 | 7,51 | 7,51 |

**Заключение.** Изложен подход к идентификации неизвестных параметров модели ухода гироскопа, сводящейся к нелинейной задаче фильтрации, решение которой рассмотрено с использованием процедур фильтров калмановского типа, при линеаризации уравнений динамики, описывающих поведение ошибок чувствительных элементов. Получены рекуррентные алгоритмы оценивания для линеаризованного и обобщенного фильтра Калмана. Результаты моделирования показали перспективность использования такого подхода при решении задач идентификации при сложном описании поведения погрешностей чувствительных элементов, в частности, при наличии составляющих, зависящих от температуры. С учетом определенной свободы выбора закона изменения точки линеаризации во времени, перспективной задачей дальнейших исследований является анализ влияния такого выбора на точность решения задачи идентификации.

**Литература**

1. Моторин А.В., Степанов О.А., Торопов А.Б. Многоальтернативная фильтрация применительно к задаче оценивания модели погрешностей датчиков // Материалы XVII Конференции молодых ученых «Навигация и управление движением». – 2015. – С. 267–274.
2. Степанов О.А. Методы обработки навигационной измерительной информации. Учебное пособие. – СПб.: Университет ИТМО, 2017. – 196 с.
3. Моторин А.В., Степанов О.А. Сравнение методов идентификации моделей ошибок датчиков, основанных на вариациях Аллана и алгоритмах нелинейной фильтрации // Материалы XXI Санкт-Петербургской международной конференции по интегрированным навигационным системам. – 2014. – С. 98–103.
4. Тупысев В.А., Круглова Н.Д., Моторин А.В. Субоптимальные алгоритмы идентификации погрешностей навигационных датчиков, описываемых марковским процессом // Гироскопия и навигация. – 2016. – Т. 24. – № 3(94). – С. 55–62.
5. Hernandez-Gonzalez M., Basin M., Stepanov O. Discrete-time state estimation for stochastic polynomial systems over polynomial observations // International Journal of General Systems. – 2018. – V. 47(5). – P. 512–528.

**Истомин Владимир Алексеевич**
Год рождения: 1996
Университет ИТМО, факультет систем управления и робототехники,
кафедра информационно-навигационных систем,
студент группы № Р4130
Направление подготовки: 24.04.02 – Системы управления движением и навигация
e-mail: vladimir.istomin@mail.ru

**Драницына Елена Викторовна**
Год рождения: 1985
Университет ИТМО, факультет систем управления и робототехники,
кафедра информационно-навигационных систем, ассистент
e-mail: dranitsyna_ev@mail.ru

**УДК 681.7.068**

# ИДЕНТИФИКАЦИЯ ШУМОВОЙ СОСТАВЛЯЮЩЕЙ ТРИАДЫ ВОЛОКОННО-ОПТИЧЕСКИХ ГИРОСКОПОВ И ЕЕ УЧЕТ В РАБОТЕ КУРСОУКАЗАТЕЛЯ

**Истомин В.А.**
**Научный руководитель – ассистент Драницына Е.В.**

Для повышения точности курсоуказания следует учесть всевозможные ошибки конструктивных особенностей триады волоконно-оптических гироскопов. В работе рассмотрена актуальность уточнения указания курса за счет уточнения модели погрешностей триады волоконно-оптических гироскопов.
**Ключевые слова:** триада, ВОГ, курсоуказатель, модель погрешностей, шумовая составляющая.

**Введение.** Гирогоризонткомпасы (курсоуказатели) на волоконно-оптических гироскопах (ВОГ) представляют собой интегрированные инерциально-спутниковые системы ориентации и навигации (ИСОН), построенные по принципу слабосвязанного комплексирования с данными глобальных навигационных спутниковых систем (ГНСС). Навигационное решение в таких системах формируется по сигналам ГНСС, а решение задачи ориентации полностью ложится на ВОГ [1]. Для обеспечения предельной погрешности определения курса менее 1° (3σ) необходимо использование дорогостоящих ВОГ среднего класса точности 0,05–0,1°/ч [2]. Существенно повысить точность систем на ВОГ тактического (1–10°/ч) класса точности позволяет применение принудительного модуляционного вращения [3].

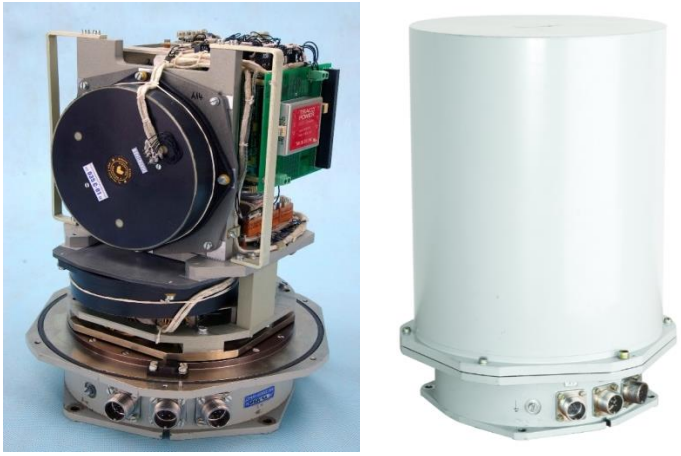


Рисунок. Прибор ВИИМ-2

Примером таких систем может послужить прибор ВИИМ-2 (рисунок). Это курсоуказатель на ВОГ с автокомпенсационным приводом вращения производства АО «Концерн «Электроприбор» (Россия).

**Актуальность, цель работы.** При использовании грубых ВОГ (1–10°/ч) значения составляющих модели погрешностей (не только смещения нулей, но и МК) может изменяться как от пуска к пуску, так и во время работы изделия. Кроме того, необходимо учитывать румбовые дрейфы горизонтальных ВОГ, постоянные в осях изделия, которые могут быть вызваны магнитным, температурным или иными полями. Увеличить точность курсоуказания системы можно, уточняя эти составляющие в ходе работы системы с использованием фильтра Калмана [4].

Цель работы заключалась в увеличении точности курсоуказания за счет уточнения коэффициентов модели погрешностей триады ВОГ в процессе работы изделия.

Для достижения поставленной цели необходимо было решить следующие задачи:

- рассмотреть существующие гирогоризонткомпасы на ВОГ с вращением;
- исследовать модели погрешностей триады ВОГ, построенных по открытой схеме;
- идентифицировать шумовые составляющие выходного сигнала ВОГ и исследовать влияние их учета на точность курсоуказания;
- оценить коэффициенты модели погрешностей (смещений нулей и МК) в ходе работы изделия при наличии одноосного автокомпенсационного вращения и исследовать влияние их учета на точность курсоуказания;
- оценить румбовые дрейфы (погрешности, зависящие от положения триады датчиков относительно строительных осей изделия) в процессе работы изделия и исследовать влияние их учета на точность курсоуказания.

**Модель погрешностей триады ВОГ**

$$\begin{aligned}\Delta\omega_{xb} &= \Delta\overline{\omega}_{xb} + \Delta\omega^{R}_{xb} + \eta_{xb},\\ \Delta\omega_{yb} &= \Delta\overline{\omega}_{yb} + \Delta\omega^{R}_{yb} + \eta_{yb},\\ \Delta\omega_{zb} &= \Delta\overline{\omega}_{zb} + \Delta M_{gzb}\omega_{zb} + \eta_{zb},\end{aligned} \quad (1)$$

где $\Delta\omega_{xb}$ – смещение нуля $i$-го гироскопа $(i = x, y, z)$; $\Delta M_{gzb}$ – квазипостоянная составляющая погрешности масштабного коэффициента азимутального гироскопа; $\eta_{ib}$ – шумовая составляющая $i$-го гироскопа $(i = x, y, z)$; $\Delta\omega^{R}_{ib}(i = x, y)$ – румбовые дрейфы горизонтальных ВОГ, которые могут быть представлены первой гармоникой разложения в ряд Фурье [5]:

$$\begin{aligned}\Delta\omega^{R}_{xb} &= \Delta A_x\cos(K-\rho) + \Delta B_x\sin(K-\rho),\\ \Delta\omega^{R}_{yb} &= \Delta A_y\cos(K-\rho) + \Delta B_y\sin(K-\rho),\end{aligned} \quad (2)$$

где $K$ – курс; $\rho$ – угол поворота ИИМ.

**Заключение.** В первую очередь для настройки и корректной работы фильтра Калмана необходимо исследовать состав шумовой составляющей ВОГ, которая может быть описана белым шумом, винеровским процессом или марковской последовательностью. Это позволит с большей точностью определить характер и величину ошибок, которые впоследствии можно будет учесть и задемпфировать, что увеличит точность курсоуказания.

**Литература**

1. Волоконно-оптический гироскоп [Электронный ресурс]. – Режим доступа:http://sf.ifmo.ru/ru/partners/projects/fog, своб.

2. Лукьянов Д.П., Распопов В.Я., Филатов Ю.В. Прикладная теория гироскопов. – СПб.: ОАО «Концерн «ЦНИИ «Электроприбор», 2015. – 316 с.
3. Optical Gyros and their Applications // NATO RTO AGARDograph. – 1999. – V. 339. – P. 23–30.
4. Lefèvre H. The Fiber-Optic Gyroscope [Электронный ресурс]. – Режим доступа: https://books.google.ru/books?id=j-PmBgAAQBAJ&printsec=frontcover&hl=ru&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false, своб.
5. Lefèvre H. Волоконно-оптические датчики. Вводный курс для инженеров и научных работников / Под ред. Э. Уэдда. – М.: Техносфера, 2008. – 520 с.

**Лысенко Дмитрий Павлович**
Год рождения: 1994
Университет ИТМО, факультет систем управления и робототехники,
кафедра информационно-навигационных систем,
студент группы № Р4230
Направление подготовки: 24.04.02 – Системы управления движением и навигация
e-mail: 174567@niuitmo.ru

**УДК 681.5.011**

# ОБЗОР МЕТОДОВ ПЛАНИРОВАНИЯ МАРШРУТА В ЗАДАЧАХ НАВИГАЦИИ

**Лысенко Д.П.**
**Научный руководитель – к.т.н., доцент Золотаревич В.П.**

В работе выполнен обзор существующих алгоритмов планирования маршрута и траекторного управления для мобильных робототехнических устройств. Рассмотрены различные подходы к решению задачи планирования, выявлены их эффективность, достоинства и недостатки.
**Ключевые слова:** планирование маршрута, построение траектории, эвристические алгоритмы, комбинаторный подход, оптимальные алгоритмы.

Планирование маршрута – одна из основных задач навигации. В данной работе задача планирования маршрута и способы ее решения рассмотрены применительно к мобильным робототехническим устройствам.

Задача планирования маршрута в робототехнике заключается в нахождении оптимального в том или ином смысле (или близкого к нему) пути из начального положения в конечное для сложных тел в некотором пространстве. При этом критерием оптимальности обычно выступает затраченное время, пройденное расстояние или же потраченное топливо. Карта, местоположение препятствий, робота и конечной точки считаются известными.

При решении задачи планирования траектории карта обычно представляется в виде конфигурационного пространства, называемого также пространством поиска. Точка соответствует конкретному положению робота, а линии, связывающие эти точки, – путям из одного положения в другое. Для упрощения задачи реализовывать все последующие алгоритмы целесообразно именно в конфигурационном пространстве [1]. Обычно для представления такого пространства и осуществления в нем поиска маршрута используется направленный граф. Комбинаторный подход подразумевает, что граф представляет собой совокупность всех возможных положений объекта в пространстве, т.е. все пространство разбивается на координатную сетку. В рамках вероятностного подхода граф лишь частично покрывает пространство поиска, но достаточно для нахождения маршрута между заданными точками. Причем вершины графа генерируются случайным образом.

В настоящей работе приведен обзор существующих на сегодняшний день алгоритмов планирования для двух точек, и обсуждаются достоинства и недостатки каждого из них. При этом были рассмотрены основные алгоритмы вероятностного (в том числе наиболее эффективный RRT-Connect алгоритм) и комбинаторного подходов.

**Обзор алгоритмов**

– Комбинаторный подход, оптимальные алгоритмы. Поиск в ширину. Данный алгоритм, по сути, представляет собой перебор всех возможных путей на графе. При этом выполняется переход от одной ячейки графа к следующей равномерно во всех направлениях. Таким образом, одинаково исследуются все возможные пути, и не учитывается положение цели в пространстве.

При этом для каждой новой исследуемой ячейки записывается число, равное количеству шагов от стартовой ячейки. При исследовании всех ячеек сетки и достижении цели строится кратчайший маршрут. Таким образом, алгоритм гарантирует нахождение оптимального решения: кратчайшего пути между точками.

– Алгоритм Дейкстры. Когда пространство представлено взвешенным графом, с целью нахождения оптимального пути, применяется алгоритм Дейкстры.

В рамках данного алгоритма происходит поочередное оценивание стоимости перемещения из каждой ячейки по всем доступным направлениям, и вводится приоритет исследования: в первую очередь переход осуществляется в ячейки, стоимость перемещения в которые меньше.

– Алгоритмы с использованием эвристики. В условиях большого количества элементов сетки, с целью быстрого нахождения кратчайшего пути, необходимо введение эвристики. Алгоритмы с использованием эвристики подразумевают введение априорных знаний или допущений с целью оптимизации порядка перебора при исследовании новых путей и улучшения алгоритма. Таким образом, можно заметно ускорить нахождение пути.
– Жадный поиск. Примером эвристического алгоритма может послужить «жадный» поиск. В жадном поиске для присвоения приоритета исследования используется оцененное расстояние до цели. Ячейка, наиболее близкая к цели, будет исследована первой [2]. При этом при оценивании расстояния препятствия не учитываются. Таким образом, поиск идет в перспективном направлении. Однако, так как при оценивании расстояния не учитываются расположение и вид препятствий, в определенных условиях, например, при наличии сложного препятствия, кратчайший маршрут может быть не найден.
– Sample-based (вероятностный) подход. Эффективность комбинаторного подхода имеет место при условии небольшой размерности пространства поиска. Когда рассматривается объект с множеством степеней свободы, например, манипулятор или имитатор движения объекта, полное разбиение пространства поиска на элементы графа нецелесообразно и неэффективно. В таком случае необходимо использовать алгоритмы вероятностного подхода.
– PRM (Probabilistic Roadmap)-алгоритм. Основной идеей метода является вероятностное построение карты местности и последующий поиск пути с ее использованием. Карта местности представляет собой ненаправленный граф, вершинами которого являются свободные от пересечений положения робота, а ребрами – свободные пути между этими положениями (рисунок) [3].

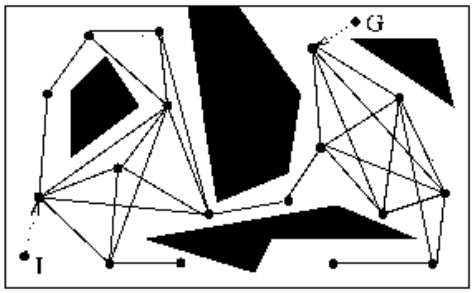



Рисунок. Построение графа с помощью PRM-алгоритма

Вершины графа генерируются случайным образом. Анализируется допустимость их соединения и наличие пересечений с препятствиями. На сгенерированном случайным образом графе ищется путь с помощью комбинаторного подхода.

– RRT/RRT-Connect алгоритмы. Метод базируется на идее последовательного исследования конфигурационного пространства путем построения древовидного графа, имеющего старт в известной начальной конфигурации [4]. Пространство исследуется путем присоединения к ветвям дерева новых вершин в направлениях. Таким образом, генерация новых вершин происходит в еще неисследованных областях [3].

– RRT-Connect. В процессе выполнения данного алгоритма строится не одно дерево, а два – из начальной и конечной конфигурации. Эти два дерева исследуют пространство навстречу друг другу, что повышает эффективность работы метода [5].

**Заключение.** Рассмотрено два основных подхода к задаче поиска пути и различные реализуемые на их основе алгоритмы. В дальнейшем предполагается расширить обзор методов, а также выбрать и применить наиболее подходящий из них к задаче планирования информативных траекторий, возникающей при навигации по геофизическим полям.

**Литература**

1. Салыкова О.С., Бондаренко М.В. Обзор алгоритмов планирования траектории движения манипуляторов [Электронный ресурс]. – Режим доступа: http://ksu.edu.kz/images/bondarenko-salykova.pdf, своб.
2. Gutin G., Yeo A., Zverovich A. Traveling salesman should not be greedy: domination analysis of greedy-type heuristics for the TSP // Discrete Applied Mathematics. – 2002. – V. 117. – № 1–3. – P. 81–86.
3. LaValle S.M. Rapidly-exploring random trees: A new tool for path planning [Электронный ресурс]. – Режим доступа: http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=42B6A2F3BCDB7E663C9B4B2C2EF39A2A?doi=10.1.1.35.1853&rep=rep1&type=pdf, своб.
4. Nissoux C., Simeon T., Laumond J.P. Visibility based probabilistic roadmaps // IEEE Int. Conf. on Intelligent Robots and Systems, Kyongju. – 1999. – P. 1316–1321.
5. LaValle S.M. Planning Algorithms. – Cambridge University Press, 2006. – 844 p.

**Овчинникова Юлия Сергеевна**
Год рождения: 1995
Университет ИТМО, факультет систем управления и робототехники,
кафедра информационно-навигационных систем,
студент группы № Р4130
Направление подготовки: 24.04.02 – Системы управления движением и навигация
e-mail: yuliya-ovchinnikova-1995@mail.ru

**Григорьев Александр Павлович**
Год рождения: 1986
Санкт-Петербургский государственный университет аэрокосмического приборостроения к.т.н., ассистент;
АО «КБ Арсенал имени М.В. Фрунзе», начальник проектно-конструкторского сектора
e-mail: alexgrig-1986@mail.ru

**УДК 681.518**

# КОМПЬЮТЕРНЫЙ ПРОЦЕДУРНЫЙ АВИАЦИОННЫЙ ТРЕНАЖЕР ШТУРМАНА ДЛЯ ПОДГОТОВКИ АВИАЦИОННЫХ СПЕЦИАЛИСТОВ

**Овчинникова Ю.С.** (Университет ИТМО)**, Григорьев А.П.** (Санкт-Петербургский государственный университет аэрокосмического приборостроения; АО «КБ Арсенал имени М.В. Фрунзе»)

Рассмотрена задача проектирования компьютерного процедурного авиационного тренажера штурмана. Рассмотрены частные прикладные задачи. Разработана модель координатного трехгранника для пересчета навигационных координат, имитатор динамики полета на базе эталонной модели (автоматический режим полета по линии заданного пути) и модели ручного управления летательным аппаратом, а также система отображения информации на базе многофункционального дисплея самолета «Akkord-201». Выбрана технология построения компьютерного процедурного авиационного тренажера штурмана, предложена его авторская «каркасно-модульная» организация.
**Ключевые слова:** компьютерный процедурный авиационный тренажер штурмана, модель движения координатного трехгранника, имитатор системы управления движением летательного аппарата, система отображения информации.

Основное назначение тренажера – постановка лабораторных работ, кроме того, проведенные исследования смогут с одной стороны служить заделом для выполняемых НИОКР на кафедре ИНС Университета ИТМО, а с другой – стимулировать студентов к самостоятельному изучению технологий, используемых при построении тренажерно-обучающих систем, что также немаловажно при организации обучающего процесса авиационных специалистов в целом. На примере специализированного навигационного тренажера штурмана (СНТШ) «РЕФРЕН-Н» [1] можно сказать, что при переходе на новое приборное оборудование разработки перспективных систем отображения информации (СОИ) на базе многофункциональных дисплеев СНТШ «РЕФРЕН-Н» требуют модернизации и подготовки к штатной эксплуатации, что, в свою очередь, предполагает решение трудоемкой и нетривиальной задачи, по совмещению, монтажу, установки и отладки нового приборного оборудования с программным обеспечением.

Целью являлась разработка нового компьютерного процедурного авиационного тренажера штурмана (КПАТШ) на основе технологий, реализующих современные приборы,

который должен быть построен на базе персонального компьютера с «гибкой» программной средой, подразумевающей возможность дальнейшей переналадки и (или) модернизации.

Рассмотрены понятия «Система координат» и «Модель земной поверхности» [2]. Модель полета и различные преобразования координат осуществляются в М-функциях MATLAB (представлены набором исполнительных файлов). Для управления в автоматическом режиме был синтезирован закон управления, обеспечивающий вывод летательного аппарата (ЛА) в заданные точки маршрута в назначенное время [3].

В эталонной модели полета (автоматический режим), в которой ЛА рассматривается как материальная точка, движущаяся с известной земной скоростью $W(t)$, с известным путевым углом (азимутом) – $A(t)$ на заданной высоте $h(t)$. Функции времени при этом задаются в виде системы дифференциальных уравнений вида: $\acute{W}(t)=u_1$; $W(t_0)=W_0$; $\acute{D}(t)=u_2(t)$; $D(t_0)=D_0$; $\acute{h}(t)=u_3$; $h(t_0)=h_0$, если функции $u_1(t)$, $u_2(t)$, $u_3(t)$ положить равными нулю, то мы получим маршрут с постоянной скоростью, азимутом и на постоянной высоте. Если же задавать их в виде кусочно-постоянных функций, то можно получить достаточно сложное движение с разворотами, разгонами, торможениями и маневрами по высоте, что, в конечном счете, и требуется. При движении из точки $M$ в точку $M_3$ (заданная) по кривой можно предложить следующее простое управление:

$$D_{\text{г}} = u_2 = \frac{gn}{W} = -\frac{gn_m}{W}\,\mu_1[(s\sin 0{,}5/D_{\text{г}} - D_{\text{г.з}}) + 1 - s^2],$$

$$s = \text{sign}[\cos 0{,}5(D_r - D_{\text{г.з}})],\ a = D_r - D_{\text{г.з}}.$$

При моделировании контура управления полетом в ЛА (ручной режим) кроме решения уравнений динамики необходимо воспроизвести действия пилотажно-навигационных приборов и органов управления, что, в свою очередь, предполагает разработку СОИ.

Разработан «каркас» компьютерного авиационного тренажера и решены следующие частные задачи, такие как:

1. разработка модели движения координатного трехгранника;
2. разработка имитатора системы управления движением ЛА по маршруту;
3. разработка СОИ.

В результате данной работы разработан процедурный тренажер штурмана, в котором реализованы современные технологии построения приложений.

На сенсорном мониторе с помощью Flash-технологий строится изображение современной приборной доски ЛА (на примере многофункционального дисплея TDS-12 французского самолета «Akkord 201»). Пользователь взаимодействует с графической средой Flash [4] (изображение приборов на экране монитора), воспринимает полетную информацию (пилотажный и навигационный кадры) и может изменять текущие параметры полета с клавиатуры. Модель полета и различные преобразования координат осуществляются в М-функциях MATLAB. Для связи модели MATLAB и СОИ служит приложение Visual C++ [5].

Достоинства СОИ созданной по технологии Flash [4] по сравнению с обычными методами разработки:

1. время разработки СОИ на Flash [4] существенно сокращается;
2. возможность легкой интеграции мультимедиа;
3. не требуется глубоких знаний программирования с использованием графических библиотек (OpenGL, DirectX).

Достоинства модели полета MATLAB:

1. удобство работы с матрицами (пересчет из одной системы координат в другую);
2. удобство отладки модели в самой программе MATLAB;
3. наличие уже готовых компонентов для решения специфических задач.

Возможности языка программирования высокого уровня C++ [5] используются для связи вышеприведенных технологий и дальнейшего развития проекта, переналадки

(адаптация под ЛА другого типа и (или) модели) и модернизации (применение более совершенных математических моделей движения ЛА) КПАТШ.

Сравнивая предложенную технологию построения КПАТШ с тренажерами ОКБ «Электроавтоматика», АО «Транзас» и других предприятий, можно сделать вывод, что выбранная технология:

1. не требует материальных затрат на приобретение реального приборного авиационного оборудования;
2. выгодно отличается расширяемостью (возможность дополнительного подключения системы оценки, базы данных, реализация сетевого взаимодействия, организация группового полета по маршруту и пр.);
3. обладает универсальностью (возможность использования тренажера в других читаемых дисциплинах, а не только в курсе «Авиационные тренажеры»);
4. характеризуется мобильностью (возможность быстрой переналадки и модернизации, за счет использования других имитаторов динамики полета, модели движения и пр.).

Данный подход имеет и ряд недостатков:

1. использование нескольких технологий (Visual C++, MATLAB, Flash) затрудняет реализацию полета в реальном масштабе времени (инерционность в расчетах, при использовании «маломощных» персональных компьютеров);
2. алгоритмическая и программная сложность разработки, за счет применения специализированного программного обеспечения и из-за использования широкой номенклатуры различных технологий.

Предложенную «каркасно-модульную» организацию КПАТШ целесообразно доработать в части:

1. разработки автоматизированной системы оценки проведенного полета;
2. разработки единой база данных полета (полета пользователя);
3. взаимодействия по сети для организации группового полета по маршруту.

**Литература**

1. Мамаев В.Я., Чернов В.А. Приборное оборудование рабочего места обучаемого СНТШ «РЕФРЕН-Н». Учебно-методическое пособие. – СПб.: Изд-во ГУАП, 2006. – 87 с.
2. Мамаев В.Я., Синяков А.Н., Петров К.К., Горбунов Д.А. Воздушная навигация и элементы самолетовождения. Учебное пособие. – СПб.: СПбГУАП, 2002. – 256 с.
3. Бабич О.А. Обработка информации в навигационных комплексах. – М.: Машиностроение, 1991. – 512 с.
4. Гурский Д. Action Script 2.0. Для профессионалов. Программирование во Flash MX 2004. – СПб.: Питер, 2006. – 860 с.
5. Круглински Д., Уингоу С., Шеферд Дж. Программирование на Microsoft Visual C++ 6.0 для профессионалов / Пер. с англ. – СПб.: Питер; М.: Русская Редакция, 2004. – 861 с.

**Савенко Руслан Валерьевич**
Год рождения: 1996
Университет ИТМО, факультет систем управления и робототехники,
кафедра информационно-навигационных систем,
студент группы № Р4130
Направление подготовки: 24.04.02 – Системы управления движением и навигация
e-mail: russavenko@gmail.com

**Аксененко Виктор Дмитриевич**
Год рождения: 1947
Университет ИТМО, факультет систем управления и робототехники,
к.т.н., доцент
e-mail: office@eprib.ru

**УДК 629.591**

# СИСТЕМА ГИРОСКОПИЧЕСКОЙ СТАБИЛИЗАЦИИ ОПТИЧЕСКОГО БЛОКА НА ВОЛОКОННО-ОПТИЧЕСКИХ ГИРОСКОПАХ

**Савенко Р.В.**
**Научный руководитель – к.т.н., доцент Аксененко В.Д.**

Для повышения эффективности морского флота совместно с ним используется морская авиация. Требуемый уровень безопасности, необходимый при посадке вертолетов, достигается за счет оснащения взлетно-посадочной площадки оптической системой посадки. Такие системы посадки состоят из ряда элементов, в том числе указателя глиссады. В работе рассмотрена автономная система трехосной гироскопической стабилизации указателя глиссады, работа которого не прекращается при прекращении поступления данных от бортовой навигационной системы.
**Ключевые слова:** оптические системы посадки, гиростабилизация, обеспечение автономности, указатель глиссады, морская авиация.

Для повышения эффективности морского флота используются самолеты и вертолеты, базирующиеся на палубах кораблей, что заметным образом расширяет спектр решаемых флотом задач. Для организации полетов вертолетов (как и самолетов) на авианесущих кораблях оборудуются взлетно-посадочные площадки (ВПП). Требуемый уровень безопасности, необходимый при посадке вертолетов, достигается за счет оснащения ВПП оптической системой посадки (ОСП). ОСП формирует ряд сигнальных огней определенного направления и цвета, обеспечивая пилота летательного аппарата информацией о его положении относительно ВПП.

Первые работы над оптическими системами посадки вертолетов начались в 1970-х годах [1]. Среди иностранных компаний следует упомянуть французскую CILAS [2], итальянскую Calzoni [3] и английскую Aeronautical & General Instruments Limited [4], немецкие LinksRechts [5] и Optonaval [6]. Среди отечественных компаний в данном направлении работают ЗАО НТЦ «Альфа-М» [7] и АО «Концерн «ЦНИИ «Электроприбор» [8].

Такие системы посадки включают в себя следующие основные элементы:
- указатель курса;
- указатель истинного горизонта;
- огни крена корабля;
- индикаторы бортовой качки корабля;

– пульт управления;
– палубные огни подсветки ВПП;
– другие средства.

Самые современные и надежные ОСП включают в себя указатель глиссады (УГ). УГ проецирует стабилизированный в горизонте видимый телесный угол с тремя цветными информационными секторами: «выше глиссады» – желтый, «на глиссаде» – зеленый, «ниже глиссады» – красный. Стабилизация оптического блока УГ в горизонте происходит по данным, поступающим от бортовой навигационной системы.

Особенностью рассматриваемой системы является ее автономность, т.е. возможность ее исправной работы при прекращении поступления данных от бортовой навигационной системы.

Цель работы заключалась в разработке и исследовании системы автономной трехосной гироскопической стабилизации оптического модуля указателя глиссады для посадки корабельных вертолетов.

Для достижения поставленной цели необходимо было решить следующие задачи:
– изучить существующие системы оптической посадки вертолетов;
– разработать структурную схему гиростабилизации оптического модуля УГ;
– определить элементный состав исследуемой системы;
– разработать математическое описание работы системы гиростабилизации блока УГ;
– провести моделирование и оценить работу гиростабилизации при разных условиях (качки и маневры корабля).

На рисунке представлена структурная схема изучаемого указателя глиссады. Отличительной чертой изучаемого глиссадного указателя является его автономность. Она достигается за счет включения в систему триады акселерометров и гироскопов. Первые закреплены на основании прибора, а вторые расположены на самой стабилизированной платформе. Данные от инерциальных датчиков обрабатываются центральным контроллером, который высчитывает необходимые углы поворота платформы для ее стабилизации в горизонте.

На схеме также отображены следующие основные элементы:
– оптический излучатель, установленный на стабилизируемой платформе;
– три датчика угла и двигателя, и управляющие ими контроллеры приводов;
– пульт управления оптической системы посадки;
– центральный контроллер, отвечающий за вычисление углов поворота платформы по данным от гироскопов и акселерометров.

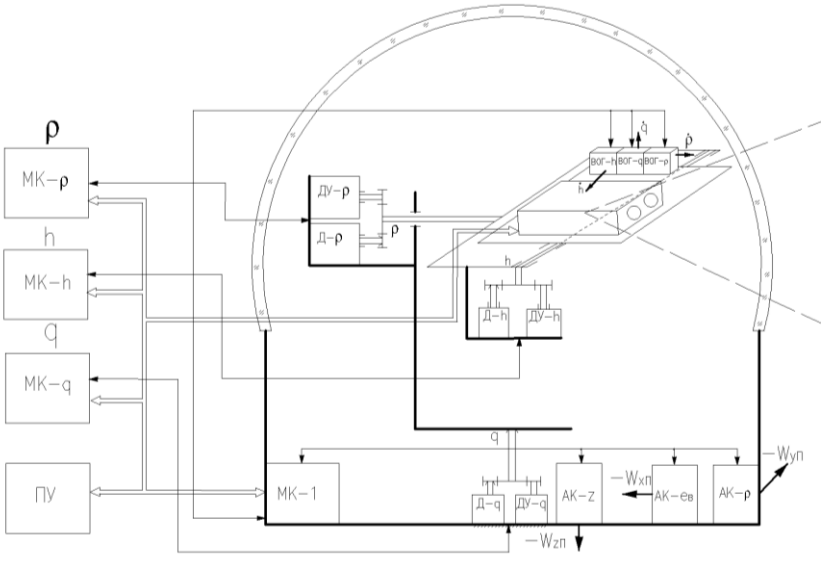



Рисунок. Структурная схема изучаемого указателя глиссады

Обеспечение автономности указателя глиссады в значительной степени повышает надежность работы оптической системы посадки, к которой предъявляются строгие требования, а также расширяет номенклатуру судов и кораблей для ее применения, в связи с этим проведение исследований в этой области является актуальным.

**Литература**

1. Technical report: NAVTRATQUIPCEN IH-265 / Computer Laboratory Naval Training Equipment Center / Computer simulation of fresnel lens optical landing system. – Orlando, Florida, 1977. – 44 p.
2. Cilas Helicopter Visual Landing Aid System Safecopter [Электронный ресурс]. – Режим доступа: https://www.cilas.com/en/glide-clope-indicator-helicopter-visual-landing-aids, своб.
3. PRODUCTS & SERVICES [Электронный ресурс]. – Режим доступа: http://www.calzoni.com/products-services, своб.
4. Naval Aviation Lighting overview [Электронный ресурс]. – Режим доступа: http://www.agiltd.co.uk/Naval-Products/Visual-Landing-Aids, своб.
5. LINKSrechts Helicopter Visual Landing Aid Systems [Электронный ресурс]. – Режим доступа: http://www.linkrechts.de/index.html, своб.
6. Optonaval Helicopter Visual Landing Aid (HVLA) Systems [Электронный ресурс] – Режим доступа: http://www.optonaval.de/products/hvla.html, своб.
7. АО «Научно-технический центр «Альфа-М» [Электронный ресурс]. – Режим доступа: http://www.alpha-m.su/index.html, своб.
8. Системы предполетной подготовки и обеспечения безопасной посадки летательных аппаратов на палубу корабля [Электронный ресурс] – Режим доступа: http://www.elektropribor.spb.ru/katalog/sistemy-predpoletnoy-podgotovki-bezopasnosti/, своб.

**Смирнов Николай Андреевич**
Год рождения: 1991
Университет ИТМО, факультет систем управления и робототехники,
кафедра информационно-навигационных систем,
студент группы № Р4230
Направление подготовки: 24.04.02 – Системы управления движением и навигация
e-mail: nsifmore@gmail.com

**Моторин Андрей Владимирович**
Год рождения: 1989
Университет ИТМО, факультет систем управления и робототехники,
кафедра информационно-навигационных систем, ассистент
e-mail: motorin.a@mail.ru

**Степанов Олег Андреевич**
Год рождения: 1949
Университет ИТМО, факультет систем управления и робототехники,
кафедра информационно-навигационных систем, д.т.н., профессор
e-mail: ostepanov@elprib.ru

**УДК 519.254**

# ВЫЧИСЛИТЕЛЬНАЯ ОПТИМИЗАЦИЯ АЛГОРИТМА ИДЕНТИФИКАЦИИ МОДЕЛИ ОШИБОК ДАТЧИКОВ

**Смирнов Н.А., Моторин А.В.**
**Научный руководитель – д.т.н., профессор Степанов О.А.**

Работа проводилась при поддержке гранта РФФИ 18-08-01101А.

Рассмотрена задача вычислительной оптимизации алгоритма идентификации модели погрешностей датчиков, основанного на принципах нелинейной байесовской фильтрации. Обсуждены цели и потенциальные программные и аппаратные пути оптимизации.
**Ключевые слова:** идентификация, банк фильтров Калмана, вычислительная оптимизация, Python, параллельные вычисления, графический процессор.

**Введение.** Современные навигационные системы опираются на данные, получаемые от множества датчиков и чувствительных элементов. Для комплексной обработки получаемой информации широкое применение получили алгоритмы оптимальной фильтрации, такие как фильтр Калмана (ФК) и его различные модификации. При таком подходе предполагается случайный характер погрешностей датчиков и чувствительных элементов, как следствие требуется предварительная идентификация моделей таких погрешностей [1–3].

Задача идентификации модели погрешностей может быть решена в рамках теории нелинейной байесовской фильтрации. При этом вводятся предположения о наличии набора альтернативных гипотез о модели погрешностей в виде формирующих фильтров, для векторов состояния и неизвестных параметров которых заданы априорные функции

плотности распределения вероятности (ф.п.р.в.). В этом случае задача может быть сформулирована следующие образом: по имеющимся измерениям требуется найти гипотезу, максимизирующую значение апостериорной вероятности, т.е. определить структуру модели, и получить оптимальные байесовские оценки и дисперсии погрешностей оценивания вектора неизвестных параметров и вектора состояния для этой гипотезы [4].

Использование аппроксимации ф.п.р.в. вектора неизвестных параметров и фиксирование его значений для каждой гипотезы позволяют свести решаемую задачу к набору линейных задач и построению алгоритма с помощью банка ФК [4].

Реализация банка ФК предусматривает необходимость проведения значительного объема вычислений. Помимо этого, существует задача определения потенциальной точности, при решении которой рассматриваемый алгоритм необходимо запускать многократно, что пропорционально увеличивает вычислительную сложность. В связи с этим встает вопрос о вычислительной оптимизации, которая позволила бы сократить реальное время, затрачиваемое на решение задачи.

**Пути оптимизации и результаты.** Оптимизируемый алгоритм идентификации предполагает большое количество вложенных циклов и матричных операций. Связано это с рекуррентным характером алгоритма, обработкой множества реализаций и нескольких альтернативных гипотез, для каждой из которых должно быть реализовано вычисление своего банка ФК. Были выделены два основных направления оптимизации работы алгоритма идентификации: программное, подразумевающее внесение изменений непосредственно в архитектуру программы и оптимизацию кода, реализующего алгоритм, и аппаратное, опирающееся на использование аппаратных ресурсов вычислительной машины, где производится расчет.

Программная оптимизация в первую очередь заключается в сокращении одинаковых расчетов и применении оптимизированных математических функций языка разработки, на котором реализуется алгоритм. При этом были учтены особенности применения алгоритма. Так, на практике часто возникает потребность в добавлении к рассмотрению новых гипотез и переопределении начальных областей неопределенности неизвестных параметров, и последующем пересчете решения. Реализация непосредственного расчета вероятностей гипотез в программе ведет к тому, что изменение даже одного из этих параметров (например, изменения области неопределенности одного параметра одной гипотезы) приводит к необходимости полного пересчета всех банков ФК для всех гипотез, т.е. большому количеству повторных вычислений. В связи с этим было решено, независимо рассчитывать параметр, характеризующий правдоподобие каждой гипотезы, а расчет вероятностей гипотез осуществлять отдельно. Такая схема позволяет при пересчете решения заново рассчитывать только тот банк ФК, параметры которого были изменены, и легко добавлять в рассмотрение новые гипотезы.

Помимо этого, была оптимизирована структура алгоритма. В частности, так как параметры ФК для разных реализаций одинаковы в рамках одной гипотезы, матрицы ковариации и коэффициент усиления фильтра могут быть рассчитаны однократно для всех реализаций. Это было осуществлено путем соответствующей организации циклов, и привело к существенному сокращению количества матричных операций, особенно в задаче вычисления потенциальной точности и, соответственно, снижению времени вычислений. Аналогично, в случае стационарного характера идентифицируемых моделей погрешностей, сокращение объема повторных вычислений было достигнуто за счет выполнения расчета за пределами цикла по времени матриц, определяющих модель, которые в этом частном случае не изменяются на каждом шаге работы алгоритма. Эффективность приемов, заключающихся в реструктуризации кода, проиллюстрирована на рис. 1.

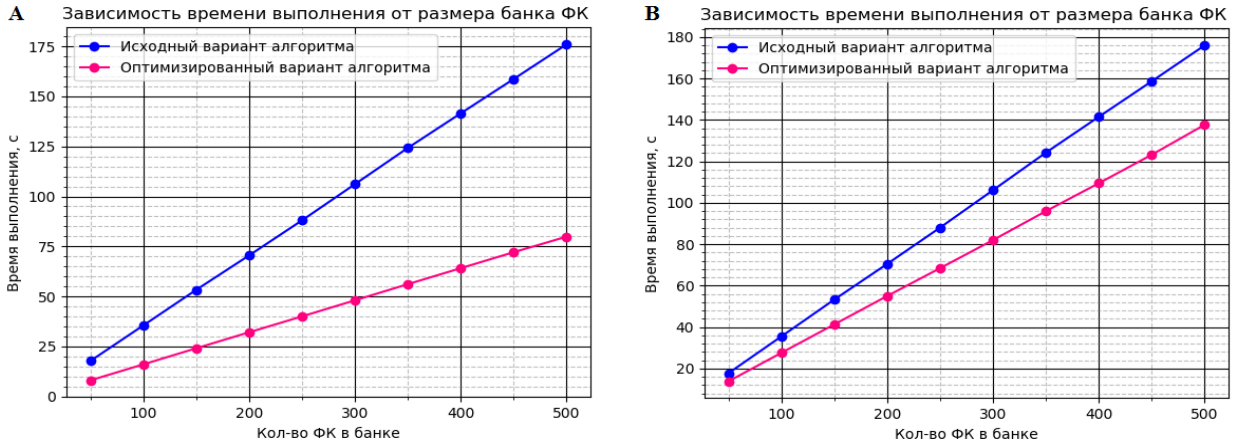
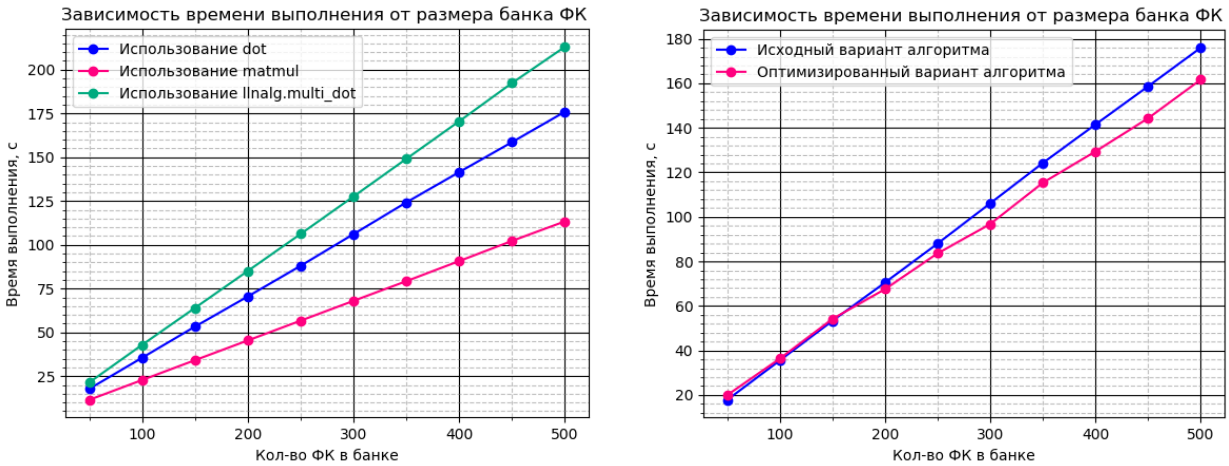



Рис. 1. Зависимость времени, затрачиваемого на решение задачи идентификации модели погрешностей, от количества ФК в банке: учет стационарного характера модели ошибок (A); вынесение вычислений ковариационного канала ФК (B)

Основным языком реализации алгоритма был выбран язык Python. Python широко используется в сфере выполнения научных расчетов. Основанием для этого служит наличие специализированного пакета NumPy, предназначенного в первую очередь для работы с матричными вычислениями. В своей работе пакет NumPy опирается на реализацию библиотеки базовых операций линейной алгебры (Basic Linear Algebra Subroutines, BLAS) на языках C или Fortran, что дает существенное ускорение по сравнению с нативной реализацией на Python. Для сравнения использовались следующие специализированные функции: dot – классическое перемножение двух матриц; linalg.multi_dot – перемножение нескольких матриц с автоматическим определением наиболее оптимального порядка операций; matmul – перемножение матриц, хранящихся в многомерных массивах, без необходимости их перебора в цикле. Поскольку функция matmul позволила избавиться от вычислений в циклах, она показала наиболее высокую эффективность (рис. 2, а). Использование функции multi_dot, напротив, замедлило работу алгоритма, что объясняется в первую очередь малыми размерностями перемножаемых матриц (не более 10), что не дает в полной мере воспользоваться преимуществами данной функции.




а б

Рис. 2. Зависимость времени, затрачиваемого на решение задачи идентификации модели погрешностей, от количества ФК в банке при: варьировании специализированных функций (а) и распараллеливании расчета банка ФК (б)

Следует отметить, что вычисление параметров ФК в банке может осуществляться параллельно. Этому также способствует широкое распространение многоядерных процессоров, позволяющих выполнять единовременно независимо друг от друга несколько

вычислительных процессов [5]. Потенциальный выигрыш от использования такого подхода пропорционален количеству доступных ядер процессора. Язык Python накладывает серьезные ограничения на использование многопоточности, тем не менее, пакет Multiprocessing предоставляет возможность распараллеливания работы алгоритма на уровне процессов, однако это приводит к дополнительным временным издержкам при межпроцессорном взаимодействии с памятью (рис. 2, б).

Другим перспективным направлением использования аппаратных возможностей для ускорения работы видится эксплуатация вычислительных ресурсов графических процессоров. Аппаратная реализация графических процессоров традиционно ориентирована на обработку графических данных, что подразумевает вычислительно эффективную реализацию операций над матрицами и массивами, а также арифметических операций с плавающей запятой [5], что согласуется с основными ресурсоемкими операциями рассматриваемого алгоритма.

**Заключение.** Рассмотрены способы вычислительной оптимизации алгоритма идентификации модели погрешностей, основанного на принципах нелинейной байесовской фильтрации, позволяющие избежать необходимости повторной обработки данных. Проиллюстрирована эффективность оптимизации кода на примере сокращения количества матричных вычислений путем их вынесения за пределы цикла, использования специализированных функций языка и распараллеливания работы алгоритма. Намечены дальнейшие пути аппаратной вычислительной оптимизации.

**Литература**

1. Емельянцев Г.И., Степанов А.П. Интегрированные инерциально-спутниковые системы ориентации и навигации. – СПб.: АО «Концерн «ЦНИИ «Электроприбор», 2016. – 235 с.
2. Драницына Е.В. Каблировка измерительного модуля прецизионной БИНС на волоконно-оптических гироскопах: дисс. ... канд. техн. наук: 05.11.03. – СПб., 2016. – 90 с.
3. Степанов О.А., Соколов А.И., Долнакова А.С. Анализ потенциальной точности оценивания параметров случайных процессов в задачах обработки навигационной информации // Материалы XII Всероссийского совещания по проблемам управления. – 2014. – Р. 3324–3337.
4. Моторин А.В., Степанов О.А. Проблемно-ориентированный подход к решению задачи идентификации моделей погрешностей навигационных датчиков и оцениваемых сигналов // Материалы пленарных заседаний 9-й Российской мультиконференции по проблемам управления. – 2016. – С. 49–60.
5. Некрасов К.А., Поташников С.И., Боярченков А.С., Купряжкин А.Я. Параллельные вычисления общего назначения на графических процессорах. – Екатеринбург: Изд-во Урал. ун-та, 2016. – 104 с.

**Титов Роман Умарович**
Год рождения: 1995
Университет ИТМО, факультет систем управления и робототехники,
кафедра информационно-навигационных систем,
студент группы № Р4130
Направление подготовки: 24.04.02 – Системы управления движением и навигация
e-mail: roman100895@rambler.ru

**Моторин Андрей Владимирович**
Год рождения: 1989
Университет ИТМО, факультет систем управления и робототехники,
кафедра информационно-навигационных систем, ассистент
e-mail: motorin.a@mail.ru

**УДК 629.05**

# СРЕДА МОДЕЛИРОВАНИЯ ЗАДАЧ ОДНОВРЕМЕННОЙ НАВИГАЦИИ И КАРТОГРАФИРОВАНИЯ В ROBOT OPERATING SYSTEM

**Титов Р.У., Моторин А.В.**
**Научный руководитель – д.т.н., профессор Степанов О.А.**

Работа посвящена моделированию задачи одновременной навигации и картографирования SLAM. Рассмотрено построение модели робота для обработки и получения реальных данных с использованием программного обеспечения ROS и MATLAB.
**Ключевые слова:** метод SLAM, модель робота, лазерный сканер.

**Введение.** В настоящее время мобильные роботы могут самостоятельно перемещаться в окружающем пространстве и выполнять множество различных действий с помощью манипуляторов. Однако даже самые современные из них не в состоянии выполнять весь комплекс работ без участия оператора-человека. В этой связи одной из актуальных современных задач навигации является создание таких систем, в которых робот, в случае потери связи с оператором-человеком, мог бы самостоятельно выполнять ряд операций, связанных с ориентацией в пространстве [1, 2].

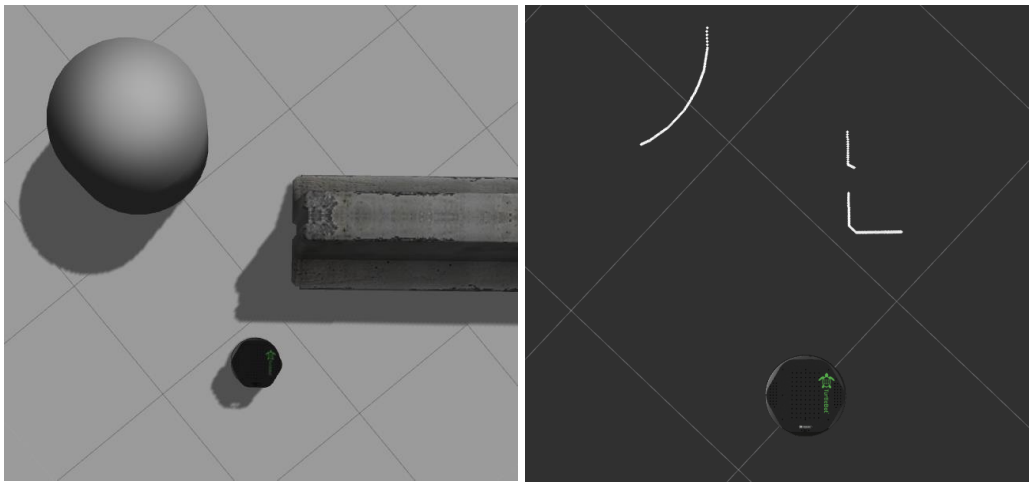
– Выбор алгоритма решения задачи картографирования и навигации. Задача автономной навигации мобильного робота включает в себя процесс картографирования и точного определения параметров собственного местоположения с помощью методов одновременной локализации и картографирования SLAM (Simultaneous Localization and Mapping). В основе метода SLAM, как правило, лежит возможность измерения расстояний до окружающих объектов и оценка изменения положения относительно них. SLAM решает одновременно две проблемы: построение карты местности, окружающей робота, и определение положения робота на этой карте. Карта помещения содержит информацию о расположении стен и других препятствий. Это позволяет роботу перемещаться в пространстве и планировать путь к цели таким образом, чтобы обходить препятствия в виде стен и объектов. Сделав первые замеры расстояний, робот запоминает их и движется в направлении других объектов. После того, как все объекты в помещении найдены, и расстояние до них измерено, робот возвращается на исходную позицию.
– Выбор технической платформы для решения задачи. Для оценки изменения положения робота в пространстве используются лазерные дальномеры (лидары) и видеокамеры. Для

осуществления навигации необходимы также автономные датчики, отслеживающие перемещения робота в пространстве, такие как: датчики угла поворота моторов (энкодеры), одометры, инерциально-измерительные устройства и другие. Для решения задачи определения параметров собственного положения и построения карт навигации наиболее предпочтительным является применение лазерного сканера HOKUYO URG-UG01. В линейке лазерных дальномеров эта модель является одной из самых компактной, легкой и энергоэффективной. Указанный сканер является одним из самых доступных дальномеров на рынке. Он позволяет выполнять измерения с точностью около 3%, имеет диапазон измерения 5,6 м, сектор сканирования 240° и интерфейс подключения USB 2.0. Лазерный дальномер URG-04LX-UG01 полностью отвечает таким требованиям, как высокая функциональность, малые габаритные размеры и низкое энергопотребление [3].

– Построение модели мобильной платформы и получение данных. Решение задачи SLAM проблематично по причине того, что необходимо моделировать окружающую обстановку. Существует разработанный пакет ROS (Robot Operating System), в котором есть среда Gazebo. ROS, работающий под управлением операционной системы Ubuntu, позволяет разработчикам использовать для роботов уже готовые решения, при этом сам программный код претерпевает минимальные изменения. Также ROS поддерживает параллельные вычисления и отлично взаимодействует с различными библиотеками, такими как Qt и OpenCV [4].

Программа Gazebo имеет гибкий дизайн и удобный интерфейс, поддерживающий одновременную работу с несколькими устройствами. В Gazebo доступен редактор, который позволяет создавать 3D-сцены без программирования. Моделируемые сенсоры: лазерный дальномер, камера, кинект-сенсор, устройство для чтения RFID-меток и бамперы [5].

С помощью пакетов ROS и Gazebo авторами был смоделирован робот «Turtlebot» (рис. 1, а), а с использованием функции «Gmapping» и модельных данных лазерного сканера построена карта местности (рис. 1, б).



а б

Рис. 1. Визуализатор работы симулятора Gazebo

В результате применения этого алгоритма и работы пакета по визуализации полученных данных «Rviz» получена картина, отображающая виртуальную модель среды и ее фиксацию на карте.

Для отображения и обработки численных значений массива дальностей до препятствий, полученных с лидара, использовался пакет Simulink математической среды MATLAB. С помощью указанного пакета получены данные, на основе которых в дальнейшем будет решена задача SLAM (рис. 2).

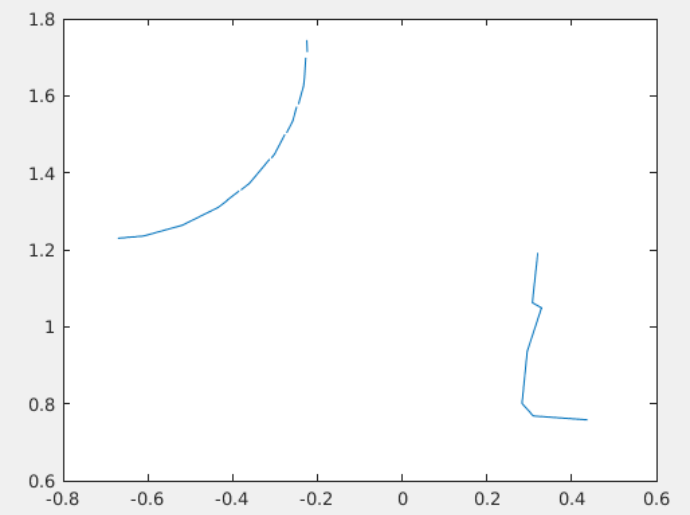



Рис. 2. Координаты препятствий в пакете Simulink

**Заключение.** В качестве программого обоспечения (ПО) для получения модельных данных выбран пакет Gazebo, мощный симулятор роботов, разработанный для операционной системы Linux. В результате на платформе ПО ROS и MATLAB в ходе симуляции были получены модельные измерения для лазерного дальномера и бортовых датчиков робота: одометра, инерциальных датчиков.

**Литература**

1. Cadena C., Carlone L., Carrillo H., Latif Y., Scaramuzza D., Neira J., Reid I., Leonard J.J. Past, Present, and Future of Simultaneous Localization And Mapping: Towards the Robust-Perception Age [Электронный ресурс]. – Режим доступа: http://ieeexplore.ieee.org/document/7747236/, своб.
2. Давыдов О.И., Платонов А.К. Метод определения позиции и ориентации мобильного робота с лазерным сканером [Электронный ресурс]. – Режим доступа: http://www.keldysh.ru/papers/2015/prep2015_45.pdf, своб.
3. Лазерный сканер HOKUYO URG-04LX-UG01 [Электронный ресурс]. – Режим доступа: http://www.wertech.ru/Products/ 145-hokuyo-urg-04lx-ug01-3d-3-.aspx, своб.
4. Обзор ROS| Robotics notes [Электронный ресурс]. – Режим доступа: http://robotics.osll.ru/2014/11/ros.html, своб.
5. Gazebo.Мощное программное обеспечение для исследования сенсорных систем и робототехники [Электронный ресурс]. – Режим доступа: http://cxem.net/software/gazebo.php, своб.

**Томеева Алина Рамилевна**
Год рождения: 1994
Университет ИТМО, факультет систем управления и робототехники,
кафедра информационно-навигационных систем,
студент группы № Р4230
Направление подготовки: 24.04.02 – Системы управления движением и навигация
e-mail: alina_tomeeva@mail.ru

**Рупасов Андрей Викторович**
Год рождения: 1987
АО «Концерн «ЦНИИ «Электроприбор», к.т.н.
e-mail: sadbender@yandex.ru

**УДК 535.8**

# СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТОЧНОСТНЫХ ХАРАКТЕРИСТИК ВОЛОКОННО-ОПТИЧЕСКОГО ГИРОСКОПА С КЛЕЕМ УФ-ОТВЕРЖДЕНИЯ ЗАРУБЕЖНОГО И ОТЕЧЕСТВЕННОГО ПРОИЗВОДСТВА

**Томеева А.Р.** (Университет ИТМО)**, Рупасов А.В.** (АО «Концерн «ЦНИИ «Электроприбор»)
**Научный руководитель – к.т.н. Рупасов А.В.** (АО «Концерн «ЦНИИ «Электроприбор»)

В работе рассмотрены точностные характеристики волоконно-оптического гироскопа с различными составами клея УФ-отверждения с целью импортозамещения клея на отечественный аналог. В данной работе были проведены экспериментальные исследования зависимости основных характеристик волоконно-оптического гироскопа от клея, используемого при стыковке оптических компонентов.
**Ключевые слова:** волоконно-оптический гироскоп, точностные параметры, клей УФ-отверждения.

В технологии производства волоконных интерферометрических датчиков угловой скорости используется клей УФ-отверждения для стыковки волонно-оптических и интегрально-оптических компонентов. Узел стыковки этих компонентов не должен влиять на параметры оптического излучения, проходящего по схеме гироскопа. Иначе, вследствие возникновения поляризационных и механических преобразований в местах клеевого соединения оптического волокна с многофункциональной интегральной оптической схемой (МИОС) может появляться паразитный фазовый сдвиг, вызывающий ошибку показаний гироскопа [1, 2].

В работе, посвященной сравнительному анализу точностных характеристик волоконно-оптического гироскопа (ВОГ) с клеем УФ-отверждения зарубежного и отечественного производства, были решены следующие задачи: проведены экспериментальные исследования влияния стыковки на чувствительность выходного сигнала ВОГ к температуре. Также проведены экспериментальные исследования по сравнению выходных параметров ВОГ с различными составами клея УФ-отверждения при воздействии температуры.

Исследование проводилось на серийном образце ВОГ. Все элементы гироскопа за исключением МИОС были помещены в термокамеру 1, где поддерживалась постоянная температура. В термокамеру 2 был помещен МИОС, где температура изменялась в заданном диапазоне (рис. 1). Для сравнения различных составов клея и оценки точностных параметров гироскопа была проведена серия стыковок.

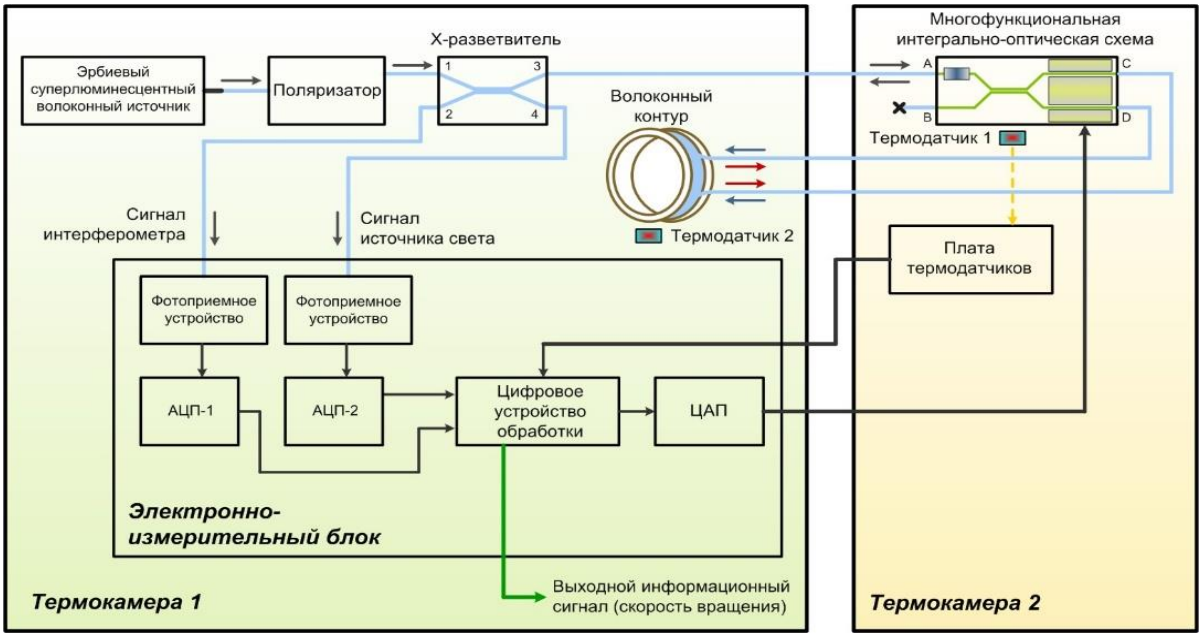



Рис. 1. Схема проводимого эксперимента

На рис. 2 видно, что максимальное отклонение сигнала у отечественного образца ЭП-22 – 0,24°/ч, притом, что у клея зарубежного производства – 0,1°/ч. Все оптические компоненты и поверхности сохранялись неизменными от стыковки к стыковке, что позволяет оценить непосредственное влияние клея на выходной сигнал ВОГ. Критериями оценки являлись такие параметры интерферометра как: надежность, спектр выходного сигнала ВОГ, оптические потери и стабильность выходного сигнала при внешнем температурном воздействии.

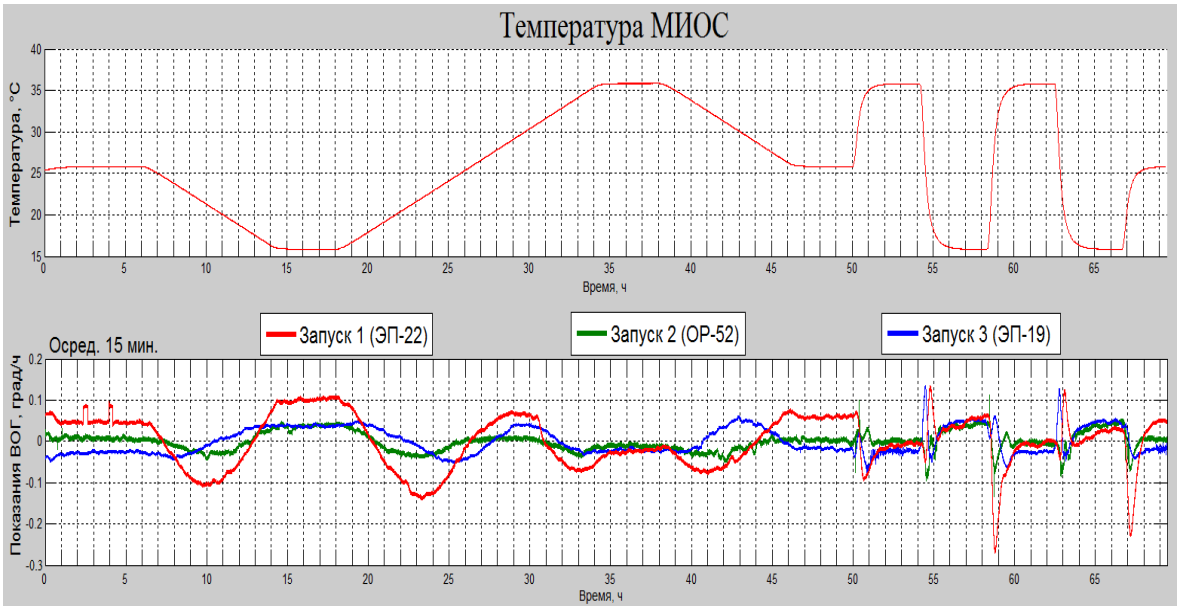



Рис. 2. Зависимость выходного сигнала ВОГ от температуры

На рис. 3 приведен график зависимость выходного сигнала гироскопа от температуры на отбраковочном термотесте, где температура изменялась от –40 до +70°С. Как и в случае с рис. 1 наихудший результат показал образец – ЭП-22. В то время как ЭП-19 приближенно равен по числу отклонения сигнала зарубежному образцу ОР-52.

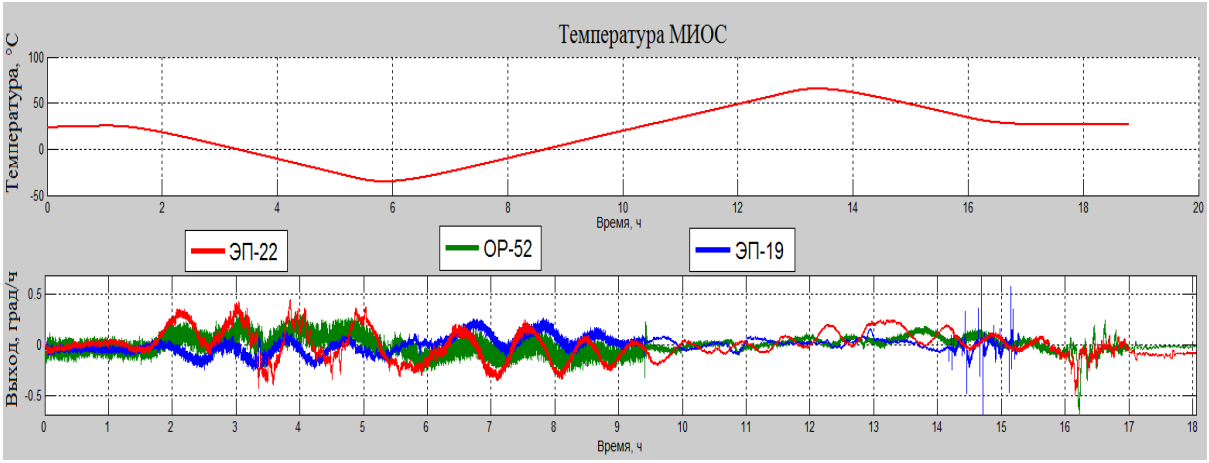



Рис. 3. Выходной сигнал ВОГ на отбраковочном термотесте

По результатам сравнительных испытаний ВОГ с различными составами клея УФ-отверждения импортного и отечественного производства можно сделать вывод, что с одним из образцов отечественного УФ-клея (ЭП-19) исследуемые параметры ВОГ находятся в допустимых пределах, также как с используемым УФ-клеем импортного производства.

**Литература**

1. Рупасов А.В. Исследование метода локального температурного воздействия и его применение для компенсации дрейфа волоконно-оптического гироскопа: дис. ... канд. техн. наук: 05.11.07. – СПб.: НИУ ИТМО, 2014. – 135 с.
2. Аксарин С.М. Исследование поляризационных методов и технологий согласования волоконно-оптических и интегрально-оптических волноводов: автореф. дис. на соиск. уч. степени канд. физико-матем. наук. – СПб.: НИУ ИТМО, 2014. – 19 с.

**Чалков Виктор Викторович**
Год рождения: 1996
Университет ИТМО, факультет систем управления и робототехники,
кафедра информационно-навигационных систем,
студент группы № Р3430
Направление подготовки: 24.03.02 – Системы управления движением и навигация
e-mail: rozertreit@gmail.com

**УДК 537.6**

# РАЗРАБОТКА ПРОГРАММНО-МАТЕМАТИЧЕСКОЙ МОДЕЛИ КВАНТОВОГО ДАТЧИКА ВРАЩЕНИЯ ДЛЯ ОТРАБОТКИ АЛГОРИТМОВ УПРАВЛЕНИЯ МАГНИТНОЙ СИСТЕМОЙ

**Чалков В.В.**
**Научный руководитель – Шевченко А.Н.**

Работа посвящена разработке программно-математической модели квантового датчика вращения.
**Ключевые слова:** квантовый датчик вращения; обработка алгоритмов; программно-математическая модель.

Одна из важнейших проблем, возникающая при реализации квантового датчика вращения, это нестабильность магнитного поля по оси $Z$ (чувствительности), что приводит к нестабильности смешения нуля, а по осям $X$ и $Y$ приводит к нестабильности положения оси чувствительности [1, 2].

Для решения этой проблемы используется система генерации и стабилизации магнитных полей, которая предназначена для управления исполнительными устройствами и обеспечения следующих задач:

- генерация и стабилизация продольного магнитного поля, задающего ось чувствительности квантового датчика вращения;
- генерация опорного частотного сигнала;
- генерация продольного переменного магнитного поля на частоте щелочного металла;
- генерация поперечных переменных магнитных полей на частотах изотопов ксенона;
- компенсация постоянных поперечных магнитных полей.

Система генерации и стабилизации магнитных полей включает в себя следующие подсистемы:

- подсистема генерации и стабилизации продольного магнитного поля служит для выработки и удержания с заданной точностью постоянного тока обмоток соленоида, формирующего магнитное поле, которое задает ось чувствительности квантового датчика вращения;
- подсистема генерации продольного переменного магнитного поля на частоте щелочного металла служит для выработки переменного тока обмоток соленоида, формирующего переменное магнитное поле;
- подсистема генерации поперечных переменных магнитных полей на частотах изотопов ксенона служит для выработки переменного тока системы;
- подсистема компенсации постоянных двух поперечных магнитных полей служит для выработки двух постоянных токов для обмоток систем катушек, формирующих поперечные магнитные поля $X$ и $Y$, и состоит из двух усилителей. Данные магнитные поля формируются при помощи тех же обмоток, что и формируют поперечные переменные магнитные поля на частотах изотопов ксенона, следовательно, должна быть предусмотрена система суммирования токов [3].

Перед проведением моделирования было разработано математическое описание сигналов на выходах фотодиодов в зависимости от процессов, протекающих в газовой ячейке. На основании данной модели была разработана в системе Simulink. Структура модели квантового датчика вращения представлена на рис. 1.

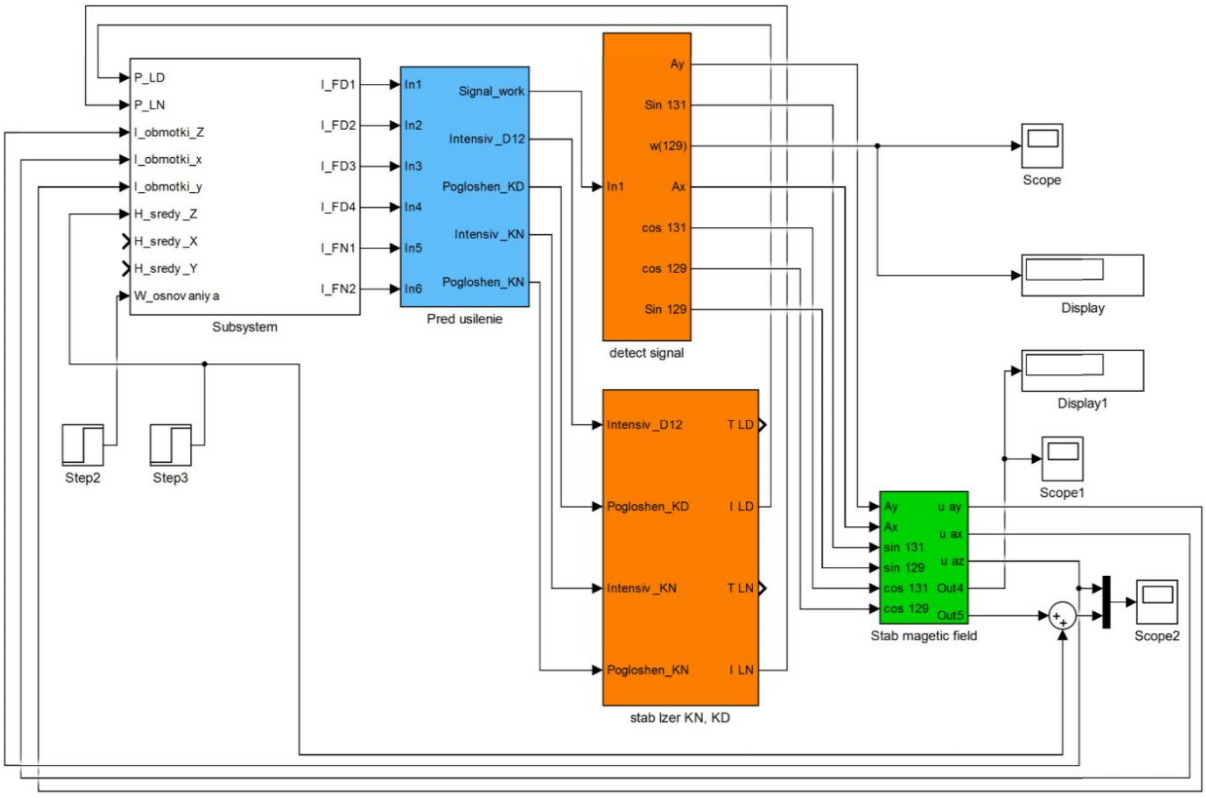



Рис. 1. Структура программно-математической модели управления магнитной системой квантового датчика вращения

В модель входят следующие блоки:

- блок первичного усиления магнитной системы квантового датчика вращения;
- блок управлением лазерами;
- блок стабилизации по осям *X*, *Y*, *Z* магнитной системы квантового датчика вращения;
- блок выработки сигнала управления магнитной системы квантового датчика вращения.

На рис. 2 показана структура модели квантового датчика вращения, а именно участок преобразования сигнала с фотоприемника до сигнала, получаемого системой стабилизации магнитных полей.

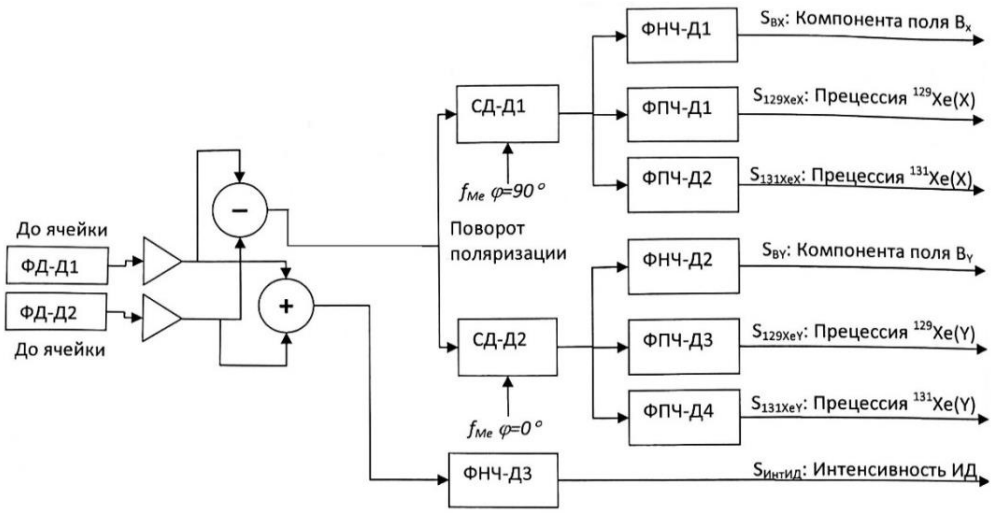



Рис. 2. Структура модели управления магнитной системой квантового датчика вращения

С помощь программно-математической модели были выбраны коэффициенты дробно-рациональных фильтров, используемых в алгоритмах детектирования сигналов ядерно-магнитного резонанса изотопов ксенона 129 и 131.

Полосовые фильтры ФПЧ S129X и ФПЧ S129Y выбраны в виде фильтров Баттерворта 5-го порядка со следующей передаточной функцией:

$F(s) = \frac{T_1^5 s^5 + 3{,}24T_1^4 s^4 + 5{,}24T_1^3 s^3 + 5{,}24T_1^2 s^2 + 3{,}24T_1 s + 1}{T_2^5 s^5 + 3{,}24T_2^4 s^4 + 5{,}24T_2^3 s^3 + 5{,}24T_2^2 s^2 + 3{,}24T_2 s + 1}$, где $T_1 = \frac{1}{116 \cdot 2\pi}$, а $T_2 = \frac{1}{120 \cdot 2\pi}$.

Полосовые фильтры ФПЧ S131X и ФПЧ S131Y выбраны в виде фильтров Баттерворта 5-го порядка со следующей передаточной функцией:

$F(s) = \frac{T_1^5 s^5 + 3{,}24T_1^4 s^4 + 5{,}24T_1^3 s^3 + 5{,}24T_1^2 s^2 + 3{,}24T_1 s + 1}{T_2^5 s^5 + 3{,}24T_2^4 s^4 + 5{,}24T_2^3 s^3 + 5{,}24T_2^2 s^2 + 3{,}24T_2 s + 1}$, где $T_1 = \frac{1}{33 \cdot 2\pi}$, а $T_2 = \frac{1}{37 \cdot 2\pi}$.

Фильтры низких частот ФНЧ SBX и ФНЧ SBY выбраны в виде фильтров Баттерворта 5-го порядка со следующей передаточной функцией:

$F(s) = \frac{1}{T_1^5 s^5 + 3{,}24T_1^4 s^4 + 5{,}24T_1^3 s^3 + 5{,}24T_1^2 s^2 + 3{,}24T_1 s + 1}$, где $T_1 = \frac{1}{2\pi}$.

Пропорционально-интегрально-дифференцирующие (ПИД) регуляторы для линий регулирования по сигналам SBX и SBY выбраны апериодических звеньев первого порядка:

$F(s) = \frac{-0{,}01}{0{,}1s+1}$.

Фильтр низких частот ФНЧ dS153 выбран в виде фильтра Баттерворта 5-го порядка со следующей передаточной функцией:

$F(s) = \frac{1}{T_1^5 s^5 + 3{,}24T_1^4 s^4 + 5{,}24T_1^3 s^3 + 5{,}24T_1^2 s^2 + 3{,}24T_1 s + 1}$, где $T_1 = \frac{1}{2\pi}$.

ПИД-регулятор для линий регулирования по сигналам dS153 выбран в виде апериодических звеньев первого порядка $F(s) = \frac{-0{,}000000009}{(4s+1)(20s+1)s}$.

Фильтры низких частот ФНЧ dS131X и ФНЧ dS131Y выбраны в виде фильтров Баттерворта 5-го порядка со следующей передаточной функцией $F(s) = \frac{1}{T_1^5 s^5 + 3{,}24T_1^4 s^4 + 5{,}24T_1^3 s^3 + 5{,}24T_1^2 s^2 + 3{,}24T_1 s + 1}$, где $T_1 = \frac{1}{2\pi}$.

Результатом данной работы являлась разработанная программно-математическая модель квантового датчика вращения, позволяющая отработать алгоритмы управления магнитной системой, и были выбраны коэффициенты дробно-рациональных фильтров, используемых в алгоритмах детектирования сигналов ядерно-магнитного резонанса изотопов ксенона 129 и 131. Результаты работы могут быть использованы для дальнейших исследований магнитной системы квантового датчика вращения с учетом внешних возмущающих факторов.

**Литература**

1. Пешехонов В.Г. Современное состояние и перспективы развития гироскопических систем // Гироскопия и навигация. – 2011. – № 1. – С. 3–17.
2. Meyer D., Larsen M. Nuclear Magnetic Resonance Gyro for Inertial Navigation // Gyroscopy and Navigation. – 2014. – V. 5. – № 2. – P. 75–82.
3. Вершовский А.К., Литманович Ю.А., Пазгалёв А.С., Пешехонов В.Г. Гироскоп на ядерном магнитном резонансе: предельные характеристики // Гироскопия и навигация. – 2018. – № 1(100). – С. 55–80.

**Шевченко Александр Николаевич**
Год рождения: 1982
АО «Концерн «ЦНИИ «Электроприбор»
e-mail: standw.shev@gmail.com

**Кислицина Елена Андреевна**
Год рождения: 1993
Университет ИТМО, факультет систем управления и робототехники, кафедра информационно-навигационных систем, аспирант
Направление подготовки: 12.06.01 – Фотоника, приборостроение, оптические и биотехнические системы и технологии
e-mail: keasunrise@gmail.com

**Безмен Глеб Владимирович**
Год рождения: 1976
АО «Концерн «ЦНИИ «Электроприбор», к.т.н.
e-mail: gbezmen@elprib.ru

**УДК 537**

# МЕТОДИКА ФОРМИРОВАНИЯ ТРЕБОВАНИЙ К ГРАДИЕНТУ МАГНИТНОГО ПОЛЯ ПРИ ОПРЕДЕЛЕНИИ МЕТРОЛОГИЧЕСКИХ ХАРАКТЕРИСТИК ЯЧЕЕК ЯДЕРНОГО МАГНИТНОГО ГИРОСКОПА

**Шевченко А.Н.** (АО «Концерн «ЦНИИ «Электроприбор»)**,**
**Кислицина Е.А.** (Университет ИТМО)
**Научный руководитель – к.т.н. Безмен Г.В.** (АО «Концерн «ЦНИИ «Электроприбор»)

Работа посвящена разработке методики формирования требований к градиенту магнитного поля для исследования параметров ячеек ядерного магнитного гироскопа. Была определена зависимость достижимой чувствительности ядерного магнитного гироскопа от метрологических характеристик ячеек. Выведена зависимость скорости релаксации атомов благородного газа от градиента магнитного поля.
**Ключевые слова:** градиент магнитного поля, метрологические характеристики, ядерный магнитный резонанс, поперечная релаксация атомов.

В настоящее время наблюдается развитие исследований и разработок в области создания гироскопа на эффекте ядерного магнитного резонанса (ЯМР) [1]. Квантовый датчик вращения или ядерный магнитный гироскоп может работать как в режиме датчика угловой скорости, так и в режиме датчика угла. В режиме датчика угловой скорости рассматриваются частоты сигнала ЯМР, в то время как в режиме датчика угла работа ведется с фазой сигналов гироскопа. Чувствительным элементом такого гироскопа является стеклянная ячейка, заполненная изотопами благородного газа и парами щелочного металла. Состав и давление газов в ячейке во многом определяет точность показаний, снимаемых детектирующим

лазером. Кроме того, в конструкции гироскопа присутствует система задания магнитных полей [2]. Неоднородность создаваемых магнитных полей влияет на метрологические характеристики гироскопа, в особенности на скорость релаксации ядер благородных газов в ячейке [3]. Время релаксации максимально при нулевом градиенте и уменьшается с ростом неоднородности.

В работе, посвященной определению требований к градиенту магнитного поля на лабораторных установках, с помощью которых определяются метрологические характеристики ячейки ядерного магнитного гироскопа, было решено две задачи: определена зависимость достижимой чувствительности ядерного магнитного гироскопа от характеристик ячейки и зависимость этих метрологических характеристик от градиента магнитного поля.

Основными метрологическими характеристиками газовых ячеек является время релаксации ядер благородного газа и отношение сигнал-шум. С помощью этих двух характеристик может быть определена предельно достижимая чувствительность ARW ядерно-магнитного гироскопа (1):

$$ARW = \frac{1}{T(S/N)\sqrt{\Delta f}}, \qquad (1)$$

где $T$ – время релаксации ядер благородного газа, с; $S/N$ – отношение сигнал/шум, дБ/Гц; $\Delta f$ – полоса пропускания, Гц.

Более наглядно это уравнение можно представить на графике (рис. 1). В том случае, когда известно время поперечной релаксации ксенона (Xe) и отношение сигнал/шум, можно определить предельно достижимую чувствительность для рассматриваемой ячейки при условии, что сама конструкция гироскопа не вносит никаких искажений.

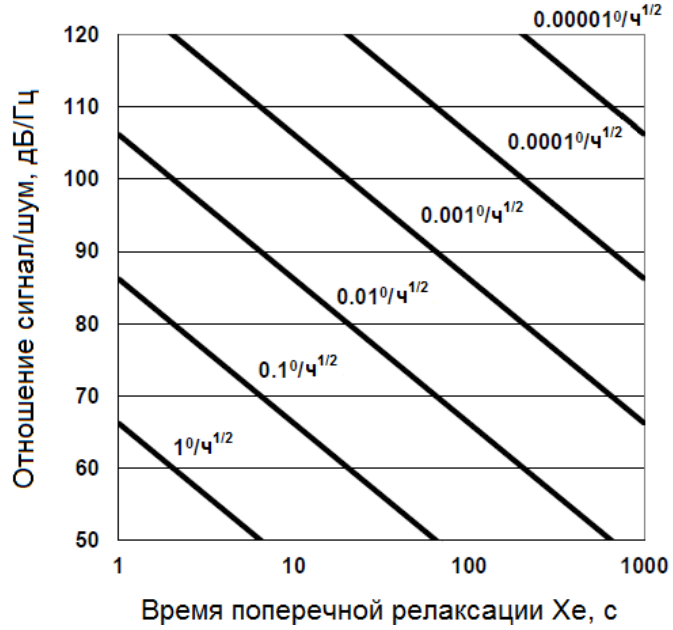
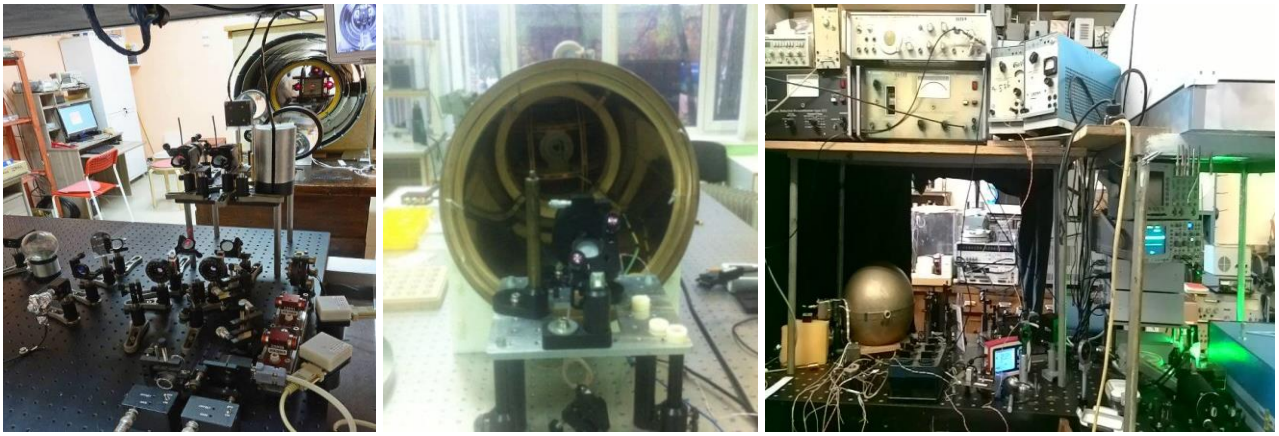



Рис. 1. Коэффициент случайного блуждания как функция отношения сигнал/шум и времени релаксации

Время поперечной релаксации в разных организациях определяется на различных стендах. Общим элементом всех стендов является наличие магнитного экрана, в который устанавливается ячейка, и оптических элементов, служащих для накачки спинов и детектирования прецессии атомов щелочных металлов. Конструкции магнитного экрана могут сильно отличаться у разных производителей. Для рассматриваемой задачи преимущественно применяют цилиндрические экраны (рис. 2, а, б), однако эксперименты проводились, в том числе и со сферическим экраном (рис. 2, в).



а б в

Рис. 2. Лабораторные стенды для исследования эффектов ЯМР с магнитными экранами: цилиндрической формы (а), (б); сферической формы (в)

При измерении параметров одной и той же ячейки на разных стендах, результаты измерений получаются разные. Причиной, по которой выходные характеристики ячейки не совпадают, является наличие неоднородности магнитного поля, которая способствует ускорению процесса релаксации. Величина, обратная времени жизни изотопа, – скорость релаксации атомов благородного газа. В свою очередь, релаксация – это разрушение когерентного состояния атома. Разрушение когерентного состояния атома может быть вызвано столкновениями атомов благородного газа с атомами щелочного металла, столкновениями атомов благородного газа со стенками ячейки, а также наличием неоднородности магнитного поля (2). Две первые величины относятся в первую очередь к характеристикам самой ячейки, в то время как последнее слагаемое во многом зависит от характеристик стенда, на котором проводятся измерения.

$$\Gamma_{total} \approx n_{Rb}\left(\sigma\bar{v}+\frac{\gamma_m\chi}{n_{Xe}}\right)+\Gamma_{wall}+\frac{8R^4\gamma^2}{175D}\left(\frac{\partial B_z}{\partial z}\right)^2=a\left(\frac{\partial B_z}{\partial z}\right)^2+c, \qquad (2)$$

где $n_{Rb}$ – плотность паров щелочного металла; σ – постоянная спинобменного взаимодействия; $\bar{v}$ – средняя относительная тепловая скорость ($\bar{v}=\sqrt{8k_BT/\pi m}$, где $m$ – уменьшенная при столкновениях щелочь-благородный газ масса, $k_B$ – постоянная Больцмана, $T$ – температура ячейки); $\gamma_m$ – константа Г.Д. Кейта; χ – коэффициент, зависящий от ядерного спина и концентрации паров щелочного металла; $n_{Xe}$ – плотность благородного газа; $R$ – радиус газовой ячейки; γ – гиромагнитное отношение атома благородного газа; $D$ – коэффициент диффузии атомов благородного газа в ячейке; $\partial B_z/\partial z$ – градиент магнитного поля.

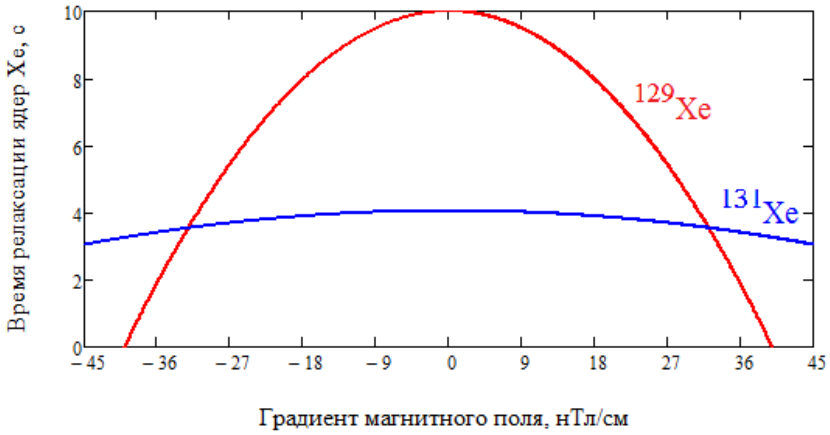



Рис. 3. Зависимость времени поперечной релаксации ядер 129 и 131 изотопов ксенона от градиента магнитного поля ячейки

В ходе исследования на одном из стендов был искусственно внесен градиент магнитного поля. После этого была измерена скорость поперечной релаксации атомов благородного газа. С помощью упрощенной модели, полученной в уравнении (2), была выведена зависимость времени поперечной релаксации ядер двух изотопов ксенона от градиента магнитного поля (рис. 3). При повторном проведении эксперимента на той же установке, но с другой ячейкой, наблюдалась такая же зависимость, однако значения изменились на целый порядок.

На следующем этапе исследования на одном из вышеприведенных лабораторных стендов были произведены замеры значений времен поперечной релаксации 129 изотопа ксенона в отсутствие градиента магнитного поля и при искусственном внесении градиента 20 нТл/см (рис. 4), что дало возможность оценить влияние градиента на время поперечной релаксации ядер – при градиенте 20 нТл/см время релаксации уменьшилось почти вдвое.

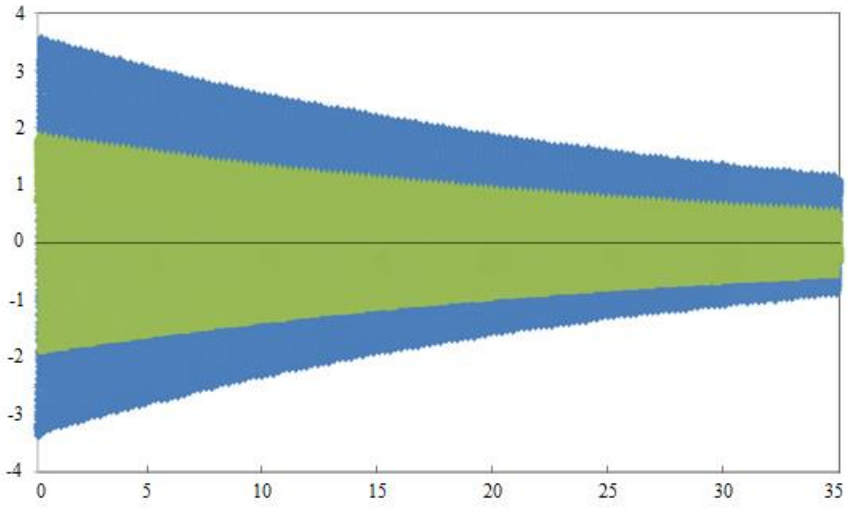


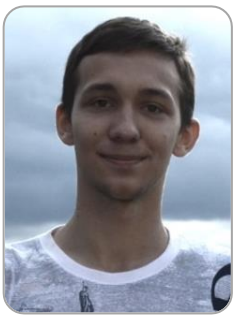

Рис. 4. Зависимость времени поперечной релаксации ядер $^{129}$Xe от градиента магнитного поля ячейки: ■ – без градиента, ■ – градиент магнитного поля равен 20 нТл/см

Таким образом, в результате исследования была определена зависимость достижимой чувствительности ядерного магнитного гироскопа от метрологических характеристик газовой ячейки. Также была выведена зависимость скорости релаксации атомов благородного газа от градиента магнитного поля. По результатам проведенной работы, для того чтобы сформировать требования к градиенту магнитного поля необходимо определить: требуемую точность оценки чувствительности гироскопа ARW, диапазон давлений в исследуемых газовых ячейках и уровень отношения сигнал/шум по сигналам ксенона. Оперируя этими данными, можно сформировать требования к лабораторному стенду, который может быть в дальнейшем использован для исследования параметров ячеек ядерного магнитного гироскопа.

**Литература**

1. Larsen M., Bulatowicz M. Nuclear Magnetic Resonance Gyroscope: For DARPA's micro-technology for positioning, navigation and timing program // Frequency Control Symposium (FCS) IEEE International. – 2012. – P. 1–5.
2. Meyer D., Larsen M. Nuclear Magnetic Resonance Gyro for Inertial Navigation // Gyroscopy and Navigation. – 2014. – V. 5. – № 2. – P. 75–82.
3. Mirijanian J.J. Techniques to characterize vapour cell performance for a nuclear-magnetic-resonance gyroscope [Электронный ресурс]. – Режим доступа: https://digitalcommons.calpoly.edu/cgi/viewcontent.cgi?article=1766&context=theses, своб.

**Ерофеев Михаил Александрович**
Год рождения: 1993
Университет ИТМО, факультет систем управления и робототехники, кафедра мехатроники, аспирант
Направление подготовки: 15.06.01 – Машиностроение
e-mail: mr.mikhail-erofeev@yandex.ru



**Овчаров Алексей Олегович**
Год рождения: 1996
Университет ИТМО, факультет систем управления и робототехники, студент группы № Р3440
Направление подготовки: 27.03.04 – Управление в технических системах
e-mail: ovcharov.a@protonmail.com

**УДК 531.1: 612.766**

## РАЗРАБОТКА УПРАВЛЯЕМОГО ОРТЕЗА НИЖНЕЙ КОНЕЧНОСТИ

**Ерофеев М.А., Овчаров А.О.**
**Научный руководитель – к.т.н., профессор Мусалимов В.М.**

В работе рассмотрен подход к созданию управляемого ортеза нижней конечности человека на основе данных измерений кинетических и кинематических сгибания и разгибания в коленном и тазобедренном суставе в период совершения шага, полученных в лаборатории кинезиологии и биомеханики Тартуского университета Эстонии. Проведено исследование движения манипулятора по полученным биомеханическим показателям.
**Ключевые слова:** управляемый ортез, фазы шага, биомеханика, экзоскелет, траекторное управление.

Уже долгое время медицинские организации используют для лечения и реабилитации инвалидов ортезы-аппараты и экзоскелеты. Наиболее часто такие устройства используются после инсультов, в результате нейродегенеративных процессов, при переломах и травмах позвоночника. В этом случае ортезы-аппараты несут опорную функцию – поддержание вертикального положения и помогают восстановить двигательную активность.

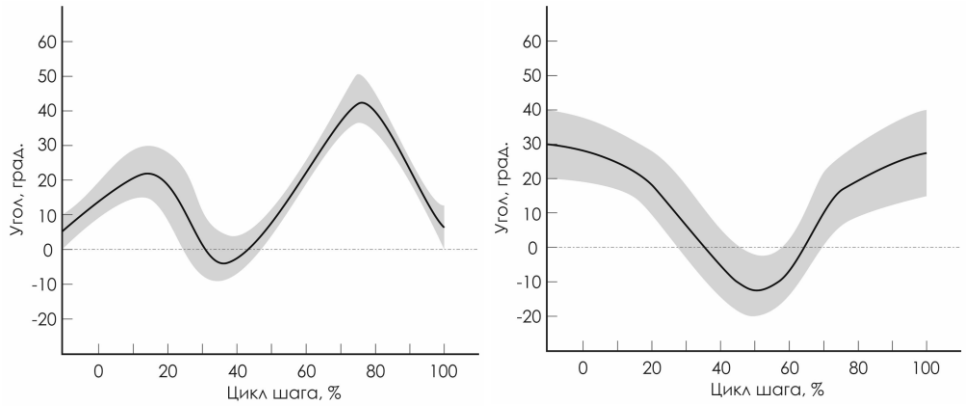
Целью работы являлось рассмотрение возможности использования кинетических и кинематических параметров совершаемого шага, в частности – углов сгибания и разгибания в коленном и тазобедренном суставе, для системы управления механизма манипулятора и дальнейшей адаптации для системы управления ортезом-аппаратом.

Настоящая работа опирается на экспериментальные данные, полученные в результате исследований в лаборатории кинезиологии и биомеханики Тартуского университета с помощью оптической маркерной системы. Геометрические параметры сегментов тела пациентов были измерены антропометрическими методами. Кинетические характеристики шага исследовались при помощи оптоэлектронной системы для анализа движений Elite (BTS Engineering S.p.A., Италия) [1, 2].

В результате исследования были получены массивы данных об изменении угловых показателей сгибания и разгибания основных суставов за период совершения цикла шага. Результирующие зависимости углов от цикла шага представлены на рис. 1.

Полученные данные были аппроксимированы и адаптированы для тестирования на манипуляторе. Для тестов исполнения траектории ходьбы по полученным данным использовался робот-манипулятор платформы KUKA YouBot, который состоит из

манипулятора с 5-ю степенями подвижности и мобильной платформы. Манипулятор, задействованный для данного исследования, работает на двух типах бесщеточных двигателей: maxon EC 32 flat и maxon EC 45 flat, а также энкодере maxon MR encoder, type L. Управляющая система построена на базе Robotic Operating System (ROS).




а б

Рис. 1. Изменение угла флексии/экстензии для коленного сустава (а) и тазобедренного сустава (б)

Траекторное управление осуществлялось скоростным регулятором, который представлен на рис. 2. Здесь: $q^*, \dot{q}^*$ – желаемые угол и угловая скорость; $q_{ctrl}$ – управляющая скорость; $q_{real}$ – текущая скорость звена манипулятора. Блок motor controller выполняет управление уже непосредственно скоростью двигателей и помощью подчиненного регулятора.

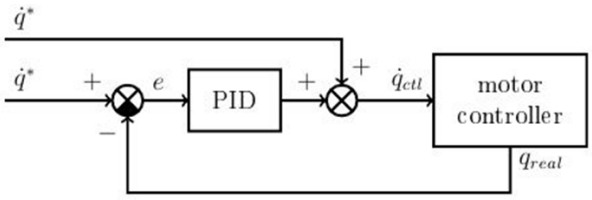



Рис. 2. Скоростной регулятор

Исполнение регулятором траектории представлено на рис. 3. Здесь: $q_i$ ; $\dot{q}_i$ , $i$=2–4 – углы и угловые скорости второго–четвертого звеньев манипулятора соответственно. Ошибка $q_i$ – разница между желаемым и реальным углами $i$-го звена.

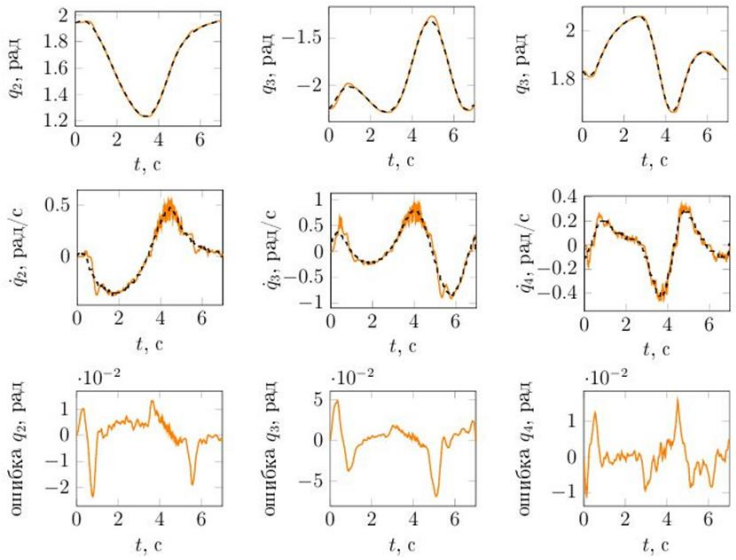



Рис. 3. Исполняемая регулятором траектория

Полученные данные позволяют сделать вывод о возможности использования и адаптации данных, полученных в результате исследования антропометрических и биомеханических показателей совершаемого человеком шага, для системы управления манипулятором. Этот результат будет использован в дальнейшей работе для создания самостоятельного управляемого макета движения нижний конечности и разработки управляемого ортеза-аппарата.

**Литература**

1. Gapeyeva H., Ereline J., Haviko T., Aibast H., Martson A.,Paasuke M. Gait characteristics and muscle strength in total knee arthroplasty patients with patellofemoral pain syndrome before and six months after surgery // Acta Kinesiologiae Universitatis Tartuensis. – 2011. – V. 17. – P. 37–52.
2. Мусалимов В.М., Паасуке М., Гапеева Е., Ерелине Я., Ерофеев М.А. Моделирование динамики опорно-двигательной системы // Научно-технический вестник информационных технологий, механики и оптики. – 2017. – Т. 17. – № 6. – С. 1159–1166.

**Защитин Роман Александрович**
Год рождения: 1996
Университет ИТМО, факультет систем управления и робототехники, кафедра мехатроники, студент группы № Р3325
Направление подготовки: 15.03.06 – Мехатроника и робототехника
e-mail: romzes.kolomna@gmail.com

**Коваленко Павел Павлович**
Год рождения: 1984
Университет ИТМО, факультет систем управления и робототехники, кафедра мехатроники, к.т.н., доцент
e-mail: kovalenko_p.p@mail.ru

**Перепелкина Светлана Юрьевна**
Год рождения: 1979
Университет ИТМО, факультет систем управления и робототехники, кафедра мехатроники, к.т.н., доцент
e-mail: svetlana.yu.perepelkina@gmail.com

**УДК 621.8**

# ПРОЕКТИРОВАНИЕ ЭНЕРГОЭФФЕКТИВНОГО ПОЗВОНОЧНИКА БИОМИМЕТИЧЕСКОГО РОБОТА-ГЕПАРДА

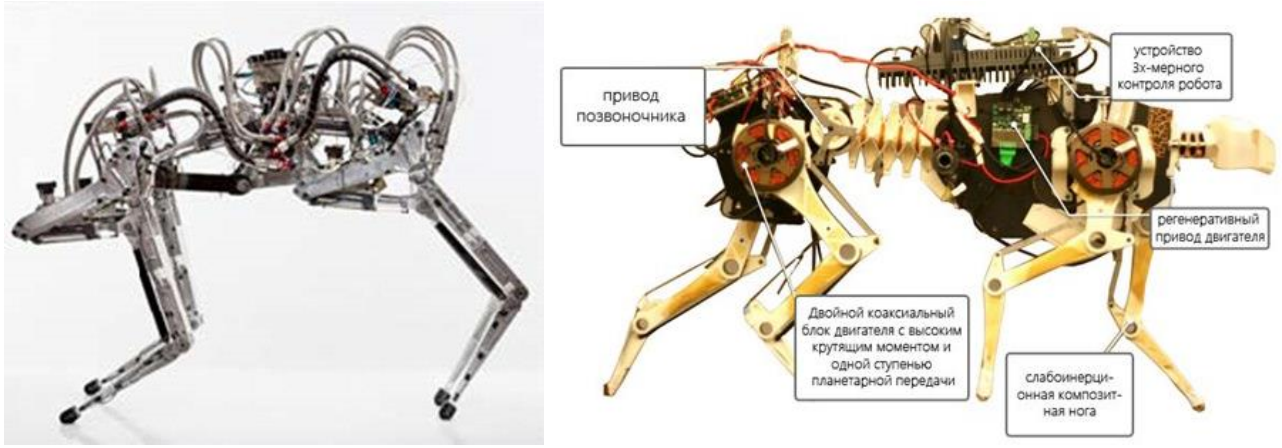
**Защитин Р.А., Коваленко П.П., Перепелкина С.Ю.**
**Научный руководитель – к.т.н., доцент Коваленко П.П.**

Работа выполнена в рамках темы НИР № 713546 «Нелинейное и адаптивное управление сложными системами».

В работе на основе обзора и анализа научных статей и справочной литературы выявлено конструкторское решение для реализации энергоэффективного биомехатронного позвоночника робота-гепарда, с целью увеличения скорости бега робота и максимального сходства с реальным строением опорно-двигательного аппарата гепарда.
**Ключевые слова:** биомиметика, энергетическая эффективность роботов, электроактивные полимеры.

С каждым годом возрастает актуальность использования роботов и механизмов во всех сферах деятельности человека. Так, с развитием робототехники перед конструкторами возникают различные проблемы, связанные с энергоэффективностью и использованием альтернативы электромоторам в роботах и механизмах. Создатели роботов все чаще заимствуют свои идеи у самой природы и не могли обойти стороной гепарда, являющегося самым быстрым животным на планете. Уже неоднократно предпринимались попытки создать роботизированного гепарда и существуют рабочие прототипы. В работе рассмотрены наиболее успешные конструкторские решения компаний, различных конструкторов и ученых.

Кандидат из Boston Dynamics (рис. 1, а) является первым в своем роде роботом-гепардом. Он развивает скорость до 46 км/ч. Конструкция основана на пневмоклапанах. Конструкторы делали упор в первую очередь на скоростные параметры робота и достигли этого с помощью видоизменения конечностей. Время автономной работы увеличивают за счет установки большого количества аккумуляторных батарей, а сама конструкция выполнена из металлических частей.




а б

Рис. 1. Робот-гепард Boston Dynamics (а) и робот-гепард из MIT [2] (б)

Робот из MIT (Массачусетский технологический институт) (рис. 1, б) ушел дальше своего предшественника и развивает скорость 56 км/ч, во главе конструкции лежит электродвигатель с высоким крутящим моментом. Робот обладает жестким позвоночником, а энергоэффективность поддерживается благодаря рекуперации части обычно рассеиваемой энергии. Устойчивость сохраняется благодаря особому строению конечностей, а каркас состоит из легкого композитного материала [1].

Робот-гепард из университета Твенте (рис. 2) является самым энергоэффективным. Его вес составляет 2,5 кг, имеет общую длину 30 см и развивает скорость до 20 км/час. Если принять, что роботизированная модель гепарда имеет такие же габариты и вес, что и живое существо, то он бы расходовал всего на 15% больше энергии во время бега, что является рекордным показателем. Основным элементом конструкции является пружинный аналог спинного хребта, исключающий использование сегментов и аналогов межпозвоночных дисков, накапливающий и использующий энергию при беге [2].

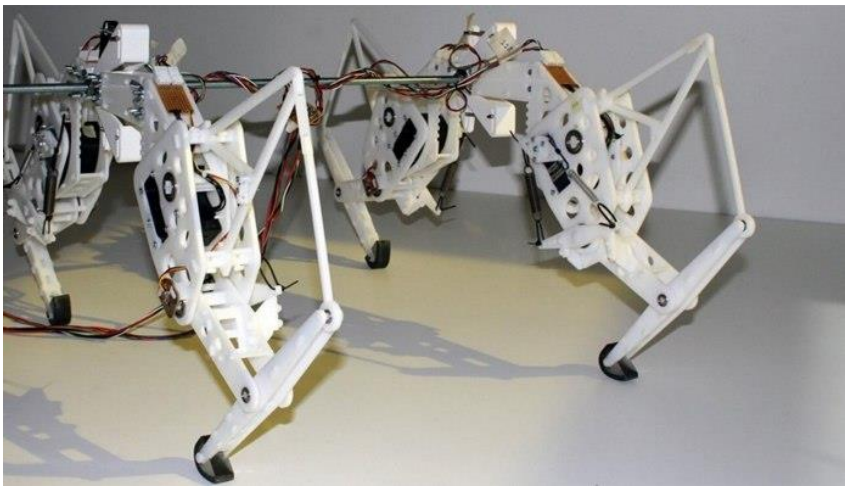


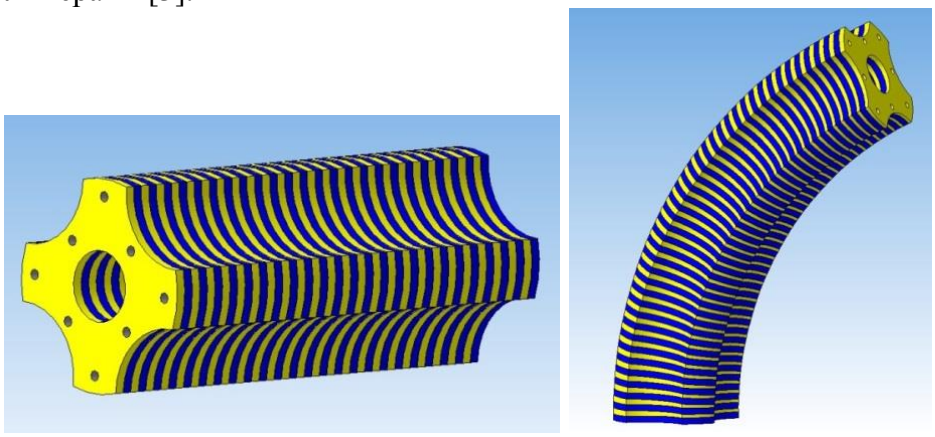
Рис. 2. Робот-гепард из Твенте [3]

Во всех этих решениях конструкторы делали упор на конечности и приводы роботов, пытаясь увеличить скорость и энергоэффективность конструкций. Если взглянуть на

реальное строение гепарда, то можно заметить, что около 70% мышц сосредоточены вдоль позвоночника. Сам позвоночник очень гибок и благодаря ему гепард достигает феноменальных скоростей. При беге немаловажным являются конечности гепарда. Сухожилия работают практически как пружины. Пружина – это маятник, и при резонансе будет самый наименьший расход энергии. Энергия не тратится на сгибание и разгибание тела или конечностей, а только на раскачку. Таким образом, гепард подбирает резонанс под нужную скорость, напрягая тонус мышц. Следовательно, конструкция будущего роботизированного гепарда должна обладать гибким, эластичным, прочным позвоночником и энергоэффективными, пружинящими конечностями.

Для реализации подобного механизма нет электроприводов, сопоставимых с работой мышц. Также реализация конструкции на пневмоклапанах или приводах будет отрицательно сказываться на энергозатратной составляющей робота и его веса. Интересным решением в данном вопросе может являться использование электроактивных полимеров.

В настоящей работе выбор пал на диэлектрический эластомер. При попадании данного полимера в электрическое поле, полимер сокращается подобно мышцам (рис. 3). Особенность используемого диэлектрического эластомера заключается в лучших показателях растяжения и сжатия при использовании меньшего электрического поля. Это возможно также из-за эффективного преобразования энергии электрического поля в механическую, которая составляет 90%. И несомненным плюсом является сохранение свойств при множестве циклов работы, легкость и высокая прочность материала в сравнении с другими полимерами [3].



а б

Рис. 3. Структура позвоночника: без воздействия электрического поля (а); под воздействием электрического поля (б)

Таким образом, позвоночник будущего робота-гепарда будет состоять из диэлектрического эластомера. Для усиления жесткостных параметров позвоночника эластомер будет чередоваться с силиконовой резиной, что позволит не только более эффективно управлять позвоночником, но и придать позвоночнику реальные механические свойства. Поскольку пассивные характеристики используемого материала являются ключевым фактором для воссоздания работы и гибкости позвоночника, были проведены испытания на растяжение/сжатие, чтобы найти количественные данные о пассивных свойствах некоторых коммерчески доступных силиконовых резиновых смесей. Эти материалы сравнивались с акцентом на их механические свойства, и был выбран материал, наиболее близкий к естественным мышцам [4].

Слои эластомера и резины пронизывают восемь управляющих проводов из меди, на которых при подаче электричества создается электрическое поле, которое сокращает искусственные мышцы. Такая конструкция позволяет имитировать работу позвоночника гепарда во время бега, когда угол, образующийся позвоночником, составляет 15–20°.

Полученные результаты будут взяты за основу в дальнейшем проектировании опорно-двигательного аппарата робота-гепарда. Будут рассчитаны жесткостные, прочностные параметры конструкции и произведено моделирование в CAE-системе. Планируется разбор и анализ существующих инженерных решений конечностей роботизированных гепардов и проектирование метода крепления управляющей аппаратуры и конечностей к позвоночнику.

**Литература**

1. Park H.-W., Kim S. The MIT Cheetah, an Electrically-Powered Quadrupedal Robot for High-speed Running // JRSJ. – 2014. – V. 32. – № 4. – P. 323–328.
2. Folkertsma G.A., van der Schaft A.J., Stramigioli S. Morphological computation in a fast-running quadruped with elastic spine // IFAC-PapersOnLine. – 2015. – V. 48. – № 13. – P. 170–175.
3. Shankar R., Ghosh T.K., Spontak R.J. Electroactive Nanostructured Polymers as Tunable Actuators // Adv. Mater. – 2007. – № 19. – P. 2218–2223.
4. Laschi C., Mazzolai B., Mattoli V., Cianchetti M., Dario P. Design of a biomimetic robotic octopus arm // IOP Publishing. – 2009. – V. 4. – № 1. – P. 8–15.

**Казначеева Анна Олеговна**
Год рождения: 1980
Университет ИТМО, факультет систем управления и робототехники, кафедра мехатроники, к.т.н.
e-mail: a_kazn@mail.ru

**УДК 004.932.2**

## ФРАКТАЛЬНЫЙ АНАЛИЗ ПОПЕРЕЧНЫХ СРЕЗОВ ГОЛОВНОГО МОЗГА

**Казначеева А.О.**

В работе исследована зависимость фрактальной размерности магнитно-резонансного изображения от влияющих на контрастность тканей условий сканирования, алгоритма сбора данных и пространственного разрешения. Расчеты выполнены box-counting методом для аксиальных срезов головного мозга и для серии параллельных срезов показывают сохранение характера изменения фрактальной размерности от положения среза при различных условиях.
**Ключевые слова:** изображение, контрастность, фрактальная размерность, томография, box-counting.

Одной из актуальных задач анализа изображений является поиск универсальных количественных оценок, позволяющих автоматизировать диагностику в различных областях. Одним из направлений является исследование возможности фрактального анализа для поиска структурных изменений объекта. Так, фрактальный анализ изображений образцов горных пород позволяет оценить их физические и коллекторские свойства [1], при оценке сварных соединений – описать геометрию излома и установить взаимосвязь с параметрами усталости [2]. В медицине фрактальный подход используется для анализа самоподобных структур, например, вещества головного мозга [3], однако сложность обработки заключается в необходимости учета влияния условий исследования на характеристики изображений [4, 5].

Трудность анализа изображений, полученных методом магнитно-резонансной (МР) томографии, заключается в отсутствии стандарта исследования и универсального протокола. Интенсивность сигнала от тканей при выполнении исследований на разном оборудовании даже при идентичных протоколах будет отличаться. Для медицинской диагностики основным критерием является контрастность тканей в выбранном режиме, а не абсолютное значение интенсивности, которое может отличаться в несколько раз в зависимости от алгоритма реконструкции [6] и сбора данных [7]. Для количественной оценки отличие интенсивности может иметь существенное значение. В данной работе исследовалась зависимость фрактальной размерности от пространственного разрешения, алгоритма заполнения *k*-пространства, импульсной последовательности.

В МР-томографии пространственное разрешение по осям, как правило, отличается, так как уменьшение матрицы в направлении фазового кодирования сокращает время исследования. Размер воксела $r$ рассчитывается с учетом поля сканирования FOV и матрицы **m** в соответствующем направлении, а также толщины среза $th$ и межсрезового интервала $sp$:

$$r_x = \frac{FOV_x}{m_x}, \quad r_y = \frac{FOV_y}{m_y}, \quad r_z = th + sp,$$

где $r_x$ и $r_y$ – разрешение по осям $x$ и $y$ для аксиального среза; $r_z$ – разрешение по оси $z$.

Динамический диапазон изображения отражает интервал значений $[0, L_{\max}]$ яркостей пикселов МР-изображения и зависит от импульсной последовательности (режима). В зависимости от положения среза динамический диапазон отдельных изображений в серии

может отличаться в 1,5–2 раза. Гистограммы яркости для одного среза, полученного в разных режимах, также будут отличаться по количеству и расположению пиков, и можно предположить влияние этих факторов на фрактальную размерность изображения.

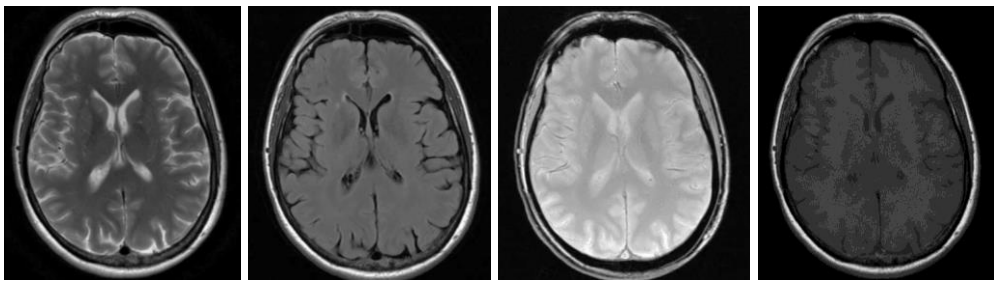
Для оценки симметрии структур головного мозга и обнаружения изменений служит фрактальная размерность $D$, принимающая нецелые значения для самоподобных объектов с сильно изрезанной формой. Для двумерного случая расчет может выполняться box-counting методом в случае МР-изображения, заключающимся в разбиении на клетки со стороной $R \to 0$ так, чтобы каждая точка объекта попадала в ту или иную клетку. Изменение числа ячеек $N(R)$ будет происходить по степенному закону:

$$N(R) \propto R^{-D}.$$

При уменьшении размера клетки некоторое их количество будет попадать в область за границами объекта, содержащими только шум. Однако исследования, посвященные фильтрации шумов на изображении [8], показали, что для гауссова шума порядок фильтрации (винеровским методом) не существенен, тогда как порядок фильтрации импульсного шума (медианным фильтром) влияет на значение фрактальной размерности [9] и других оценок [6, 8].

В работе исследовалось влияние условий сканирования (протокола) на рассчитанное значение фрактальной размерности. Анализировались серии из 20 изображений аксиальных срезов головного мозга, полученные в наиболее распространенных режимах (рис. 1):

- быстрое спин-эхо с высоким сигналом от жидкости T2 FSE (режим K1);
- с подавлением сигнала от движущейся жидкости T2 Flair (режим K2);
- градиентное эхо, чувствительное к магнитной восприимчивости T2×GRE (режим K3);
- спин-эхо с низким сигналом от жидкости T1 SE (режим K4).



а б в г

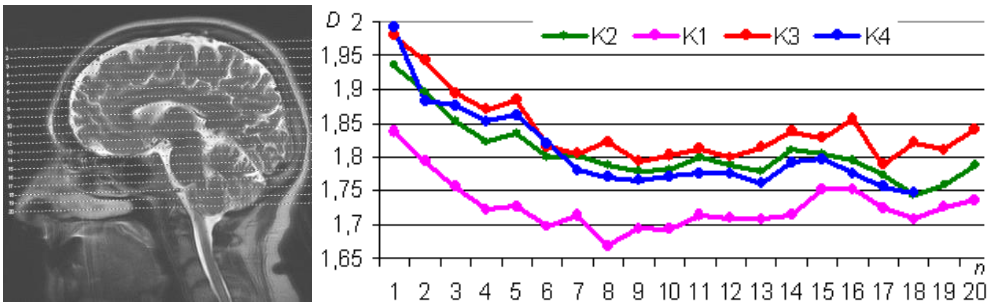
Рис. 1. Изображения среза головного мозга, полученные в режимах: T2 FSE (а); T2 Flair (б); T2×GRE (в); T1 SE (г)

Анализируемые изображения здоровых добровольцев получены на МР-томографе HDxt (GE) с полем 3Тл с использованием 8-канальной катушки для головного мозга. На первом этапе сканирование выполнялось во всех режимах с параметрами: FOV=240 мм, $th$=5 мм, $sp$=1 мм, матрица 288×288 интерполированная до 512×512, что обеспечивало пространственное разрешение $r_x$=$r_y$=0,83 мм. Затем в базовом протоколе для последовательности T2 FSE матрица изменялась на стандартную 480×480 (разрешение 0,5×0,5 мм), а в режиме T2 Flair – на 352×224 (разрешение 0,68×1,07 мм). По оси $z$ во всех случаях разрешение оставалось постоянным (6 мм). Оценка влияния алгоритма заполнения $k$-пространства на фрактальную размерность оценивалось для режима T2 FSE для быстрого построчного заполнения (FSE), параллельного заполнения с многократным перекрытием низкочастотной области (Propeller) и одновременным заполнением всех строк (EPI FSE). Таким образом, для одного пациента необходимо было получить 8 серий из $n$ 20 изображений (сверху вниз, рис. 2, а) с общей продолжительностью сканирования 23 минуты.

Фрактальная размерность рассчитана в пакете MATLAB, показавшим хороший результат для выявления структурных отличий по фрагментам изображения [10]. Анализ выполнялся box-методом для интерполированных изображений 512×512, размер ячейки

изменялся от 1/16 до 1/256 (так как размер матрицы МР-изображения кратен 16) для нормализованных данных и 100 итераций. Регрессия выполнена методом наименьших квадратов.

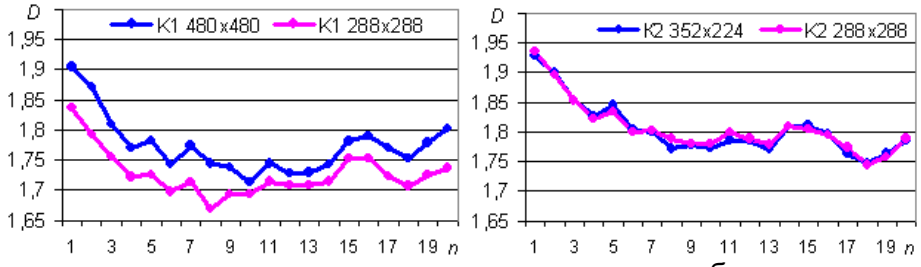
Результат для базового протокола показывает, что во всех случаях для верхних срезов, где доля заполнения объектом матрицы меньше, и для нижних срезов, включающих больше типов тканей, наблюдается увеличение фрактальной размерности (рис. 2, б). Для режимов K2–K4 фрактальная размерность имеет близкие значения в диапазоне 1,79–1,82, что может объясняться низкой контрастностью тканей и меньшим динамическим диапазоном. В режиме K1 фрактальная размерность меньше (1,715) при большем динамическом диапазоне.




а б

Рис. 2. Положение срезов (а) и рассчитанная фрактальная размерность (б)

Необходимость анализа влияния пространственного разрешения на фрактальную размерность вызвана отсутствием стандартной матрицы и частыми случаями уменьшения пользователем матрицы в фазовом направлении для сокращения времени исследования. При этом поле FOV меняется крайне редко и составляет 240 мм как в базовом протоколе исследования, что позволяет говорить о зависимости разрешения от выбранной матрицы. Анализ выполнен для наиболее используемых серий T2 FSE и T2 Flair со стандартной для каждой серии матрицей (480×480 и 352×224 соответственно) и выбранной для базового протокола (288×288). Изменение фрактальной размерности для срезов различного положения аналогично описанному выше – для верхних и нижних срезов значение выше (рис. 3).




а б

Рис. 3. Зависимость фрактальной размерности от матрицы для T2 FSE (а), T2 Flair (б)

Для серии T2 FSE уменьшение пространственного разрешения почти в 2 раза привело к незначительному уменьшению фрактальной размерности с 1,754 до 1,715. Изменение разрешения не сказалось на фрактальной размерности T2 Flair изображений. Несмотря на меньшее, чем в предыдущем случае, изменение матрицы, можно считать полученную размерность $D$=1,79 характерной для данного режима, так как большая матрица используется крайне редко из-за существенного увеличения времени исследования, а меньшая – также редко из-за размытия изображения.

Влияние алгоритма сбора данных для серии T2 FSE оказалось невозможно проанализировать для случая быстрого одновременного заполнения всех строк EPI FSE (рис. 4, а), что связано с высокой чувствительностью алгоритма к неоднородностям поля. Как и в предыдущих случаях характерно увеличение фрактальной размерности для верхних и нижних срезов. Выбор алгоритма построчного или параллельного сбора данных меняет значение $D$ на 0,035.

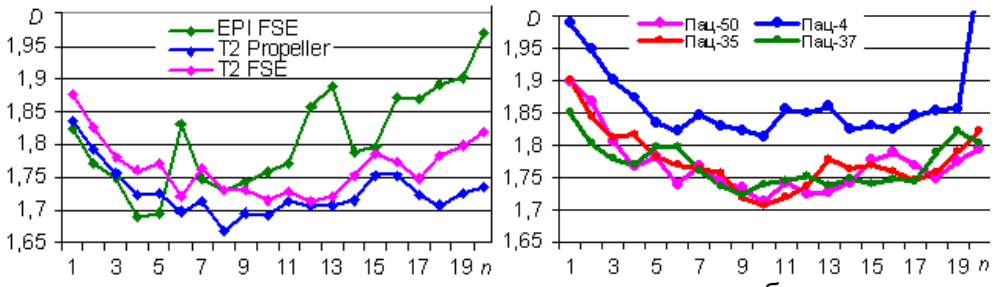



Рис. 4. Зависимость фрактальной размерности от алгоритма (а) и возраста пациента (б)

Отдельный интерес представляет анализ влияния возрастных изменений МР-сигналов на фрактальную размерность изображения. Для анализируемой выборки видно, что для любых срезов фрактальная размерность у детей выше, чем у взрослых (рис. 4, б). Однако для расчета норм *D* в различных возрастных группах требуется отдельное исследование.

Анализ значений фрактальной размерности для серий МР-изображений, полученных в различных режимах, показывает зависимость результата от положения среза и контрастности составляющих его тканей. Изображения, на которых объект занимает малую часть площади, характеризуются резко увеличенным значением $D \to 2$. Пространственное разрешение не влияет на фрактальную размерность, в то время как выбранный режим (импульсная последовательность) может изменять размерность *D* изображения при достижении высокой контрастности тканей (1,715 для T2 FSE). Это позволяет сделать вывод, что наличие структурных изменений, контрастных по отношению к здоровым тканям, также приведет к существенному изменению фрактальной размерности, что требует отдельных исследований для различных клинических случаев. Для анализируемой выборки отмечено, что фрактальная размерность у детей выше, чем у взрослых, на 0,1–0,15.

**Литература**

1. Тупысев А.М. Фрактальный анализ цифровых изображений образцов горных пород // Автоматизация, телемеханизация и связь в нефтяной промышленности. – 2017. – № 1. – С. 11–15.
2. Рудакова О.А. Фрактальный подход к анализу особенностей усталостного разрушения сварных швов // Вестник ПНИПУ. Машиностроение, материаловедение. – 2012. – Т. 14. – № 4. – С. 102–107.
3. Молчатский С.Л. Фрактальная организация и самоорганизация нейронных структур мозга. – Самара, 2015. – 133 с.
4. Казначеева А.О. Разработка методов и средств шумоподавления в томографии: дис. … канд. техн. наук. – СПб., 2006. – 167 с.
5. Иванников В.П., Суфиянов В.Г., Белых В.В., Степанов В.А. Фрактальный анализ рентгенограмм // Вестник ИжГТУ. – 2009. – № 3. – С. 150–154.
6. Сизиков В.С. Обратные прикладные задачи и MatLab. – СПб.: Лань, 2011. – 256 с.
7. Казначеева А.О. Возможности и ограничения высокопольной магнитно резонансной томографии (1,5 и 3 Тесла) // Лучевая диагностика и терапия. – 2010. – № 4. – С. 83–87.
8. Сизиков В.С., Экземляров Р.А. Предшествующая и последующая фильтрация шумов в алгоритмах восстановления изображений // Научно-технический вестник информационных технологий, механики и оптики. – 2014. – № 1. – С. 112–122.
9. Казначеева А.О. Фрактальный анализ зашумленности магнитно-резонансных томограмм // Альманах современной науки и образования. – 2013. – № 2. – С. 73–76.
10. Виноградова А.А., Казначеева А.О., Мусалимов В.М. Фрактальный анализ томограмм головного мозга // Изв. вузов. Приборостроение. – 2013. – Т. 56. – № 12. – С. 14–19.

**Нуждин Кирилл Андреевич**
Год рождения: 1991
Университет ИТМО, факультет систем управления и робототехники, кафедра мехатроники, аспирант
Направление подготовки: 15.06.01 – Машиностроение
e-mail: nkirill_74@mail.ru

**УДК 621.8.039**

# ИССЛЕДОВАНИЕ И МОДЕЛИРОВАНИЕ РЕКУПЕРАЦИОННЫХ МЕХАНИЗМОВ В ПАКЕТЕ SIMMECHANICS

**Нуждин К.А.**
**Научный руководитель – д.т.н., профессор Мусалимов В.М.**

Работа выполнена в рамках темы НИР № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность».

В работе рассмотрены рекуперационные устройства на основе упругих элементов. Проведен анализ и построение модели механизма с пружинным аккумулятором, а также приведена оценка рекуперационных свойств полученного устройства.
**Ключевые слова:** энергоэффективность, рекуперация энергии, пружинный аккумулятор, SimMechanics, построение механической модели.

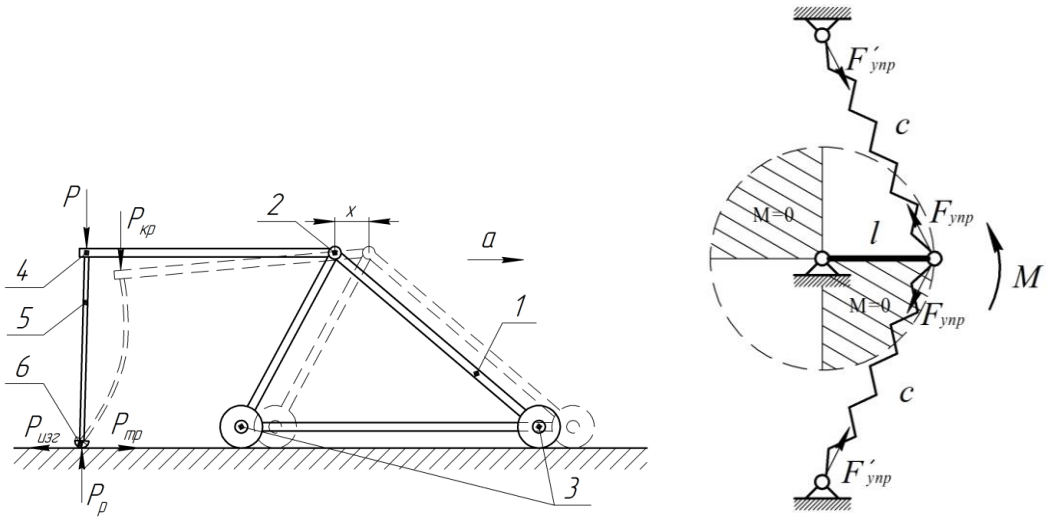
В настоящее время одной из главных проблем при проектировании роботизированных и мехатронных устройств является их энергоэффективность. Несомненно, снижение энергопотребления способствует увеличению времени автономной работы различных механизмов и актуаторов. В связи с этим в настоящий момент широкое распространение приобретают различные рекуперационные механизмы, целью которых является частичное восстановление затраченной энергии (как тепловой и электрической, так и механической) для повторного использования или ее аккумулирования.

Настоящая работа посвящена исследованию рекуперационных механизмов, применяемых для восстановления механической энергии. Известно два вида данных устройств:

1. рекуперационный механизм исполнительного устройства, предназначенного для преобразования прикладываемого воздействия в поступательное движение, где частичная регенерация энергии происходит за счет упругих свойств рабочего звена в процессе восстановления первоначальной формы. Схема данного устройства представлена на рис. 1, а, где: 1 – основание; 2 – шарнирный узел; 3 – подвижные опоры, оборудованные храповым механизмом; 4 – подвижное звено для передачи приложенной силы нагружения $P$; 5 – упругий элемент; 6 – полукруглый опорный наконечник; $P_{кр}$ – критическая сила нагружения; $P_{тр}$ – сила трения; $P_{изг}$ – изгибающая сила; $P_{р}$ – сила реакции опоры; $x$ – смещение движителя) [1–3];
2. пружинный аккумулятор с выходным поворотным звеном, используемый при вращательном движении [4].

Рассмотрим второе устройство более подробно. Схема вращательного рекуперационного механизма с пружинным аккумулятором представлена на рис. 1, б.

Рабочий цикл поворота механизма, т.е. полный оборот исполнительного звена вокруг оси вращения, можно мысленно разделить на четыре части (рис. 1, б). Незаштрихованные области соответствуют стадии «зарядки» пружинного аккумулятора. Здесь под действием крутящего момента привода совершается вращательное движение рабочего звена, которое, в свою очередь, воздействуя на пружины, выводит их из состояния равновесия, сжимая одну и растягивая другую.




а б

Рис. 1. Схема исполнительного устройства на основе упругого элемента (а); схема механизма с пружинным аккумулятором (б)

В этой части следует сделать некоторое пояснение: согласно теории катастроф и теории устойчивости, данный механизм с пружинным аккумулятором, состоящим из двух одинаковых пружин, имеет два положения устойчивости, т.е. такие условия, при которых не совершаются колебания рабочего звена, а состояние и положение пружин не меняются сколь угодно много времени. В данном случае в начальный момент времени механизм находится в первом устойчивом состоянии, равном нулевому отклонению рабочего звена относительно оси вращения. Второе устойчивое положение симметрично ему, т.е. расположено в точке отклонения исполнительного звена, равному 180°. Данные два положения являются своего рода аттракторами соответственно для правой и левой полуокружностей траектории движения рабочего звена.

Заштрихованные области траектории исполнительного звена соответствуют циклу работы пружинного аккумулятора. Здесь происходит отключение привода, и движение производиться только за счет накопленной энергии пружин.

На следующем этапе работы была построена модель данного механизма, выполненная с использованием библиотеки SimMechanics пакета Simulink среды MATLAB (рис. 2).

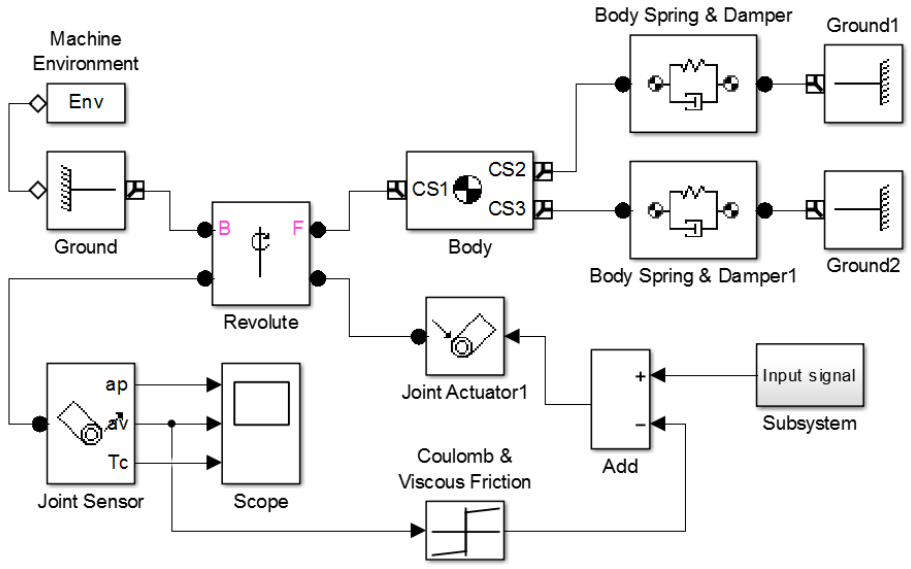



Рис. 2. Модель рекуперационного механизма с нелинейным пружинным аккумулятором

Блоки Machine Environment, Ground1 и Ground2 задают соответственно гравитационные силы для модели и условия крепления и положения частей механизма. Revolute, Body – формируют геометрию вращающегося рабочего звена. Joint Actuator1 является кинематическим приводом, обеспечивающим вращательное движение. Joint Sensor предназначен для получения выходных характеристик рабочего (исполнительного) звена. Блок Coulomb & Viscous Friction используется для учета влияния трения в шарнирном соединении Revolute. Body Spring & Damper1 выполняют роли нелинейных пружин. Блок Subsystem задает входной сигнал, подаваемый на привод Joint Actuator1.

Данная модель построена таким образом, что ось вращения рабочего звена лежит на одной прямой с осями вращения шарнирного сочленения пружин и стойки. Исходная длина данных пружин принимается равной 0,1 м, кроме этого в процессе функционирования механизма каждая из них находится в деформированном (растянутом) состоянии и достигает исходной (начальной) длины лишь в момент времени, когда другая пружина имеет наибольшую величину растяжения. Описанное расположение позволяет наиболее эффективно применять пружинный аккумулятор для рекуперации энергии, затраченной приводом вращательного движения.

Далее проводился ряд экспериментов для оценки рекуперационных свойств полученного механизма. В качестве исходного (идеального) устройства рассматривался механизм без использования пружинного аккумулятора. Для сравнения свойств двух данных устройств на их входы блока привода подавался один и тот же сигнал, соответствующий одному полному обороту исполнительного звена. После этого снимались данные, характеризующие угол поворота исполнительного звена (Angle, град.), угловую скорость вращения (Angular velocity, град./с) и крутящий момент привода (Torque, Н·м). Полученные графические результаты представлены на рис. 3.

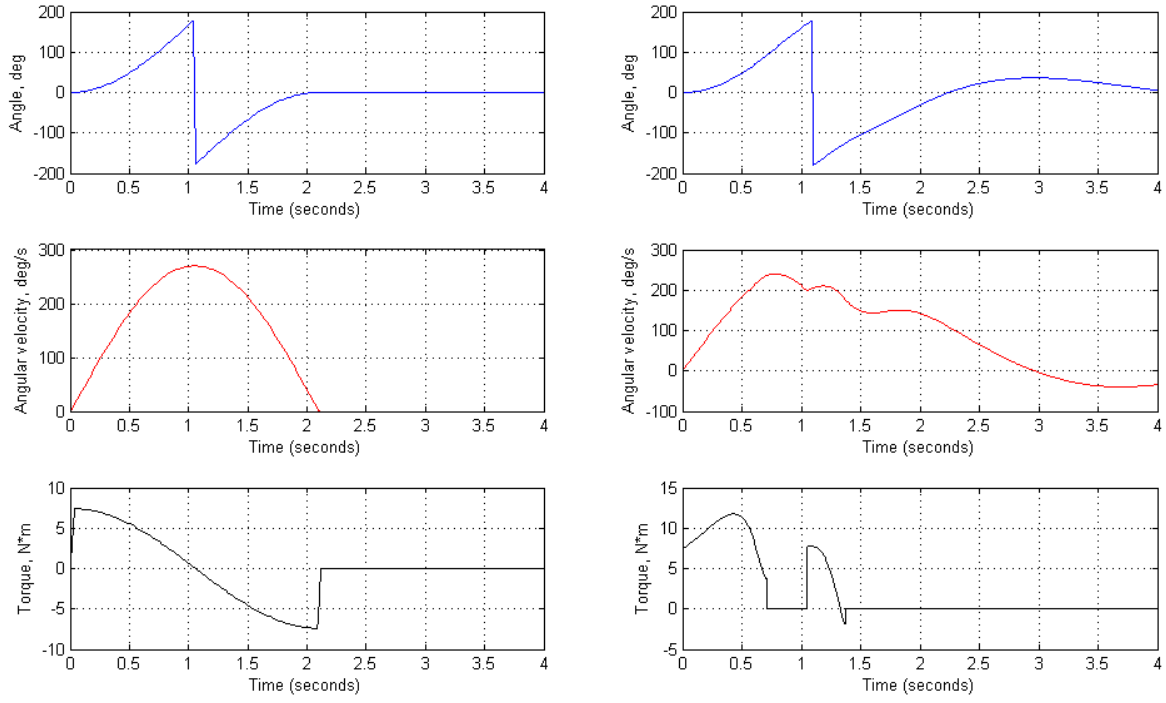



Рис. 3. Полученные результаты для исходного (идеального) механизма (а) и механизма с пружинным аккумулятором (б)

Анализируя полученные результаты можно заметить, что применение пружинного аккумулятора позволяет значительно уменьшить время работы привода, что соответственно приводит к уменьшению энергопотребления (это можно увидеть при сравнении графиков

Torque/Time). Однако, с другой стороны, использование упругих элементов повышает частоту колебаний рабочего звена, тем самым увеличивая время выполнения рабочего цикла.

В итоге, в ходе проведения работы с использованием пакета прикладных программ MATLAB и библиотеки SimMechanics авторы смогли построить модель рекуперационного механизма и на ее примере показать целесообразность применения пружинных аккумуляторов в цикловых вращательных механизмах для восстановления энергии.

**Литература**

1. Нуждин К.А. Проблемы создания актуаторов на основе упругих элементов // Изв. вузов. Приборостроение. – 2018. – Т. 61. – № 2. – С. 148–153.
2. Nuzhdin K. Recuperation Mechanisms Based on Elastic Elements // Proceedings of the 17th International Symposium Topical Problems in the Field of Electrical and Power Engineering, Doctoral School of Energy and Geotechnology, Tallinn university of technology, Kuressaare. – 2018. – P. 268–271.
3. Пат. 172799 Российская Федерация, МПК B62M 29/02, F16H 21/00, A63G 19/10. Исполнительное устройство на основе упругого элемента / Мусалимов В.М., Нуждин К.А.; заявитель и патентообладатель Университет ИТМО. – № 2017100380; заявл. 09.01.2017; опубл. 24.07.2017, Бюл. № 13. – 6 с.
4. Пелупесси Д.С., Жавнер М.В. Пружинные аккумуляторы с выходным поворотным звеном для шаговых перемещений // Изв. вузов. Машиностроение. – 2016. – № 10(679). – С. 9–17.

**Шураева Оксана Тахировна**
Год рождения: 1996
Университет ИТМО, факультет систем управления и робототехники, кафедра мехатроники, студент группы № Р3425
Направление подготовки: 15.03.06 – Мехатроника и робототехника
e-mail: Burst.19.dsf@gmail.com

**Коваленко Антон Александрович**
Год рождения: 1996
Университет ИТМО, факультет систем управления и робототехники, кафедра мехатроники, студент группы № Р3425
Направление подготовки: 15.03.06 – Мехатроника и робототехника
e-mail: Strateg7602@gmail.com

**УДК 608**

# РАЗРАБОТКА БИОМИМЕТИЧЕСКОГО РОБОТА-УЛИТКИ

**Шураева О.Т., Коваленко А.А.**
**Научный руководитель – к.т.н., доцент Монахов Ю.С.**

Работа посвящена исследованию принципов локомоции гастроподов и воспроизведению их в мехатронном устройстве. Проведен обзор существующих аналогов и предложен свой вариант технического решения в формате биомиметического робота-улитки. Приведены результаты моделирования устройства и его расчетные характеристики. Намечены цели для дальнейшей работы.
**Ключевые слова:** робототехника, биомехатроника, биомиметика, компьютерное моделирование, робот-улитка.

Представители класса гастроподов, к которым относятся различные улитки и слизни, известны как природные внедорожники, способные перемещаться по поверхностям самой разной структуры под различными углами к горизонту. Воспроизведение подобной системы перемещения позволит создать сравнительно компактные мехатронные устройства, способные преодолевать практически любые препятствия, что может найти свое применение, например, при исследовании завалов или других объектов с трудным ландшафтом, в которых роботы с более традиционными средствами локомоции окажутся неэффективны.

Записи локомоторной активности улиток Ахатина, сделанные через стеклянную поверхность, по которой они ползли, позволили сделать выводы о механике движения ноги улитки [1]. Мышцы ноги движутся волнообразно, то расслабляясь, то сокращаясь, создавая волну, протекающую от хвоста к голове улитки, тем самым двигая ее вперед. Однако ключевой особенностью гастроподов, обеспечивающей им столь завидные локомоторные характеристики является вырабатываемый ими секрет – муцин. Именно муцин обеспечивает улиткам надежный контакт с поверхностью, по которой они перемещаются.

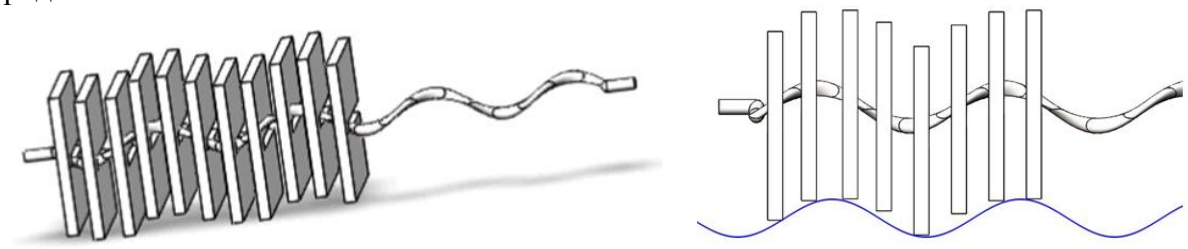
Робот, наиболее близко воспроизводящий движения улиток, был разработан в Массачусетском технологическом институте в 2003 году и представлял собой пять пластин, соединенных друг другом, на каждую из которых со стороны сцепления с поверхностью нанесен тонкий слой адгезивной жидкости на базе глицерина. Соединение пластин осуществлялось нитиловыми нитями, и все пластины были нанизаны на общую направляющую. В ходе движения передняя пластина перемещалась вперед на

фиксированное расстояние, а все остальные пластины попеременно подтягивались к ней [2]. Очевидно, что такая конструкция сделана лишь в качестве демонстрации принципиальной возможности перемещения по наклонным поверхностям за счет использования адгезивных соединений и не годится для полевого использования с резкими перепадами углов поверхности.

Еще одно мехатронное устройство, представляющее интерес в рамках данной темы – робот SAW [3] – одноактуаторный робот, перемещающийся за счет вращения спирали и создания пропелляционной синусоидальной волны, а для регулирования направления движением использует одно колесо. Его устройство подтверждает принципиальную возможность перемещения улиток по горизонтальным поверхностям исключительно за счет волнообразного движения мышц ноги без использования муцина. Впрочем, конструкция данного робота не подразумевает каких-либо технических решений для перемещения по наклонным поверхностям, что ограничивает его локомоторные характеристики по сравнению с настоящими улитками.

Еще ряд технических устройств носят названия робот-улитка, однако их конструкция не имеет ничего общего с принципами локомоции гастроподов.

В результате данной работы было предложено биомиметическое решение адаптации принципов перемещения улиток. Для воспроизведения волнообразного движения ноги улитки используется массив пластин из ABS-пластика нанизанных на металлическую спираль, при вращении которой прилегающая к поверхности сторона робота создает синусоидальную волну (рис. 1). Для управления направлением движения (вправо-влево) таких массивов два, и на каждый массив для вращения спирали приходится один электродвигатель постоянного тока.



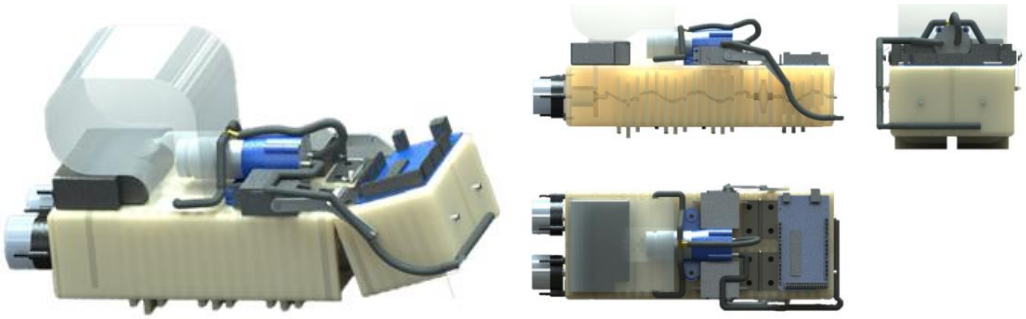
а б

Рис. 1. Формирование волнообразного движения: изометрия (а); вид сбоку (б)

Для того чтобы робот мог подниматься на препятствия с резкими перепадами угла, его передняя часть имеет возможность подниматься с помощью сервоприводов, установленных на корпусе. Передача вращательного движения из тела робота в голову осуществляется с помощью фрикционных муфт (рис. 2).

В качестве муцина в рамках модели предложено использование 95% раствора глицерина. Выбор сделан на основе расчета свойств вязкого трения, требуемого для удержания мехатронного устройства на вертикальной поверхности, а также исходя из факторов доступности и цены материала. На практике же при создании опытного образца предполагается проведение экспериментов с другими жидкостями, в том числе неньютоновскими.

Для хранения муцина на корпусе робота установлен контейнер, который с помощью поливинилхлоридных шлангов соединен через соленоидный поршневой насос с передней частью, благодаря чему при перемещении обеспечивается постоянное смазывание поверхности сцепления адгезионным материалом. Питание двигателей, насоса и контроллера обеспечивает 12-вольтный аккумулятор емкостью 0,8 Ач, обеспечивающий роботу до 80 мин автономной работы.



а б

Рис. 2. Трехмерная модель робота-улитки (а), проекционные виды (б)

Для обеспечения единого волнового фронта поверхности сцепления тело и голова робота-улитки обтянуты снизу эластичной (нитриловой) прослойкой.

Размеры устройства составляют 332×180×135 мм, а приблизительная масса – 2,5 кг.

Таким образом, в результате данной работы получена конструкция биомиметического робота-улитки, воспроизводящего принципы локомоции гастроподов. Данное мехатронное устройство может позволить детальнее изучить характеристики движения реальных улиток, и факторы на них влияющие, а также найти практическое применение в исследовательских целях в районах с труднопроходимым ландшафтом.

В дальнейшем цель работы состоит в создании опытного образца устройства и проведения испытаний и расчетов с целью определения наиболее оптимального аналога улиточного муцина.

**Литература**

1. Tyrakowski T., Kaczorowski P., Pawłowicz W., Ziółkowski M., Smuszkiewicz P., Trojanowska I., Marszaek A., Żebrowska M., Lutowska M., Kopczyńska E., Lampka M., Hoyłńska-Iwan I., Piskorska E. Discrete Movements of Foot Epithelium during Adhesive Locomotion of a Land Snail // Folia Biologica. – 2012. – V. 60. – № 1-2. – P. 99–108.
2. Chan B., Ji S., Koveal C., Hosoi A.E. Mechanical Devices for Snail-like Locomotion // Journal of Intelligent Material Systems and Structures. – 2007. – V. 18. – № 2. – P. 111–116.
3. Zarrouk D., Mann M., Degani N., Yehuda T., Jarbi N., Hess A. Single actuator wave-like robot (SAW): design, modeling, and experiments // Bioinspiration & Biomimetics. – 2016. – V. 11. – № 4. – P. 046004.

**Александрова Софья Александровна**
Год рождения: 1990
Университет ИТМО, факультет систем управления и робототехники, кафедра систем управления и информатики, аспирант
Направление подготовки: 27.06.01 – Управление в технических системах
e-mail: alexandrova_sophie@mail.ru

**Николаев Николай Анатольевич**
Год рождения: 1978
Университет ИТМО, факультет систем управления и робототехники, кафедра систем управления и информатики, к.т.н., доцент
e-mail: nikona@yandex.ru

**Слита Ольга Валерьевна**
Год рождения: 1980
Университет ИТМО, факультет систем управления и робототехники, кафедра систем управления и информатики, к.т.н., доцент
e-mail: o-slita@yandex.ru

**УДК 62.50**

# СПОСОБ УПРАВЛЕНИЯ МОСТОВЫМ ПРЕОБРАЗОВАТЕЛЕМ НАПРЯЖЕНИЯ С МЯГКИМ ПЕРЕКЛЮЧЕНИЕМ ПУТЕМ ИЗМЕНЕНИЯ НЕСУЩЕЙ ЧАСТОТЫ

**Александрова С.А., Николаев Н.А., Слита О.В.**
**Научный руководитель – к.т.н., доцент Слита О.В.**

Работа выполнена в рамках темы НИР № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность».

Предложен способ управления мостовым преобразователем напряжения постоянного тока, напряжение питания которого меняется в широком диапазоне, основанный на изменении несущей частоты. Управление реализовано в виде пропоционально-интегрального регулятора с настраиваемыми в процессе функционирования параметрами. Предлагаемый способ позволяет выполнить ограничение максимальных токов, коммутируемых силовыми ключами, что увеличивает срок службы дорогостоящих полупроводниковых элементов.
**Ключевые слова:** мостовой инвертор, мягкая коммутация, фазовое управление, ПИ-регулятор с настраиваемыми параметрами, индуктивность рассеивания, несущая частота.

При низком входном напряжении и требуемых высоких выходных напряжения и мощности применяется мостовая схема преобразователя напряжения с повышающим трансформатором и добавочной индуктивностью, введенной для обеспечения мягкой коммутации силовых ключей и исключения насыщения сердечника [1, 2]. При изменении входного напряжения возможно получение параметрически робастной системы с использованием метода модального управления [3–5]. Однако предлагаемые подходы проигрывают по быстродействию и затрачиваемым ресурсам пропоционально-

интегральному (ПИ)-регулятору с настраиваемыми параметрами. Для импульсных преобразователей также часто используется подход подчиненного регулирования [1, 2], который включает внутренний контур регулирования тока и внешний – напряжения. Данный подход находит применение в системах с фиксированной несущей частотой широтно-импульсной модуляции (ШИМ) и при отклонении входного напряжения от заданного не более, чем на 20%.

В настоящей работе предложен способ фазового управления мостовым преобразователем по выходному напряжению, основанный на изменении несущей частоты, выбор значения которой зависит от величины напряжения питания и от допустимого значения пикового тока, коммутируемого транзисторами мостового инвертора.

**Постановка задачи.** Перечислим основные заданные параметры разрабатываемого повышающего преобразователя напряжения: напряжение питания может изменяться в диапазоне от 175 до 320 В, номинальный диапазон изменения напряжения питания 250–280 В, значение выходного стабилизированного напряжения должно составлять 610 В. Максимальный коммутируемый ток выбранных транзисторов – 1250 А. Номинальная выходная мощность должна составлять 60 кВт. Параметры основных силовых элементов установки: коэффициент трансформации трансформатора 1:6, емкость батареи конденсаторов фильтра 9900 мкФ.

На рис. 1 показана функциональная схема силовой части преобразователя, где *DC* – источник напряжения постоянного тока; *VT*1–*VT*4 – IGBT-транзисторы мостового инвертора; *VD*1–*VD*4 – диоды; *L* – добавочная индуктивность; *T* – высокочастотный повышающий трансформатор; $C_f$ – емкостной фильтр; $R_l$ – активное сопротивление нагрузки.

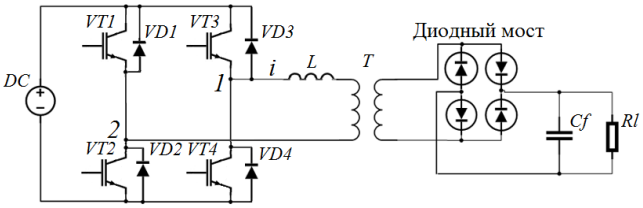



Рис. 1. Функциональная схема силовой части преобразователя

Рассмотрим передаточную функцию заданного преобразователя «напряжение на выходе–управляющий сигнал» [1]:

$$W(s)=\frac{U_{\text{вых}}}{D}=\frac{nU_{\text{пит}}}{s^2L'C_f+s(\frac{L'}{R_l}+R_dC_f)+\frac{R_d}{R_l}+1}, \quad (1)$$

где $U_{\text{вых}}$ – напряжение выхода; $D$ – коэффициент заполнения, сигнал управления замкнутой системы; $U_{\text{пит}}$ – напряжение питания; $1/n$ – коэффициент трансформации; $f_{sw}$ – несущая частота ШИМ; $L'$ – эквивалентная суммарная индуктивность инвертора, приведенная к вторичной обмотке трансформатора; $L_s$ – эквивалентная суммарная индуктивность инвертора, равная сумме индуктивностей рассеивания трансформатора и добавочной, $R_d=4n^2f_{sw}L_s$.

В [6] проведен анализ тепловых процессов и коммутационных потерь, приведший к выводу, что оптимальная частота ШИМ $f_{sw0}$ для исследуемого преобразователя составляет 7,25 кГц, и выведены зависимости максимального тока, коммутируемого транзисторами, и среднего тока выхода инвертора $I_{av}$ от коэффициента ШИМ $K_{\text{ШИМ}}$ и $f_{sw}$:

$$I_{\max}\approx\frac{U_{\text{пит}}K_{\text{ШИМ}}}{f_{sw}L},\ I_{av}=\frac{I_{\max}(L'/R_c+I_{\max}/U_{\text{пит}})}{T_{ШИМ}}, \quad (2)$$

где $R_c$ – эквивалентное суммарное сопротивление схемы замещения инвертора; $T_{\text{ШИМ}} = 1/f_{sw}$ – период несущей частоты.

Из (2) можно сделать вывод, что при фиксированных значениях $I_{\max}$, $L'$, $R_c$ поддержание величины среднего тока на выходе инвертора при увеличении напряжения его питания достижимо только при увеличении несущей частоты ШИМ. Так, ее оптимальное значение применимо для минимального значения напряжения питания и максимального значения $K_{\text{ШИМ}}$.

Обеспечим требуемые показатели качества рассматриваемой системы, передаточная функция которой (1) зависит от настраиваемой несущей частоты, введением обратной связи по напряжению с помощью ПИ-регулятора [7]:

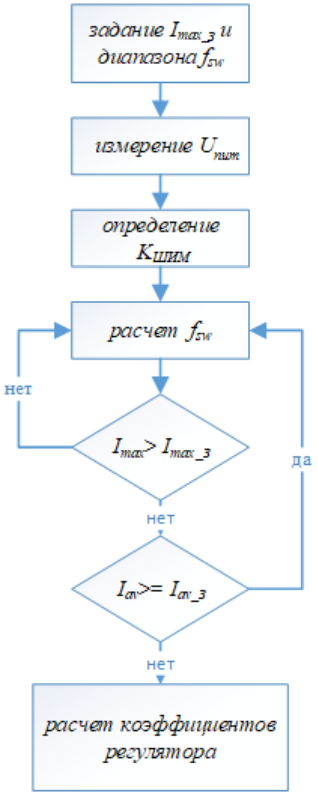
$$W_{pi}(s) = k(1 + \frac{1}{Ts}).$$

Найдем параметры ПИ-регулятора $k_0, T_0$ для минимального значения напряжения питания $U_{\text{пит0}} = 175$ В и установленного минимального значения несущей частоты ШИМ $f_{sw0} = 7{,}25$ кГц. Время переходного процесса должно быть не более 0,5 с, запас по фазе должен быть 80 градусов:

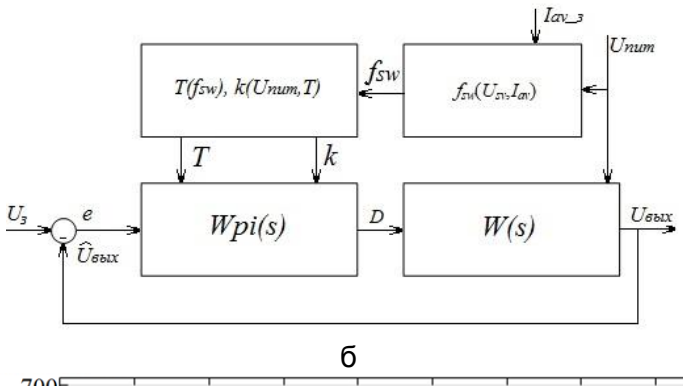
$$W_{pi0}(s) = 12 \cdot 10^{-4}(1 + \frac{1}{1{,}63 \cdot 10^{-5} s}).$$

При изменении входного напряжения несущая частота будет изменяться, а параметры ПИ-регулятора настраиваться по выражениям:

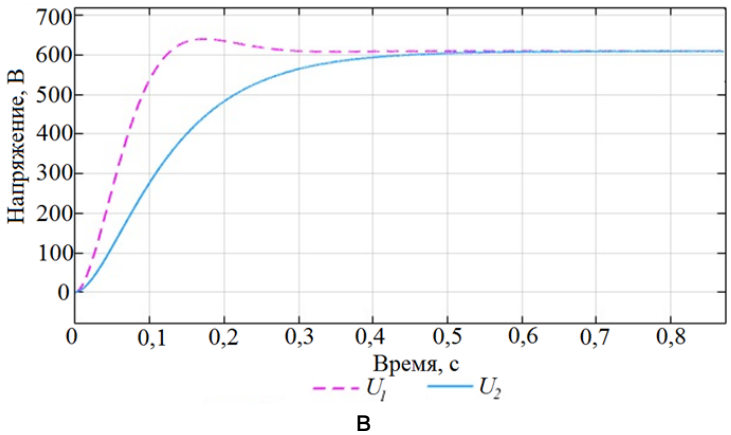
$$T = \frac{T_0 f_{sw0}}{f_{sw}}, \quad k = \frac{k_0 T U_{\text{пит0}}}{T_0 U_{\text{пит}}}. \qquad (3)$$




а




б




в

Рис. 2. Блок схема предлагаемого способа (а); структурная схема замкнутой системы (б); графики переходных процессов замкнутой системы (в)

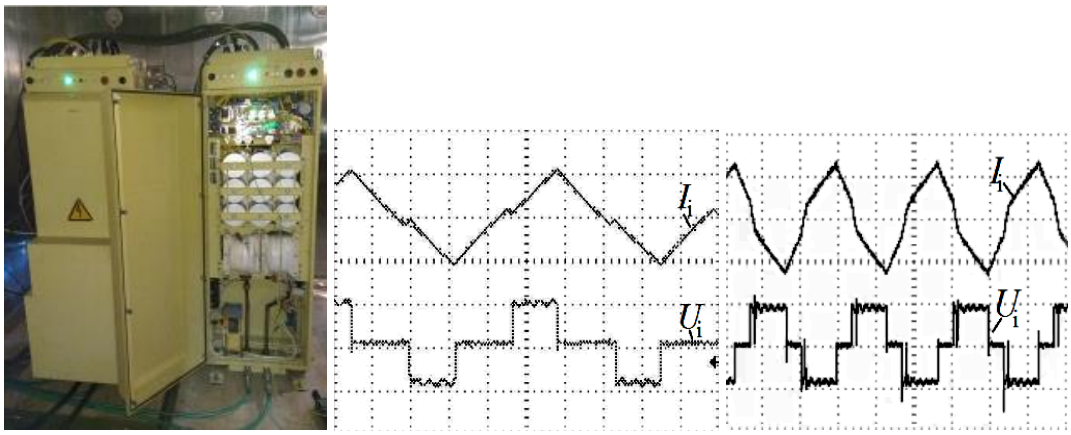
На рис. 2, а, представлена блок-схема предлагаемого алгоритма, условия проверяются по (2), расчет коэффициентов регулятора выполняются по (3), а на рис. 2, б, представлена структурная схема синтезированной замкнутой системы.

На рис. 2, а, б, $\hat{U}_{\text{вых}}$ – измеренное значение напряжение выхода преобразователя; $e$ – отклонение выхода от заданного значения $U_{\text{з}}$; $I_{av\_\text{з}}$ – заданный средний ток выхода инвертора; $I_{\max\_\text{з}}$ – заданный максимальный ток, коммутируемый транзисторами.

На рис. 2, в, приведены графики переходных процессов замкнутой системы для максимального значения напряжения питания $U_{\text{пит}} = 320$ В: $U_1$ – переходная характеристика с фиксированными параметрами регулятора $k_0, T_0$ и $f_{sw0} = 7{,}25$ кГц; $U_2$ – переходная характеристика с настраиваемыми параметрами регулятора $k$, $T$ и $f_{sw} = 10$ кГц.

Настройка параметров улучшает показатели качества переходного процесса: перерегулирование 0%.

На рис. 3, а, представлен опытный образец – преобразователь мощностью 60 кВт, входящий в состав частотного преобразователя. На рис. 3, б, в, приведены экспериментальные данные: напряжение (инвертированное) $U_i$ и ток $I_i$ выхода мостового инвертора при $U_{\text{пит}} = 187$ В, $K_{\text{ШИМ}} = 0{,}27$, $f_{sw} = 7{,}35$ кГц (190 В/дел и 600 А/дел) (рис. 3, б); напряжение $U_i$ и ток $I_i$ выхода мостового инвертора для малого $K_{\text{ШИМ}} = 0{,}16$, $U_{\text{пит}} = 320$ В, $f_{sw} = 10$ кГц (320 В/дел и 1200 А/дел) (рис. 3, в).




а б в

Рис. 3. Частотный преобразователь (а); экспериментальные результаты (б) и (в)

Рис. 3 демонстрируют работу силовых ключей в режиме мягкой коммутации и ограничение пикового тока до заданного значения 1000 А.

Предложен способ управления мостовым преобразователем с настройкой параметров регулятора в зависимости от напряжения питания инвертора, достоверность которого подтверждается приведенными осциллограммами, снятыми с реального устройства. Разработанный метод можно доработать и использовать и при одновременном изменении нагрузки в широком диапазоне от 10% до 100%.

**Литература**

1. Erickson R., Maksimovic D. Fundamentals of power electronics. – Norwell: Kluwer Academic, 2001. – 885 p.
2. Мелешин В.И., Овчинников Д.А. Управление транзисторными преобразователями электроэнергии. – М.: Техносфера, 2011. – 576 с.

3. Слита О.В., Никифоров В.О., Ушаков А.В. Управление в условиях неопределенности: адаптивные и неадаптивные алгоритмы. – Saarbrucken: LAP LAMBERT Academic Publishing, 2012. – 283 с.
4. Akunov T.A., Alexandrova S.A., Slita O.V., Sudarchikov S.A., Ushakov A.V. The problem of qualitative research of the Khariton robust stability of continuous systems // International scientific and technical journal «Problems of Control and Informatics». – 2016. – № 4. – P. 100–108.
5. Ibrahim O., Nor Z.Y., Nordin S., Khalid Y.A. Development of Observer State Output Feedback for Phase-Shifted Full Bridge DC-DC Converter Control // IEEE Open Access Journal. – 2017. – V. 5. – P. 18143–18154.
6. Alexandrova S., Baev A., Goncharenko M., Nikolaev N., Slita O. Practical Implementation of High Power and Efficiency Dc-dc Full-Bridge PWM Boost Converter // Proceedings of the International Conf. on Information and Digital Technologies. – 2017. – P. 29–35.
7. Aidan O'Dwyer Handbook of PI and PID controller tuning rules. – 3nd Edition. – London: Imperial College Press, 2009. – 608 p.

**Бантус Ольга Дмитриевна**
Год рождения: 1994
Университет ИТМО, факультет систем управления и робототехники,
кафедра систем управления и информатики,
студент группы № Р4240
Направление подготовки: 27.04.04 – Управление в технических системах
e-mail: bantusolga@gmail.com

**УДК 629.3**

# АДАПТИВНЫЙ КРУИЗ-КОНТРОЛЬ, ВОЗМОЖНОСТИ, ОСОБЕННОСТИ ВЗАИМОДЕЙСТВИЯ С ДРУГИМИ СИСТЕМАМИ АВТОМОБИЛЯ

**Бантус О.Д.**
**Научный руководитель – к.т.н., доцент Быстров С.В.**

Работа выполнена в рамках темы НИР № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность».

В работе описана работа системы адаптивного круиз-контроля, проведен сравнительный анализ существующих систем. Выявлены их возможности и недостатки, а также приведено исследование взаимодействия системы адаптивного круиз-контроля с другими автоматизированными системами автомобиля.
**Ключевые слова:** адаптивный круиз-контроль, управление, датчик расстояния, датчик скорости, информация, автомобиль.

В современном мире все большее внимание занимает замена труда человека автоматизированными системами управления. Одна из таких систем еще не получила широкого распространения как в России, так и за рубежом, так как является очень сложной и дорогостоящей. Это система адаптивного круиз-контроля.

Круиз-контроль (КК) – это система помощи водителю, которая управляет продольной динамикой движущейся машины. Путем модуляции сигнала дроссельной заслонки автомобиля он пытается поддерживать запрошенную пользователем скорость. Адаптивный круиз-контроль (АКК) расширяет эту систему, определяя присутствие ведущего транспортного средства и регулируя скорость вашего транспортного средства соответственно. Большинство разработанных систем АКК предназначены только для малого диапазона скоростей и часто имеют минимальную скорость около 30 км/ч.

Системы Stop & Go были разработаны для дальнейшего расширения диапазона АКК, чтобы иметь возможность обрабатывать эти более медленные скорости и стиль вождения, который идет с ним. В разработке Йошинори Ямамура [1] системы Stop & Go обсуждаются некоторые проблемы, возникающие в результате малоскоростного движения, включая меньшие промежуточные интервалы и более частые изменения скорости.

Адаптивный круиз-контроль и другие системы помощи водителям были активной областью исследований в течение ряда лет и, как результат, тема довольно разнообразна. Однако, несмотря на их различия, большинство систем АКК имеют, по меньшей мере, две вещи. Во-первых, любая реализация АКК требует метода получения информации об окружающей среде. Информация необходима как для принимающего транспортного средства (скорость, ускорение и т.д.), а также информация о наличии и поведении лидера транспортного средства. Информация о состоянии транспортных средств может быть получена с использованием датчиков, которые уже являются частью транспортного средства. Примером этого является датчик скорости колеса, который предоставляет информацию водителю об их скорости через спидометр.

Информация о непрерывном состоянии ведущего транспортного средства сложнее и требует дополнительного оборудования. Наиболее распространенный метод получения этой информации заключается в установке радиолокационных датчиков на переднюю часть автомобиля. В эту категорию входят микроволновые и допплеровские радары.

В рамках процесса разработки [2] авторы проводят сравнение трех из этих типов датчиков. Доплеровский радар: была обнаружена хорошая работа на скоростных шоссе со своим диапазоном дальности 100 м. Он также имеет возможность предоставлять информацию о диапазоне, дальности и азимуте для нескольких целей. Азимут может быть полезен при определении того, будет ли какое-либо из ведущих транспортных средств находится в процессе изменения полос движения. Однако доплеровский радар не способен обнаруживать транспортные средства с нулевой относительной скоростью. Микроволновый радар, работающий в миллиметровом диапазоне волн, оказался полезным только в ситуациях Stop & Go, поскольку он имел дальность всего 40 м. У лидаров был недостаток, что его выход предоставляется в виде значений расстояния и интенсивности для плоскости просмотра. В результате данные должны были пройти обработку до того, как система могла понимать поведение ведущего транспортного средства.

Другие системы АКК [3] дополняют информацию от их радиолокационного датчика, предполагая, что ведущий автомобиль будет передавать информацию о скорости и ускорении.

Второй аспект, который должны включать все системы АКК – это способность получать и обрабатывать информацию, предоставляемую датчиками, и использовать ее для реализации какой-либо формы контроля.

Хотя методы, используемые для реализации этого элемента управления, могут значительно варьироваться от одной системы к другой, любая система АКК должна быть в состоянии безопасно регулировать свою скорость в присутствии лидера и поддерживать заданное значение скорости в отсутствие впереди движущейся машины. С этой целью системе АКК предоставляется доступ к дросселю транспортного средства и тормозам, каждый из них должны использоваться по мере необходимости.

Основная цель системы адаптивного круиз-контроля – поддерживать постоянную скорость, замедлять движение транспортного средства или ускорять его. В случае, когда перед автомобилем нет автомобиля, система поддерживает скорость, установленную водителем. Если автомобиль перестроен или заторможен, система ускорится до установленной ранее скорости.

Для лучшей работы адаптивного круиз-контроля можно дополнительно установить навигационную систему GPS, систему экстренного торможения и другие вспомогательные системы. Фактически, АКК является основной системой автономного вождения.

Если говорить о стоимости адаптивного круиз-контроля, то многое будет зависеть от марки и модели автомобиля. В качестве примера для бренда BMW стоимость АКК будет стоить около 130–150 тысяч руб. (исключая проводку и монитор в салоне). Использованный комплект, в среднем, будет стоить 1200 евро, но уже с полным набором, но также нет гарантий, что этот вариант будет на 100% работать как оригинальный комплект. Стоимость самого датчика небольшая, в среднем около 2000 руб., а самой дорогой частью системы является блок управления.

Рассмотрим взаимодействие элементов системы АКК с другими системами автомобиля, представленное на рисунке.

Система состоит из рулевого колеса (1), блока управления рулевого колеса (2), шины передачи информации CAN-комфорт (3), приборной панели (4), блока управления двигателем (5), шины передачи информации CAN-привод (6), блока управления системы ABS (7), датчика системы АКК (8), датчика поддержки тормозного усилия (9), блока управления АКП (10).

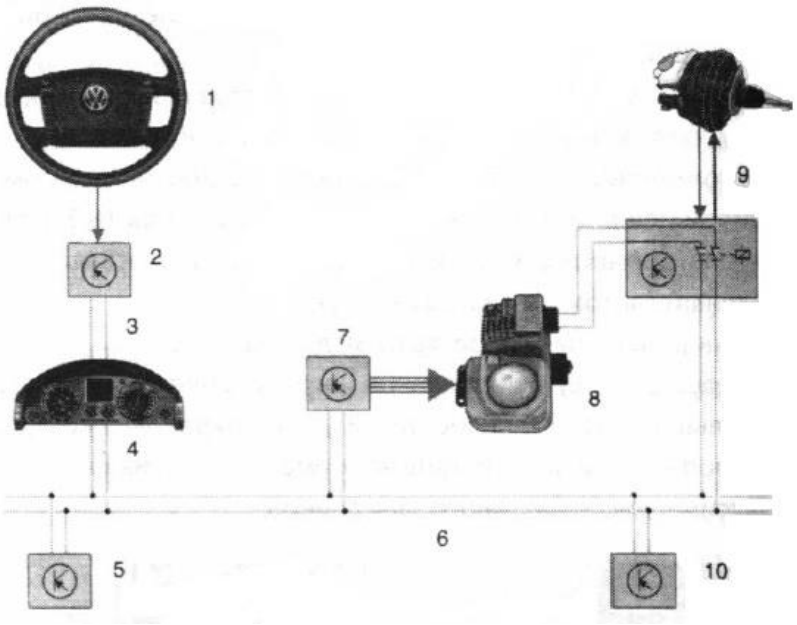



Рисунок. Взаимодействие элементов системы

Датчик системы АКК (8) является основным компонентом адаптивного круиз-контроля и имеет передающее и принимающее устройство измерения расстояния, блок электронной обработки информации и микропроцессор для определения состояния дороги и распознавания объектов, управления расстоянием и скоростью и для управления различными связанными системами. В адаптивном датчике круиз-контроля также встроены самодиагностика, функции контроля и ошибки памяти. Связь с соответствующими системами осуществляется через шину данных CAN.

Управление осуществляется с помощью рулевого колеса (1). Минимальное расстояние, которое может быть выбрано, всегда больше минимального расстояния, разрешенного в соответствии с законом. Поскольку расстояние зависит от скорости, определяется только время, необходимое для перемещения транспортного средства на расстояние до впереди идущего транспортного средства.

Используя различные индикаторы на приборной панели (4), водитель узнает, включена ли система адаптивного круиз-контроля, фиксируется ли автомобиль заранее, какая скорость и какое расстояние задано, и должен ли водитель активно тормозить.

Блок управления двигателем (5) передает информацию о текущем крутящем моменте двигателя и положении педали газа и должен выполнять данные для уменьшения или увеличения крутящего момента двигателя. Условием этого является электронное регулирование мощности двигателя (электронный газ).

Блок управления системы ABS или системы контроля стабильности информирует вас о скорости автомобиля, ускорении автомобиля, скорости вращения отдельных колес и контрольных действиях. Необходимое торможение для уменьшения скорости с целью поддержания расстояния может осуществляться самой системой управления стабильностью или с помощью электронного усилителя тормозного усилителя (9).

Система (10) управления передачей передает информацию о текущей передаче и положении рычага коробки. В положениях рычага селектора N, R или P круиз-контроль не может быть включен или, если он уже включен, выключен. Адаптивный круиз-контроль также возможен в сочетании с механической коробкой передач. В этом случае требуется переключатель сцепления.

В рамках исследования был проведен анализ существующих систем адаптивного круиз-контроля, рассмотрена их работа и взаимодействие с другими системами автомобиля. В

дальнейшем будет проведен анализ возмущающих воздействий, действующих на систему АКК, разработаны алгоритмы управления и реагирования системы на эти воздействия.

**Литература**

1. Yamamura Y., Tabe M., Kanehira M. and Murakami T. Development of an Adaptive Cruise Control System with Stop-and-Go Capability // SAE. – 2001. – P. 38–45.
2. Girard A.R., Spry S., Hendrick K. Intelligent cruise control applications: Real-time embedded hybrid control software // IEEE Robotics & Automation Magazine. – 2005. – V. 12(1). – P. 22–28.
3. Breimer B. Design of an adaptive cruise control model for hybrid systems fault diagnosi [Электронный ресурс]. – Режим доступа: https://macsphere.mcmaster.ca/bitstream/11375/12839/1/fulltext.pdf, своб.

**Головин Артем Андреевич**
Год рождения: 1994
Университет ИТМО, факультет систем управления и робототехники,
кафедра систем управления и информатики,
студент группы № Р4235
Направление подготовки: 15.04.06 – Мехатроника и робототехника
e-mail: asd-1234@yandex.ru

**УДК 681.5.04**

# СОГЛАСОВАНИЕ ХАРАКТЕРИСТИК СИЛОВОГО УСИЛИТЕЛЯ И ПЬЕЗОАКТЮАТОРА ДЛЯ МЕХАТРОННОГО МОДУЛЯ

**Головин А.А.**
**Научный руководитель – к.т.н., доцент Бойков В.И.**

Работа выполнена в рамках темы НИР № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность».

В данной работе рассмотрен способ настройки параметров цепи питания пьезоактюатора на максимальное быстродействие. Проведено исследование энергетических процессов и влияние параметров на динамику работы. Обозначена рекомендация использования индуктивного компенсатора в цепи с усилителем мощности. Предложен способ настройки на технический оптимум, соответствующий минимальному времени переходного процесса, с помощью нормированного представления Вышнеградского.
**Ключевые слова:** максимальное быстродействие, настройка параметров, диаграмма Вышнеградского, пьезоактюатор, технический оптимум, индуктивный компенсатор.

Исполнительные устройства, реализованные на принципах пьезоэффекта, можно с уверенностью отнести к особому классу быстродействующих объектов. Они отлично подходят для эффективного решения задач точного скоростного позиционирования.

Это идеальный инструмент в решении задач медицины, в составе микроскопов, микромоторов для хирургии и генных манипуляторов. Они хорошо зарекомендовали в автомобильной промышленности, оптике, точной механике, микролитографии. Повышение их быстродействия позволит увеличить производительность устройств, качество работы и эффективность применения.

Основная проблема при создании устройств для микроперемещений – возбуждение высокочастотных колебаний, которые сам пьезоактюатор подавить не в состоянии. В качестве аналога такого поведения можно представить движение массы на пружине с определенной упругостью, величина которой в мире малых перемещений оказывается достаточно существенной. При попытке синтеза скоростного управления возникают проблемы из-за колебательных свойств системы.

Настройка параметров цепи подключения пьезоактюатора и высоковольтного усилителя мощности на максимальное быстродействие является важным стартовым этапом перед разработкой и применением оптимальных, релейных алгоритмов в задаче повышения быстродействия управления.

В ходе изучения способов управления пьезоактюатором в работе [1] был сделан вывод, что наилучшим и простым способов является управление по напряжению. Рассмотрим схему моделирования модели пьезоактюатора с усилителем мощности (рис. 1).

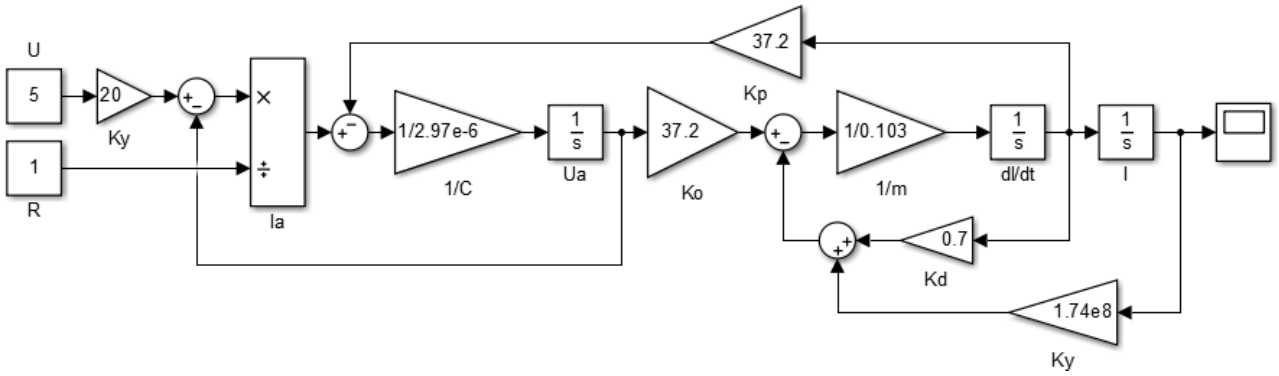
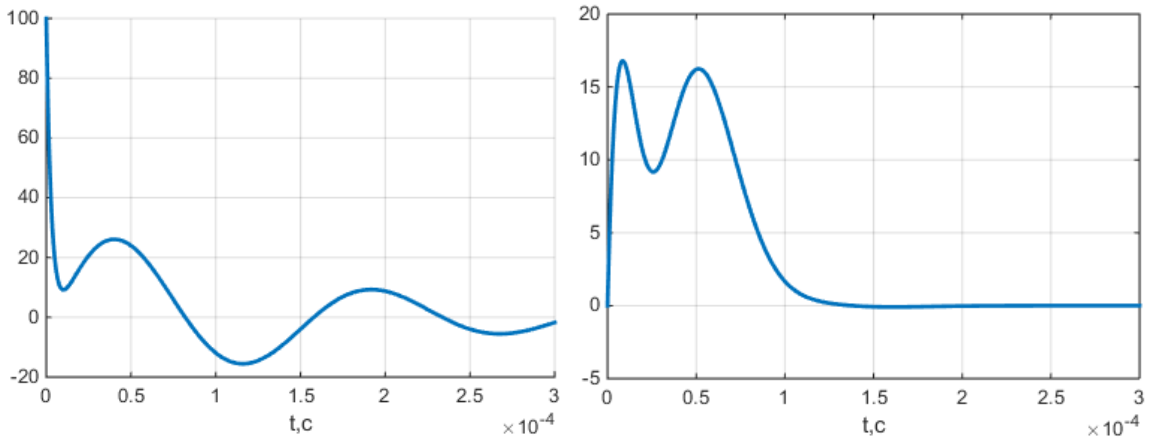



Рис. 1. Схема моделирования пьезоактюатора с усилителем мощности

Передаточная функция такого объекта не имеет нулей и определяется характеристическим полиномом третьей степени в знаменателе, который имеет два комплексно-сопряженных корня и один вещественный. Внутреннее сопротивление усилителя напрямую влияет на характер переходного процесса, с его уменьшением в системе возрастает колебательность.

Если выбран мощный усилитель, то у пьезоактюатора появится резонансный выброс, с другой стороны, если усилитель слабый, то достаточное движение не возбуждается, управление простое, переходной процесс плавный. Отсюда возникает задача в определении оптимального значения, при котором процесс будет близок к апериодическому, сходиться за наименьшее время, иметь малое перерегулирование.

Исследование энергетических показателей процесса привело к выводу, что большая колебательность связана с пиковыми значениями тока и электрической мощности в начале переходного процесса. Одним из решений может быть введение в цепь питания пьезоактюатора индуктивного компенсатора [2, 3], который сведет скачки тока в момент короткого замыкания к минимальным значениям. На рис. 2 приведены графики тока через пьезоактюатор с компенсатором и без него. Индуктивность в цепь вводится для нивелирования емкостного характера нагрузки. Такой способ позволит увеличить быстродействие за счет демпфирования колебания.




а б

Рис. 2. Исследование энергетики: без компенсатора (а); с компенсатором (б)

Передаточная функция пьезоактюатора с индуктивным компенсатором имеет четвертый порядок и определяется двумя парами комплексно-сопряженных корней. Схема моделирования такого объекта в MATLAB представлена на рис. 3. С точки зрения настройки эта является более гибкой, необходимо подобрать соотношение двух параметров для достижения минимального времени регулирования.

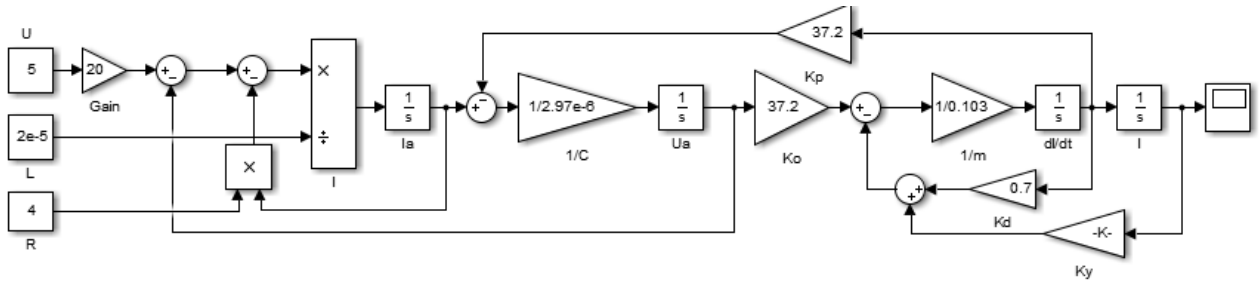



Рис. 3. Схема моделирования пьезоактюатора с усилителем мощности и индуктивным компенсатором в цепи питания

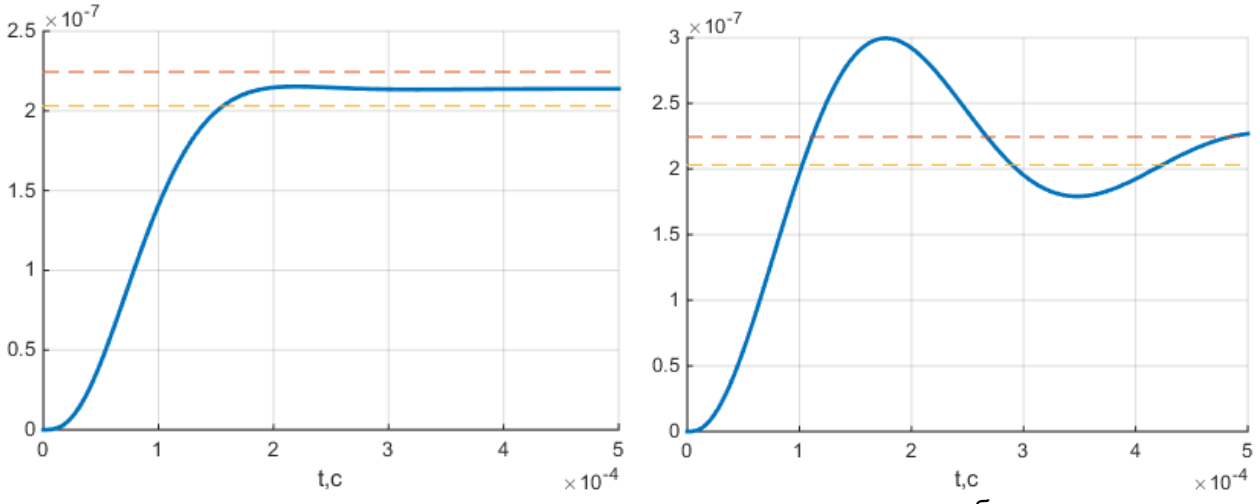
Для согласования параметров цепи и достижения желаемых показателей качества системы можно использовать широко известную диаграмму Вышнеградского [4]. Суть заключается в том, что используя всего два коэффициента характеристического уравнения можно задать необходимый вид переходного процесса. В таблице приведены значения коэффициентов для системы третьего и четвертого порядков, настроенных на некоторый технический оптимум, который соответствует минимальному показателю колебательности системы с перерегулированием не более 5%.

Таблица. Коэффициенты полинома, соответствующие наименьшему времени регулирования

| Порядок | Коэффициенты уравнения | | | | |
|---|---|---|---|---|---|
| 3 | 1 | 2,05 | 2,39 | 1 | |
| 4 | 1 | 2,6 | 3,8 | 2,8 | 1 |

Однако из-за того, что один регулируемый параметра влияет на оба безразмерных коэффициента результат не идеален, но максимально приближен и позволяет получить приемлемый переходной процесс. Для вычисления можно использовать итеративный метод наименьших квадратов либо встроенные поисковые функции MATLAB.

На рис. 4, приведены графики систем с индуктивным компенсатором и без него, настроенные на максимальное быстродействие.




а б

Рис. 4. Переходной процесс выхода: с компенсатором (а); без компенсатора (б)

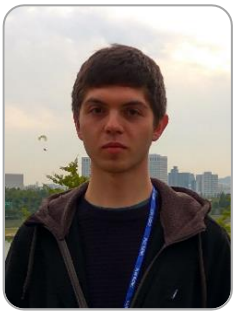
Стоит отметить, что изначально перед настройкой системы можно задаться некоторым желаемым временем переходного процесса. Обозначить эту связь предлагается через постоянные времени. С одной стороны – это механическая постоянная, обусловленная инерционностью общей массы керамики и полезной нагрузки, а с другой – электрическая, которая определяется образуемой RC-цепочкой. Минимумом в данной ситуации предполагается принять механическую постоянную и задать желаемое время переходного

процесса, как ее трехкратное значение. Далее требуется задать расположение корней, следуя следующему правилу: меньшее время регулирования можно получить при выборе некратного расположения комплексных корней; корни должны лежать на одинаковом расстоянии от мнимой оси.

Используя подход, заключающийся в нахождении оптимального значения параметров цепи питания пьезоактюатора, представляется возможность достижения требуемого качества процесса. Первоочередный расчет индуктивности и сопротивления позволяет грамотно выбрать нужный высоковольтный усилитель мощности, добившись согласования по энергетическим и качественным показателям. Включение в схему индуктивного компенсатора поможет убрать нежелательные скачки тока, и как следствие, позволит использовать такую схему подключения пьезоактюатора в режиме ШИМ управления, а также применить к объекту оптимальные алгоритмы.

**Литература**

1. Головин А.А. Повышение быстродействия силовых пьезоактюаторов // Сборник трудов VI Конгресса молодых ученых. – 2017. – С. 56–59.
2. Tan T., Yana Z. Optimization study on inductive-resistive circuit for broadband piezoelectric energy harvesters // AIP Advances. – 2017. – V. 7. – P. 7–18.
3. Fleming A.J., Behrens S., Reza S.O. Moheimani Reducing the inductance requirements of piezoelectric shunt damping systems // Smart Materials and Structures. – 2003. – V. 12. – P. 57–64.
4. Красовский А.А., Поспелов Г.С. Основы автоматики и технической кибернетики. – М.-Л.: Госэнергоиздат, 1962. – 601 с.
5. Irschik H., Belyaev A., Krommer M. Dynamics and Control of Advanced Structures and Machines. – Springer International Publishing, 2017. – 234 p.



**Дема Николай Юрьевич**
Год рождения: 1995
Университет ИТМО, факультет систем управления и робототехники,
кафедра систем управления и информатики,
студент группы № Р4135
Направление подготовки: 15.04.06 – Мехатроника и робототехника
e-mail: Nicko_Dema@protonmail.com

**Колюбин Сергей Алексеевич**
Год рождения: 1986
Университет ИТМО, факультет систем управления и робототехники,
кафедра систем управления и информатики, к.т.н., доцент
e-mail: s.kolyubin@corp.ifmo.ru

**Овчаров Алексей Олегович**
Год рождения: 1996
Университет ИТМО, факультет систем управления и робототехники,
кафедра систем управления и информатики,
студент группы № Р3440
Направление подготовки: 27.03.04 – Управление в технических системах
e-mail: a.ovcharov@corp.ifmo.ru

**УДК 681.5**

# ИССЛЕДОВАНИЕ МЕТОДОВ РЕШЕНИЯ ОБРАТНОЙ ЗАДАЧИ КИНЕМАТИКИ ДЛЯ МАНИПУЛЯТОРОВ ИЗБЫТОЧНОЙ КИНЕМАТИКИ

**Дема Н.Ю., Колюбин С.А., Овчаров А.О.**
**Научный руководитель – к.т.н., доцент Колюбин С.А.**

Работа выполнена в рамках темы НИР № 370101 «Разработка адаптивных методов очувствления, планирования и управления движением биомехатронных систем».

В работе представлен обзор методов решения обратной задачи кинематики для последовательных манипуляторов избыточной кинематики.
**Ключевые слова:** обратная задача кинематики, избыточность, коллаборативные роботы.

Основной проблемой обеспечения безопасности при разделении рабочего пространства и организации совместной деятельности людей и роботов является сложность, а порой и невозможность предсказания поведения человека: для кооперации и совместной деятельности люди часто прибегают к невербальным средствам общения – естественным для человека, но тяжело формализуемым и интерпретируемым для робототехнических систем.

Постоянный контроль за движениями человека, посредством внешних датчиков (например, оптических или глубинных камер) позволяет успешно избегать столкновений робота и человека в общем рабочем окружении, но постоянное избегание роботом контактов с человеком исключает возможности к той кооперации, которая возникает между людьми.

С другой стороны, поведение робота также может быть непредсказуемо для человека. Существует огромное множество методов и алгоритмов организации движения сложных

робототехнических систем, и их возможная неестественность может сбивать человека с толку, отвлекать от основной деятельности, что, в свою очередь, может мешать роботу, выполнять свою часть работ.

Наиболее перспективными коллаборативными типами роботов являются манипуляторы последовательной избыточной кинематики. Движение таких роботов во много определяется способом решения обратной задачи кинематики (ОЗК). Ввиду наличия сингулярных состояний в конфигурационном пространстве робота задача нетривиальна и является предметом исследований множества исследователей по всему миру.

Целью проведения исследований в данной работе являлось определение подходов к решению ОЗК, способствующих естественности движений избыточного манипулятора при траекторном управлении.

Использование якобиана системы для линеаризации ОЗК является наиболее распространенным подходом к ее решению. Ввиду вырождения якобиана для сингулярных конфигураций используются различные пути его псевдообращения. На рис. 1 показана такая операция, где $\theta_i$ – $i$-ая обощенная координата, $\mathbf{s}_i$ – положение рабочего органа и $t$ – цель в операционном пространстве.

К наиболее распространенным методам данного класса относят: метод Мора-Пенроуза, метод транспонированного якобиана, метод сингулярного разложения матриц, метод затухающих наименьших квадратов и их различные вариации [1]. Некоторые из этих методов подвержены проблеме дрожания в сингулярных конфигурациях, а также в случае недостижимости целевой конфигурации. Альтернативный метод, предложенный в [2] лишен недостатков, связанных с сингулярными конфигурациями, в нем обратная задача кинематики рассматривается в формализме теории управления.

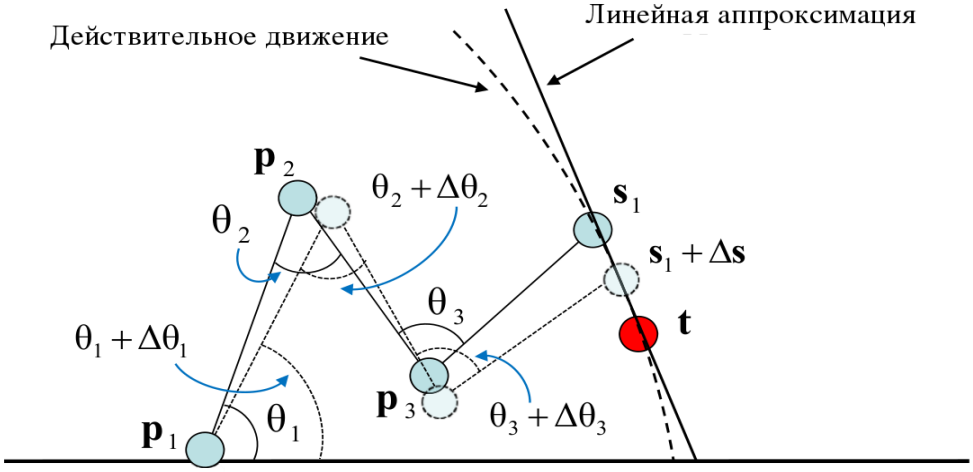



Рис. 1. Линейная аппроксимация движения робота при использовании методов, основанных на псевдообращении якобиана

Также известны так называемые методы Ньютона, основу которых составляет разложение в ряд Тейлора второго порядка следующей целевой функции:

$$f(x+\sigma) = f(x) + [grad(f(x))]^T \sigma + \frac{1}{2}\sigma^T \mathbf{H}_f(x)\sigma,$$

где $\mathbf{H}$ – матрица Гессе. Такой подход позволяет получать гладкие траектории движения, включать ограничения для движения сочленений, и не подвержен проблеме дрожания [3]. Методы Ньютона не получили широкого распространения ввиду сложности их реализации и значительных требований к вычислительным ресурсам.

Большую популярность в робототехническом сообществе приобрели методы, основанные на быстрорастущих деревьях (RRT). Такие методы обеспечивают высокую скорость исследования пространства конфигураций и неплохо зарекомендовали себя при решении задач большой размерности [4]. Более того, при разработке алгоритма исследования

можно учесть кинематические особенности, и решать обратную задачу кинематики, как по положению, так и для скоростей. Однако такие методы, как и другие, основанные на вероятностных дорожных картах, в общем случае обладают плохой сходимостью, когда области, обеспечивающие связность отдельных компонент пространства конфигураций, имеют малый размер.

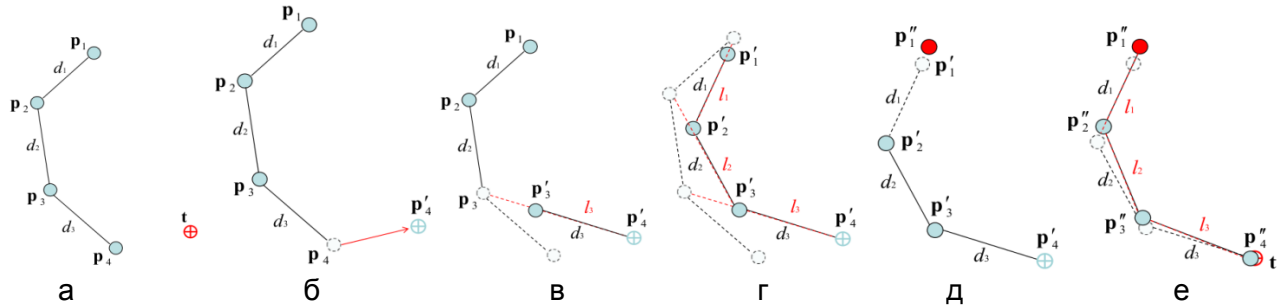



Рис. 2. Пример решения ОЗК используя FABRIK

Также известны итеративные эвристические алгоритмы решения ОЗК. Из них наиболее популярными являются CCD и FABRIK [5]. На рис. 2 представлен пример одной итерации FABRIK, где $\mathbf{p}_i$ – координаты $i$-го сочленения в операционном пространстве. Данные алгоритмы характеризуются простотой реализации, не требовательностью к вычислительным ресурсам. Основным недостатком, ограничивающим их применение в задачах робототехники, является неучет скоростей и ускорений в сочленениях.

Таким образом, решение обратной задачи кинематики является на сегодняшний день актуальной проблемой. Авторы ставят перед собой задачу более детального изучения итеративных эвристических алгоритмов с целью их адаптации для задач робототехники.

**Литература**

1. Buss S.R. Introduction to inverse kinematics with jacobian transpose, pseudoinverse and damped least squares methods // IEEE JRA. – 2004. – V. 17. – № 1-19. – P. 16.
2. Alexandre N. Pechev. Inverse kinematics without matrix invertion // IEEE International Conference on Robotics and Automation. – 2008. – P. 2005–2012.
3. Zhao J. and Badler N.I. Inverse kinematics positioning using nonlinear programming for highly articulated figures // ACM Transactions on Graphics (TOG). – 1994. – V. 13(4). – P. 313–336.
4. LaValle S.M. Planning Algorithms. – New York: Cambridge University Press, 2006. – 842 p.
5. Aristidou A. and Lasenby J. FABRIK: a fast, iterative solver for the inverse kinematics problem // Graphical Models. – 2010. – V. 73(5). – P. 243–260.

**Зенкин Артемий Михайлович**
Год рождения: 1997
Университет ИТМО, факультет систем управления и робототехники,
кафедра систем управления и информатики,
студент группы № Р3335
Направление подготовки: 15.03.06 – Мехатроника и робототехника
e-mail: zenkinartem1997@gmail.com

**Осинкин Егор Александрович**
Год рождения: 1997
Университет ИТМО, факультет систем управления и робототехники,
кафедра систем управления и информатики,
студент группы № Р3335
Направление подготовки: 15.03.06 – Мехатроника и робототехника
e-mail: egoros97@yandex.ru

**Баев Пётр Альбертович**
Год рождения: 1997
Университет ИТМО, факультет систем управления и робототехники,
кафедра систем управления и информатики,
студент группы № Р3335
Направление подготовки: 15.03.06 – Мехатроника и робототехника
e-mail: perry322lol@gmail.com

**УДК 623.746–519**

## ДВИЖЕНИЕ КВАДРОКОПТЕРА PARROT ARDRONE 2.0 ПО ЗАДАННЫМ КООРДИНАТАМ

**Зенкин А.М., Осинкин Е.А., Баев П.А.**
**Научный руководитель – к.т.н. Капитонов А.А.**

В работе рассмотрен один из подходов к решению задачи движения квадрокоптера Parrot ARDrone 2.0. по заданным координатам в закрытых помещениях или местах, в которых по какой-либо причине недоступна система GPS. Данный метод опирается на алгоритм визуального позиционирования квадрокоптера, основанный на Parallel Tracking and Mapping, который был предложен Якобом Энгелем, Юргеном Штурмом и Даниэлем Кремерсом Технического университета Мюнхена, Германия.
**Ключевые слова:** навигация квадрокоптера, движение по заданным координатам, позиционирование ARDrone 2.0, PTAM, визуальная навигация.

В последнее время наблюдается резкий рост интереса к беспилотным летательным аппаратам (БПЛА), в особенности к квадрокоптерам, в связи с относительной простотой управления и достаточно большой доступностью. Как следствие, данные аппараты стали все чаще использоваться не только для съемок фото- и видеоматериалов, но и для транспортировки и доставки легких грузов. Особую сложность составляет полет по траектории в закрытых помещениях или места, в которых Global Positioning System (GPS) по какой-либо причине не доступна. Основные устройства ориентирования БПЛА, которые сейчас применяются – это устройства, которые получают сигнал от навигационных систем: ГЛОНАСС (Глобальная навигационная спутниковая система) и GPS. Данный метод не позволяет получить достаточно точные данные о положение БПЛА и используется в тех случаях, когда не нужна высокая точность, например, полет над заповедниками для

отслеживания браконьеров. Второй способ ориентирования квадрокоптера в пространстве – это использование инерциальной системы (акселерометр, гироскоп, барометр, магнитометр и дальномер). Данный способ также не позволяет достичь точной навигации БПЛА в пространстве. В данной работе предлагается рассмотреть метод визуальной навигации квадрокоптера, который позволяет достаточно точно позиционировать недорогие квадрокоптеры в пространстве.

Навигационная система состоит из трех основных компонентов. Монокулярный SLAM (Simultaneous Localization and Mapping), основанный на Parallel Tracking and Mapping (PTAM) [1], для визуального отслеживания квадрокоптера [2]. Для того чтобы объединить все данные, которые поступают с квадрокоптера, используется Extended Kalman Filter (EKF), который включает в себя полную модель динамики полета квадрокоптера и реакцию на команды управления [3]. Для достижения желаемой цели квадрокоптером используется пропорционально-интегрально-дифференцирующий регулятор (ПИД-регулятор). Для каждой степени свободы используется свой регулятор, коэффициенты которого были подобраны экспериментальным путем. В работе данной системы наблюдаются задержки до 250 мс между захватом кадра, поступающего с камеры квадрокоптера, и моментом, когда команда управления, которая была вызвана этим кадром, достигнет дрона. Точность значений зависит от качеств беспроводного соединения и определяется комбинацией регулярных Internet Control Message Protocol (ICMP) запросов, посылаемых на квадрокоптер [4]. Для решения этой проблемы используются временные метки со станции, в нашем случае – ноутбука.

В настоящей работе были рассмотрены два алгоритма полета по заданным координатам:

1. использование аппарата функции Ляпунова;
2. использование регулятора скорости по каждой из оси.

Рассмотрим первый алгоритм. Эскиз квадрокоптера, который движется к своей цели в свободном пространстве, приведен на рис. 1.

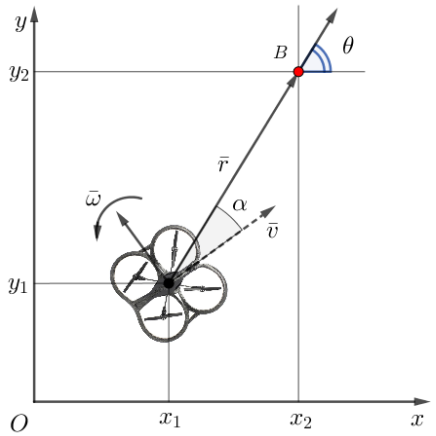



Рис. 1. Эскиз квадрокоптера: *r* – расстояние до целевой точки; θ – азимут, угол между осью *Ox* и направлением на цель; α – курсовой угол, разность между курсом и азимутом; *υ* – линейная скорость робота

Математическая модель (1), описывающая движение квадрокоптера в заданную точку, имеет следующий вид:

$$\begin{cases} \dot{r} = -\upsilon \cos a, \\ \dot{a} = -\omega + \upsilon \dfrac{\sin a}{r}, \\ \dot{\theta} = -\upsilon \dfrac{\sin a}{r} \end{cases} \quad (1)$$

Таким образом, квадрокоптером можно управлять путем изменения значений линейной и угловой скорости $(\upsilon, \omega)$, следовательно, необходимо найти такие значения этих переменных, чтобы выполнялись следующие условия: $(r \to 0, a \to 0)$. Для решения данной задачи воспользуемся аппаратом функции Ляпунова [5]. В данном случае – это квадратичная функция (2), которая включает в себя курсовой угол и расстояние до цели:

$$\upsilon(r,\alpha) = \frac{1}{2}r^2 + \frac{1}{2}\alpha^2. \quad (2)$$

Для того чтобы курсовой угол и расстояние до цели не возрастали, производная по времени должна быть неположительна. Производная (3) от нашей квадратичной функции имеет следующий вид:

$$\dot{\upsilon}(r,\alpha) = \dot{r}r + \dot{\alpha}\alpha. \quad (3)$$

После того, как мы выразим производную через систему уравнений (1), получим следующее уравнение (4):

$$\dot{\upsilon}(r,\alpha) = -r\upsilon\cos\alpha + \alpha(-\omega + \upsilon\frac{\sin\alpha}{r}). \quad (4)$$

Данная производная будет отрицательно определена, если мы выберем в качестве линейной и угловой скорости (5) следующие значения:

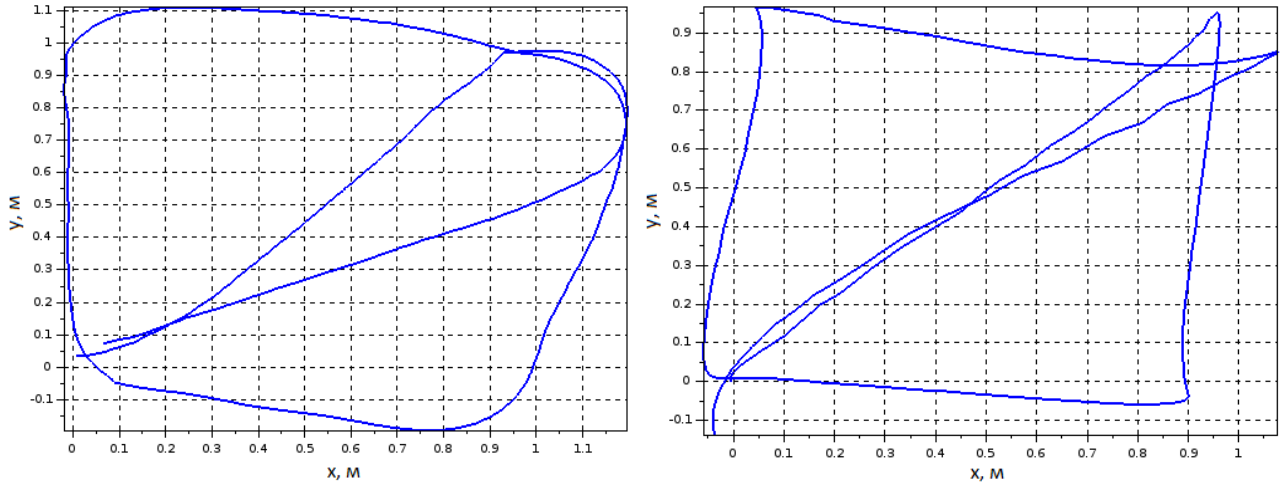
$$\begin{cases} \upsilon = \upsilon_{\max}\tanh r\cos\alpha, \\ \omega = k_\omega\alpha + \upsilon_{\max}\dfrac{\tanh r}{r}\sin\alpha, k_\omega > 0 \end{cases}. \quad (5)$$

Все это позволит квадрокоптеру достичь своей цели.

Рассмотрим второй алгоритм. Опишем математическую (6) модель, описывающую навигацию квадрокоптера к цели:

$$\begin{cases} \dot{x} = \upsilon_x, \\ \dot{y} = \upsilon_y, \\ \dot{\theta} = \omega_{yaw} \end{cases}. \quad (6)$$

На рис. 2 приведены результаты моделирования полета квадрокоптера ARDrone 2.0 по квадрату со стороной 1 м в симуляторе Gazebo.




а б

Рис. 2. Траектория движения: первый алгоритм (а); второй алгоритм (б)

В алгоритме (рис. 2, а) квадрокоптер достаточно точно достигал заданные точки, это можно проследить на рисунке. Практически все точки: (0;1), (1;1), (1;0), (0;0) были достигнуты, хотя в данном регуляторе используется только пропорциональная

составляющая. Большим недостатком является большое время выполнения, которое составило 36,34 с, а также затрат места на разворот квадрокоптера. В алгоритме (рис. 2, б) были достаточно большие ошибки по достижению заданных точек, это можно проследить на приведенном выше рисунке. Тут также использовалась только пропорциональная составляющая регулятора. Плюсом данного метода является скорость выполнения программы, которая составила всего 13,2 с, что практически в три раза меньше, чем в алгоритме (рис. 2, а).

**Литература**

1. Engel J., Sturm J., Cremers D. Scale-aware navigation of a low-cost quadrocopter with a monocular camera // Robotics and Autonomous Systems. – 2014. – V. 62. – № 11. – P. 1646–1656.
2. Klein G. and Murray D. Parallel tracking and mapping for small AR workspaces // Proc. IEEE Intl. Symposium on Mixed and Augmented Reality (ISMAR). – 2007. – P. 225–234.
3. Daniel L. Mälardalen University, School of Innovation, Design and Engineering, M.Sc. thesis in Extended Kalman Filtration for attitude and orbital determination of satellites. – 2015.
4. Engel J.J. Autonomous Camera-Based Navigation of a Quadrocopter [Электронный ресурс]. – Режим доступа: https://vision.in.tum.de/_media/spezial/bib/engel2011msc.pdf, своб.
5. Ferreira A., Pereira F.G., Vassallo R.F., Bastos Filho T.F., Sarcinelli Filho M. An approach to avoid obstacles in mobile robot navigation: the tangential escape // Sba: Controle & Automação Sociedade Brasileira de Automatica. – 2008. – V. 19(4). – P. 395–405.

**Низовцев Сергей Игоревич**
Год рождения: 1992
Университет ИТМО, факультет систем управления и робототехники, кафедра систем управления и информатики, аспирант
Направление подготовки: 09.06.01 – Информатика и вычислительная техника
e-mail: glenmetthews@gmail.com

**УДК 044.67**

# ЗАДАЧА МНОГОСЕНСОРНОЙ ИДЕНТИФИКАЦИИ ПАРАМЕТРОВ ВЫСОТНЫХ СООРУЖЕНИЙ

**Низовцев С.И.**
**Научный руководитель – к.т.н. Шаветов С.В.**

Работа выполнена в рамках темы НИР № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность».

В работе рассмотрена структура систем мультисенсорной идентификации параметров высотных строительных сооружений. На основе аналитического обзора предложена своя последовательность разработки системы мониторинга. Описаны первоначальные этапы установки аппаратного обеспечения, его местоположение относительно сооружения. Приведены результаты эксперимента, проведенного для сравнения теоретических и практических значений динамических параметров сооружения.
**Ключевые слова:** мониторинг, мультисенсорная система, динамические параметры, высотное сооружение, акселерометр, тензометр.

Высотные здания становятся отличительной особенностью современного крупного города. Увеличение числа и этажности зданий приводит к необходимости обеспечения безопасности как при строительстве, так и при дальнейшей эксплуатации. Учитывая сложность инженерного сооружения, требуется контролировать техническое состояние различных компонентов – инженерных сетей, грунтового массива, конструкций в целом и их отдельных элементов. Одними из важнейших этапов разработки системы мультисенсорной идентификации параметров сооружения является подбор оборудования, методик, разработка программного обеспечения. В общем случае задача идентификации параметров высотных строительных сооружений сводится к задаче мониторинга текущего состояния сооружения.

По результатам обзора существующих внедренных решений можно сделать заключение о недостаточной комплексности систем мониторинга, поскольку большинство из них строится на основе однотипных измерительных элементов (тензометры, акселерометры). Количество используемых датчиков также является недостаточным для анализа текущего состояния строительного сооружения. Количественное ограничение не позволяет оценивать состояние отдельных конструктивных элементов [1].

Выделив основные критерии оценки качества систем мониторинга была предложена своя последовательность разработки такой системы. Основными этапами разработки явились следующие шаги:

1. по результатам анализа существующих аналогов проводится разработка методики проведения идентификации параметров высотного строительного сооружения;
2. проверка работоспособности оборудования, чувствительных элементов, сетей передачи данных;
3. разработка алгоритма обработки получаемых данных;
4. тестирование системы, проверка поведения при различных сценариях;
5. внедрение на объект.

Структурная схема функционирования системы мониторинга представлена на рис. 1.

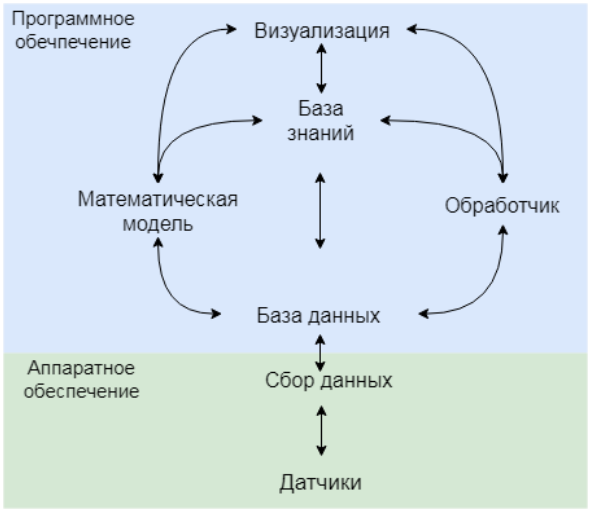



Рис. 1. Структурная схема системы мониторинга

Стоит уточнить, что все измерения и вычисления производились на примере строящегося высотного сооружения в городе Санкт-Петербург. Первым этапом любого строительства уникального объекта является проектирование сооружения и построение его математической модели с учетом всех внешних факторов, которые могут оказывать влияние на его состояние. На основе математической модели рассчитываются теоретические параметры здания, включающие предельные напряжения на отдельных элементах, поведение грунта основания, динамические характеристики (моды и предельные амплитуды колебаний, декременты затухания) [2].

По одобренному проекту начинается строительство, в процессе которого монтируются различные чувствительные элементы (датчики). На объекте: в сваях, грунте и фундаментной плите устанавливаются тензометры и датчики порового давления, по этажам – тензометры монтируются в колонны. На рис. 2 представлено графическое отображение результатов математического моделирования. Башни и небоскребы в своем роде типичные сооружения, хотя и являются уникальными. Такие здания включают в себя свайное поле, фундаментную плиту, ядро жесткости и периферические колонны, которые соединяются с ядром системой аутригеров для распределения нагрузки.

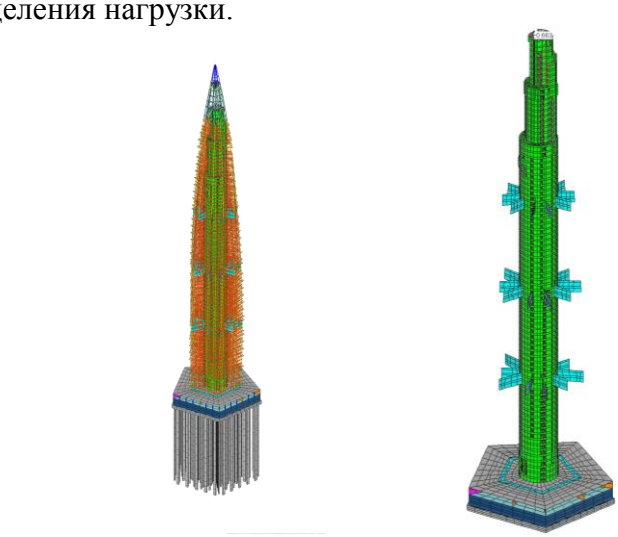


Рис. 2. Графическое отображение результатов математического моделирования

Для проверки теоретически рассчитанных значений параметров были проведены измерения частотного состава и амплитуд на строящемся объекте. На рис. 3 представлена таблица мод колебаний, полученных в результате математического моделирования.

Представлена амплитудно-частотная характеристика сигналов, полученных при эксперименте. Измерения проводились велосиметрами на уровне 78 этажа. Как видно, экспериментальных значения параметров практически полностью совпадают с теоретическими значениями. Погрешность возможна из-за различия в массах из-за неоконченного строительства. Этот эксперимент можно назвать частью мультисенсорной идентификации параметров высотного сооружения, так как были получены его динамические характеристики и сравнены с теоретическими, пусть и в ручном, не автоматическом режиме.

| Моды колебаний | Частота $f_i$, Гц | Период $T_i$, с | Круговая частота $\omega_i$, $с^{-1}$ |
|---|---|---|---|
| 1 | 0.122 | 8.178 | 0.768 |
| 2 | 0.126 | 7.959 | 0.789 |
| 3 | 0.444 | 2.254 | 2.787 |
| 4 | 0.488 | 2.048 | 3.067 |
| 5 | 0.509 | 1.964 | 3.198 |
| 6 | 0.781 | 1.281 | 4.904 |
| 7 | 0.801 | 1.249 | 5.03 |
| 8 | 1.048 | 0.954 | 6.583 |
| 9 | 1.118 | 0.894 | 7.023 |
| 10 | 1.159 | 0.862 | 7.281 |
| 11 | 1.293 | 0.773 | 8.121 |
| 12 | 1.529 | 0.654 | 9.601 |

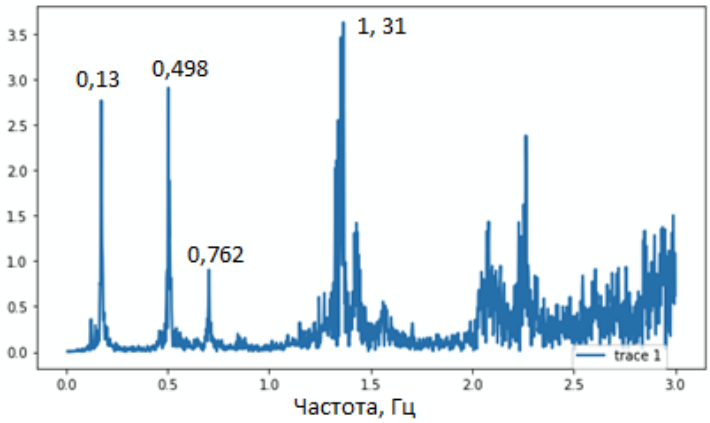



Рис. 3. Результаты эксперимента

Дальнейшая разработка системы идентификации параметров заключается в выводе алгоритма обработки данных, получаемых с измерительных элементов, для оценки текущего состоянии и прогнозирования состояния сооружения.

**Литература**

1. Kuckartza J., Collier P., Hutchinson G. The Design of an Integrated Structural Monitoring System for a High-Rise Building Based on Tiltmeters and GNSS [Электронный ресурс]. – Режим доступа: http://dma.lsgi.polyu.edu.hk/JISDM-Proceeding/Proceeding/Full%20paper/164.pdf, своб.
2. Kuckartza J., Collier P. A User-Centric Approach to the Design of Structural Health Monitoring Systems [Электронный ресурс]. – Режим доступа: https://www.fig.net/resources/proceedings/2011/2011_lsgi/session_1e/kuckartz_collier.pdf, своб.

**Осинкин Егор Александрович**
Год рождения: 1997
Университет ИТМО, факультет систем управления и робототехники,
кафедра систем управления и информатики,
студент группы № P3335
Направление подготовки: 15.03.06 – Мехатроника и робототехника
e-mail: egoros97@yandex.ru

**Баев Пётр Альбертович**
Год рождения: 1997
Университет ИТМО, факультет систем управления и робототехники,
кафедра систем управления и информатики,
студент группы № P3335
Направление подготовки: 15.03.06 – Мехатроника и робототехника
e-mail: perry322lol@gmail.com

**Зенкин Артемий Михайлович**
Год рождения: 1997
Университет ИТМО, факультет систем управления и робототехники,
кафедра систем управления и информатики,
студент группы № P3335
Направление подготовки: 15.03.06 – Мехатроника и робототехника
e-mail: zenkinartem1997@gmail.com

**УДК 004.93+004.942**

## МОНОКУЛЯРНЫЙ SLAM ДЛЯ КВАДРОКОПТЕРА PARROT ARDRONE 2.0

**Осинкин Е.А., Баев П.А., Зенкин А.М.**
**Научный руководитель – к.т.н. Капитонов А.А.**

В работе рассмотрен один из подходов к решению задачи одновременного картирования и локализации в заранее неизвестном окружении. Этот подход основан на извлечении и отслеживании ключевых точек в каждом кадре с последующей оценкой поворота и смещения камеры между кадрами. Таким образом, данные для одометрии дрон получает посредством одной камеры.
**Ключевые слова:** компьютерное зрение, локализация, картирование, проективная геометрия, эпиполярная геометрия, feature-based SLAM.

Задача одновременного картирования и локализации SLAM (Simultaneous Localization and Mapping) является одной из главных проблем компьютерного зрения. Она включает в себя множество низкоуровневых подзадач, таких как калибровка камеры или стереопары, извлечение и отслеживание ключевых точек, построение карты глубины, триангуляция, оценка перемещения камеры. Однако, помимо хорошо изученных подзадач, SLAM также включает в себя сложные методы оптимизации, такие как bundle adjustment [1]. Набор подзадач варьируется в зависимости от подхода к решению задачи одновременного картирования и локализации.

По плотности карты SLAM подразделяется на плотный, полуплотный и разреженный; по количеству камер – на монокулярный и стерео. Также для задач картирования и локализации часто используют RGBD-камеры и лидары. Из всех вышеперечисленных способов монокулярный SLAM является наиболее оптимальным для квадрокоптера Parrot ARDrone 2.0, обладающего небольшой грузоподъемностью. Установка RGBD-камеры или

стереопары неизбежно ухудшит динамику дрона и только монокулярный подход не требует никаких конструктивных изменений. Главным недостатком картирования по одной камере является то, что абсолютный масштаб невозможно определить без использования дополнительных датчиков, например, дальномера, расположенного в нижней части дрона.

Как правило, результатом монокулярного SLAM, основанного на поиске ключевых точек, является разреженная карта, однако существует решение [2] с использованием сверточных нейронных сетей, которое позволяет построить плотную карту. В работе рассмотрен классический способ получения разреженной карты.

Описание алгоритма SLAM начато с модели камеры. Для точки в X-трехмерном пространстве рис. 1, а, формула проекции на плоскость изображения выглядит следующим образом: $x = \mathbf{K}[\mathbf{R}|\mathbf{t}][X\ 1]^T$, где $\mathbf{K}$ – матрица внутренних параметров камеры; $\mathbf{R}$ – ортогональная матрица поворота размерностью; $\mathbf{t}$ – вектор-столбец смещения, а $[\mathbf{X}\ 1]^T$ – вектор-столбец положения реальной точки, записанный в однородных координатах.

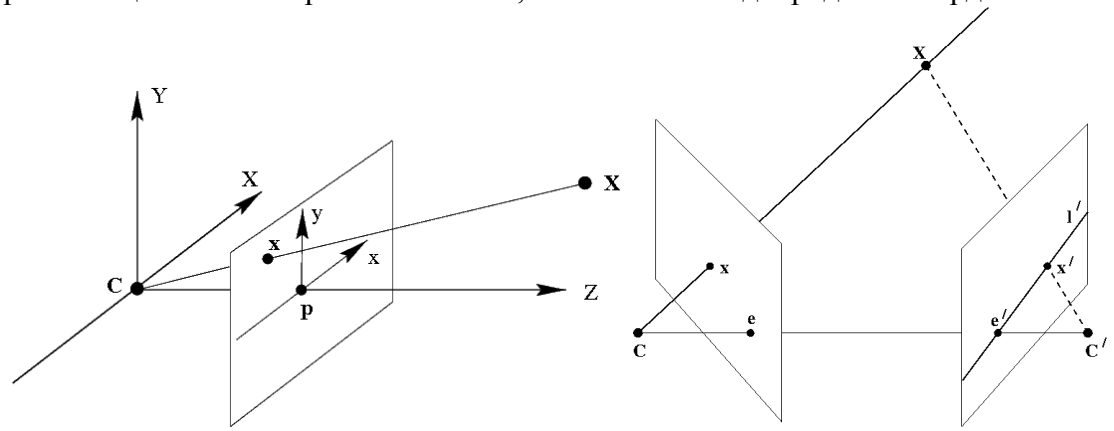
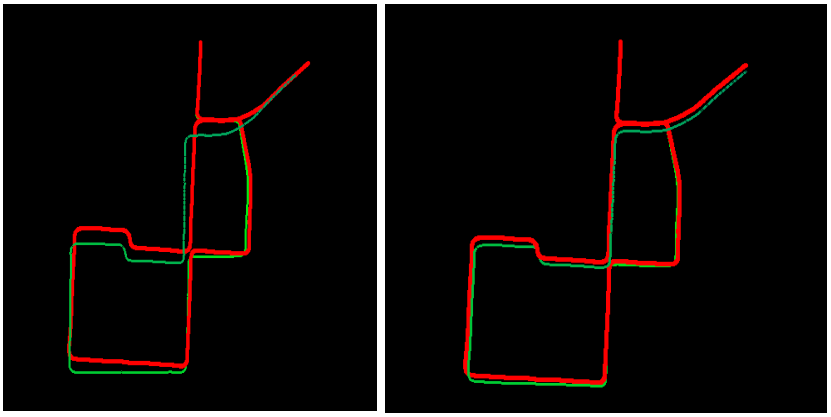



Рис. 1. Модель камеры (а); эпиполярное ограничение (б)

Поиск ключевых точек производился при помощи алгоритмов FAST и ORB. Отслеживание ключевых точек FAST осуществлялось с использованием метода KLT tracker [3], а для ключевых точек ORB был использован метод библиотеки OpenCv brute-force matching. В случае с brute-force matching для качественного отслеживания ключевых точек необходимо осуществлять проверку и удалять ложные соответствия. Одним из критериев проверки является утверждение, что наилучшее соответствие из первого изображения во второе должно совпадать с наилучшим соответствием из второго в первое. Самой эффективной фильтрацией является фильтрация по эпиполярному ограничению рис. 1, б, которая подразумевает, что наблюдаемые точки, лежащие на одной линии для первого положения камеры, также будут лежать на одной линии после смещения камеры [1]. В основе метода KLT лежит оценка области, в которой ключевая точка окажется на следующем кадре. Отследив ключевые точки в двух последовательных кадрах, оценим поворот и смещение камеры, для этого необходимо знать сущностную матрицу $\mathbf{E}$ размерностью $3 \times 3$, такую, что $(x_1')^T \mathbf{E}\, x_2' = 0$, где $x_1'$и $x_2'$ – нормализованные однородные координаты одной точки в двух последовательных кадрах. Наиболее эффективным, с точки зрения производительности и робастности, является пятиточечный [4] алгоритм поиска матрицы $\mathbf{E}$. Матрицы поворота $\mathbf{R}$ и смещения $\mathbf{t}$ получаются путем сингулярного разложения $\mathbf{E}$ [1].

Примем, что в начальный момент времени вращение и смещение отсутствуют, таким образом матрица $\mathbf{R}_0$ является единичной матрицей $3 \times 3$, а $\mathbf{t}_0 = [0\ 0\ 0]^T$. Перемещение камеры между кадрами записывается как $\mathbf{R}_i = \mathbf{R} \cdot \mathbf{R}_{i-1}$, $\mathbf{t}_i = \mathbf{t}_{i-1} + \mathbf{R} \cdot t, i = 1,2 \ldots n$.

Тестирование визуальной одометрии с использованием FAST и ORB проводилось на наборе данных «KITTI odometry data set». Набор данных представляет собой последовательность изображений, снятых с камеры, закрепленной на автомобиле.



а б

Рис. 2. Красным цветом обозначена истинная траектория, зеленым – траектория на основе визуальной одометрии с использованием сочетаний: ORB/brute-force matcher (а) и FAST/KLT tracker (б)

Как можно видеть сочетание алгоритмов FAST и KLT дает более точную оценку траектории рис. 2, однако со временем ошибка неизбежно накапливается, что ведет к серьезному отклонению от истинной траектории. Еще одна проблема возникает, когда не наблюдается ни одной ключевой точки, например, в какой-то момент времени камера была закрыта препятствием или движение было слишком быстрым, и кадр оказался размытым. Такие нарушения препятствуют продолжению работы простейшего алгоритма визуальной одометрии, поэтому возникает необходимость реинициализации. Вышеуказанные проблемы решаются представлением позиций камеры в виде иерархической [5] системы графов, где вершины хранят информацию о кадре, в том числе ключевые точки, которые также служат набором визуальных слов, на основе которого можно произвести повторную инициализацию. Ребра графа представляют перемещение камеры. Фреймворк g2o позволяет решить задачу bundle adjustment, т.е. минимизировать дрейф.

Алгоритм монокулярного SLAM широко применим за рамками проекта с квадрокоптером Parrot ARDrone 2.0, поскольку для его работы необходима лишь одна откалиброванная камера. Визуальная одометрия может быть использована для коррекции информации о местоположении робота в случаях, когда другие датчики имеют значительную ошибку, которая накапливается с течением времени. Карта, полученная в результате работы алгоритма, является разреженной и не подходит для точных измерений, однако позволяет составить общее представление о видимых препятствиях. В дальнейшем эта карта может быть конвертирована в структуру octomap, удобную для решения задач поиска пути.

**Литература**

1. Structure from motion – классическая реализация [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/post/228525/, своб.
2. Tateno K., Tombari F., Laina I. and Navab N. CNN-SLAM: Real-time dense monocular slam with learned depth prediction [Электронный ресурс]. – Режим доступа: http://openaccess.thecvf.com/content_cvpr_2017/papers/Tateno_CNN-SLAM_Real-Time_Dense_CVPR_2017_paper.pdf, своб.
3. Tomashi C. and Kanade T. Detection and tracking of point features // Tech. Rep. CMU-CS-91-132. – 1991. – P. 1–22.
4. Li H. and Hartley R. Five-Point Motion Estimation Made Easy // 18th International Conference on Pattern Recognition. – 2006. – P. 630–633.
5. Grisetti G., Kummerle R., Stachniss C., Frese U. and Hertzberg C. Hierarchical optimization on manifolds for online 2d and 3d mapping [Электронный ресурс]. – Режим доступа: http://www2.informatik.uni-freiburg.de/~stachnis/pdf/grisetti10icra.pdf, своб.

**Сергеева Екатерина Андреевна**
Год рождения: 1995
Университет ИТМО, факультет систем управления и робототехники,
кафедра систем управления и информатики,
студент группы № Р4141
Направление подготовки: 27.04.04 – Управление в технических системах
e-mail: e.a.sergeeva9@yandex.ru

**УДК 681.5**

# РАЗРАБОТКА СИСТЕМЫ УПРАВЛЕНИЯ ПРОИЗВОДСТВЕННЫМ ПОМЕЩЕНИЕМ

**Сергеева Е.А.**
**Научный руководитель – к.т.н. Нуйя О.С.**

Работа выполнена в рамках темы НИР № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность».

В работе произведены расчет, моделирование и разработка системы автоматического управления птицефермой. Устройство контролирует температуру, влажность, качество воздуха и освещение в помещении, рассчитанном на содержание до двух сотен перепелов. Моделирование произведено в системе MATLAB, устройство построено на базе Arduino. Была произведена проверка работы устройства. Разработанное устройство соответствует всем техническим требованиям, собрано на недорогих компонентах и удобно в использовании.
**Ключевые слова:** Arduino, птицеферма, автоматическое управление, микроклимат.

Микроклимат помещения сильно влияет на здоровье и производительность птиц. Высокая температура приводит к увеличению смертности, низкая – к повышению потребления корма и снижению продуктивности. Высокая влажность отрицательно влияет на санитарное состояние помещения, и отклонение от рекомендуемой влажности приводит к различным заболеваниям. Высокое содержание вредных газов: углекислого газа, аммиака и сероводорода свидетельствует о плохой вентиляции и нарушении норм содержания птиц. Для поддержания микроклимата на птицефабриках, предназначенных для содержания нескольких тысяч птиц, разработаны различные системы контроля, к примеру, разработки фирмы «Дейтамикро». Для птицеферм, где содержатся до нескольких сотен птиц, использование подобных устройств нецелесообразно ввиду высокой стоимости и сложности эксплуатации. Как правило, микроклимат на птицефермах регулируется управляющим персоналом. Малогабаритные фермы, как правило, размещаются в малых помещениях, микроклимат которых быстро меняется с течением дня, и обслуживаются ручным трудом. Это делает вероятность отклонения одного или нескольких параметров микроклимата достаточно высокой.

Целью данной работы являлся расчет, разработка и моделирование системы автоматического управления птицефермой, поддерживающей постоянную температуру и влажность, а также регулирующую освещение и информирующую пользователя об аварийных ситуациях. На основе полученных данных необходимо было создать устройство на платформе Arduino Uno, и проверить работоспособность устройства в реальном техническом помещении [1].

Для максимальной продуктивности на птицеферме следует установить прерывистый 20-ти часовой световой день, при этом свет должен переключаться плавно [2]. Разрабатываемое устройство должно обеспечить требуемые параметры микроклимата: температура 20–22°C, относительная влажность 60–70%, освещенность 20 люкс.

Arduino в начале работы получает информацию с модуля реального времени и с установленных датчиков. В случае если свет по расписанию должен быть включен, и в данный момент уровень освещения, измеряемый фоторезистором низок, а также освещение не включено, запускается плавное включение освещения. Процесс осуществляется при помощи диммера. Когда освещение полностью включено, диммер постоянно работает как реле. Когда контроль над освещением завершен, начинается контроль микроклимата. В случае если влажность или температура не соответствуют требуемым значениям, и если температура и влажность воздуха вне помещения ближе к требуемым значениям, вентиляция начинает регулировку этих параметров. Если внешняя температура слишком низкая, использование вентиляции сокращается. Если регулировка при помощи вентиляции не возможна, температура повышается при помощи обогревателя, управляемого реле, влажность повышается при помощи увлажнителя, управляемого реле. Понижение влажности и температуры ниже значения внешних влажности и температуры невозможно. Если значение качества воздуха завышено, включается вентиляция. В случае если в течение продолжительного времени один из параметров значительно отклонен от нормы, Arduino посылает сигнал на модуль GSM.

**Расчет математической модели.** Маломощный DC-двигатель вентилятора замещает воздух помещения наружным воздухом, постепенно приближая влажность воздуха в помещении к значению влажности наружного воздуха. Подобран пропорциональный регулятор (P) регулятор, *Kp*=10. Из-за низкой производительности вентилятора дальнейшее повышение коэффициента не влияет на работу системы [3]. Увлажнитель управляется реле и повышает влажность до 65%.

Для расчета математической модели помещения учитаны размеры и материалы помещения [4].

Полученная передаточная функция помещения:

$$W(p)_{\text{пм}} = \frac{Q + t_{\text{н}}(k_{\text{огр}} S_{\text{огр}})}{(m_{\text{пм}} c - k_{q\text{пт}} N) p + k_{\text{огр}} S_{\text{огр}}},$$

где $Q$ – отдаваемая на нагрев энергия, ккал/ч; $t_{\text{н}}$ – температура вентиляции, К; $k_{\text{огр}}$ – коэффициент теплопроводности стен, Вт/(м$^2$·К); $S_{\text{огр}}$ – площадь стен, м$^2$; $m_{\text{пм}}$ – масса воздуха в помещении, кг; $c$ – удельная теплоемкость, Дж/(кг·К); $k_{q\text{пт}}$ – выделяемое тепло, Дж; $N$ – количество птиц.

Температура регулируется вентилятором за счет температурного баланса:

$$t_{\text{в2}} = \frac{V_{\text{пм}} t_{\text{в}} - V_{\text{вент}} t_{\text{в}} + V_{\text{вент}} t_{\text{н}}}{V_{\text{пм}}},$$

где $V_{\text{вент}}$ – объем вентиляции, м$^3$; $t_{\text{в}}$ – температура внутреннего воздуха, °C.

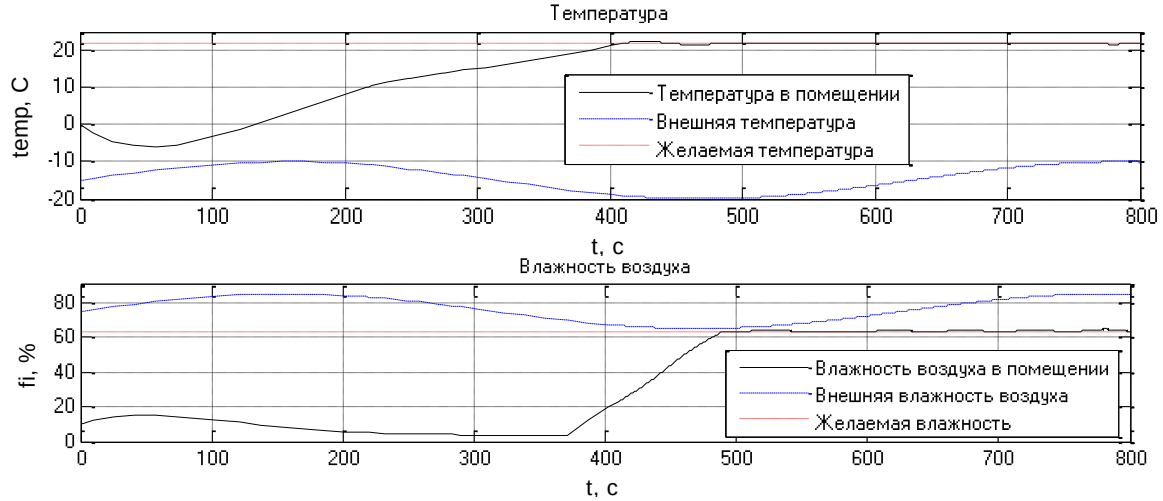



Рис. 1. Графики переходных процессов в помещении

Полученные графики представлены на рис. 1. Полученная модель полностью удовлетворяет техническим требованиям. Для нагрева помещения требуется 400 с, после чего обогреватель отключается и регулировку температуры осуществляет вентиляция. Без контроля температуры при наружной температуре –15°С, установившаяся температура внутри помещения достигает 38°С, что является недопустимо высоким значением. График показывает, что данная модель управления обеспечивает достижение требуемой температуры с минимальными погрешностями.

Проверка работы устройства проводилась в помещении объемом 8 м$^3$, содержащим 100 птиц. Температура вне помещения: 8°С, влажность: 47%. Как следует из графиков, представленных на рис. 2, устройство справилось со своей задачей. Также была произведена и доказана работоспособность управления освещением фермы.

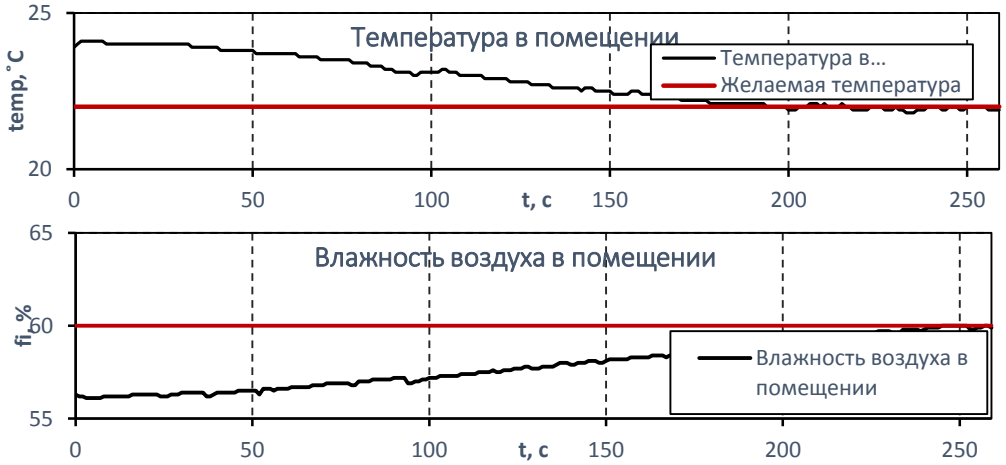



Рис. 2. Графики регулировки температуры и влажности в техническом помещении

**Литература**

1. Разработки фирмы «Дейтамикро» [Электронный ресурс]. – Режим доступа: http://www.datamicro.ru/, своб.
2. Серебряков А.И. Перепела: содержание, кормление, разведение. – Пензенская область, 2010. – 89 с.
3. Гулевский В.А. Нормализация температурно-влажностных параметров воздушной среды птицеводческих помещений путем обработки воздуха пластинчатыми теплообменниками дис. канд. техн. Наук. – Воронеж, 2014. – 327 с.
4. Щекин Р.В. Справочник по теплоснабжению и вентиляции. Книга первая. Отопление и теплоснабжение. – Киев: Будівельник, 1976. – 416 с.

**Сомов Сергей Николаевич**
Год рождения: 1994
Университет ИТМО, факультет систем управления и робототехники,
кафедра систем управления и информатики,
студент группы № Р4240
Направление подготовки: 27.04.04 – Управление в технических системах
e-mail: s.somov@corp.ifmo.ru

**Громов Владислав Сергеевич**
Год рождения: 1990
Университет ИТМО, факультет систем управления и робототехники,
кафедра систем управления и информатики,
к.т.н., ассистент
e-mail: gromov@corp.ifmo.ru

**Борисов Олег Игоревич**
Год рождения: 1991
Университет ИТМО, факультет систем управления и робототехники,
кафедра систем управления и информатики,
к.т.н., ассистент
e-mail: borisov@corp.ifmo.ru

**Пыркин Антон Александрович**
Год рождения: 1985
Университет ИТМО, факультет систем управления и робототехники,
кафедра систем управления и информатики,
д.т.н., профессор
e-mail: a.pyrkin@gmail.ru

**Волошин Дмитрий**
Год рождения: 1994
Университет ИТМО, факультет систем управления и робототехники,
кафедра систем управления и информатики,
студент группы № Р4240
Направление подготовки: 27.04.04 – Управление в технических системах
e-mail: voloshin@corp.ifmo.ru

**УДК 681.5.015**

## РОБАСТНОЕ УПРАВЛЕНИЕ ПО ВЫХОДУ ФИЗИЧЕСКОЙ МОДЕЛЬЮ НАДВОДНОГО СУДНА С АНТИВИНДАП-КОРРЕКЦИЕЙ

**Сомов С.Н., Громов В.С., Борисов О.И., Пыркин А.А., Волошин Д.**
**Научный руководитель – д.т.н., профессор Пыркин А.А.**

Работа выполнена в рамках темы НИР № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность».

В работе рассмотрена реализация робастного управления по выходу физической моделью надводного судна с антивиндап-коррекцией. Алгоритм робастного управления по выходу основан на последовательном компенсаторе. Он был дополнен внутренней моделью, которая позволяет устранить статическую ошибку и реализовать антивиндап-схему, чтобы уменьшить превышение выходной переменной. В результате был получен закон управления, который генерирует ограниченный управляющий сигнал и компенсирует возмущения на надводное судно.
**Ключевые слова:** робастное управление, управление по выходу, антивиндап-коррекция, параметрическая неопределенность, многоканальные системы.

Реальные технические системы имеют нелинейности и некоторые различные ограничения. Данное исследование было направлено на синтез алгоритмов управления, которые могут быть применимы для различных технических систем с ограниченными входами и неизвестными параметрами. Сигналы управления, генерируемые регуляторами, перенасыщены из-за аппаратных ограничений. Кроме того, интегральная составляющая внутри контроллера может привести к снижению производительности, потере стабильности. Эту проблему можно решить с помощью метода «антивиндап», предотвращающего накопление ошибок. Алгоритм управления основан на методе последовательного компенсатора [1]. Основным преимуществом этого метода является простое внедрение в роботизированные системы в различных случаях неопределенности параметров установки и недоступности оценки производных.

В работе рассмотрено роботизированное надводное судно, которое является хорошим примером системы MIMO с неопределенностями для реализации робастного управления по выходу с антивиндап-коррекцией [2–4]. Цель исследования – получить закон управления $u$, используя только измерения выходной переменной $y$ такие, что под действием внешних возмущений выполняется условие:

$$\lim_{t\to\infty} y(t) = 0. \quad (1)$$

Был выбран закон управления формы:

$$\upsilon = -\kappa\left(c_q^T\xi + y\right) - \gamma\eta, \quad (2)$$

$$\dot{\xi} = \mathbf{A_q}\xi + \mathbf{b_q}y, \quad (3)$$

$$\dot{\eta} = \kappa\left(c_q^T\xi + y\right) + \nu\chi(\upsilon), \quad (4)$$

$$\chi(\upsilon) = \upsilon - \mathrm{sat}(\upsilon), \quad (5)$$

где $\chi(\upsilon)$ – нелинейный сигнал антивиндап-коррекции, $\kappa > 0$, $\gamma > 0$, $\nu > 0$, матрица $\mathbf{A_q}$ и векторы $\mathbf{b_q}$, $\mathbf{c_q}$ имеют вид:

$$\mathbf{A_q} = \begin{bmatrix} -\dot{q}_2\sigma & 1 \\ -\dot{q}_1\sigma^2 & 0 \end{bmatrix},\ \mathbf{b_q} = \begin{bmatrix} \dot{q}_2\sigma \\ \dot{q}_1\sigma^2 \end{bmatrix},\ \mathbf{c_q} = \begin{bmatrix} q_1 \\ q_2 \end{bmatrix},$$

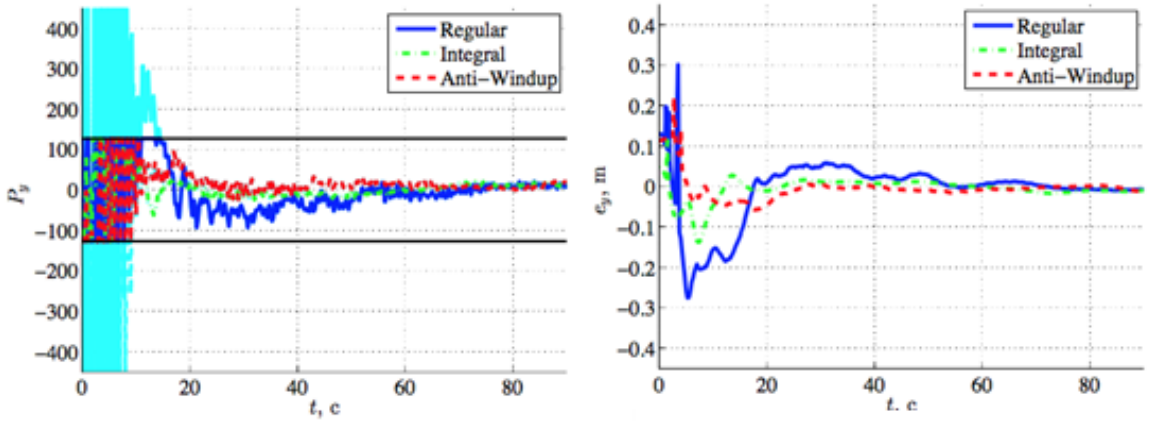
где $\sigma > 0$.

Регулятор (2)–(3) был дополнен внутренней моделью (4), которая позволяет устранить статическую ошибку и реализовать антивиндап-схему (5), чтобы уменьшить превышение выходной переменной, при условии ограниченного входа, который вызван аппаратными ограничениями.

Экспериментальные исследования проходили на робототехнической установке, включающей в себя макет судна с размерами: длина 0,432 м, ширина 0,096 м, высота 0,052 м. Местом проведения экспериментов выступал экспериментальный бассейн, представляющий собой рабочее пространство для лодки с размерами: длина 1,5 м, ширина 1,1 м, высота 0,1 м.

Роль компьютерного зрения для определения расположения лодки относительно бассейна выполняет цифровая камера, подвешенная над бассейном с помощью штатива и подключенная к компьютеру [5].

По результатам работы были получены графики (рисунок), робастное управление приводит к небольшой статической ошибке, вызванной нелинейным входом исполнительных механизмов.




а б

Рисунок. Графики: управления $P_y(t)$ (а) и ошибки $e_y(t)$ (б) сигналов замкнутой системы вдоль оси $y$ при различных регуляторах

Небольшие значения ошибки приводят к малому значению управления, что недостаточно для противодействия волнам и перемещения лодки. Этот эффект устраняется путем введения внутренней модели, которая накапливает значение ошибки и увеличивает управляющий сигнал. Но увеличение параметров контроллера нежелательно, так как это может привести к автоколебаниям лодки и увеличению перерегулирования. Гладкая кривая достигается с помощью метода антивиндап-коррекции, который обладает энергосберегающим управлением и уменьшает перерегулирование. Небольшие колебания лодки вызваны волновыми возмущениями и шумом в каналах измерений.

Полученный новый подход применим для установок с ограниченными входами и неопределенными параметрами. Его полезной особенностью является возможность указать пределы генерируемого управляющего сигнала с уменьшением нежелательного превышения выходной переменной. Это важно для реальных технических систем из-за их аппаратных ограничений.

**Литература**

1. Bobtsov A. Robust output-control for a linear system with uncertain coefficients // Automation and remote Control. – 2002. – V. 63. – № 11. – P. 1794–1802.
2. Pyrkin A., Bobtsov A., Kolyubin S., Surov M., Vedyakov A., Feskov A., Vlasov S., Krasnov A., Borisov O. and Gromov V. Dynamic positioning system for nonlinear mimo plants and surface robotic vessel // IFAC Proceedings Volumes (IFAC-PapersOnline). – 2013. – P. 1867–1872.
3. Wang J., Pyrkin A., Bobtsov A., Borisov O., Gromov V., Kolyubin S. and Vlasov S. Output control algorithms of dynamic positioning and disturbance rejection for robotic vessel // IFAC-PapersOnLine. – 2015. – V. 48. – № 11. – P. 295–300.
4. Borisov O., Gromov V., Pyrkin A., Bobtsov A., Petranevsky I. and Klyunin A. Output robust control with anti-windup compensation for robotic boat // 21st International Conference on Methods and Models in Automation and Robotics. – 2016. – P. 13–18.
5. Громов В.С., Власов С.М., Борисов О.И., Пыркин А.А. Система технического зрения для роботизированного макета надводного судна // Научно-технический вестник информационных технологий, механики и оптики. – 2016. – Т. 16. – № 4(104). – С. 749–752.

**Тихоненко Дмитрий Сергеевич**
Год рождения: 1995
Университет ИТМО, факультет систем управления и робототехники,
кафедра систем управления и информатики,
студент группы № Р4141
Направление подготовки: 27.04.04 – Управление в технических системах
e-mail: ds.tikhonenko@gmail.com

**Мелешко Нина Владимировна**
Год рождения: 1995
Университет ИТМО, факультет систем управления и робототехники,
кафедра систем управления и информатики,
студент группы № Р4140
Направление подготовки: 27.04.04 – Управление в технических системах
e-mail: meleshk.nina@gmail.com

**УДК 681.58**

# РАЗРАБОТКА ВСПОМОГАТЕЛЬНОГО УСТРОЙСТВА ДЛЯ ЛЮДЕЙ, СТРАДАЮЩИХ ИДИОПАТИЧЕСКИМ ДРОЖАНИЕМ РУК, БОЛЕЗНЬЮ ПАРКИНСОНА ИЛИ ДРУГИМИ ПОХОЖИМИ ЗАБОЛЕВАНИЯМИ

**Тихоненко Д.С., Мелешко Н.В.**
**Научный руководитель – к.т.н., доцент Чежин М.С.**

В работе рассмотрены методы проектирования устройства для компенсации тремора рук. Предложены подходы к моделированию специального стабилизирующего элемента способного к работе на частоте тремора. Представлены результаты моделирования упрощенной модели устройства для различной частоты возмущающего воздействия.
**Ключевые слова:** тремор рук, болезнь Паркинсона, умная ложка, компенсация тремора рук.

У каждого здорового человека имеется так называемый физиологический тремор, выраженный в той или иной степени, хотя у большинства людей он настолько слаб, что его трудно заметить. Главным симптомом тремора рук являются мышечные колебательные сокращения непроизвольного характера. Они могут наблюдаться как у лиц с нарушениями двигательной системы, так и среди здоровых людей. При утомлении, сильных эмоциональных нагрузках, а также при патологии нервной системы тремор существенно усиливается. Кроме того, очень часто проявляется эссенциальный тремор, который является патологией нервной системы. В некоторых случаях тремор может привести к социальной изоляции, так как мешает нормальным повседневным действиям, таким как письмо или питание. Причина возникновения тремора неизвестна. Однако он часто передается по наследству, его часто называют семейный тремор. У детей родителей с тремором есть 50% шанс унаследовать состояние. В случаях, когда в семейной истории тремора нет, могут играть определенную роль другие факторы, такие как токсины, хотя это только предположение [1–3].

На данный момент медицина не может полностью излечить данное заболевание. Многие фармакологические и хирургические решения, а также большинство технических решений непрактичны из-за повышенного риска побочных эффектов. С каждым годом растет число устройств, которые направлены на улучшение качества жизни. Сейчас существуют технические методы борьбы с тремором рук. Они развиваются в трех основных направлениях: изоляция, физическое подавление,

активная компенсация. Сравнение этих технических решений между собой показывает, что устройства, основанные на технологии активной компенсации тремора, превосходят другие методы по многим параметрам, небольшие размеры устройств, довольно низкая стоимость (по сравнению с другими направлениями), простота в использовании и высокий уровень комфорта – главные достоинства этого способа. Метод активной компенсации является очень перспективным направлением. При таком подходе тремор никуда не исчезает, но все его действия компенсируются через устройство, которое взаимодействует с пользователем.

В работе рассмотрена разработка устройства, которое будет компенсировать тремор рук, чтобы облегчить прием пищи. Были выбраны параметры для устройства:

– устройство способно компенсировать дрожание рук с частотой в диапазоне 1–5 Гц;
– амплитуда выходного сигнала должна быть уменьшена более чем в 5 раз;
– размеры устройства должны быть сопоставимы с размерами обычных столовых приборов (в пределах 200 мм);
– масса устройства должна быть менее 400 г для комфортного использования.

Для решения поставленной задачи, была предложена конструкция на основе стабилизирующего элемента (рис. 1, б), эскиз которого изображен на рис. 1. На эскизе представлен также подход к проектированию устройства для компенсации идиопатического дрожания рук (рис. 1, а).

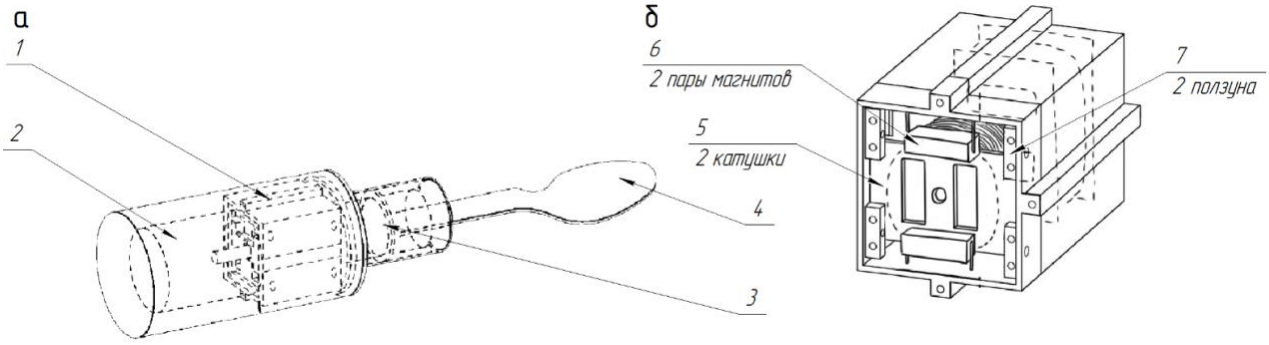



Рис. 1. Эскиз устройства для компенсации идиопатического дрожания рук:
1 – стабилизирующий элемент; 2 – корпус устройства; 3 – захватный элемент; 4 – насадка (ложка) (а); эскиз стабилизирующего элемента: 5 – катушка индуктивности; 6 – постоянный магнит; 7 – ползун (б)

Предложена структура и параметры математической модели. Устройство было промоделировано в среде MATLAB с помощью пакета Simulink. Результаты моделирования, с различной частотой входного воздействия, представлены на рис. 2.

Полученные графики наглядно иллюстрируют результат работы устройства. Отклонение от начального сигнала на рис. 2, а, вызвано коэффициентами демпфирования и жесткости. Анализ графиков показывает, что в результате работы устройства амплитуда дрожания уменьшается в 5–11 раз.

Результаты моделирования вспомогательного устройства для людей, страдающих идиопатическим дрожанием рук, болезнью Паркинсона или другими похожими заболеваниями иллюстрируют существенное сглаживание дрожания, что является главной задачей устройства. Расчеты показывают, что ложка при своих размерах достаточно комфортно сидит в руке и она не тяжелая. В качестве насадки может быть использована также вилка, ключ, карандаш или даже предмет для создания макияжа. В дальнейшем планируется продолжить работу по оптимизации и улучшению качества стабилизирующего элемента и устройства в целом.

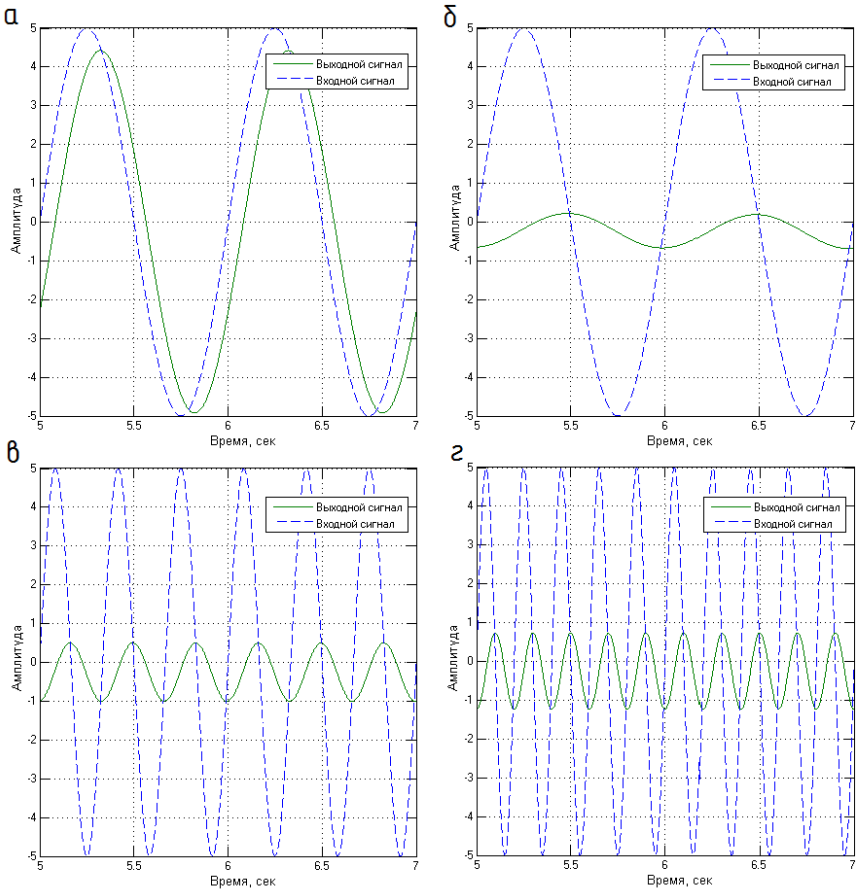



Рис. 2. Результаты моделирования проектируемого устройства без использования компенсации (а); отработка входного воздействия в 1 Гц (б); 3 Гц (в); 5 Гц (г)

**Литература**

1. Pathak A. The Development of an Antagonistic SMA Actuation Technology for the Active Cancellation of Human Tremor [Электронный ресурс]. – Режим доступа: https://deepblue.lib.umich.edu/bitstream/handle/2027.42/76010/apathak_1.pdf, своб.
2. Пат. № US8308664 B2, US 12/716,860. Tremor stabilizing system for handheld devices / Anupam Pathak, 2012.
3. Пат. № US20140052275 A1, US 13/250,000. System and method for stabilizing unintentional muscle movements / Anupam Pathak, 2014.

**Чащина Мария Максимовна**
Год рождения: 1995
Университет ИТМО, факультет систем управления и робототехники,
кафедра систем управления и информатики,
студент группы № Р4135
Направление подготовки: 15.04.06 – Мехатроника и робототехника
e-mail: marichaschina@mail.ru

**УДК 681.518.5**

# ИССЛЕДОВАНИЕ АЛГОРИТМОВ УПРАВЛЕНИЯ МОБИЛЬНЫМ РОБОТОМ В СРЕДЕ С НЕОПРЕДЕЛЕННОСТЯМИ

**Чащина М.М.**
**Научный руководитель – к.т.н., доцент Литвинов Ю.В.**

Работа выполнена в рамках темы НИР № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность».

В работе предложен алгоритм управления колесным роботом на пересеченной местности по заданному маршруту. Выполнена проверка работоспособности предложенных алгоритмов с помощью математического моделирования и экспериментальных исследований на колесной платформе фирмы «Odyssey» и блока управления на базе платы Arduino UNO. Робот функционирует в автономном режиме. Интеллектуальность робота заключается в возможности изменять свое поведение в зависимости от характера местности.
**Ключевые слова:** мобильный робот, траектория объезда, алгоритм движения, техническое зрение, пересеченная местность.

Существуют различные методы определения расстояния от мобильного робота до препятствия: использование ультразвуковых, инфракрасных датчиков, лазеров, стереозрения (две видеокамеры) [1, 2] и т.д.

Рассмотрим вариант определения расстояния от робота до препятствия с помощью одной камеры.

Сущность метода состоит в том, что, когда робот перемещается ближе к препятствию, камера, установленная на роботе, будет записывать изображение препятствия в два разных момента: $t_0$ и $t_1$, а затем передавать информацию в компьютер. Компьютер, получив информацию об изображении, выполняет обработку информации и дает два значения площади препятствия, соответствующие двум моментам времени. Определив площадь препятствия $S_0$ (в пикселях) в момент времени $t_0$ и $S_1$ в момент времени $t_1$, можно найти расстояние $\Delta L$, пройденное роботом за интервал времени $\Delta t=t_1-t_0$ по формуле:

$$\Delta L = V \cdot \Delta t,$$

где $V$ – скорость движения робота

Вычисляем расстояние $L_1$ от робота до препятствия в момент $t_1$ по следующей формуле:

$$L_1 = \frac{\Delta L \sqrt{\frac{S_0}{S_1}}}{1-\sqrt{\frac{S_0}{S_1}}}.$$

$$\frac{a}{f} = \tan\alpha_1 = \frac{h}{L};\ \frac{b}{f} = \tan\alpha_2 = \frac{h}{L-\Delta L} \Rightarrow \frac{a}{b} = \frac{h}{L} : \frac{h}{L-\Delta L} = \frac{L-\Delta L}{L} = 1-\frac{\Delta L}{L}$$

$$\Rightarrow L = \frac{\Delta L}{1-\frac{a}{b}} = \frac{\Delta L}{1-\sqrt{\frac{S_0}{S_1}}} \Rightarrow L_1 = L - \Delta L = \frac{\Delta L\sqrt{\frac{S_0}{S_1}}}{1-\sqrt{\frac{S_0}{S_1}}}.$$

Камера фиксирует изображения на светочувствительных матрицах, и расстояние от объектива камеры до матриц составляет значение $f$, где $f$ – фокусное расстояние камеры; $a$, $b$ – высоты препятствия на кадре изображения в моменты $t_0$ и $t_1$; $h$ – реальная высота препятствия.

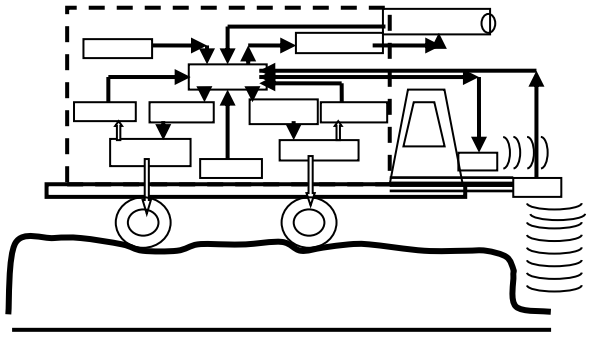


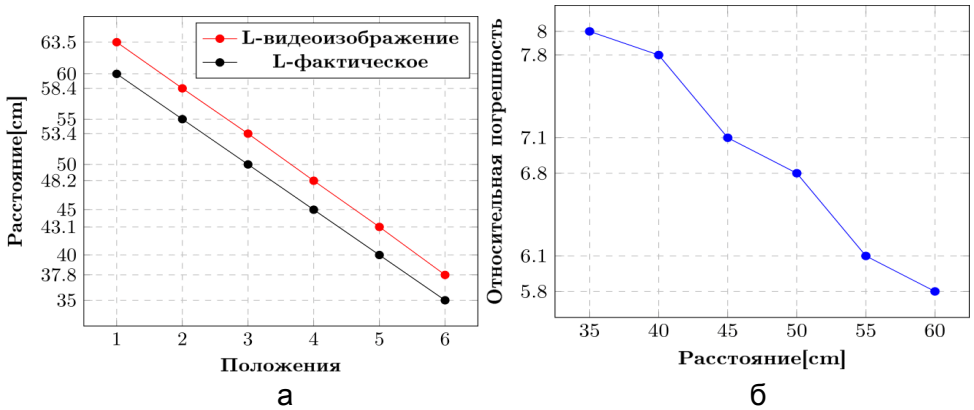
Рис. 1. Эксперимент по определению дальности до препятствия

Был проведен эксперимент по определению дальности до препятствия по видеоизображению (рис. 1). В качестве мобильного робота была использована 6-ти колесная платформа «Odissey» под управлением микропроцессора Arduino Uno и простейшая вэб-камера. Для обработки видеоизображения использовался ноутбук. Результаты, полученные в ходе эксперимента, представлены в таблице.

Таблица. Результаты эксперимента

| | | | | | | |
|---|---|---|---|---|---|---|
| $S_0$ – площадь препятствия в пикселях в момент времени $t_1$ | 34338 | 39954 | 47086 | 56317 | 68607 | 85448 |
| $S_1$ – площадь препятствия в пикселях в момент времени $t_2$ | 39954 | 47086 | 56317 | 68607 | 85448 | 109125 |
| $L_э$ – расстояние по видеоизображению (см) | 63,5 | 58,4 | 53,4 | 48,2 | 43,1 | 37,8 |
| $L$ – фактическое расстояние (см) | 60 | 55 | 50 | 45 | 40 | 35 |
| Погрешность $\Delta$ (см) | 3,5 | 3,4 | 3,4 | 3,2 | 3,1 | 2,8 |
| $\delta = \frac{\Delta L}{L}\cdot 100\%$ | 5,8 | 6,1 | 6,8 | 7,1 | 7,8 | 8,0 |

По результатам эксперимента были построены зависимости (рис. 2).




а б

Рис. 2. Сравнение результатов: измерений и фактического расстояния (а); относительной погрешности измерений расстояний (б)

Из приведенных результатов видно, что погрешность предлагаемого алгоритма достаточно мала.

Преимущества:

- низкая стоимость, поскольку используется только одна камера;
- простота реализации: разместить одну камеру на роботе намного проще, чем две камеры;
- одновременно с измерением расстояния, можно определить и вид препятствия (автомобили, люди, строения или деревья и т.п.);
- низкие требования к вычислительным ресурсам, так как используются простые вычислительные алгоритмы;
- данные о препятствии можно записывать в процессе движения мобильного робота в формате видео, что является удобным для дальнейшего анализа и исследований.

В работе предложен алгоритм определения расстояния от мобильного робота до препятствия с помощью одной видеокамеры. Основа алгоритма – измерение площади препятствия на кадре изображения в два разных момента времени, из которых рассчитывается расстояние до препятствия. Результат анализа работы предложенного алгоритма показывает его работоспособность и позволяет не только определить дальность до препятствия, но и его вид, обеспечивая возможность организации слежения за выбранным объектом [3, 4].

**Литература**

1. Bay H., Ess A., Tuytelaars T., Van Gool L. SURF: Speeded Up Robust Features // Computer Vision and Image Understanding. – 2008. – V. 110. – № 3. – P. 346–359.
2. Geiger A., Roser M., Urtasun R. Efficient Large-Scale Stereo Matching // Asian Conference on Computer Vision. – 2010. – P. 25–38.
3. Евстигнеев М.И., Литвинов Ю.В., Мазулина В.В., Чащина М.М. Локация мобильного робота с использованием структурного анализа изображений // Изв. вузов. Приборостроение. – 2017. – Т. 60. – № 9. – С. 858–862.
4. Rosten E., Porter R., Drummond T. Faster and better: A machine learning approach to corner detection // IEEE Trans. Pattern Analysis and Machine Intelligence. – 2010. – V. 32. – № 1. – P. 105–119.

**Шокатаев Адиль Сакенович**
Год рождения: 1997
Университет ИТМО, факультет систем управления и робототехники,
кафедра систем управления и информатики,
студент группы № Р3335
Направление подготовки: 15.03.06 – Мехатроника и робототехника
e-mail: L0lB0y1337@gmail.com

**Исхаков Мурат Ришатович**
Год рождения: 1997
Университет ИТМО, факультет систем управления и робототехники,
кафедра систем управления и информатики,
студент группы № Р3335
Направление подготовки: 15.03.06 – Мехатроника и робототехника
e-mail: mur1897@yandex.ru

**Бондаренко Владимир Андреевич**
Год рождения: 1997
Университет ИТМО, факультет систем управления и робототехники,
кафедра систем управления и информатики,
студент группы № Р3335
Направление подготовки: 15.03.06 – Мехатроника и робототехника
e-mail: MrBoxap@ya.ru

**Росина Яна Михайловна**
Год рождения: 1998
Университет ИТМО, факультет информационных технологий
и программирования, кафедра информационных систем,
студент группы № М3306
Направление подготовки: 09.03.02 – Информационные системы
и технологии
e-mail: rosina-yana98@mail.ru

**УДК 681.5**

## РАЗРАБОТКА СИСТЕМЫ УПРАВЛЕНИЯ МОБИЛЬНЫМ АВТОНОМНЫМ ЦЕНТРОМ ИССЛЕДОВАНИЯ ВОДНЫХ ГЛУБИН, ПРИМЕНЯЮЩИМ ТЕХНОЛОГИИ РОЕВОГО ИНТЕЛЛЕКТА

**Шокатаев А.С., Исхаков М.Р., Бондаренко В.А., Росина Я.М.**

В работе рассмотрена разработка системы управления глубоководным мобильным исследовательским комплексом, и описана структура данного комплекса.
**Ключевые слова:** глубоководный исследовательский центр, роевой интеллект, мультиагентный комплекс, система управления.

На сегодняшний день в сфере глубоководных исследований чаще используются управляемые необитаемые подводные аппараты (НПА), нежели автономные. Этот метод сильно ограничен, что негативно отражается на результатах проводимых работ. Однако во время подводных исследований необходимо работать с невероятно большими территориями,

для чего и уже существующие автономные необитаемые подводные аппараты (АНПА) оказываются недостаточными [1, 2].

Проведенный анализ современного рынка подводных исследований показал, что необходимо повысить надежность проводимых исследований, уменьшить затраты временных ресурсов и покрыть наибольшие подводные территории каждым исследованием. Таким образом, использование роевого интеллекта позволяет в значительной мере оптимизировать основные факторы, влияющие на исследования как в управляемых, так и в автономных НПА, используемых в настоящий момент в мире.

Составленная система включает в себя множество АНПА, именуемых юнитами. Юниты подразделяются на различные типы: юниты поиска, анализа, рабочие юниты, базовые юниты, количество которых варьируется в соответствии с поставленной задачей.

Разделение на виды обусловлено распределением задач, стоящих перед комплексом. Юнит поиска предназначен для проведения грубой оценки пространства на объекты исследования, юнит анализа – для обработки данных и отправки обработанного юнита рабочему, а последний, в свою очередь, выполняет более подробную оценку и необходимую в исследовании работу. База сохраняет всю информацию о проводимом исследовании и непрерывно получает информацию о собственных координатах.

Как видно на рисунке, база обменивается информацией как с рабочими юнитами, так и с юнитами анализа, которые, в свою очередь, связаны между собой, а последние осуществляют связь с юнитами поиска посредством гидроакустической передачи данных.

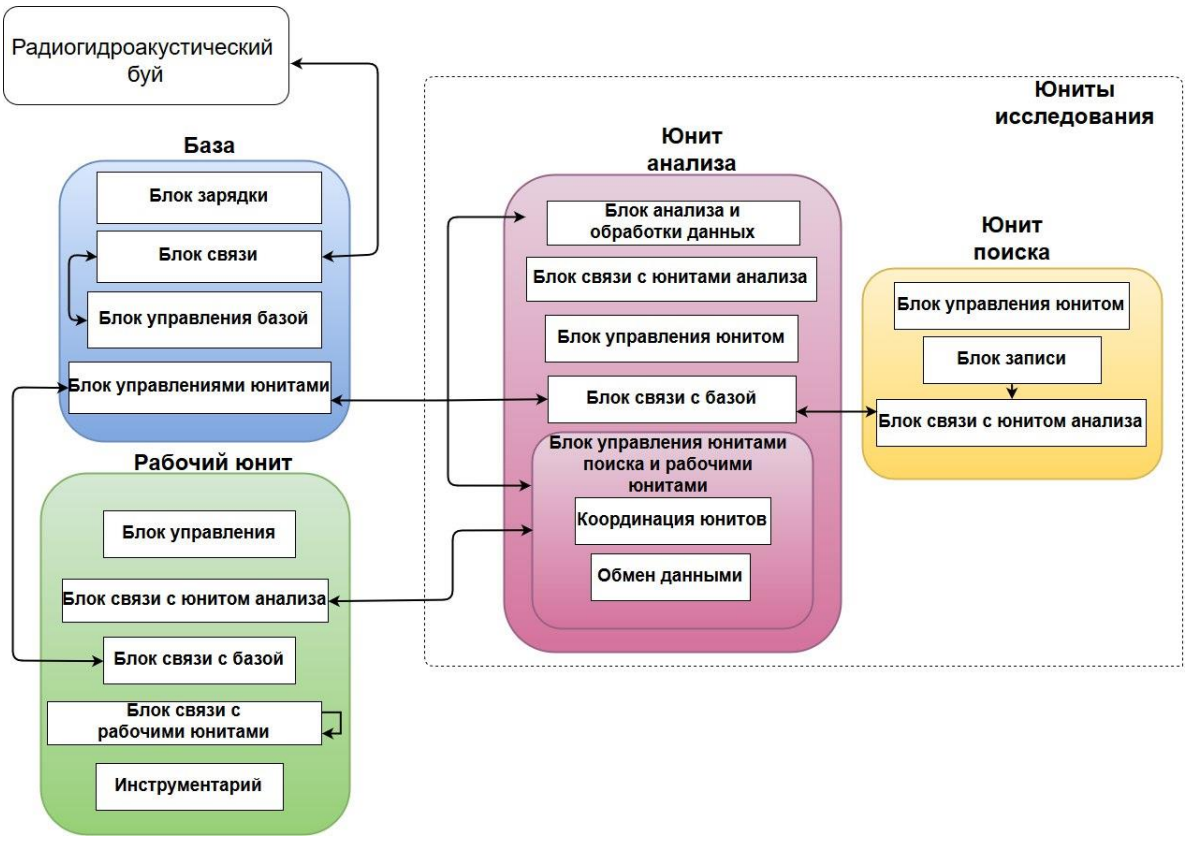



Рисунок. Функциональная схема комплекса

Каждый из юнитов снабжен двигательной системой и аккумуляторными блоками. Так же в каждом из них имеются блоки контроля внешней и внутренней среды, для отрицательной обратной связи и запусков экстренных протоколов при отказах систем соответственно.

После спуска комплекса выполняется расстыковка юнитов и начало исследования.

Каждый юнит поиска управляется юнитом анализа в целях оптимального исследования своего сегмента, записывая информацию в процессе движения до истощения заряда с расчетом на обратный путь, при наступлении которого возвращается к юниту анализа для оптического обмена данными и подзарядки. Фактически, юнит поиска осуществляет лишь грубую проверку на вероятность присутствия искомого объекта в пройденной области.

Юнит анализа выполняет четыре задачи:

- координацию областей исследования юнитов поиска;
- прием данных с юнитов поиска;
- анализ данных;
- формирование и передачу списка точек с использованием гидроакустики рабочему юниту.

Рабочие юниты, связываясь между собой, синхронизируют список точек и их потенциалов всех исследованных областей. Каждый из них высчитывает наиболее приоритетную для него точку, основываясь на ее потенциале и расстоянию между ними, после чего меняет статус точки на занятую и проводит ее полноценное изучение в зависимости от задачи.

База проводит зарядку юнитов анализа и рабочих по мере необходимости и удерживает свое положение в геометрическом центре местоположений юнитов. Также несет на себе все необходимое специфическое массивное оборудование и крепления для подъема различных объектов со дна.

Формула движения юнита анализа зависит от нескольких компонент, влияющих на вектор движения:

1. компонента свободы – смещает вектор движения в сторону неизученной области;
2. компонента рабочий-исследователь – смещает вектор движения в сторону рабочего тем сильнее, чем дальше данный юнит находится от ближайшего рабочего;
3. компонента анализ-анализ – смещает вектор движения в сторону оптимального расстояния до ближайшего юнита анализа.

Рабочие юниты используют модифицированный муравьиный алгоритм для нахождения оптимального пути к областям с высоким потенциалом. Они проходят оптимально через все вершины графа, построенного на данных с рабочих юнитов, и находят точку с наивысшим в данный момент потенциалом.

Предложенный комплекс решает задачу автоматизации глубоководных исследований, использование технологий роевого интеллекта позволяет изучать одновременно значительные области дна, что в сравнении с используемыми к 2018 году продуктами значительно оптимизирует этот процесс.

**Литература**

1. Сахопотинов Г.А. Исследование местности с помощью группы роботов, управляемых алгоритмом роевого интеллекта [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/issledovanie-mestnosti-s-pomoschyu-gruppy-robotov-upravlyaemyh-algoritmom-roevogo-intellekta (дата обращения: 28.03.2018).
2. Сахопотинов Г.А., Сыркин И.С. Проблемы практического применения роевого интеллекта и построение устойчивых управляемых групп роботов [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/problemy-prakticheskogo-primeneniya-roevogo-intellekta-i-postroenie-ustoychivyh-upravlyaemyh-grupp-robotov, своб.

**Абрамов Лев Олегович**
Год рождения: 1993
Университет ИТМО, факультет систем управления и робототехники, кафедра технологии приборостроения, студент группы № Р4277
Направление подготовки: 12.04.01 – Приборостроение
e-mail: lewabramov@yandex.ru

**Андреев Юрий Сергеевич**
Год рождения: 1984
Университет ИТМО, факультет систем управления и робототехники, кафедра технологии приборостроения, к.т.н., доцент
e-mail: ysandreev@corp.ifmo.ru

**УДК 681.518.5**

# АВТОМАТИЗАЦИЯ ПРОЦЕССА КОНТРОЛЯ ПРОИЗВОДСТВЕННОГО ОБОРУДОВАНИЯ И ДЕЯТЕЛЬНОСТИ ПЕРСОНАЛА ПРИ ПОМОЩИ МОБИЛЬНОГО УСТРОЙСТВА

**Абрамов Л.О., Андреев Ю.С.**
**Научный руководитель – к.т.н., доцент Андреев Ю.С.**

В работе рассмотрены причины появления систем автоматизации контроля производственного оборудования и деятельности персонала, проанализированы преимущества и недостатки веб-ориентированного варианта исполнения подобных систем, исследованы варианты их усовершенствования при помощи использования мобильных устройств, а также создано мобильное приложение для осуществления контроля производственного оборудования и деятельности персонала.
**Ключевые слова:** информационная система, облачные технологии, киберфизические системы, мониторинг, мобильные технологии.

Развитие цифровых технологий в области производства оказывает большое влияние на различные этапы изготовления конечного продукта [1]. Внедрение компьютерных систем, высокопроизводительного оборудования, большого количества датчиков требует создания нового подхода к управлению предприятием. В связи с этим остро встают вопросы мониторинга за всеми этапами производственного процесса. Одним из решений является внедрение информационных систем, позволяющих проводить статистический анализ причин некорректной работы оборудования, выявлять причины его поломок, ускорять процесс взаимодействия между сотрудниками предприятий, повышая эффективность производства [2]. Одним из вариантов решения данной задачи становится создание единой информационно-технологической платформы цифрового производства. Такая платформа должна обладать: возможностью получения доступа, хранения и обработки данных в режиме реального времени 24 ч в сутки 7 дней в неделю, возможностью построения графов и логических выводов. Кроме того, организация такой платформы требует максимальной гибкости программного обеспечения, которое позволит сократить расходы и повысит конкурентоспособность продукта. Одним из существующих решений на рынке является web-ориентированная платформа «Winnum SDK» [3]. На базе производственного полигона

кафедры ТПС Университета ИТМО была развернута данная система (рис. 1) и проанализированы все ее преимущества и недостатки [4].

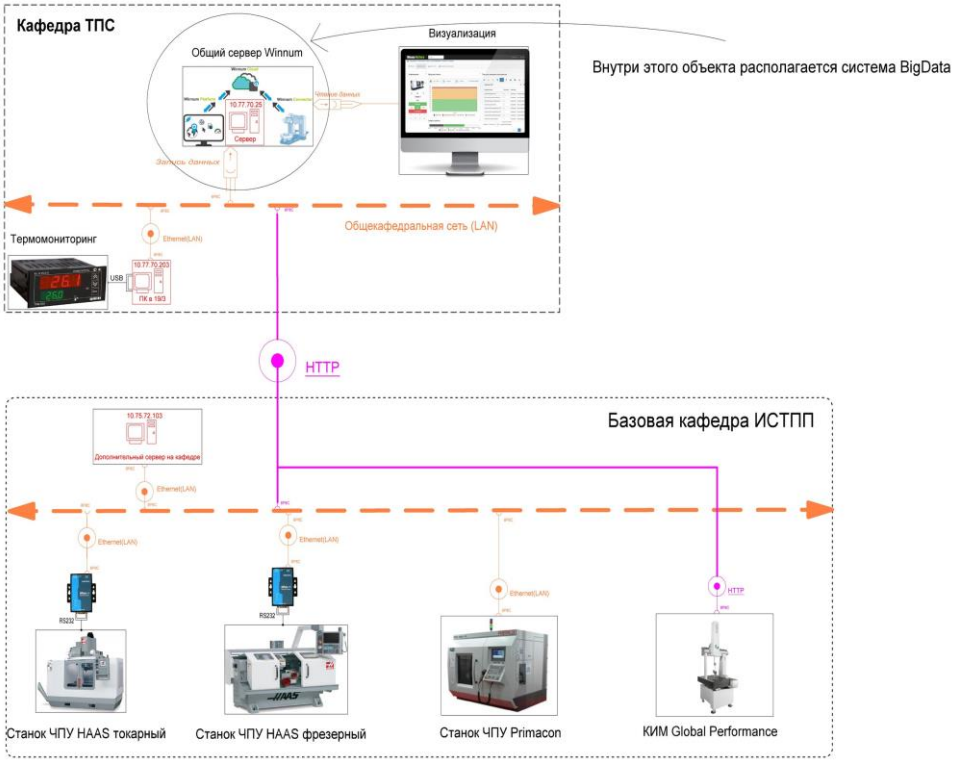
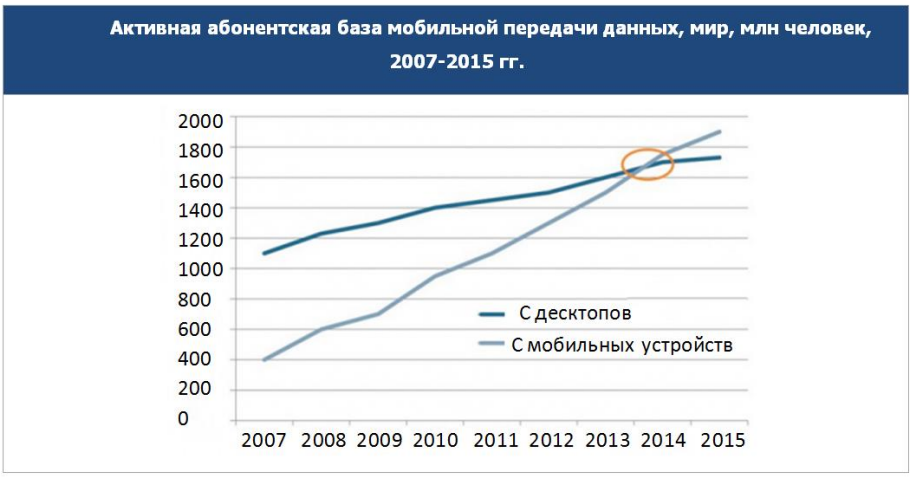



Рис. 1. Информационно-технологическая платформа, развернутая на базе полигона кафедры

Система «Winnum» является модульной и состоит из трех частей: хранилище, «облако» и платформа [5]. Самым главным компонентом системы является «облако» данных, куда поступает и в дальнейшем обрабатывается вся информация. Для взаимодействия с «облаком» необходимо наличие универсального программного обеспечения, позволяющего вести запись и производить считывание данных. Основной проблемой является то, что каждый из видов оборудования имеет собственный протокол взаимодействия с оборудованием, вследствие чего можно говорить лишь о частичной универсальности программного обеспечения. Хранилище системы «Winnum», как было описано выше, выполнено в форме нереляционной базы данных. Данная платформа обеспечивает взаимодействие с данными и позволяет делать анализ, выгружать данных, строить графики. Отдельным преимуществом данной платформы является возможность написания и запуска диагностических алгоритмов для любого вида оборудования.

Однако, как и у любой системы, у «Winnum» есть свои недостатки. Реализация информационно-технологической платформы в виде web-ориентированного приложения, где доступ к информации осуществляется через браузер с любого устройства, имеющего выход в Интернет, является универсальным, но не всегда удобным с точки зрения конечного пользователя. Основными недостатками приложения «Winnum Platform» является невозможность преобразования интерфейса под нужды пользователя, интуитивно непонятный интерфейс, отсутствие быстрого доступа к необходимым опциям анализа и информации. Кроме того, как показали исследования, скорость доступа к конечной информации крайне важна для конечного пользователя, особенно в условиях производства, что требует выдачи на первом этапе лишь наиболее необходимой информации с возможностью дальнейшего уточнения. Данное условие несет за собой и требование в разграничении ролей пользователей приложения, так как потребности разных звеньев управления предприятием различны.

Вышеописанные проблемы можно решить путем написания уникального мобильного приложения. Кроме того, на статистическом графике (рис. 2) видно, что развитие мобильных гаджетов уже на рубеже 2013–2014 годов позволило превысить абонентскую базу, использующих мобильные гаджеты вместо десктопных компьютеров для использования сети Интернет, в связи с этим было принято решение о создании приложения для мобильной платформы.




*Источник: comScore, 2014г.*

Рис. 2. Статистика использования мобильных устройств в сравнении с десктопными

Данное приложение должно иметь полную связь с платформой, но в то же время хранить часть данных в памяти устройства, позволяя пользователю работать с некоторыми функциями приложения без использования сети Интернет. Также подобное приложение должно иметь возможность загрузки в фоновом режиме некоторых данных, позволяя пользователю работать с уже сформированными аналитическими диаграммами и отчетами, без необходимости ожидания формирования и загрузки последних, обеспечивая высокую скорость доступа к конечной информации. Еще одним важным преимуществом приложения может стать разграничение ролей пользователей приложения, что позволяет каждому звену работников видеть наиболее актуальную информацию для них. Так, например, наладчику, работающему со станками числового программного управления важна информация по каждому из станков, в то время как административному персоналу важна лишь сводная информация по производству.

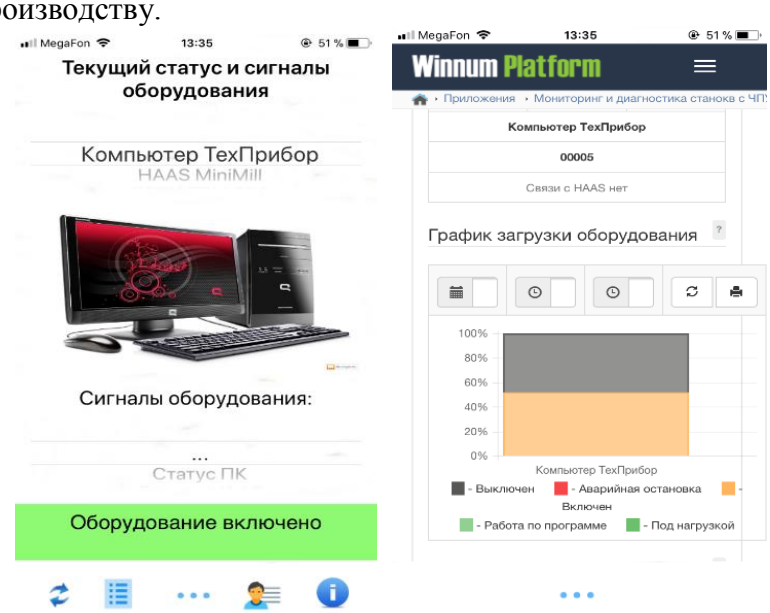



Рис. 3. Мобильное приложение на базе IoS

Программное обеспечение было написано на базе IoS (рис. 3), в котором есть возможность выбрать интересующее оборудование из списка, узнать статус и значение сигналов, быстро построить график загрузки за текущий день, получить инструкцию и описание к выбранному оборудованию, а также связаться с ответственным сотрудником прямо из приложения.

К сожалению, подход к созданию автоматизированной процесса контроля производственного оборудования и деятельности персонала с использованием интегрированной связки мобильного приложения и web-ориентированной платформы имеет свои недостатки. Основным недостатком является необходимость компиляции и переустановки мобильных приложений, что может потребовать от пользователя определенных навыков, кроме того, создание мобильного приложения требует высокой квалификации работников, что влечет за собой финансовые затраты.

В результате данной работы была исследована и создана интегрированная система автоматизации контроля производственного оборудования и деятельности персонала при помощи мобильного устройства, на базе информационно-технологической платформы цифрового производства испытательного полигона Университета ИТМО кафедры ТПС.

**Литература**

1. Козлецов А.П., Решетников И.С. Сбор данных в MES-системах. Основные подходы. – Автоматизация производства // Рациональное управление предприятием. – 2013. – № 1. – – С. 74–76.
2. СМИ PLM Эксперт. Инновации в промышленности // Журнал PLM Эксперт. – 2017. – С. 38–43.
3. Куркова Ю., Васильев А., Ловыгин А., Степанов В. Системы мониторинга станков с ЧПУ в России. Обзор технологий и рынка за 2016 г. // Планета CAM. – 2017. – С. 62–104.
4. Абрамов Л.О. Исследование и создание системы мониторинга параметров технологического оборудования с применением облачного программного обеспечения и нереляционных баз данных // Альманах научных работ молодых ученых Университета ИТМО. – 2017. – Т. 5. – С. 4–7.
5. Signum Winnum CNC 2.4. Удаленный мониторинг изделий // Учебный курс. – 2017. – С. 1–50.

**Гибадуллин Ильсур Наилевич**
Год рождения: 1993
Университет ИТМО, факультет систем управления и робототехники, кафедра технологии приборостроения, аспирант
Направление подготовки: 12.06.01 – Фотоника, приборостроение, оптические и биотехнические системы и технологии
e-mail: gibadullinilsur@mail.ru

**УДК 621.81.004.17**

# ИССЛЕДОВАНИЕ ПРИМЕНИМОСТИ ПРОФИЛЕЙ ПОВЕРХНОСТЕЙ В КАЧЕСТВЕ КРИТЕРИЯ ОЦЕНКИ ШЕРОХОВАТОСТИ ПОВЕРХНОСТЕЙ ДЕТАЛЕЙ ПРИБОРОВ

**Гибадуллин И.Н.**
**Научный руководитель – д.т.н., профессор Валетов В.А.**

Работа выполнена в рамках темы НИР № 615863 «Научные основы создания цифрового производства в приборостроении».

Рассмотрены проблемы профильной оценки шероховатости поверхности. Представлен метод оценки и контроля шероховатости, использующий в качестве критерия изображения профилей поверхностей. Для этого было разработано специальное программное обеспечение, позволяющее качественно оценить степень схожести профилей исследуемых поверхностей. Было проведено исследование применимости разработанной методики на реальных поверхностях, полученных различными методами обработки, результаты которого приведены в данной работе.
**Ключевые слова:** шероховатость, профиль поверхности, критерий оценки, графические критерии, контроль поверхности.

В семидесятых годах XX века В.А. Валетовым впервые был предложен новый метод оценки и контроля микрогеометрии поверхностей деталей, который был назван непараметрическим. Сущность метода заключается в использовании в качестве критериев оценки и контроля микрогеометрии поверхностей деталей графических изображений различных функций. В менее «ответственных» случаях это могут быть графики опорных кривых (кривых Аббота) и функций распределения ординат или тангенсов углов наклона профилей, а для более точной оценки и контроля – графики плотности распределения ординат и тангенсов углов наклона профилей. Но наиболее точной оценки можно достичь, если в качестве критериев использовать графики самих профилей, так как наибольшей информацией о профиле обладает сама профилограмма [1, 2].

Методика контроля микрогеометрии, использующая в качестве критерия профили поверхностей, выглядит следующим образом. Исследователь выбирает реальную поверхность изделия (эталон), микрогеометрия которой была признана наилучшей из возможных в процессе испытаний для нужного функционального свойства, а соответствующий профиль этой микрогеометрии принимается в качестве эталона, с которым производится сравнение контролируемой серийной продукции. При этом для эталонного профиля предварительно задается поле допуска. Величина поля допуска выбирается в зависимости от назначения и ответственности поверхности контролируемого изделия [3].

Для оценки микрогеометрии поверхности ее сначала получают, производя измерение профиля поверхности с помощью специальных приборов – профилометров. Они работают по принципу ощупывания исследуемой поверхности алмазной иглой индукционного датчика. При протаскивании этой иглы по поверхности она повторяет все выступы и впадины, которые способна уловить. Полученный таким образом профиль, как правило, сохраняется

на компьютере в виде файла, описывающего профиль поверхности. Данный файл в общем случае будет содержать информацию об ординатах профиля и соответствующих им абсциссах, записанных с определенным шагом.

Для сравнения контролируемого профиля с эталонным, согласно разработанной методике, необходимо выполнение трех условий:

– контролируемый профиль должен быть длиннее эталонного;
– сравниваемые профили должны быть отфильтрованы, для исключения из профиля таких факторов, как помехи, погрешность установки и волнистость;
– контролируемый и эталонный профили должны иметь равные шаги снятия точек по оси абсцисс.

Для быстрого, надежного и недорогого контроля микрогеометрии поверхностей при помощи сравнения их профилей была разработана программа для платформы .NET Framework 4.5 в среде разработки Microsoft Visual Studio 2015 Comunity на языке C#. Для отображения профилей исследуемых поверхностей используется ZedGraph версии 5.1.5.

Метод сравнения основан на поиске наибольшего совпадения ординат контролируемого профиля с ординатами эталонного профиля. Сравнение производится по алгоритму, представленному на рис. 1.

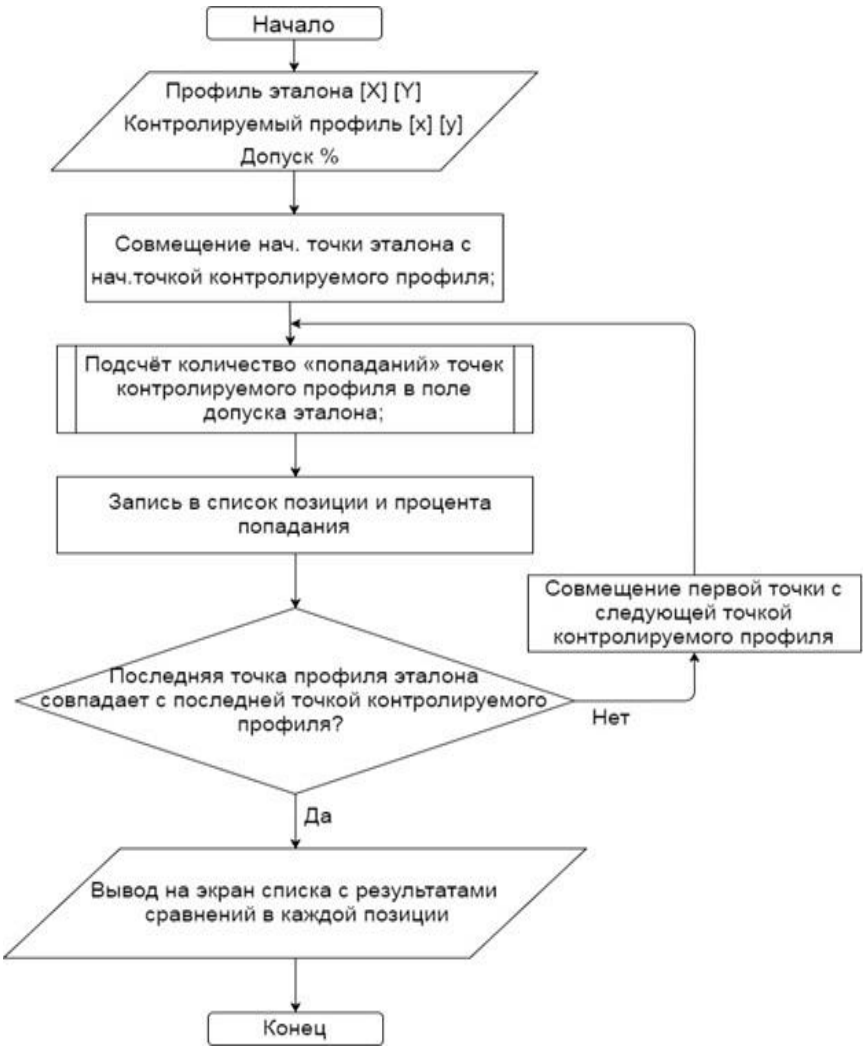



Рис. 1. Алгоритм сравнения профилей

Согласно данному алгоритму, на вход поступают координаты точек профиля эталона, контролируемого профиля и значение допуска (в процентах). Затем начальная точка профиля эталона совмещается с первой точкой контролируемого профиля. В этой позиции

подсчитывается количество «попаданий» точек контролируемого профиля в поле допуска эталона. После этого в список записывается данная позиция и процент «попаданий» контролируемого профиля в поле допуска эталона. Следующим шагом идет совмещение первой точки эталона со следующей (*i*-ой) точкой контролируемого профиля. Эти операции повторяются до тех пор, пока последняя точка эталона не совпадет с последней точкой контролируемого профиля. После окончания цикла на экран выводится список с позициями сравнения и соответствующими им процентами совпадений.

Результат сравнений для каждой позиции выводится на экран в виде выпадающего списка. Выбирая определенные позиции в этом списке, можно вывести на экран сравниваемые профили, расположенные в соответствии с выбранной позицией (рис. 2).

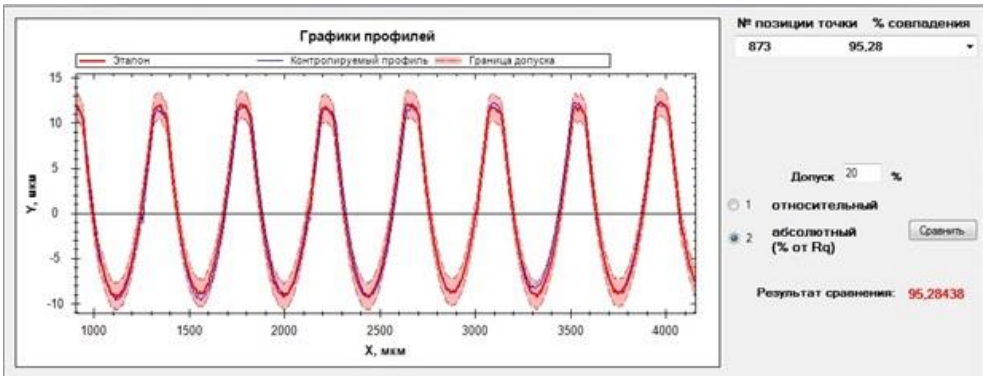



Рис. 2. Выводимый результат сравнения профилей

Для проверки выдвинутой гипотезы о применении профилей исследуемых поверхностей в качестве графических критериев и разработанного программного обеспечения (ПО) было проведено исследование по сравнению профилей поверхностей, полученных гидроабразивной обработкой.

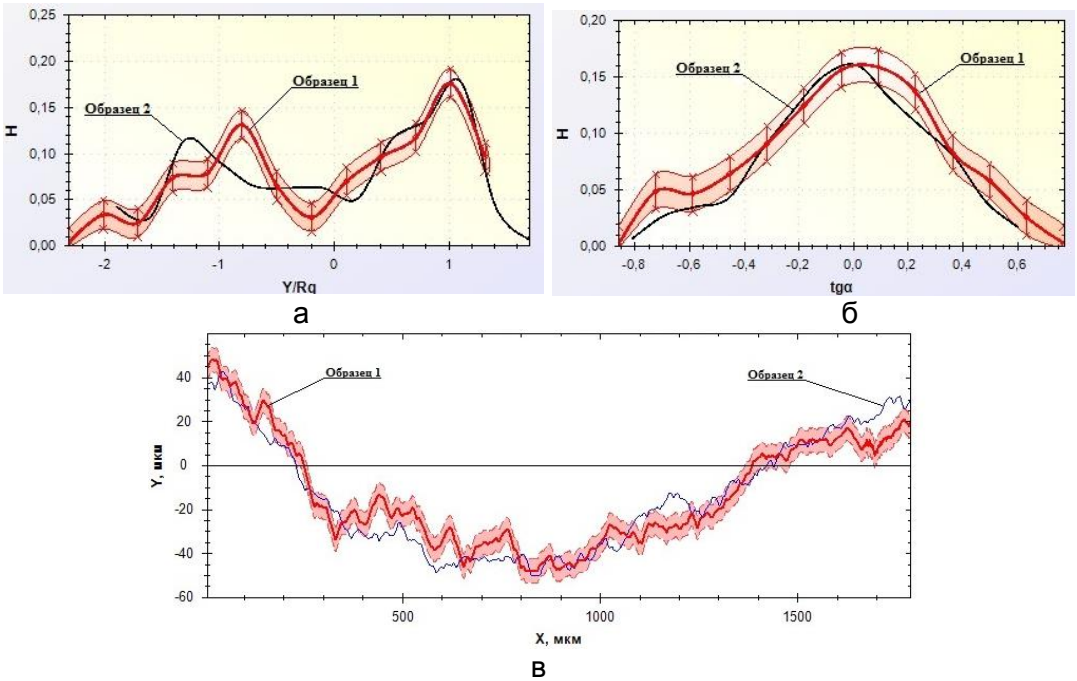



Рис. 3. Сравнение графических критериев образцов, полученных гидроабразивной обработкой: график плотности распределения ординат профиля: *H* – отношение количества ординат данной величины к общему количеству; *Y* – ординаты профиля; *Rq* – среднеквадратическое отклонение ординат исходного профиля (а); график плотности распределения тангенсов местных углов наклона профиля (б); график сравнения профилей поверхностей образцов (в)

Рассмотрим образцы поверхности, полученные гидроабразивной резкой. В качестве материала образцов использовалась нержавеющая сталь 12Х18Н10Т. Было изготовлено два образца по одной технологии. Измеренные параметры шероховатости: для образца №1 – $Ra$=3,77 мкм; для образца №2 – $Ra$=3,76 мкм. На рис. 3, а, б, представлены графические критерии, полученные с помощью программы «Лемминг», на рис. 3, в, представлен график сравнения профилей поверхностей образцов, полученный с помощью ПО, разработанной автором. Для эталонного критерия было выбрано поле допуска соответствующее 20% от среднего значения ординат графика ($H_{\text{ср}}$). Для эталонного профиля выбрано поле допуска соответствующее 20% от среднеквадратичного отклонения профиля ($Rq$). В результате сравнения профилей разработанной программой установлено, что при выбранном поле допуска профили совпадают лишь на 42,38%.

Графические изображения различных функций несут в себе гораздо больше информации, чем любой из нормируемых параметров. Отсюда целесообразно использовать для оценки и контроля профиля поверхности различных его статистических представлений.

В данной работе проведены исследования возможности использования в качестве критерия оценки и контроля микрогеометрии графическое изображение самого профиля, что делается впервые. Исследования показали, что этот путь требует дополнительного изучения и нахождения более удобных методов сравнения профилей. В то же время проведенные исследования выявили очень существенные недостатки профильной оценки микрогеометрии вообще, что делает невозможным на данном этапе использование изображения профиля исследуемой поверхности в качестве графического критерия оценки шероховатости поверхности. Причина этого заключается в том, что профиль поверхности является реализацией случайной функции, и вероятность его точного повторения у двух разных поверхностей пренебрежимо мала. По этой причине оказалось более эффективным использовать в качестве критериев не сам профиль, а различные его статистические характеристики (плотности или функции распределения). Однако проведенные исследования показали, что для качественного сравнения профилей разработанные методики показали практически приемлемый результат. К тому же разработанные методики позволяют сравнивать профили не субъективно, а с помощью приборов, и притом автоматизированно при помощи разработанной программы.

**Литература**

1. Валетов В.А., Иванов А.Ю. Микрогеометрия поверхностей деталей и их функциональные свойства // Изв. вузов. Приборостроение. – 2010. – Т. 53. – № 8. – С. 6–11.
2. Валетов В.А., Филимонова Е.А. Программа оценки и контроля шероховатости поверхностей деталей на основе их микротопографий // Технологии упрочнения, нанесения покрытий и ремонта: теория и практика: материалы 15-й Международной научно-практической конференции. – 2013. – Т. 1. – С. 245–247.
3. Валетов В.А. Проблемы оптимизации микрогеометрии поверхностей деталей для обеспечения их конкретных функциональных свойств // Изв. вузов. Приборостроение. – 2015. – Т. 58. – № 4. – С. 250–267.

**Дроздов Александр Геннадьевич**
Год рождения: 1994
Университет ИТМО, факультет систем управления и робототехники, кафедра технологии приборостроения, аспирант
Направление подготовки: 12.06.01 – Фотоника, приборостроение, оптические и биотехнические системы и технологии
e-mail: aleksd@corp.ifmo.ru

**УДК 62.07**

# ПОСТРОЕНИЕ ИМИТАЦИОННОЙ МОДЕЛИ РОБОТИЗИРОВАННОЙ ПРОИЗВОДСТВЕННОЙ ЯЧЕЙКИ В 3DEXPERIENCE

**Дроздов А.Г.**
**Научный руководитель – к.т.н., доцент Яблочников Е.И.**

В работе описана методика создания имитационной модели роботизированной производственной ячейки. Разработка модели ячейки производилась в рамках лаборатории кафедры ТПС Университета ИТМО в модулях CATIA и DELMIA системы 3DEXPERIENCE. Описано выбранное оборудование, рассчитаны геометрические и временные параметры производственной ячейки, составлен технологический процесс литья полимерных изделий, выполнено объединение элементов производства на основе I/O контроллеров, получены данные по расчету производительности.
**Ключевые слова:** роботизированная производственная ячейка, имитационное моделирование, 3DEXPERIENCE, DELMIA, ТПА.

Имитационное моделирование в наше время становится все более популярным методом исследования реального производства. Многие современные предприятия используют имитационные модели для определения большого количества параметров при изготовлении изделий, что позволяет оценить все плюсы и минусы, риски, экономические и временные затраты в реальном производстве.

Целью работы являлось создание модели роботизированной производственной ячейки (РПЯ) и расчет ее производительности. Актуальность темы подтверждается тем, что в настоящее время множество предприятий используют данную технологию, позволяющую решить организационные аспекты производства, используя как итоговый результат графики параметров работы производственной линии. Данная работа показала не только математические расчеты, но и визуальную составляющую.

На основе проведенного анализа видов имитационного моделирования был выделен наиболее подходящий для данной работы метод дискретно-событийного моделирования. С помощью него проводится моделирование производственных процессов ячейки литьевого участка в системе 3DEXPERIENCE [1].

В лаборатории кафедры ТПС Университета ИТМО изначально располагался только термопластавтомат (ТПА) фирмы Ferromatic Milacron Electra Evolution EE30-55. Остальное необходимое оборудование для имитации роботизированного производства отсутствовало. В данной работе для достижения итоговых результатов имитационного моделирования требовалось выполнить следующий список задач:

1. выбрать необходимые элементы для построения роботизированной производственной ячейки;
2. смоделировать элементы роботизированной ячейки;
3. расположить оборудование, учитывая геометрическое положение помещения, взяв во внимание план литьевого участка, где будет находиться роботизированная производственная ячейка;

4. составить временные циклы, включающие параметры: впрыск, выдержка под давлением, охлаждение, движение литьевой формы, извлечение, также время движения роботов, систем перемещения и отрезки литников на лазерном станке;
5. на основе созданной 3D-модели выполнить имитационное моделирование.

На первом этапе в качестве исходных данных для моделирования выступает информация о составе располагающегося оборудования: ТПА, роботы, столы, схваты, лазерный станок, системы перемещения, программируемый логический контроллер (ПЛК). Также к исходным данным относятся 3D-модели отдельных станков и технологической оснастки, роботов и других устройств автоматизации и механизации.

На втором этапе были определены виртуальные контроллеры для каждого исполнительного устройства. Затем была организована связь между ними на уровне входных и выходных (Input/Output или I/O) сигналов. Посылаемые между устройствами команды сообщают каждому элементу РПЯ, в какой момент следует выполнять требуемую операцию, достигая, таким образом, совместное взаимодействие при выполнении имитационного моделирования процесса работы участка.

На третьем этапе были смоделированы основные и вспомогательные операции для отдельных устройств, такие как литье полимера, извлечение из формы и перемещения роботами полученной отливки, обработка на станке лазерной резки (с целью удаления литниковой системы), передвижение по системе перемещения и т.д. Для обеспечения синхронной работы и своевременного выполнения задач несколькими устройствами в программу каждой отдельной задачи были введены переменные, инициирующие или останавливающие движение исполнительных устройств.

На четвертом этапе была построена общая модель технологического процесса с применением инструментов имитационного моделирования системы DELMIA 3DEXPERIENCE. Временные параметры технологических операций и циклов были получены с помощью моделирования процесса литья в CAE-системе Moldex3D на операционном уровне [2]. На рисунке можно увидеть выполненную модель роботизированной производственной ячейки.

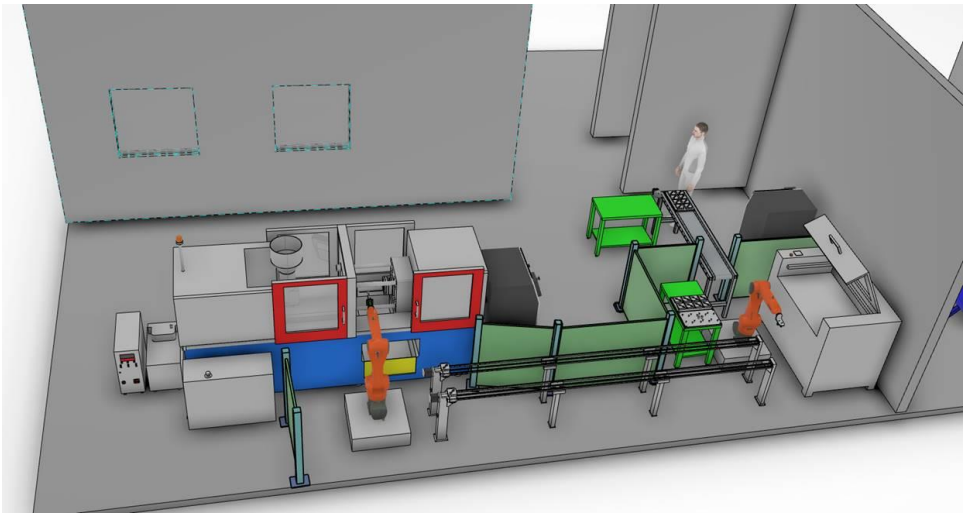


Рисунок. Итоговая версия роботизированной производственной ячейки

Результатов имитационного моделирования следующий:

1. четырехмерная (3D+время) модель автоматизированного участка полимерного литья;
2. управляющие программы для промышленных роботов;
3. алгоритм взаимодействия оборудования;
4. модели технологической оснастки;
5. определение и оптимизация времени производственного цикла;
6. расчет производительности автоматизированного литьевого участка [3].

На основании выполненной работы были получены следующие данные по имитационному моделированию РПЯ за восьмичасовой рабочий день: диаграмма Ганта, показывающая такты циклов всех операций, произведенных за период работы на литьевом участке; среднее время изготовления одной отливки; степень загруженности элементов ячейки в процентах. Навыки, накопленные за время работы с проектом, будут использованы для улучшения данного прототипа производства, а также перехода в более сложную форму представления виртуального производства, когда используются технологии построения «цифровых двойников» [4].

**Литература**

1. Официальный сайт разработчика программы 3DEXPERIENCE [Электронный ресурс]. – Режим доступа: http://3ds.com, своб.
2. Yablochnikov E., Pirogov A., Vasilkov S., Andreev Y. and Demkovich N. Developing and modeling production processes for manufacturing polymeric optical items in a distributed integrated medium // Journal of Optical Technology. – 2017. – V. 84. – № 1. – P. 52.
3. Абаев Г.Е., Яблочников Е.И., Демкович Н.А. Роль и задачи имитационного моделирования на этапе перехода от цифрового производства к «умным фабрикам» // VIII всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности «имитационное моделирование. Теория и практика». – 2017. – С. 74.
4. Толуев Ю.И. Задачи имитационного моделирования при реализации концепции индустрия 4.0 в сфере производства и логистики // VIII всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности «имитационное моделирование. Теория и практика». – 2017. – С. 57–65.

**Звонарев Олег Владимирович**
Год рождения: 1987
Университет ИТМО, факультет систем управления и робототехники, кафедра технологии приборостроения, аспирант
Направление подготовки: 09.06.01 – Информатика и вычислительная техника
e-mail: ovzvonarev@corp.ifmo.ru

**УДК 658.511.3**

# УПРАВЛЕНИЕ ТРЕБОВАНИЯМИ НА РАННИХ ЭТАПАХ ПРОЦЕССА ПРОЕКТИРОВАНИЯ ВЫСОКОТЕХНОЛОГИЧНЫХ ИЗДЕЛИЙ

**Звонарев О.В.**
**Научный руководитель – к.т.н., доцент Яблочников Е.И.**

В работе рассмотрены вопросы автоматизации ранних этапов разработки высокотехнологичных изделий. Рассмотрено применение систем управления требованиями и жизненным циклом изделий. Обоснована целесообразность применения инженерии требований на всем протяжении процесса проектирования и производства. Проведен анализ источников требований, выявлены аспекты, требующие первоочередной проработки для формирования методик построения базы знаний системы управления источниками требований. Сформулированы направления дальнейшей работы по данной тематике.

**Ключевые слова:** инженерия требований, источники требований, реинжиниринг, система автоматизированного проектирования, система управления требованиями.

Современное развитие человечества в области создания объектов новой техники невозможно представить без использования автоматизированных систем проектирования (САПР). За последние годы расширение функциональных возможностей и увеличение производительности САПР привело к существенным изменениям в технологии проектирования и производства в приборостроении, авиастроении, ракетно-космической промышленности и других наукоемких отраслях. Можно выделить следующие тенденции:
- представление конструкторской и технологической документации в электронном виде;
- переход на электронное межкорпоративное взаимодействие;
- увеличение роли электронной структуры изделия (ЭСИ);
- перевод эксплуатационной и ремонтной документации в интерактивную форму.

Возрастающая наукоемкость создаваемых изделий, территориальное распределение производства, усиливающаяся конкуренция и повсеместная фрагментарная автоматизация процессов проектирования диктуют необходимость выработки комплексного подхода в организации процесса. Основная задача исследования сводится к применению концепции управления требованиями в процессе проектирования высокотехнологичных изделий и разработке на ее основе методик и средств проектирования, что должно привести к повышению качества конструкторской, технологической и программной документации.

С точки зрения управления требованиями для процесса проектирования высокотехнологичных изделий следует выделить следующие особенности:
- множество изменений требований из-за длительности процесса;
- постоянные уточнения требований из-за многоэтапности;
- сложность взаимоувязки и актуализации требований из-за разделения проекта на составные части с различными исполнителями;
- целесообразность хранения данных об изделии и совокупности требований для повторного использования.

За последние годы в конструкторских организациях были успешно внедрены системы управления данными об изделии (Product Data Management, PDM), системы управления ресурсами, сформированы различные электронные информационные справочники. Неотъемлемой частью процесса проектирования стали средства 2D- и 3D-моделирования и системы инженерных расчетов. Однако вопрос автоматизации ранних этапов процесса проектирования, к которым относятся этапы выявления потребностей и установки требований к изделию, до сих пор остается актуальным. Включение данных этапов в единую автоматизированную цепочку требует внедрения системы управления требованиями (СУТ) в общее информационное пространство и реинжиниринг процесса проектирования в целом.

Работа с требованиями является важным компонентом любой инженерной деятельности. Одна из наиболее часто допускаемых ошибок состоит в том, что управление требованиями считают обособленным процессом, который осуществляется и завершается на ранних этапах проектирования изделия. На самом деле управление требованиями или инженерия требований проходит через весь цикл разработки изделия и подразумевает широкий спектр различных действий, таких как выявление, анализ, разработка, изменение и верификация требований [1]. За процесс разработки изделия отвечает система управления жизненным циклом изделия (PLM-системы). Автономное применение СУТ без привязки к электронной структуре изделия является малоэффективным, поэтому следует рассматривать СУТ исключительно в составе PLM-системы. В настоящее время существует множество отдельных СУТ и PLM-систем, а комплексные решения представлены в единичных экземплярах [2].

Качество документации зависит от ее технического и информативного содержания, а также физического состояния. Техническое содержание документации определяется структурой, устройством и принципом работы изделия, внутренними и внешними связями его функциональных частей, устанавливает требования к техническому уровню и качеству изделия. Информативное содержание заключается в описании принятых технических решений единым техническим языком с применением норм ЕСКД. Физическое состояние определяется пригодностью для хранения и обращения. С развитием САПР и технологии электронного документооборота факторы информативного содержания и физического состояния оказывают все меньшее влияние на качество документации. Повышение качества в части технического содержания документации можно достигнуть за счет эффективного использования механизма управления требованиями в процессе проектирования. Качество конструкторской документации в конечном итоге проверяется производством и эксплуатацией изделия, что подтверждает необходимость интеграции процессов проектирования и производства в разрезе СУТ.

Ранние этапы процесса проектирования отличаются высокой динамичностью изменения требований и служат источником наибольших рисков, связанных с концептуальным определением изделия, и поэтому представляют особый интерес для проводимого исследования. В ходе анализа процесса управления требованиями на ранних этапах проектирования выявлены аспекты, не нашедшие отражения в существующих программных решениях:

- отсутствие интеграции СУТ с источниками требований;
- неадаптированность методологии управления требованиями под реальные процессы проектирования.

В рамках исследования для решения перечисленных аспектов сформулированы первоочередные задачи:

- систематизация источников требований;
- построение модели зависимости «ЭСИ – требования – источники требований»;
- проектирование структуры базы знаний для управления требованиями.

Среди источников требований можно выделить техническое задание и договорные документы на создание изделия, нормативно-правовые акты (федеральные законы,

постановления по отрасли), внутренние и внешние нормативные документы (ГОСТ, ОСТ, документы системы менеджмента качества, ограничительные перечни материалов, стандартных и прочих изделий и т.д.). Источники требований нестатичны, появляются новые технологии, заказчик изменяет свои требования, меняется законодательство и вопросы технического регулирования и выявляются ошибочные требования, заявленные ранее [3]. Изменения могут произойти в любой точке жизненного цикла изделия, поэтому необходимо контролировать изменение источников требований. Здесь становятся важными вопросы актуализации, преемственности и противоречивости источников требований. Возможным решением данных вопросов является создание системы связей между требованиями и конкретными элементами содержимого источников требований.

В рамках исследования предлагается представление источника в виде структуры элементов (разделы, абзацы, участки текста и т.д.), внутренние связи элементов внутри источника и внешние связи между элементами различных источников. Например, на одном из поздних этапов проектирования выявилась коллизия требований. С помощью модели зависимости «ЭСИ – требования – источники требований» возможно автоматическое выявление источников коллизии и выработка рекомендаций по разрешению конфликта.

Другим прорабатываемым вопросом является построение базы знаний, содержащей информацию как о структуре изделия, так и о связанных требованиях. Это позволит всесторонне оценить последствия каждого отдельного изменения требования на процесс разработки документации на изделие. Например, при использовании имеющегося задела в новых разработках, база знаний позволит выявить неактуальные требования через связанные с ними источники и предложит необходимые корректировки для заимствования.

На основании затронутых выше аспектов следует более детально рассмотреть источники требований. Разработка базы знаний источников требований и выработка методик управления источниками видится наиболее перспективным решением. Кроме того, выявлена необходимость реинжиниринга существующих процессов разработки конструкторской, программной и технологической документации под эффективное применение концепции управления требованиями на всех стадиях жизненного цикла изделия.

**Литература**

1. Халл Э., Джексон К., Дик Д. Инженерия требований. – М.: ДМК Пресс, 2017. – 224 с.
2. Яблочников Е.И., Фомина Ю.Н., Саломатина А.А. Компьютерные технологии в жизненном цикле изделия. Учебное пособие. – СПб.: СПбГУ ИТМО, 2010. – 188 с.
3. Брук П.А. Решения Dassault Systemes для управления требованиями // Рациональное Управление Предприятием. – 2014. – № 4 – Р. 20–22.

**Киприянов Кирилл Васильевич**
Год рождения: 1987
Университет ИТМО, факультет систем управления и робототехники,
кафедра технологии приборостроения
e-mail: 142739@niuitmo.ru

**УДК 65.011.56:621:9**

# АЛГОРИТМЫ ОПЕРАТИВНОГО ПЛАНИРОВАНИЯ В ПРОИЗВОДСТВЕННОЙ МНОГОАГЕНТНОЙ СИСТЕМЕ

**Киприянов К.В.**

В работе рассмотрена производственная многоагентная система и алгоритмы, позволяющие реализовать централизованный, децентрализованный и смешанный подходы к оперативному планированию.
**Ключевые слова:** планирование, многоагентная система, цифровизация, информатизация, киберфизический, производство.

**Введение.** Оперативное планирование связано с непосредственным выпуском продукции и заключается в определении исполнителей и времени выполнения для операций и процессов. Данный вид планирования выполняется различными методами, позволяющими получать оперативные планы различной степени точности. Чем достовернее используемая информация, тем достовернее полученные планы, поэтому к планированию также привлекаются исполнители, так как они обладают актуальной информацией, что в результате повышает степень достоверности исходных данных.

Производственные системы в виду информатизации («digitalization») стали широко рассматриваться совместно с киберфизические системами, в которых физические объекты, тесно связаны с информационными объектами. Такие информационные объекты, предоставляют информацию и осуществляют управление физическими объектами. В развитии тематики такие возможности информационных объектов были представлены как сервисы, а принципы построения систем, основанных на сервисах, получили название сервис-ориентированных архитектур. Оборудование в таких системах представляет собой киберфизические компоненты, предоставляющие различные сервисы. Одним из способов управления такими компонентами является использование агентных технологий. Производственная система трансформировалась в производственную многоагентную систему [1].

В условиях повсеместной персонализации продукции увеличивается разнообразие типов продуктов, и сокращаются объемы выпуска. Непрерывный технологический прогресс приводит к сокращению жизненного цикла изделий, вследствие их быстрого морального устаревания. Все это выдвигает современные требования к производству, одним из которых является возможность к быстрому переходу на выпуск новой продукции. Достигнуть этого возможно благодаря использованию механизмов реконфигурации и адаптации на всех этапах функционирования производства. Рассмотрим использование этих механизмов во время оперативного планирования в производственной многоагентной системе.

**Основные определения.** Определим понятия, используемые для описания производственной многоагентной системы и деятельности по оперативному планированию:

– продукт – изделие, изготавливаемое согласно требованиям заказчика. За каждым продуктом закреплен процесс его изготовления в данной производственной системе;

– процесс – последовательность операций, выполнение которых необходимо для получения готового продукта. Процесс в производственной многоагентной системе представляет собой параметризованный маршрутный технологический процесс. В таком процессе операции рассматриваются укрупненно, например, обработка детали в обрабатывающем центре является одной операцией;
– ресурс – оборудование, используемое для выполнения операций.

Указанные определения позволяют сформировать определения для ресурсо-независимых и ресурсо-зависимых процессов:

– ресурсо-независимый процесс – процесс, в котором операции закреплены за группой ресурсов. В таком процессе операции закреплены не за конкретным оборудованием, а за оборудованием, удовлетворяющим определенным требованиям. Например, операция, выполняемая на трехкоординатном фрезерном станке;
– ресурсо-зависимый процесс – процесс, в котором операции закреплены за конкретным ресурсом. В таком процессе операции закреплены за конкретным оборудованием. Например, операция, выполняемая на трехкоординатном фрезерном станке EMCO Concept MILL 55.

С учетом приведенных терминов можно дать определение оперативного планирования.

Оперативное планирование – деятельность по назначению ресурсов на выполнение операций и определению времени их использования.

В результате оперативного планирования ресурсо-независимый процесс становится ресурсо-зависимым процессом.

**Производственная многоагентная система.** Производственная многоагентная система состоит из множества взаимодействующих между собой агентов. Основными агентами в этой системе являются агент-продукт, агент-процесс и агент-ресурс, представляющие в информационном пространстве продукты, процессы и ресурсы. В состав производственной многоагентной системы входят вспомогательные агенты, одним из которых является агент-планировщик, участвующий в деятельности по оперативному планированию [2].

Вначале агент-продукт запускает агент-процесс, содержащий ресурсо-независимый процесс изготовления изделия. Далее агент-процесс, в результате переговорного процесса, подбирает агент-ресурсов для выполнения каждой из операций процесса изготовления. После подбора всех исполнителей, процесс изготовления изделия становится ресурсо-зависимым и может быть выполнен (рисунок).

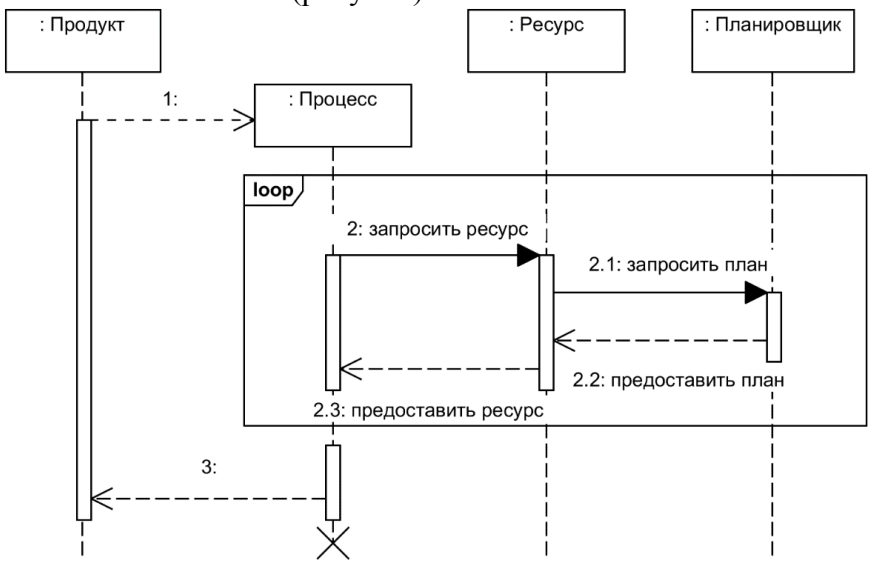



Рисунок. Взаимодействие агент-продукта, агент-процесса, агент-ресурса и агент-планировщика в производственной многоагентной системе

**Алгоритмы оперативного планирования.** Оперативное планирование осуществляется во время переговорного процесса между агентом-процессом и агентом-ресурсом. Во время определения ресурса для выполнения очередной операции, агент-процесс отправляет запросы на предоставление ресурса всем подходящим для выполнения операции агент-ресурсам. Получив такой запрос, агент-ресурс принимает решение и сообщает о нем агент-процессу. При наличии в системе агент-планировщика, агент-ресурс может дополнительно провести консультацию у него. Обработав ответы от всех опрошенных агент-ресурсов, агент-процесс принимает окончательное решение и назначает ресурс на выполнение операции.

Общение между агент-процессом и агент-ресурсом без посредников позволяет реализовать централизованный, децентрализованный и смешанный подходы к оперативному планированию.

В централизованном подходе решение о назначении ресурса принимается агент-планировщиком, он подготавливает ответы для каждого из агентов-ресурсов, а они только передают эти ответы агент-процессу. Рассмотрим эту ситуацию на примере – на выполнение операции могут быть назначены ресурс 1, ресурс 2 или ресурс 3. Агент-процесс, осуществляет запрос на предоставление ресурса каждому из связанных агент-ресурсов, а те, в свою очередь, консультируются у агент-планировщика. Агент-планировщик, подготавливает ответы для каждого из агент-ресурсов, например, агент-ресурс 1 – отказаться, агент-ресурс 2 – согласиться, агент-ресурс 3 – отказаться. Так как все агент-ресурсы кроме одного отказались, то вследствие отсутствия выбора будет назначен тот агент-ресурс, который соответствует принятому агент-планировщиком решению.

В децентрализованном подходе решение о назначении ресурса принимается агент-ресурсом самостоятельно. Каждый из агент-ресурсов подготавливает ответ и передает ответ агент-процессу, включая в ответ стоимость предоставления ресурса. Агент-процесс собирает ответы и выбирает ресурс на основе указанной стоимости предоставления. При расчете стоимости предоставления ресурса, агент-ресурс использует доступную ему информацию, учитывающую приоритеты операций, затраты на переналадку и т.д.

В смешанном подходе решение о назначение ресурса принимается агент-ресурсом и агент-планировщиком совместно. В данном подходе агент-ресурс также рассчитывает стоимость предоставления ресурса, но при ее расчете уже учитывается информация, доступная как агент-ресурсу, так и агент-планировщику. Агент-ресурс формирует приоритеты по операциям, а агент-планировщик формирует приоритеты по продуктам. Стоимость предоставления ресурса вычисляется на основе этих двух приоритетов – приоритета по операциям и приоритета по продуктам. Например, агент-ресурс определяет, что токарные операции имеют больший приоритет, чем фрезерные операции, а агент-планировщик определяет, что продукт категории 1, имеет больший приоритет, чем продукт категории 2. Теперь возможно определить стоимости предоставления ресурса для токарных и фрезерных операций, для продуктов категорий 1 и 2.

**Экспериментальная база.** Рассмотренные алгоритмы оперативного планирования проходят апробацию на учебно-экспериментальном стенде производственной многоагентной системы [2, 3].

Стенд состоит из условных станций, выполняющих технологические операции, и мобильных роботов, выполняющих транспортные операции. Станции совместно с мобильными роботами размещены на специально размеченной площадке, имитируя таким образом производственный участок.

Станции представлены одноплатными компьютерами Raspberry-Pi3 под управлением Raspbian OS, а мобильные роботы – Lego-Mindstorms под управлением Lejos. Многоагентная система разработана с использованием программной библиотеки JADE.

**Заключение.** Предлагаемая схема взаимодействия элементов производственной многоагентной системы позволяет реализовывать оперативное планирование в реальном времени. Указанная схема позволяет осуществлять оперативное планирование используя централизованный, децентрализованный и смешанный подходы.

**Литература**

1. Kashevnik A., Teslya N., Yablochnikov E., Arckhipov V., Kipriianov K. Development of a prototype Cyber Physical Production System with help of Smart-M3 // 42nd Conference of the Industrial Electronics Society. – 2016. – P. 4890–4895.
2. Архипов, В.А., Киприянов К.В., Яблочников Е.И., Makio J. Разработка учебного тренажера индустриальной киберфизической системы // Компьютерная интеграция производства и ИПИ-технологии: материалы VIII Всероссийской научно-практической конференции. – 2017. – С. 150–154.
3. Makio J., Makio-Marusik E., Yablochnikov E., Arckhipov V., Kipriianov K.V. Teaching cyber physical systems engineering // 43nd Conference of the Industrial Electronics Society. – 2017. – P. 3530–3535.

**Ушаков Александр Витальевич**
Год рождения: 1997
Университет ИТМО, факультет систем управления и робототехники, кафедра технологии приборостроения, студент группы № Р3475
Направление подготовки: 09.03.01 – Информатика и вычислительная техника
e-mail: sasha-ushakov@mail.ru

**Киприянов Кирилл Васильевич**
Год рождения: 1987
Университет ИТМО, факультет систем управления и робототехники, кафедра технологии приборостроения
e-mail: 142739@niuitmo.ru

**УДК 65.011.56:621.9**

# МНОГОАГЕНТНАЯ СИСТЕМА ДЛЯ МОДЕЛИРОВАНИЯ РАБОТЫ РАСШИРЕННОГО ПРЕДПРИЯТИЯ

**Ушаков А.В.**
**Научный руководитель – Киприянов К.В.**

В работе рассмотрена разработка многоагентной системы для моделирования работы расширенного предприятия. Описаны компоненты предприятия и агенты, представляющие их.
**Ключевые слова:** многоагентная система, расширенное предприятие.

**Введение.** В прошлом производство было организовано в первую очередь на местном уровне, в относительной изоляции. Развитие транспортных средств и информационных технологий позволило как рынку, так и производству расширить их коммуникационные возможности с поставщиками и клиентами на региональном, федеральном и впоследствии на международном уровне. Такая глобализация привела к изменениям в скорости и структуре процессов принятия решений на производстве, а также к значительному росту числа звеньев, связей и партнерских отношений [1]. Компания в классическом представлении достигла предела своего развития, и ей на смену пришло расширенное предприятие, открытое и гибкое [2].

Расширенное предприятие включает в себя следующие компоненты:
- поставщики сырья, компонентов, изделий, людских ресурсов;
- производственные объекты, такие как производственные линии, заводы, компании;
- распределительная инфраструктура, включающая в себя транспорт, посредников, склады;
- клиенты, которыми могут быть как физические, так и юридические лица.

Совместная кооперационная сеть подразумевает объединение на базе информационных технологий географически удаленных организаций и предприятий. Компаниям необходимо организовать совместное использование информации о выпускаемом продукте, его структуре, составе выполняемого проекта в целом и управлении их взаимодействием. С этой целью следует обеспечить взаимодействие участников проекта в едином информационном пространстве с возможностью получить в режиме реального времени необходимую информацию о текущих проектах, документах, моделях, расчетах и их исполнителях [3].

Для решения интеграции межорганизационных процессов и обмена данными в техническом и технологическом аспектах, была разработана система выполнения задач,

основанная на автономных агентах для обеспечения управления процессами обработкой исключительных ситуаций, предлагая свои собственные усовершенствования и функции.

В такой системе программные компоненты берут на себя полную ответственность за подготовку, выполнение и компенсацию процессов, при этом каждый агент контролирует только определенные операции [4].

Агент – это автономный программный компонент, который представляет физические или логические объекты системы и способен действовать самостоятельно для достижения поставленных целей.

Три основных свойства программного компонента, который может быть идентифицирован как агент:

1. автономность, т.е. возможность принимать решения независимо от человека;
2. сотрудничество, т.е. агенты должны работать совместно для решения проблемы;
3. обучаемость, т.е. при выполнении задания агент должен получать знания и использовать их для принятия будущих решений.

Многоагентная система – это группа агентов, которые для достижения индивидуальных или глобальных целей могут общаться, договариваться и взаимодействовать друг с другом, когда у них недостаточно знаний или навыков для выполнения задания самостоятельно. Многоагентные системы используются для решения задач, которые могут быть невыполнимы для отдельных агентов.

**Модель расширенного предприятия.** Главной задачей предприятия является получение чистой прибыли за отчетный период. Основными способами достижения этой цели являются выполнение конкретных заказов и продажа продукции со склада.

Все решения, касающиеся использования денежных ресурсов, принимает специальный финансовый отдел, исходя из своих знаний о бухгалтерском балансе организации. Главная цель – получить прибыль с заказа, учитывая при этом постоянные и переменные затраты производства. Все остальные задачи каждый отдел решает самостоятельно.

Заказы поступают от заказчика и состоят из наименований изделий, их количества, стоимости и срока выполнения. Эти требования не могут быть изменены исполнителем, он может только принять или отклонить заказ. Заказчик же в любой момент может отказаться от заказа, и тогда товар, если он уже был произведен, отправляется на склад для последующей реализации.

Готовая продукция после производства всегда поступает на склад. Если клиент не отказался от заказа, товар передается ему, а выручка поступает на счет в банке. Если же товар залеживается на складе, он выставляется на продажу на рынке с использованием аукционного метода продажи. Таким образом, среди потенциальных покупателей выбирается тот, кто предлагает наибольшую цену за данный товар. Минимальная цена готового изделия вычисляется из стоимости каждого из материалов и затрат на производство единицы данного изделия.

Для производства каждой единицы продукции требуется определенное количество материалов. Эти материалы хранятся на специальном складе и могут быть переданы в производство по запросу.

**Описание многоагентной системы.** Входными данными многоагентной системы являются требования заказчика (заказ). Система сама решает, что ей нужно для выполнения заказа, изменяет параметры производства, отслеживает расходы и доходы.

Агенты, участвующие в симуляции расширенного предприятия:

- агент заказчика;
- агент рынка сбыта;
- агент продаж;
- агент финансов;

– агент закупок;
– агент рынка закупок;
– агент производства.

Агенты общаются друг с другом посредством сообщений установленного заранее формата. В каждом сообщении содержится информация о заказе или его части.

Первым делом заказ принимает агент рынка сбыта, договаривается с заказчиком о стоимости и передает его агенту продаж. Агент продаж проверяет наличие продукции на складе готовых изделий, а если товара на складе недостаточно, агент узнает, возможно ли произвести требуемые изделия, выполнить данный заказ в срок и за данную стоимость.

Наименования недостающего товара передаются агенту производства. Он, в свою очередь, рассчитывает скорость выпуска продукции, размер партии, а также определяет, какие нужны материалы для изготовления и сколько нужно работников. Агент производства запрашивает необходимые для изготовления компоненты у агента закупок, а тот, в свою очередь, проверяет их наличие на складе материалов.

Недостающее сырье закупается на рынке агентом закупок и передается агенту производства. Произведенная продукция поставляется на склад готовых изделий, после чего агентом продаж собирается заказ и передает агенту рынка сбыта, где заказ передается клиенту и обменивается на деньги.

**Реализация многоагентной системы.** Прототип многоагентной системы реализован на языке Java с использованием фреймворка JADE.

JADE (Java Agent DEvelopment Framework) – программное обеспечение, полностью разработанное на языке Java. Его целью является создание многоагентных систем и их приложений, отвечающих стандартам FIPA для интеллектуальных агентов, а также их использование и поддержка при помощи графических инструментов.

FIPA (Foundation for Intelligent Physical Agents) – это международная организация, которая занимается продвижением индустрии интеллектуальных агентов, открыто разрабатывая спецификации и стандарты, поддерживающие совместимость между агентами и приложениями, основанными на агентах.

Основной характеристикой многоагентной системы является то, что агенты взаимодействуют друг с другом посредством обмена сообщениями, поэтому агенты должны договориться заранее о формате этих сообщений. В среде разработки JADE используется формат, определенный языком общения агентов ACL (Agent Communication Language), определенным международным стандартом FIPA для совместимости агентов [5].

Сообщения типа ACL состоят из набора необходимых для выполнения конкретной задачи параметров и их значений. Полный список параметров, определенный стандартом FIPA, приведен в таблице.

Заказ представлен в виде объекта класса Order. Чтобы передавать его сообщениями ACL, объект переводится в формат JSON.

JSON (JavaScript Object Notation) – стандартный текстовый формат для представления данных, основанный на синтаксисе JavaScript.

Для записи объектов в формат JSON используется библиотека GSON. Строка с JSON-структурой записывается в поле данных ACL-сообщения.

В качестве примера можно привести структуру заказа для расширенного предприятия по покраске камней. Параметры, содержащиеся в такой структуре, представлены в таблице.

Таблица. Содержимое заказа

| Ключ | Значение |
|---|---|
| id | Уникальный идентификатор |
| deadline | Срок выполнения |
| orderList | Список изделий |

| Ключ | Значение |
|---|---|
| id | Уникальный идентификатор |
| product | Материалы одного изделия |
| amount | Количество этого изделия |
| stone | Параметры камня |
| size | Размер камня |
| paint | Параметры краски |
| color | Цвет краски |
| price | Цена материала |

Уникальный идентификатор используется для отслеживания состояния заказа на всех стадиях производства. Является значением целочисленного типа и присваивается заказу на этапе получения требований от клиента.

Срок выполнения устанавливается заказчиком и измеряется в секундах. Отсчет начинается с момента принятия заказа к выполнению, а по истечении срока, заказ снимается с производства. Однако если изделие уже произведено, оно отправится на склад.

В списке изделий содержатся объект изделия и его количество, которые необходимо произвести. В объекте изделия хранится информация о материалах для его изготовления.

**Литература**

1. Walters H.M.J. Management and improvement of the extended enterprise // IEE Colloquium on Agile Manufacturing. – 1997. – P. 5/1–5/8.
2. Ezzeddine B., Abdellatif B., Mounir B. An intelligent framework for the cooperation in the extended enterprise environment // 4th International Conference on Logistics. – 2011. – P. 379–384.
3. Грибовская А.А., Грибовский А.А., Яблочников Е.И. Подход к созданию расширенного предприятия для выпуска инновационной продукции // Изв. вузов. Приборостроение. – 2016. – Т. 59. – № 10. – С. 867–873.
4. Migar M.C. Tam, K.S. Li, Spencer K.C. Yung, Ericson K.W. Yuen, Autonomous Agent Enhanced Workspace (AAEW) for Extended Enterprise (E2) collaboration // IEEE 3rd International Conference on Cloud Computing and Intelligence Systems. – 2014. – P. 481–486.
5. FIPA Abstract Architecture Specification [Электронный ресурс]. – Режим доступа: http://www.fipa.org/specs/fipa00001/SC00001L.html, своб.

**Чукичев Артемий Валерьевич**
Год рождения: 1996
Университет ИТМО, факультет систем управления и робототехники, кафедра технологии приборостроения, студент группы № Р4177
Направление подготовки: 12.04.01 – Приборостроение
e-mail: chukichevartemiy@gmail.com

**Андреев Юрий Сергеевич**
Год рождения: 1984
Университет ИТМО, факультет систем управления и робототехники, кафедра технологии приборостроения, к.т.н., доцент
e-mail: ysandreev@corp.ifmo.ru

**УДК 678**

# ОСОБЕННОСТИ РАЗРАБОТКИ ТЕХНОЛОГИИ ИЗГОТОВЛЕНИЯ ИЗДЕЛИЯ ИЗ ПЕНОМАТЕРИАЛА

**Чукичев А.В., Андреев Ю.С.**
**Научный руководитель – к.т.н., доцент Андреев Ю.С.**

В работе представлены результаты обзора технологий изготовления изделий из пеноматериалов и выявления проблем используемого в настоящее время типового технологического процесса для изделий «Поплавок».
**Ключевые слова:** вспенивание полимеров, полимерный пеноматериал, литье со вспениванием, поплавковые датчики уровня топлива.

Объектом работы являлось изделие из пеноматериала «Поплавок», которое применяется в датчиках уровня жидкости в электрических авиационных бензиномерах.

Целью работы стало исследование технологии получения изделий из полимерных пеноматериалов, определение проблемы научно-исследовательской работы.

В настоящее время существуют следующие основные технологии получения вспененных изделий: прессовый (для линейных полимеров), беспрессовый (преимущественно для вспенивания термореактивных смол), экструзионный и литьевой методы.

Источниками газа в расплаве полимера могут служить:

– химические газообразователи (ХГО) – соединения, способные разлагаться при температуре переработки термопластов с выделением газообразных продуктов;
– физические газообразователи (ФГО) – низкокипящие жидкости, выделение газа из которых происходит за счет испарения.

По прессовому методу вначале производят смешение порошкообразной смеси полимера с газообразователем (ГО), причем ГО подбирают таким образом, чтобы его температура разложения была несколько выше температуры размягчения полимера. Далее композицию прессуют. При этом ГО разлагается, и газ равномерно распределяется по всей заготовке.

При беспрессовом методе для вспенивания термореактивных полимеров ГО подбирают таким образом, чтобы скорость выделения газа и роста ячеек была согласована с процессом образования полимера. Быстрое разложение ГО в низковязком полимере приводит к

разрушению ячеек и улетучиванию газа или к получению материала с крупноячеистой структурой. Наоборот, выделение газа после образования пространственной полимерной сетки уже не может привести к вспениванию, так как пространственный полимер не имеет текучести и не способен к высокоэластической деформации.

При экструзионном методе ХГО в виде высокодисперсного порошка дозируют в бункер экструдера вместе с гранулами полимера, где он нагревается, диспергируется в расплаве полимера и частично разлагается. Под давлением, создаваемым экструдером, выделяющийся газ растворяется в полимере. При выходе из головки экструдера в атмосферу давление расплава резко снижается, из-за чего растворимость газа падает, и он вспенивает полимер. Поверхность расплава, соприкасающаяся с холодными стенками калибрующей головки, затвердевает, сохраняя тем самым форму профиля.

Литье под низким давлением со вспениванием начинается с пластикации системы «термопласт – химический ГО» в материальном цилиндре машины. В специальных случаях вместо химических ГО используют физические ГО или сжатый газ. В ходе пластикации ХГО разлагается, выделяя газ, большая часть которого на этой стадии остается в растворенном состоянии под давлением. Затем осуществляется короткий впрыск в формующую полость, в результате которого образуется плотный поверхностный слой, поскольку пузырьки газа вблизи поверхности формы разрушаются под воздействием механических сил сжатия. Далее газы продолжают перемещаться, заставляя впрыснутую дозу расплава заполнять удаленные зоны полости и одновременно вспениваться, создавая пористую структуру.

При инжекционно-газовом литье расплав полимера инжектируется в форму, заполняя ее на 70–95%. Затем в форму через ниппель или с помощью специального сопла подается под давлением газовая смесь (ФГО), которая раздувает расплав, увеличивая тем самым толщину слоя полимера, образовавшегося при его соприкосновении с холодной стенкой формы, и способствуя заполнению конструктивных углублений. Существенная трудность технологии инжекционно-газового литья – это усложнение конструкции сопла, повышаются требования к расчету и качеству изготовления литниковой системы и сопряжений литьевых форм [1–3].

В настоящее время систем, позволяющих моделировать процессы вспенивания материалов, очень мало. К ним относятся Moldex3D, ProCAST. Эти системы предназначены для литьевых методов вспенивания. Данные системы позволяют предсказывать образование пузырьков, рост пузырьков и распространение расплава в процессе микропористого литья с целью уменьшения коробления и веса изделия. Модули также позволяют отобразить радиусы пузырьков и распределение плотности количества пузырьков для улучшения качества поверхности [4, 5].

На сегодняшний день для изготовления изделия «Поплавок» применяется технология беспрессового вспенивания материала «Тилен» в форме с применением химического газообразователя.

К изделию предъявляются следующие требования:

1. размеры и масса поплавков должны соответствовать требованиям чертежа;
2. поверхность изготовленных поплавков должна быть мелко-ячеистой, цвет – коричневый, от светлого до темных тонов;
3. на поверхности поплавков допускаются:
   - поверхностные раковины с оформившейся глянцевой поверхностью, глубиной до 1,5 мм и площадью до 0,5 $см^2$, при этом их общая площадь не должна превышать 5% от поверхности соответствующей стороны или раковины, глубиной до 0,5 мм и площадью до 1,0 $см^2$, при этом их общая площадь не должна превышать 15% от полной поверхности;
   - сколы в местах удаления выпоров глубиной до 1 мм;
   - незначительные дефекты (вспучивания, утяжины) в пределах эталона;

- сколы в местах зачистки заусенцев, величина которых не должна превышать 20% толщины стенки;
- сколы от мест разъема, отпечатки вкладышей, толкателей и других конструктивных элементов форм;

4. недопустимы: недозаливка, местные вздутия, хрупкость и рыхлость пенопласта.

По окончании операции отверждения изделий в форме проводят контроль качества. Контроль качества производится внешним осмотром и с использованием индикатора часового типа и отсчетного микроскопа МИР-2 на отсутствие недовспениваний, раковин, трещин, сколов, вмятин и др. дефектов или определение их допустимости в соответствии с требованиями к изготовленным поплавкам.

Затем все поплавки проверяют на топливопоглощение – изменение массы изделия после выдержки в топливе не должно превышать установленного значения. Для этого поплавки помещают в автоклав с топливом ТС-1, производят четыре цикла подъема и снижения давления в автоклаве и затем измеряют массу поплавков. Годные изделия, после выполнения сборочной операции, проходят контроль ОТК, где поплавки проверяют по геометрическим размерам согласно чертежам.

Данная технология сопряжена с возникновением брака. Основная проблема – несоответствие требованиям внешнего вида изделия: на поверхности образуются дефекты, недопустимые по техническим требованиям, что объясняется прилипанием изделия к форме. Количество отбраковываемых деталей из-за несоответствия их внешнего вида требованиям может достигать 50% на партию.

Для решения существующей проблемы можно выделить два возможных направления исследований:

1. внесение изменений в существующую технологию беспрессового вспенивания. Для этого необходимо провести исследования с целью выявления зависимости качества изделия от условий технологического процесса (материал форм, материал смазки и методики нанесения ее на формы, режимы отверждения, состав пеноматериала);
2. использование технологии изготовления изделия литьем с вспениванием. В данном случае необходимо провести исследования по подбору полимерного материала, удовлетворяющего требованиям к изделию и обладающего литьевыми свойствами, и анализ возможности внедрения технологии литья этого материала в литьевую машину.

В процессе подбора материала необходимо учитывать следующие физико-механические характеристики, которыми должны обладать изделия:

1. кажущаяся плотность: 170–220 кг/м$^3$;
2. топливопоглощение (после четырех циклов перепада давления): 0,0022 г/см$^3$;
3. интервал рабочих температур: от – 60 до +200°С.

На основе этих данных были выбраны следующие материалы для проведения испытаний по определению возможности их применения для изготовления данного изделия: полиэтилен вспененный литьевой и сополимер этилена с пропиленом вспененный литьевой. Результаты испытаний приведены в таблице.

Таблица. Результаты испытаний

| Обозначение образца | Объем, см$^3$ | Площадь поверхности, см$^2$ | Масса до испытаний, г | Масса после испытаний, г | Кажущаяся плотность, г/см$^3$ | Величина топливопоглощения, г/см$^2$ |
|---|---|---|---|---|---|---|
| Полиэтилен вспененный литьевой | | | | | | |
| 1 | 17,23 | 60,62 | 10,76 | 10,78 | 0,624 | 0,0003 |
| 2 | 17,18 | 60,33 | 10,77 | 10,79 | 0,626 | 0,0003 |
| Сополимер этилена с пропиленом вспененный литьевой | | | | | | |
| 3 | 17,14 | 61,31 | 10,27 | 10,31 | 0,598 | 0,0006 |
| 4 | 18,73 | 63,35 | 10,37 | 10,41 | 0,553 | 0,0006 |

По результатам испытаний можно сделать вывод, что данные образцы не соответствуют по параметру кажущейся плотности. Таким образом, необходимо продолжить исследования по подбору подходящего материала, который можно будет использовать в качестве замены материалу «Тилен».

**Литература**

1. Клемпнер Д. Полимерные пены и технологии вспенивания / Пер. с англ. / Под. ред. к.т.н. А.М. Чеботаря. – СПб.: Профессия, 2009. – 600 с.
2. Моисеев А.А., Павлов В.В., Бородин М.Я. (ред.) Пенопластмассы. Сборник статей. – М.: ОБОРОНГИЗ, 1960. – 185 с.
3. Оссвальд Т.А., Тунг Л.-Ш., Грэманн П.Дж. Литье пластмасс под давлением / Пер. с англ. / Под ред. Э.Л . Калинчева. – СПб.: Профессия, 2006. – 712 с.
4. Moldex3D. Опциональные модули [Электронный ресурс]. – Режим доступа: http://beepitron.com/soft-products/moldex3d/, своб.
5. Компания Faurecia использует моделирование процесса вспенивания полиуретана [Электронный ресурс] – Режим доступа: http://www.esi-group.com/ru/kompaniya/istorii-uspeha/kompaniya-faurecia-ispolzuet-modelirovanie-processa-vspenivaniya-poliuretana-dlya-razrabotki/, своб.

**Шорохов Сергей Александрович**
Год рождения: 1989
Университет ИТМО, факультет систем управления и робототехники, кафедра технологий приборостроения, аспирант
Направление подготовки: 12.06.01 – Фотоника, приборостроение, оптические и биотехнические системы и технологии
e-mail: stratumxspb@gmail.com

**УДК 004.102.171**

# ПРИМЕНЕНИЕ СИСТЕМ МАШИННОГО ЗРЕНИЯ В УСТРОЙСТВАХ СЕЛЕКТИВНОГО ОТВЕРЖДЕНИЯ ФОТОПОЛИМЕРА

**Шорохов С.А.**
**Научный руководитель – к.т.н., доцент Афанасьев М.Я.**

Работа выполнена в рамках темы НИР № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность».

Проектирование устройства для производства печатных плат – задача, требующая разумного компромисса между стоимостью изготовления, точностью и качеством. Использование технологии компьютерного зрения играет важную роль в автоматизации производственного процесса и делегировании рутинных операций, таких как определение размеров заготовки и калибровка станка перед началом операции. В работе приведено описание разрабатываемой системы машинного зрения с определением основных функций и требований, выбором технических средств и алгоритмов перемещения камеры.
**Ключевые слова:** машинное зрение, система управления, оборудование с ЧПУ, центрирование.

Системы машинного зрения (МЗ) в настоящее время широко используются для автоматизации рутинных задач благодаря доступным ценам на аппаратные компоненты, включая камеры и мощные вычислительные ресурсы. В результате Четвертой промышленной революции они начинают активно применяться в киберфизических производственных системах [1], которые позволяют взаимодействовать с «физическим» миром через его компоненты – через наблюдение и запись «физических» параметров окружения и событий. Основными задачами МЗ являются, прежде всего, идентификация (например, штрих-код или сканирование QR-кода), переходный и конечный контроль, заготовка (продукт) или позиционирование инструмента. За каждой задачей стоят различные алгоритмы обработки входных изображений. Однако подробный список задач зависит от конкретного вида производства и конечного продукта.

В настоящее время ни одно электронное устройство не обходится без печатных плат. Они могут отличаться конфигурацией (односторонняя, двухсторонняя и многослойная), геометрией, точностью и т.д., что в целом влияет на выбор технологии производства и размер выпускаемой партии. Тип производства определяет технологию производства в соответствии с затратами времени на производственный процесс и предварительную подготовку. Так, например, в массовом производстве обычно используются фотомаски, которые не являются прибыльными в производстве труда из-за производственных издержек.

Часто печатные платы требуются еще на стадии разработки продукта, при создании прототипа. Производство плат (особенно многослойных) является очень сложным процессом, включающим в себя такие этапы, как сверление отверстий в заготовке, покрытие заготовки светочувствительным полимером (фоторезистом), обработка фоторезиста через шаблон, удаление фоторезиста и другие [2]. Несмотря на то, что для реализации каждого

шага существует множество автоматических устройств, предназначенных для операций, все они довольно дороги, поэтому не подходят для производства прототипов.

Разрабатываемое устройство для селективного отверждения фотополимера имеет вид координатного стола с обрабатывающим устройством, включающий в себя систему управления с рядом обособленных модулей. К ним относятся основной модуль управления, модуль лазерного излучения, систему МЗ и другие [3]. В процессе проектирования системы управления устройства определены следующие основные функции системы МЗ:

– поиск и определение реперных меток на заготовке;
– самокалибровка станка, контроль за выполнением процесса обработки, а также готового изделия;
– передача трансляции на пользовательское приложение по запросу.

Следует также отметить, что в работе станка на систему могут влиять различные негативные факторы, вроде плохой освещенности, вибраций и различного мусора на заготовке, что затрудняет выполнение функций системы МЗ, поэтому необходимо тщательно подходить к выбору технических средств.

Работа системы МЗ состоит из ряда связанных между собой и с внешними модулями устройства компонентов. Основными из них являются одноплатный компьютер Odroid, реализующий алгоритмы работы системы, и камера, размещенная на каретке установки. Поскольку функция передачи видеопотока, очевидно, должна быть обособлена, чтобы не нарушать выполнение основных функций, под эту задачу должна быть выделена отдельная камера и ее связь с модулем МЗ носит ограниченный характер. Диаграмма (рисунок) показывает взаимодействие модулей системы друг с другом в процессе выполнения основных задач.

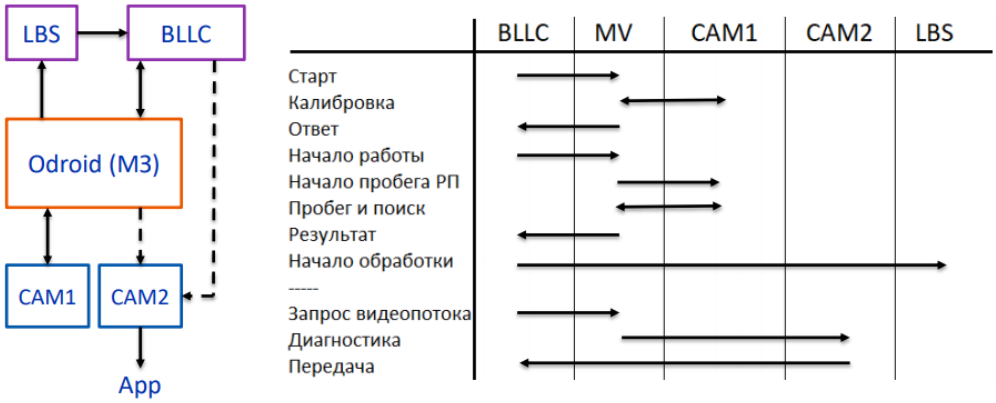



Рисунок. Взаимодействие компонентов системы МЗ

При выборе камеры для решения основных задач был проведен сравнительный анализ двух модулей камеры принципиально разного назначения, IP-камера и oCam-1MGN-U, в ходе которого было установлено, что основными преимуществами камеры oCam являются более широкий диапазон рабочих режимов, возможность смены объектива, меньшие размеры и вес, а также меньшее энергопотребление. Однако у нее нет встроенного интерфейса Wi-Fi, позволяющего получать доступ к камере со стороны других модулей системы управления. Возможность смены объективов позволяет использовать объективы без инфракрасного фильтра, который предназначен для отсечения лишней части спектра, падающего на матрицу, делая изображение приближенным к тому, что видит человеческий глаз, однако, это сильно снижает чувствительность, особенно в условиях плохой или неравномерной освещенности.

Также важной проблемой является проблема перемещения камеры по рабочему полю в процессе поиска реперных точек и центрирования. Очевидно, что самый простой способ – перемещать камеру вокруг поля по строкам, покрывая за один проход некоторую часть

рабочей области. Размер этой области зависит от области поля обзора (FOV), охватываемой камерой в одном кадре, и ее можно вычислить по уравнению:

$$S = 4h^2 \cot\frac{\alpha}{2} \cot\frac{\beta}{2},$$

где $h$ – высота от объектива камеры до поверхности заготовки, а α и β – вертикальный и горизонтальный углы FOV-камеры. Зная эти значения, можно с некоторым приближением указать координаты движений во время поиска. Однако при нахождении одного случайного маркера нельзя точно сказать, где он находится на заготовке.

Команды перемещения каретки, передаваемой модулем зрения машины на компонент числового программного управления, определяются на основе полученного изображения. Другими словами, определив маркер на нескольких кадрах подряд, можно начать центрировать камеру на нем. Зная поле обзора камеры, можно вычислить расстояние, на которое нужно перемещать каретку, в противном случае, приближение будет выполняться дискретно с определенным размером шага при каждом анализе входного изображения. Когда центральная точка кадра переполнена, шаг может быть последовательно уменьшен, например, путем деления его на два, но в этом случае центровка может занять много времени, в зависимости от разрешения камеры.

**Литература**

1. Коломбо А.В., Карнускос С, Кайнак О., Ши Ю., Инь С. Industrial cyberphysical systems: A backbone of the fourth industrial revolution // IEEE Industrial Electronics Magazine. – 2017. – № 1. – P. 6–16.
2. Брусиницына Л.А., Степановских Е.И. Технология изготовления печатных плат. – Екатеринбург: Изд-во Уральского университета, 2015. – 200 с.
3. Афанасьев М.Я., Федосов Ю.В., Крылова А.А., Шорохов С.А. Применение микросервисной архитектуры при проектировании промышленного оборудования с числовым программным управлением // Научно-технический вестник информационных технологий, механики и оптики. – 2018. – Т. 18. – № 1(113). – С. 87–97.

**Юдин Семён Алексеевич**
Год рождения: 1995
Университет ИТМО, факультет систем управления и робототехники, кафедра технологий приборостроения, студент группы № Р4177
Направление подготовки: 12.04.01 – Приборостроение
e-mail: yudinYudin7@gmail.com

**Андреев Юрий Сергеевич**
Год рождения: 1984
Университет ИТМО, факультет систем управления и робототехники, кафедра технологии приборостроения, к.т.н., доцент
e-mail: ysandreev@corp.ifmo.ru

**УДК 621.74.043.2**

# ОСОБЕННОСТИ ПОЛУЧЕНИЯ ИЗДЕЛИЙ МЕТОДОМ ЛИТЬЯ ПОД ДАВЛЕНИЕМ В УСЛОВИЯХ ЦИФРОВОГО ПРОИЗВОДСТВА

**Юдин С.А., Андреев Ю.С.**
**Научный руководитель – к.т.н., доцент Андреев Ю.С.**

В работе рассмотрены технология литья металлов под давлением и виды литейных машин. Описана концепция цифрового производства, и приведена его характеристика. Представлены особенности получения изделий методом литья металлов под давлениям в условиях цифрового производства.
**Ключевые слова:** литье металлов под давлением, цифровое производство, цифровой двойник, бизнес-процессы, автоматизация.

В металлургии существует множество способов добиться правильной формы металлического изделия, но наиболее распространенным, когда дело касается производства специальных конструкций и изделий сложной формы, на сегодняшний день остается метод литья металлов под давлением (ЛПД) [1].

Для литья металлов используют специальное оборудование – литьевые машины, которые можно разделить на машины для ЛПД с холодной или горячей камерой прессования, и с вертикальной или горизонтальной камерой прессования. В рамках исследования рассмотрен литьевой участок, оборудованный литьевой машиной литья цветных металлов под давлением CLH 160.1 с холодной горизонтальной камерой прессования. Холодная камера прессования и ее горизонтальное расположение более удобно и позволяет упростить конструкцию. При изготовлении отливок в таких машинах расплавленный металл заливают в камеру прессования. Пресс-форма состоит из двух полуформ: подвижной – пуансона, и неподвижной – матрицы. В пресс-форму металл подается под действием плунжера, полость в отливке получается металлическим стержнем. После затвердевания пресс-форма раскрывается, и отливка вынимается выталкивателями [2].

Недостатками ЛПД является дороговизна оснастки – пресс-форм, вероятности появления трещин на отливках и воздушно-газовой пористости. Применение инструментов цифрового производства поможет сократить влияние названных недостатков и вовсе исключить некоторые.

Цифровое производство (ЦП) – это концепция технологической подготовки производства в единой цифровой среде с помощью инструментов планирования, проверки и

моделирования процессов производства. ЦП предполагает единое информационное пространство и сквозную автоматизацию всех процессов производства, которая возможна благодаря переводу всей информации об изделии, производственных процессах и эксплуатации в цифровой вид, т.е. создается параллельная цепочка создания продукта, иными словами, создается цифровой двойник предприятия и изделия. Для создания ЦП необходимо выполнить следующие условия.

Во-первых, автоматизация всех производственных процессов: конструкторская разработка, технологическая подготовка производства, снабжение материалами и комплектующими, планирование производства, организация бизнес-процессов и разработка стратегий, изготовление продукции, сбыт и утилизация. Предполагается применение системы автоматизированного проектирования и системы управления жизненным циклом изделия, используются станки с числовым программным управлением и роботизированное оборудование.

Во-вторых, концепция цифрового производства предполагает наличие единого информационного пространства на предприятии, с помощью которого все автоматизированные системы управления предприятием и промышленное оборудование смогут оперативно и своевременно обмениваться информацией. Например, на технологическом уровне оно представлено инженерной инфраструктурой в виде сенсоров промышленного Интернета вещей, роботизированных производственных линий. На уровне производства – наличием систем мониторинга и аналитики, которые обрабатывают полученные с производства и оборудования данные и помогают оперативно вносить изменения и корректировки в работу цеха.

В-третьих, необходимо наличие цифровой модели (двойника) объекта или процесса и его существование в информационном пространстве на протяжении всего его жизненного цикла, начиная с отдельного узла и заканчивая всем предприятием. Предполагается появление параллельной цепочки создания продукта. Например, с минимальными затратами средств и времени можно произвести виртуальную наладку производства с помощью программного обеспечения и проведения имитационного моделирования, а затем воспроизвести эти результаты на реальное производство, при этом оптимально запустив технологический процесс [3]. Цифровая модель позволяет оценить функциональность изделия, выявить сильные и слабые стороны конструкции и в дальнейшем внести корректировки в производственный процесс или конструкцию.

От правильного сочетания технологических режимов ЛПД зависит качество изделий, а также затраты изготовление. Соблюдение условий технологичности литых деталей, подразумевает такое их конструктивное оформление, которое, не снижая основных требований к конструкции, способствует получению заданных физико-механических свойств, размерной точности и шероховатости поверхности при минимальной трудоемкости изготовления и минимальными затратами материалов. Всегда необходимо учитывать, что качество отливок, получаемых ЛПД, зависит от большого числа переменных технологических факторов, связь между которыми установить чрезвычайно сложно из-за быстроты заполнения формы.

Основными параметрами, влияющими на процесс заполнения и формирования отливки, являются: давление на металл во время заполнения и подпрессовки, скорость прессования, конструкция литниково-вентиляционной системы, температура заливаемого сплава, режимы смазки и вакуумирования. Сочетанием и варьированием этих параметров добиваются негативных влияний особенностей процесса ЛПД. Традиционными конструкторско-технологическими решениями по снижению брака являются: регулирование температуры заливаемого сплава, повышение давления на металл во время заполнения и подпрессовки, рафинирование и очистка сплава, вакуумирование и детальное конструирование литниково-вентиляционной системы [4]. ЦП предоставляет программные решения для моделирования технологического процесса литья.

Например, применение специализированных CAE-систем (AFS, SIMTEC, ProCAST, NovaFlow, PowerCAST, CastCAE) [5] позволяет визуализировать процесс литья под давлением. Благодаря этому можно выявить различные дефекты и деформации, остаточные напряжения, определить объемную и линейную усадку, провести оптимизацию режимов заливки и затвердевания отливки, а также по итогам визуализации произвести корректировки на стадии проектирования конструкции отливки и технологического процесса, что значительно снизит процент брака, а следовательно, будет значительная экономия металла, рабочего времени и электроэнергии.

Проведение имитационного моделирования бизнес-процессов, качество которых является одним из важнейших факторов конкурентоспособности современного предприятия, дает возможность выявить слабые места в организации производства и внести изменения. Автоматизированное проектирование производственных процессов и единое информационное пространство позволяет осуществлять параллельную работу конструкторского и технологического бюро – осуществление параллельной разработки технологической документации и оснастки без затрат времени на документооборот с целью доработки или утверждения; работу литейного и механического цеха – доступ к конструкторской и технологической документации с любого рабочего места.

Наличие цифрового двойника литейного участка позволит в реальном времени отслеживать показания датчиков, данные которых находятся в едином информационном пространстве, с литейной машины, установленных в камере прессования, пресс-форме, на манипуляторах, предназначенных для заливки металла и извлечения отливки. Это даст возможность проводить анализ процесса литья под давлением и контроль качества отливок, что предоставит возможность осуществлять автоматизированную корректировку технологических режимов литья без остановки производства.

Цифровой двойник представляет собой трехмерную модель литейной машины CLH 160.1, на которой обозначены положения датчиков с указанием их назначения и обратной связи, трехмерную модель манипулятора для заливки расплавленного металла и вынимания отливки.

Переход всего предприятия на цифровое производство даст преимущества массового и единичного производства в виде быстрого изготовления крупного объема продукции и кастомизации с возможностью быстрой переналадки оборудования соответственно, что существенно повысит конкурентоспособность предприятия и позволит производить новые товары и занимать новые отраслевые рынки.

**Литература**

1. Далиский А.М. и др. Технология конструкционных материалов: учебник для вузов / Под ред. А.М. Дальского. – 2-е изд. перераб. и доп. – М.: Машиностроение, 1990. – 352 с.
2. Web-сайт Fomart Slovakia [Электронный ресурс]. – Режим доступа: http://www.fomart.sk/, своб.
3. Деловой портал «Управление производством» [Электронный ресурс]. – Режим доступа: http://www.up-pro.ru/, своб.
4. Литье под давлением [Электронный ресурс]. – Режим доступа: http://материаловед.рф/, своб.
5. Журнал «САПР и Графика» [Электронный ресурс]. – Режим доступа: http://sapr.ru/, своб.

**Вавринюк Дмитрий Михайлович**
Год рождения: 1994
Университет ИТМО, факультет систем управления и робототехники, кафедра электротехники и прецизионных электромеханических систем, студент группы № Р4245
Направление подготовки: 13.04.02 – Электроэнергетика и электротехника
e-mail: sailar_salazarn@mail.ru

**УДК 621-37**

# ИСПОЛЬЗОВАНИЕ РЕКТЕННЫ ДЛЯ ПИТАНИЯ МАЛОМОЩНЫХ ЭЛЕКТРОННЫХ УСТРОЙСТВ В ГОРОДСКОЙ СРЕДЕ

**Вавринюк Д.М.**
**Научный руководитель – к.т.н., доцент Горшков К.С.**

В работе были изготовлены ректенны для частот 950 МГц (частота сетей GSM) и 549 МГц (частота цифрового телевидения) с целью проведения исследования городского массива с помощью данных устройств, для оценки плотности поля в районах Санкт-Петербурга, с дальнейшим сбором и преобразованием электромагнитного поля в электрический ток, с последующим накоплением и питанием маломощных устройства, такие как датчики, микроконтроллеры, микросхемы и т.д.
**Ключевые слова:** ректенна, Energy harvesting, Ambient energy, радиотехника, преобразователь, выпрямитель, накопитель.

Цель исследования – провести исследование по преобразованию магнитного поля из окружающей среды в электрический ток. Измерения плотности магнитного поля, изготовленными ректеннами, в условиях городской среды Санкт-Петербурга, удостоверится о возможности использования ректенны для питания маломощных электронных устройств.

В наши дни вопрос о питании устройств от бесплатной энергии весьма актуален. Питание осуществляется путем преобразования (Ambient energy) окружающей энергии, излучаемой неспециализированными источниками (станциями радиовещания, передатчиками мобильной связи и Wi-Fi и т.д.). Этот процесс в англоязычной литературе называется, Energy harvesting – сбор разнообразной энергии из окружающей среды и преобразование ее в электрическую для питания автономных миниатюрных и маломощных устройств. Устройство, которое выполняет данное преобразование, называется ректенна (Rectenna) [1]. Это устройство, состоящее из выпрямляющей антенны, колебательного контура и умножителя напряжения. К выходу ректенны (рисунок) подключается питаемое устройство. Ректенна состоит из: антенны, предназначенной для приема радиоволн, которая служит источником питания; цепи согласования, представляющей фильтр верхних частот 2-го порядка, параметры элементов которого подбираются на резонансной частоте; блока умножителя напряжения, представляющего собой диодный выпрямитель, который преобразует радиочастотную энергию в постоянное напряжение, используя цепь конденсаторов и диодов Шоттки (HSMS2850) (умножение напряжения примерно в 4 раза). На выходе подключается заряжаемый аккумулятор.

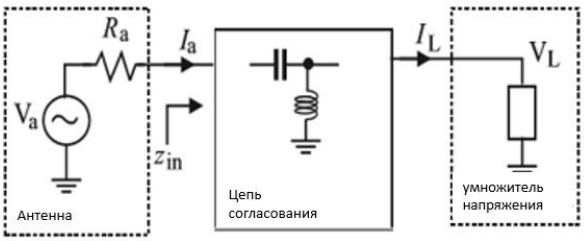



Рисунок. Блок-схема ректенны

Проведенное исследование показало, что в реальных условиях устройства позволяют получить малые мощности порядка не более 10–100 мкВт от неспециализированных источников. Энергию можно накапливать в аккумуляторе и использовать для дальнейшего питания маломощных, малых и миниатюрных устройств с непродолжительными активными периодами работы, такие как: датчики, видеокамеры, микроконтроллеры, микросхемы и т.д. Экспериментально стало известно, что напряжение на выходе ректенны мало. Решено было использовать микросхему BQ25504, задача которой выпрямлять и приумножать входное напряжение [2]. Для обеспечения уровня напряжения холодного старта этой микросхеме необходимо подать на вход 330 мВ. На выходе получим стабильное выпрямленное напряжение равное 1,8 В.

Для обеспечения напряжения холодного старта были проведены измерения магнитного поля ректеннами, работающими на частотах 950 МГц (GSM) и 549 МГц (частота цифрового телевидения). Результаты измерений на синей ветке метро города Санкт-Петербург приведены в таблице.

Таблица. Результаты измерений на синей ветке метро города Санкт-Петербург

| Станция метро | 950 Мгц, мВ | 549 Мгц, мВ | Станция метро | 950 Мгц, мВ | 549 Мгц, мВ |
|---|---|---|---|---|---|
| Парнас | 3 | 39,8 | Сенная площадь | 1,3 | 1,9 |
| Проспект Просвещения | 1 | 164 | Технологический институт | 1 | 6,9 |
| Озерки | 1,2 | 126,1 | Фрунзенская | 1,9 | 8,8 |
| Удельная | 2,8 | 34,6 | Московские ворота | 0,7 | 24,2 |
| Пионерская | 0,5 | 167,6 | Электросила | 4,9 | 9,8 |
| Черная речка | 1,4 | 99,8 | Парк Победы | 2,7 | 9,8 |
| Петроградская | 1,9 | 11,6 | Московская | 2 | 6,1 |
| Горьковская | 4,1 | 9,5 | Звездная | 2,4 | 4,1 |
| Невский проспект | 4,1 | 2,7 | Купчино | 2,8 | 8,8 |

Из полученных результатов следует вывод, что получить желаемое напряжение холодного старта, используя только одно устройство, невозможно. Необходимо использовать несколько ректенн на самых распространенных частотах, таких как 950 МГц, 549 МГц и 2,4 ГГц (частота сети Wi-Fi) [3, 4].

**Литература**

1. Tavares J., Barroca N., Saraiva H.M., Borges L.M., Velez F.J., Loss C., Carvalho N.B. Spectrum opportunities for electromagnetic energy harvesting from 350 mhz to 3 ghz // Medical Information and Communication Technology. – 2013. – P. 126–130.
2. Parks A.N., Sample A.P., Zhao Y. A wireless sensing platform utilizing ambient RF energy // Proceedings of the 2013 IEEE topical conference on biomedical wireless technologies, networks, and sensing systems. – 2013. – P. 331–333.
3. Zakaria Z., Zainuddin N.A., Husain M.N., Abidin M.Z. Current Developments of RF Energy Harvesting System for Wireless // Advances in information Sciences and Service Sciences. – 2013. – P. 328–338.
4. Грецких Д.В. Грецких Д.В., Гомозов А.В., Назаренко В.А., Аль-Самарай Ш.Ф.А. Методика расчета приемно-выпрямительных элементов ректенн систем беспроводной передачи энергии // Авіаційно-космічна техніка і технологія: зб. наук. пр., Нац. аерокосм. ун-т «ХАІ». – 2011. – Вып. 4(81). – С. 94–105.

**Вертегел Денис Александрович**
Год рождения: 1994
Университет ИТМО, факультет систем управления и робототехники,
кафедра электротехники и прецизионных электромеханических систем,
студент группы № Р4245
Направление подготовки: 13.04.02 – Электроэнергетика
и электротехника
e-mail: vertegeldenis@gmail.com

**УДК 621.341.572**

# ИССЛЕДОВАНИЕ АЛГОРИТМА ПРОСТРАНСТВЕННО-ВЕКТОРНОЙ МОДУЛЯЦИИ В МНОГОУРОВНЕВЫХ ИНВЕРТОРАХ НАПРЯЖЕНИЯ

**Вертегел Д.А.**
**Научный руководитель – к.т.н., доцент Томасов В.С.**

Одним из основных путей повышения качества регулируемого электропривода является минимизация пульсаций формируемого преобразователем частоты тока статора. Решение этой проблемы может быть достигнуто за счет применения многоуровневых структур инверторов напряжения, а также за счет совершенствования алгоритмов управления силовыми ключами. В работе был представлен сравнительный анализ различных алгоритмов широтно-импульсной модуляции для пятиуровневого каскадного инвертора напряжения.
**Ключевые слова:** многоуровневые преобразователи частоты, алгоритмы управления, приборный электропривод, силовая электроника, инверторы напряжения.

На сегодняшний день в связи с развитием силовых полупроводниковых ключей и повышением требований к качеству потребляемой из сети электроэнергии многоуровневые инверторы напряжения находят все более широкое применение в различные системах электропитания, в том числе в прецизионных регулируемых электроприводах [1, 2]. Основными достоинствами многоуровневых топологий преобразователей частоты являются снижение уровня высших гармоник в выходном напряжении и токе инвертора, а также увеличение диапазона регулирования напряжения на нагрузке, что обеспечивается за счет сочетания в преобразователе двух типов модуляции: амплитудной и широтно-импульсной, что позволяет достичь высокого качества регулирования скорости и момента в электроприводах переменного тока [3, 4]. Однако улучшение гармонического состава формируемого напряжения и тока, а также потребляемого тока инвертором, достигается не только за счет применения многоуровневых топологий преобразователей, но и за счет использования различных алгоритмов управления силовыми ключами. При этом следует учитывать, что увеличение числа уровней приводит к усложнению алгоритмов управления, что обусловлено увеличением количества полупроводниковых ключей преобразователя и, в свою очередь, является одним из основных недостатков таких устройств [5].

Целью данной работы являлась разработка оптимального алгоритма управления многоуровневым инвертором напряжения, обеспечивающего наименьший уровень пульсаций электромагнитного момента двигателей переменного тока.

Величина пульсаций электромагнитного момента непосредственно связана с качеством формируемого преобразователем тока статора. Таким образом, для минимизации пульсаций момента двигателя следует обеспечить как можно лучший гармонический состав формируемого тока статора. При этом следует учитывать, что, так как величина момента двигателя пропорциональна обобщенному вектору тока статора, то оценку качества формируемого преобразователем тока корректней производить посредством коэффициента вариации, который определяется как отношение действующего значения всех гармоник обобщенного вектора тока статора к среднему значению его модуля [4]:

$$CV = \frac{\sqrt{\frac{1}{T_1}\int_0^{T_1}\left(|\underline{I}|(t) - \overline{|\underline{I}|}\right)^2 dt}}{\overline{|\underline{I}|}}, \quad (1)$$

где $\overline{|\underline{I}|} = \frac{1}{T_1}\int_0^{T_1}|\underline{I}|(t)dt$ – среднее значение модуля вектора тока статора за время $T_1$.

Для того чтобы произвести сравнительный анализ качества тока статора, формируемого с помощью пятиуровневого каскадного преобразователя частоты с использованием различных алгоритмов широтно-импульсной модуляции (ШИМ), в пакете программ MATLAB/Simulink были реализованы соответствующие математические модели.

В основе пространственно-векторной модуляции заложено представление возможных состояний инвертора в виде базовых векторов, которые разбивают плоскость между фазными осями на треугольные сегменты и секторы, образующие равносторонние треугольники с концами соответствующих векторов в вершинах. При этом сигнал модуляции также представляется вектором, который, вращаясь внутри ограниченной базовыми векторами области, представляющей собой шестигранник, формирует мгновенные фазные напряжения в виде проекций на соответствующие фазные оси. На рис. 1 представлено разбиение плоскости базовых векторов для пятиуровневого инвертора напряжения. Числа в вершинах векторов обозначают соответствующие состояния каждой из фазных стоек преобразователя.

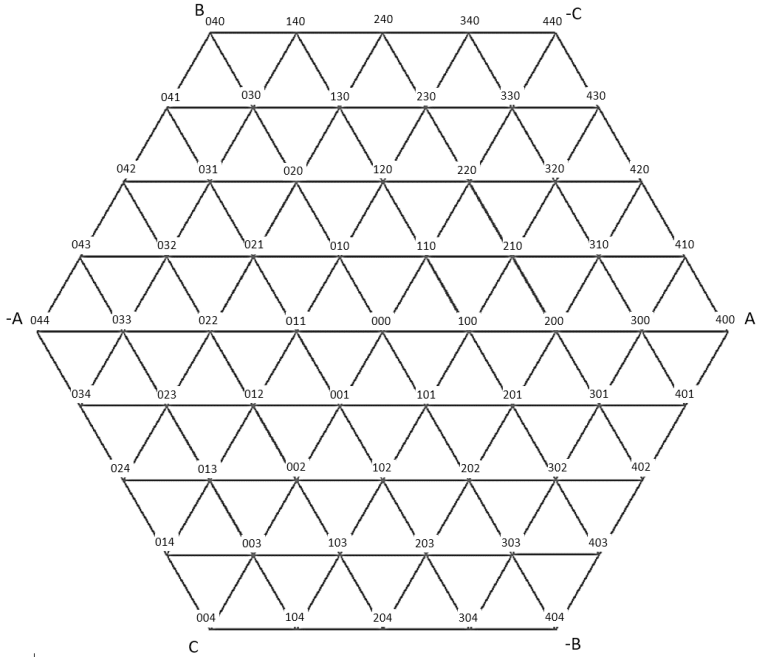



Рис. 1. Плоскость базовых векторов пятиуровневого инвертора напряжения

Для формирования требуемого напряжения в фазах инвертора, равного проекциям вектора модуляции $\underline{U}^* = U^* e^{j\vartheta^*}$ на соответствующие фазные оси, необходимо последовательно формировать базовые вектора сегмента, в котором находится конец вектора модуляции, с длительностями, пропорциональными косоугольным проекциям вектора модуляции на соответствующие стороны сегмента. Длительности включения каждого из векторов в сумме дают период модуляции $T_c = \text{const}$. Соответственно, в функции микроконтроллера входят задачи вычисления сегмента и сектора, в которых находится вектор модуляции, а также требуемых длительностей формирования базовых векторов [4].

В ходе реализации алгоритма пространственно-векторной ШИМ следует обязательно учитывать то, что изменение последовательности формирования базовых векторов за период

модуляции может приводить к увеличению уровня пульсаций выходного тока инвертора, что необходимо учитывать при изменении направления вращения вектора модуляции.

На рис. 2 приведены полученные результаты моделирования для идентичных значений индекса модуляции амплитуды. В данной работе рассмотрены четыре алгоритма формирования сигналов управления силовыми ключами преобразователя частоты: пространственно-векторная модуляции (ПВМ), ШИМ с пассивной фазой ($ШИМ_{ПФ}$), ШИМ с предмодуляцией третьей гармоникой ($ШИМ_{Пр3г}$), а также синусоидальная ШИМ ($ШИМ_{син}$).

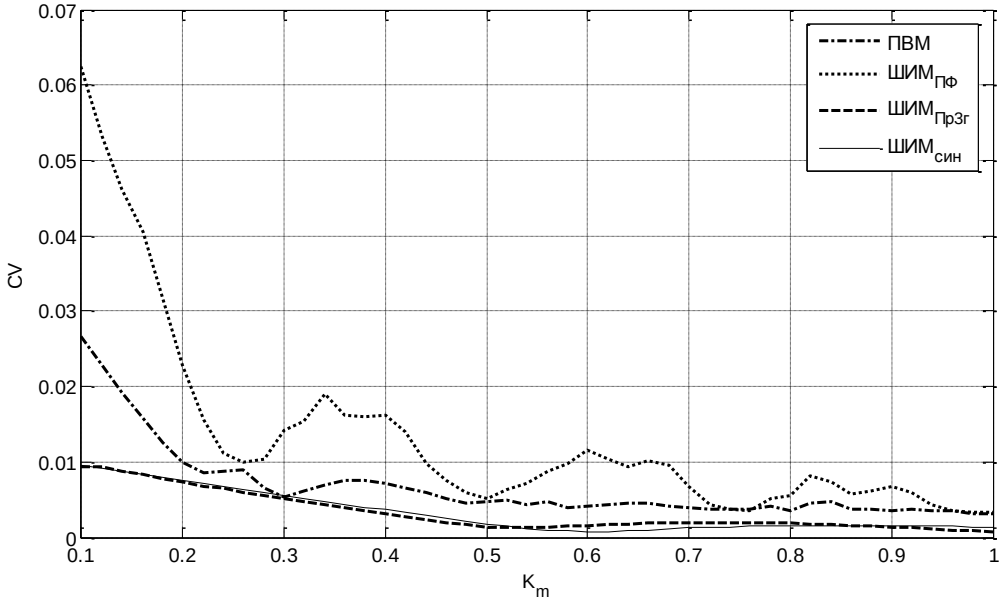



Рис. 2. Зависимость коэффициент вариации вектора тока статора от индексам модуляции амплитуды для различных алгоритмов ШИМ

Из представленных результатов моделирования можно сделать вывод, что в регулируемых электроприводах переменного тока применение ШИМ с предмодуляцией третьей гармоникой является предпочтительнее, так как данный алгоритм обеспечивает меньший коэффициент вариации вектора тока статора во всем диапазоне изменения индекса модуляции амплитуды, что, в свою очередь, обеспечивает меньший уровень пульсаций электромагнитного момента.

**Литература**

1. Донской Н., Иванов А.Г., Матисон В.А. Многоуровневые инверторы для электропривода и электроэнергетики // Силовая электроника. – 2008. – Т. 15. – № 1. – С. 43–46.
2. Михеев К.Е., Томасов В.С. Анализ энергетически показателей многоуровневых полупроводниковых преобразователей систем электропривода // Научно-технический вестник ИТМО. – 2012. – № 1(77). – С. 46–52.
3. Кумаков Ю.А. Инверторы напряжения со ступенчатой модуляцией и активная фильтрация высших гармоник [Электронный ресурс]. – Режим доступа: http://www.news.elteh.ru/arh/2005/36/12.php, своб.
4. Томасов В.С., Усольцев А.А., Вертегел Д.А., Стжелецки Р. Пространственно-векторная модуляция в многоуровневых инверторах сервоприводов телескопов траекторных измерений // Изв. вузов. Приборостроение. – 2017. – Т. 60. – № 7. – С. 624–634.
5. Лазарев Г.Б. Высоковольтные преобразователи для частотно-регулируемого электропривода. Построение различных схем [Электронный ресурс]. – Режим доступа: http://www.indautomation.ru/downloads/ab/pf/vysokovoltnye_preobrazovateli_doklad.pdf, своб.

**Воробьев Константин Александрович**
Год рождения: 1991
Университет ИТМО, факультет систем управления и робототехники, кафедра электротехники и прецизионных электромеханических систем, аспирант
Направление подготовки: 09.06.01 – Информатика и вычислительная техника
e-mail: yakko@nxt.ru

**Поляков Николай Александрович**
Год рождения: 1988
Университет ИТМО, факультет систем управления и робототехники, кафедра электротехники и прецизионных электромеханических систем, к.т.н.
e-mail: polyakov_n_a@corp.ifmo.ru

**УДК 621.314.5: 681.537**

# АЛГОРИТМ ПРОСТРАНСТВЕННО-ВЕКТОРНОЙ МОДУЛЯЦИИ ДЛЯ ПОЛУПРОВОДНИКОВЫХ ПРЕОБРАЗОВАТЕЛЕЙ СИСТЕМ ЭЛЕКТРОПРИВОДА

**Воробьев К.А., Поляков Н.А.**
**Научный руководитель – к.т.н., доцент Томасов В.С.**

Работа выполнена в рамках темы НИР № 713567 «Исследование, анализ и синтез электромеханических систем с двухсторонним обменом энергией».

В работе рассмотрено математическое описание алгоритма трехмерной пространственно-векторной модуляции в применении к активному выпрямителю напряжения. Исследована возможность параллельной работы преобразователей. Показана невозможность их работы при использовании классических алгоритмов пространственно-векторной модуляции из-за возникновения токов нулевой последовательности. Была разработана модель в пакете MATLAB/Simulink системы управления активным выпрямителем и исследована возможность параллельной работы двух преобразователей при использовании алгоритма трехмерной пространственной модуляции с целью контроля токов нулевой последовательности. В результате удалось создать действующую имитационную модель преобразователей с предложенной системой управления, в которой достигаются условия работы при минимальных токах нулевой последовательности.
**Ключевые слова:** пространственно-временная модуляция, активный выпрямитель напряжения, полупроводниковый импульсный преобразователь, активный преобразователь.

На данный момент полупроводниковые преобразователи с широтно-импульсной модуляцией получили широкое практическое применение. Существует множество реализаций систем управления ими и их практического применения. В частности, широкое применение нашли преобразователи с методом управления, основанном на пространственно-векторной модуляции (ПВМ) [1, 2].

В данной работе рассмотрена параллельная работа активных выпрямителей напряжения (АВН) с управлением комбинированным методом 3D ПВМ (рис. 1), предложенный для трехфазных управляемых инверторов. Важным достоинством данного метода управления по сравнению с классической αβ ПВМ – контроль токов нулевой последовательности [3–5].

АВН имеют существенный недостаток, ограничивающий их возможность параллельной работы – наличие тока нулевой последовательности, циркулирующего между

преобразователями, что в лучшем случае ведет к значительному уменьшению КПД, а в худшем может привести к отказу, ввиду протекания больших токов между преобразователями [6, 7].

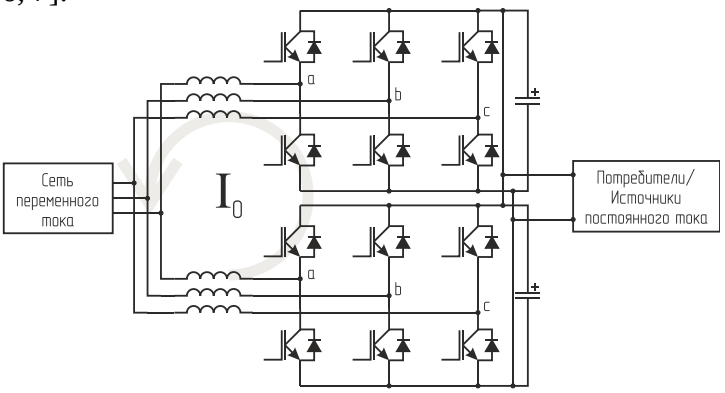



Рис. 1. Упрощенная схема параллельного включения АВН

Фактически 3D ПВМ является αβ ПВМ, но дополнительно добавляется еще одна координата для нулевой составляющей (обозначена как γ для исключения путаницы с началом координат). Для перехода к αβ0 из симметричной трех фазной системы координат выполняется известное преобразование Кларка [1, 4]:

$$\begin{bmatrix} v_\alpha \\ v_\beta \\ v_0 \end{bmatrix} = \frac{1}{3} \begin{bmatrix} 1 & -\frac{1}{2} & -\frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} & -\frac{\sqrt{3}}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{bmatrix} \begin{bmatrix} v_a \\ v_b \\ v_c \end{bmatrix}.$$

Все вектора, которые возможно сформировать в нормализованном виде к напряжению звена постоянного тока приведены в табл. 1.

Таблица 1. Формируемые преобразователем векторы

| Вектор | Координаты *abc* | | | Координаты αβ0 | | |
|---|---|---|---|---|---|---|
| | $v_a$ | $v_b$ | $v_c$ | $v_\alpha$ | $v_\beta$ | $v_0$ |
| $V_0$ | –1 | –1 | –1 | 0 | 0 | –1/2 |
| $V_1$ | 1 | –1 | –1 | 2/3 | 0 | –1/6 |
| $V_2$ | 1 | 1 | –1 | 1/3 | $1/\sqrt{3}$ | 1/6 |
| $V_3$ | –1 | 1 | –1 | –1/3 | $1/\sqrt{3}$ | –1/6 |
| $V_4$ | –1 | 1 | 1 | –2/3 | 0 | 1/6 |
| $V_5$ | –1 | –1 | 1 | –1/3 | $-1/\sqrt{3}$ | –1/6 |
| $V_6$ | 1 | –1 | 1 | 1/3 | $-1/\sqrt{3}$ | 1/6 |
| $V_7$ | 1 | 1 | 1 | 0 | 0 | 1/2 |

В 3D ПВМ 6 активных векторов делят пространство на 6 призм, каждая из которых может быть разделена на два тетраэдра. Каждая призма включает в себя 4 вектора – 2 активных и 2 нулевых. В свою очередь, призма включает два тетраэдра, гранями которых являются два активных вектора и один нулевой [3].

Вектор напряжения определяется как в 2D ПВМ:

$$T_d \bar{v} = \bar{V}_x t_x + \bar{V}_y t_y + \bar{V}_z t_z,$$

где $T_d$ – период модуляции, $\bar{V}_x = \begin{bmatrix} v_\alpha^x & v_\beta^x & v_0^x \end{bmatrix}^T$, $\bar{V}_y = \begin{bmatrix} v_\alpha^y & v_\beta^y & v_0^y \end{bmatrix}^T$ – активные векторы, $\bar{V}_z$ – нулевые векторы, $t_x$, $t_y$ и $t_z$ – время включения векторов. Выбор $x$ и $y$ осуществляется по табл. 2.

Таблица 2. Селектор номеров векторов в призме

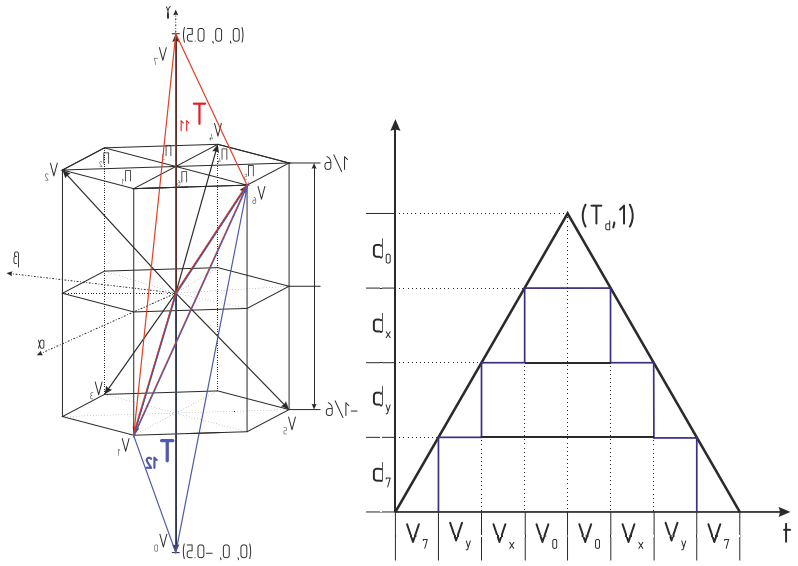
| | $П_1$ | $П_2$ | $П_3$ | $П_4$ | $П_5$ | $П_6$ |
|---|---|---|---|---|---|---|
| $x$ | 1 | 3 | 3 | 5 | 5 | 1 |
| $y$ | 2 | 2 | 4 | 4 | 6 | 6 |

Коэффициент заполнения определяются из выражений (1) и (2):

$$\begin{bmatrix} d_x \\ d_y \\ d_z \end{bmatrix} = M_\tau \cdot \begin{bmatrix} v_\alpha \\ v_\beta \\ v_0 \end{bmatrix}, \quad (1)$$

где τ – номер тетраэдра.

$$\begin{aligned} d_7 &= 0,5(1 - d_x - d_y + d_z) \\ d_0 &= 0,5(1 - d_x - d_y - d_z) \end{aligned} \quad (2)$$




а б

Рис. 2. Пространство векторов αβγ (αβ0) (а) и сечение αβ0 (б)

Для формирования импульсов управления полупроводниковыми вентилями используется симметричная модуляция (рис. 2, б).

На основании предложенного метода была разработана имитационная модель преобразователя в системе MATLAB/Simulink. В частности, была рассмотрена параллельная работа АВН с входным LCL Т-образным фильтром, в одном из которых реализована 3D ПВМ, в другом – 2D. Выходное напряжение АВН выбрано 750 В, нагрузка активная – 75 Ом.

В случае идеального равенства параметров фильтра и синхронного запуска преобразователей токи нулевой последовательности должны отсутствовать. Такой вариант работы преобразователей в реальных условиях не осуществим, в силу технологических допусков изготовления компонентов и асинхронного пуска преобразователей.

Первым был рассмотрен случай асинхронного пуска, при котором сигналы запуска преобразователей расходились на 0,1 мс (рис. 3, а). Коэффициент нелинейных искажений (КНИ) фазных токов до включения контроля тока нулевой последовательности составил 1,15% для обоих преобразователей из параллели. После включения контроля преобразователь с 2D ВПМ имел КНИ 0,94%, с 3D – 1,3%. Амплитуда тока нулевой последовательности в последствие не превышала 100 мА.

Далее был рассмотрен случай расхождения на 20% емкостей конденсаторов входных фильтров (рис. 3, б). Токи нулевой последовательности также в последствие не превысили 100 мА. КНИ как и предыдущем варианте имеют схожие порядки.

Следующими были рассмотрены случаи расхождения номиналов индуктивностей фильтров на 5% и 10% (рис. 3, в, г). В обоих случаях результирующий ток нулевой последовательности не превышал 100 мА. КНИ до включения контроля также в обоих вариантах составлял порядка 2%, после токи в преобразователе с 2D ПВМ имели КНИ 0,90–0,93%, а с 3D ПВМ порядка 1,5%.

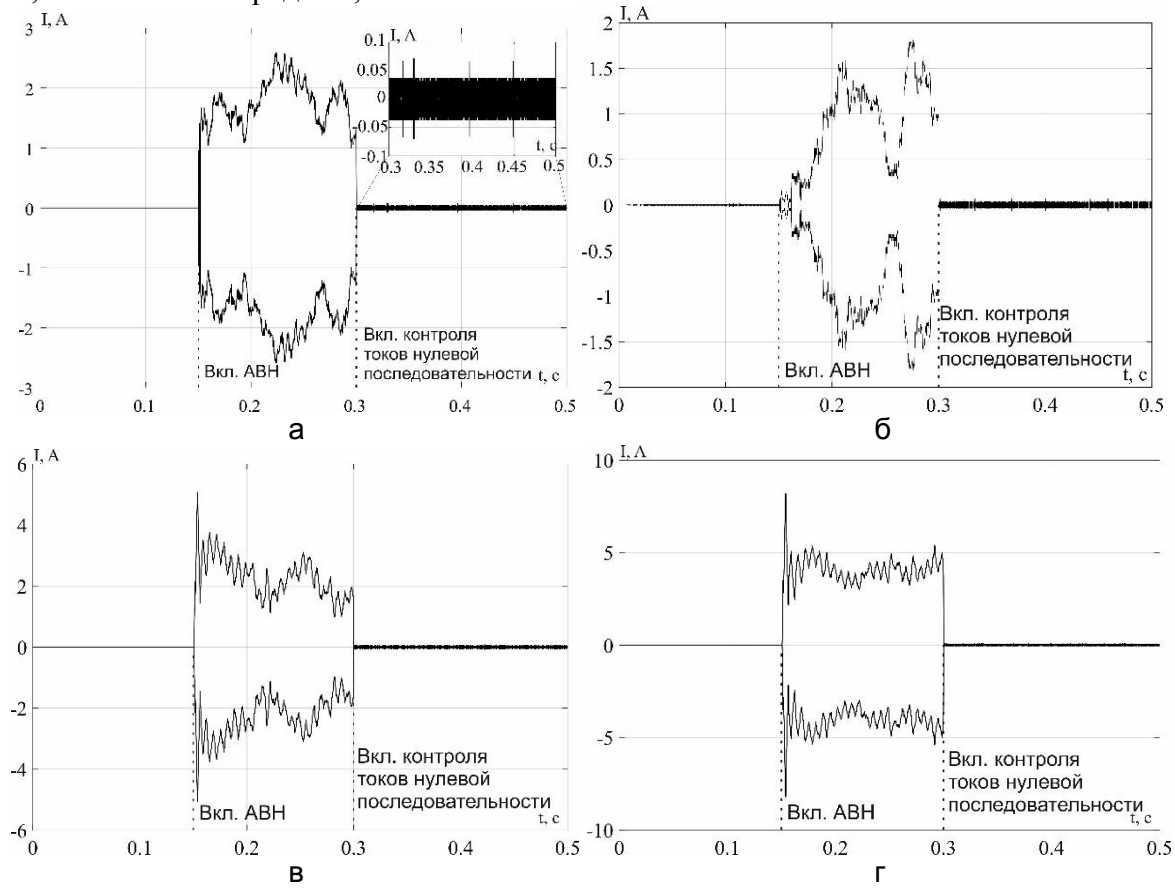



Рис. 3. Токи нулевой последовательности при асинхронном пуске (а) и при расхождении емкостей фильтров на 20% (б); номиналов индуктивностей фильтров на 5% (в) и 10% (г)

В результате была получена модель, в которой показан метод управления АВН с помощью ПВМ, препятствующий появлению токов нулевой последовательности между преобразователями, что и предполагалось достичь в данной работе.

**Литература**

1. Neacsu D.O. Switching Power Converters Medium and High Power. – CRC Press, 2014. – 567 p.
2. Premgamone T. и др. Three-dimension space vector modulation for three-level four-leg inverters with DC-link capacitor voltage balancing and switching loss minimization // IEEE. – 2017. – P. 578–584.
3. Albatran S., Fu Y., Albanna A. A hybrid 2D-3D SVM control algorithm for three phase voltage source inverters // IEEE. – 2012. – P. 1–6.
4. Albatran S., Fu Y., Albanna A. Switching function notation for hybrid 2D-3D space vector modulation // IEEE. – 2013. – P. 1–7.
5. Xiong Liu, Peng Wang, Poh Chiang Loh A Hybrid AC/DC Microgrid and Its Coordination Control // IEEE Transactions on Smart Grid. – 2011. – V. 2(2). – P. 278–286.
6. Abe R. и др. Development of multiple space vector control for direct connected parallel current source power converters // IEEE. – 1997. – P. 283–288.
7. Ye Z., Boroyevich D., Lee F.C. Modeling and control of zero-sequence current in parallel multi-phase converters // IEEE. – 2000. – P. 680–685.

**Григорьев Игорь Станиславович**
Год рождения: 1992
Университет ИТМО, факультет систем управления и робототехники,
кафедра электротехники и прецизионных электромеханических систем,
студент группы № Р4245
Направление подготовки: 13.04.02 – Электроэнергетика
и электротехника
e-mail: grigoryev.igor.st@gmail.com

**УДК 681.5.033.5**

# ИССЛЕДОВАНИЕ И СРАВНИТЕЛЬНЫЙ АНАЛИЗ РЕАКЦИЙ НА ДИНАМИЧЕСКИЕ ВОЗМУЩЕНИЯ СЛЕДЯЩИХ ЭЛЕКТРОПРИВОДОВ СИСТЕМ НАВЕДЕНИЯ КВАНТОВО-ОПТИЧЕСКИХ КОМПЛЕКСОВ

**Григорьев И.С.**
**Научный руководитель – к.т.н., доцент Толмачев В.А.**

Работа выполнена в рамках темы НИР № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность».

Рассмотрены варианты построения систем управления электроприводом исполнительных осей телескопа с учетом предъявляемых требований к максимальным значениям ошибки, а также скорости ее изменения и ускорения. Рассмотрены системы регулирования угла с внутренним контуром скорости и без него. Получены аналитические выражения для динамического отклонения угла в структурах с одномассовым механизмом.
**Ключевые слова:** следящий электропривод, подчиненное регулирование, система наведения, наблюдатель момента нагрузки, динамическое отклонение угла.

При построении систем управления электроприводом исполнительных осей телескопа могут предъявляться требования к мгновенному значению ошибки слежения, что приводит к необходимости исследования динамических ошибок, обусловленных влиянием моментов нагрузки [1]. Работа посвящена сравнительному анализу динамических характеристик двухконтурной и трехконтурной систем управления следящего электропривода оси опорно-поворотного устройства (ОПУ) с позиции подавления возмущений, вызванных нагрузкой.

Анализ влияния динамических возмущений на процессы слежения проводится с использованием понятия динамического отклонения угла, как функции зависимости от времени величины отклонения угла, вызываемого моментом возмущения на оси, относительно заданной величины.

Механизм исполнительной оси – двухмассовый со следующими параметрами:
- момент инерции первой массы $J_1$=10 кг·м$^2$;
- момент инерции второй массы $J_2$=2095 кг·м$^2$;
- коэффициент жесткости $c_{12}$=8,4·10$^7$ Н·м/рад.

Для принятого объекта с использованием алгоритма, представленного в работе [2], синтезированы трехконтурная (рис. 1) и двухконтурная (рис. 2) структуры системы регулирования угла. На рис. 1 и 2 введены следующие обозначения: $U_{зад}$ – сигнал задания; $Kp_3$, $Ti_3$ – коэффициент пропорциональности и постоянная времени пропорционально-интегрального регулятора (ПИ-регулятора) угла; $Kp_2$, $Ti_2$ – коэффициент пропорциональности и постоянная времени регуляторов скорости внутреннего и внешнего контура соответственно; $K_m$, $K_\omega$, $K_\alpha$ – коэффициенты передачи датчиков момента скорости и угла соответственно; $K_{pd}$, $Td$, $Tv$ – коэффициент пропорциональности и постоянные времени ПД-регулятора углового контура.

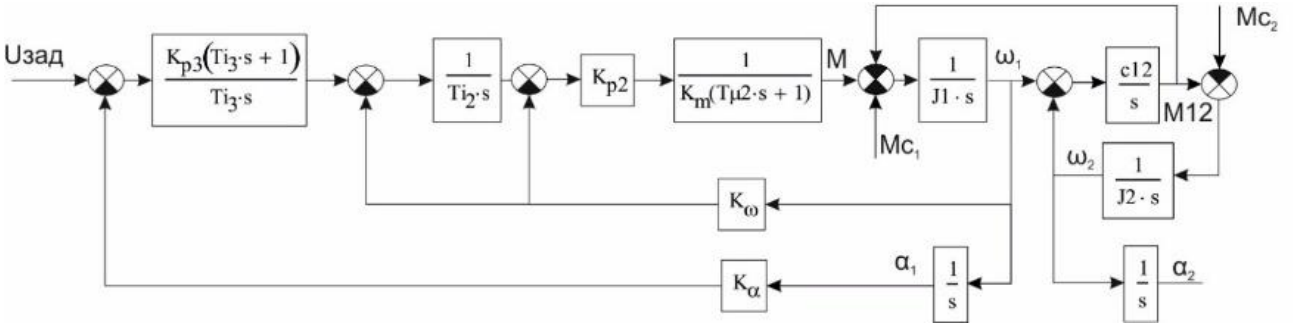



Рис. 1. Трехконтурная система регулирования угла

Для каждой из структур проведен анализ характеристик точности и быстродействия, полученных при использовании как одномассовой модели (без учета нежесткости), так и двухмассовой моделей механизма исполнительной оси.

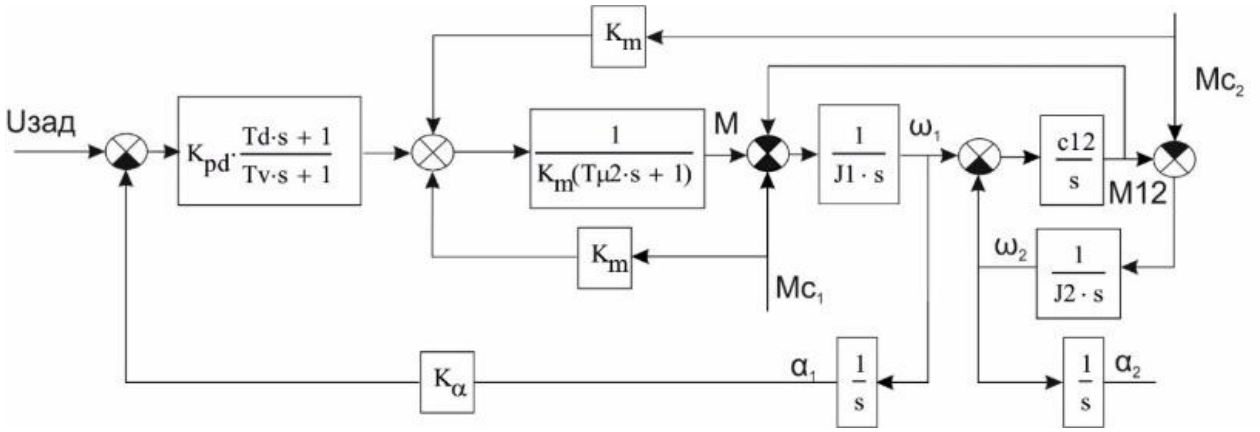



Рис. 2. Двухконтурная система регулирования угла

Двухконтурная система (рис. 2) не обладает астатизмом по возмущению, при этом действие возмущающего момента компенсируется добавкой $K_m \cdot Mc_1 + K_m \cdot Mc_2$ на входе контура регулирования момента. При получении аналитического выражения для динамического отклонения угла компенсация момента нагрузки принимается идеальной, однако для ее реализации в системе синтезируется наблюдатель согласно [3], входным сигналом которому служит момент двигателя. По результатам анализа переходных характеристик (при скачкообразном изменении момента нагрузки) получены выражения максимумов динамического отклонения угла для системы управления эквивалентным одномассовым механизмом:

$$\alpha_{3k\_\max} = \frac{-0,42Mc}{J_\Sigma} T\mu 4^2,\ \alpha_{2k\_\max} = \frac{-2,1Mc}{2J_\Sigma} T\mu 3^2, \qquad (1)$$

где $\alpha_{3k\_\max}, \alpha_{2k\_\max}$ – максимум динамического отклонения для трехконтурной и двухконтурной структур, рад; $J_\Sigma$ – эквивалентный суммарный момент инерции, кг·м$^2$; $T\mu 4$, $T\mu 3$ – некомпенсируемые постоянные времени углового контура в трехконтурной и двухконтурной структурах, с; $Mc$ – величина скачка момента нагрузки, Н·м.

Значения максимальных отклонений, полученные по выражениям (1), полностью совпадают с результатами моделирования (рис. 3). Для учета инерционности наблюдателя достаточно скорректировать некомпенсируемую постоянную времени углового контура на величину постоянной времени наблюдателя.

При рассмотрении двухмассовой модели механизма система регулирования угла с контуром скорости (рис. 2) была реализована согласно методике [1]. Угловой контур в двухконтурной структуре настраивается на симметричный оптимум с учетом частоты среза $\omega_{0res}$ и полученной постоянной времени $T\mu f$ аналогично [2]. При этом быстродействие

синтезированной двухконтурной системы повышается в 4 раза по отношению к трехконтурной, поскольку на резонансную частоту настраивается непосредственно угловой контур. Это, в свою очередь, приводит к уменьшению величины динамического отклонения угла.

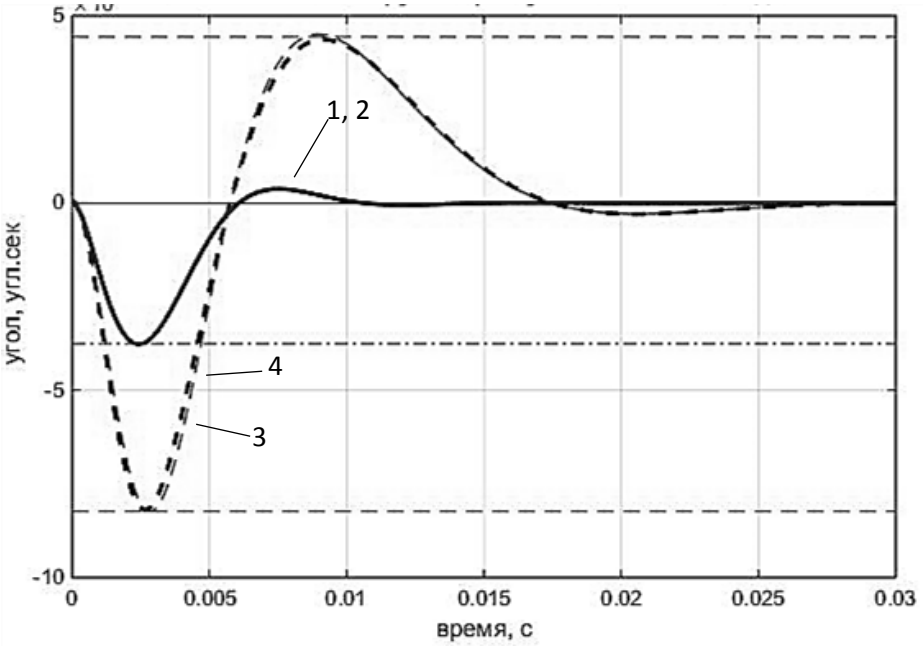



Рис. 3. Реакция на скачок возмущающего воздействия $Mc_1$=100 Н·м: кривые 1, 2 – расчетный и полученный на модели угол поворота оси в двухконтурной системе регулирования; кривые 3, 4 – расчетный угол и полученный на модели угол поворота оси в трехконтурной системе регулирования

Моделирование систем с двухмассовой моделью механизма показало, что аналитические выражения для расчета динамического отклонения угла, полученные для системы с одномассовой моделью механизма применимы и к системе с двухмассовой моделью механизма при выборе трехконтурной структуры системы. Расчет динамического отклонения угла с использованием вышеуказанных соотношений для двухконтурной структуры с двухмассовым механизмом приводит к значительной погрешности (рис. 4).

Для двухконтурной структуры с двухмассовым механизмом был синтезирован наблюдатель момента нагрузки по методике работы [3], входным сигналом которого служит электромагнитный момент двигателя. Наблюдатель момента нагрузки в данном случае восстанавливает сумму значений моментов нагрузок на массах, что, тем не менее, позволяет обеспечить их компенсацию. Моделирование двухконтурной структуры с наблюдателем показало, что наблюдатель корректно восстанавливает значение суммы моментов нагрузок на осях, в том числе величину ветрового момента нагрузки, обеспечивая таким образом его компенсацию (рис. 5).

Полученные аналитические выражения динамического отклонения угла для обеих структур позволяют как провести математически точное сравнение двух структур по заданным показателям в случае нагрузки, представленной объектом с жесткими связями, так и оценить систему управления с выбранной структурой на соответствие заданным критериям на этапе ее проектирования. Аналитически показано и подтверждено результатами моделирования, что увеличение быстродействия за счет отказа от контура регулирования скорости в трехконтурной структуре уменьшает величину динамического отклонения угла, вызванного возмущающим моментом.

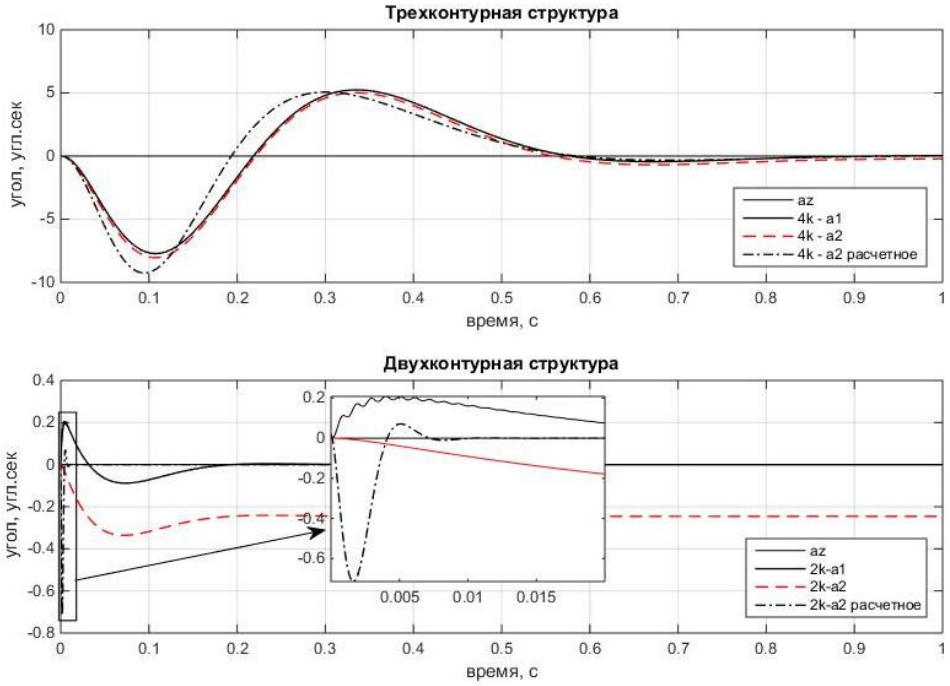



Рис. 4. Реакция систем на скачок возмущающего воздействия $M_{c2}$=100 Н·м: *az* –угол задания равный 0 угл. сек.; *a*1 – угол поворота первой массы; *a*2 – угол поворота второй массы; зависимости представлены в угловых секундах

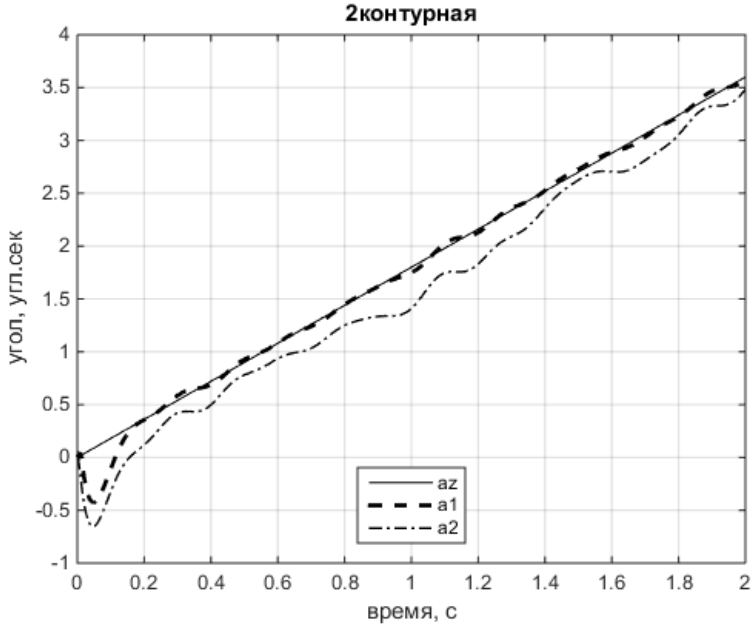



Рис. 5. Процессы слежения за линейно изменяющимся сигналом задания со скоростью 18 угл. сек./с в двухконтурной системе с наблюдателем момента нагрузки: *a*1, *a*2 – угол поворота первой и второй масс

**Литература**

1. Gawronski W. Single Loop antenna control [Электронный ресурс]. – Режим доступа: https://ipnpr.jpl.nasa.gov/progress_report/42-151/151D.pdf, своб.
2. Толмачев В.А. Синтез следящего электропривода оси опорно-поворотного устройства // Приборостроение. – 2008. – № 3. – С. 68–72.
3. Абдуллин А.А., Толмачев В.А. Система регулирования скорости двухмассового механизма с использованием наблюдателя // Приборостроение. – 2011. – № 5. – С. 66–71.

**Мухамбедьяров Бекбол Бокейханович**
Год рождения: 1993
Университет ИТМО, факультет систем управления и робототехники, кафедра электротехники и прецизионных электромеханических систем, аспирант
Направление подготовки: 09.06.01 – Информатика и вычислительная техника
e-mail: mukhambedyarovb@gmail.ru

**Лукичев Дмитрий Вячеславович**
Год рождения: 1979
Университет ИТМО, факультет систем управления и робототехники, кафедра электротехники и прецизионных электромеханических систем, к.т.н., доцент
e-mail: ludimit@yandex.ru

**УДК 681.537**

# СПОСОБЫ ПОВЫШЕНИЯ ЭНЕРГЕТИЧЕСКОЙ ЭФФЕКТИВНОСТИ АВТОНОМНЫХ СИСТЕМ С ФОТОЭЛЕКТРИЧЕСКИМИ ПРЕОБРАЗОВАТЕЛЯМИ

**Мухамбедьяров Б.Б., Лукичев Д.В.**
**Научный руководитель – к.т.н., доцент Лукичев Д.В.**

В работе рассмотрены различные способы повышения энергетической эффективности фотоэлектрических преобразователей. В частности, представлен обзор нескольких популярных видов алгоритма поиска точки максимальной мощности. Приведено сравнение показателей их эффективности и сложности реализации. Также рассмотрены системы ориентации солнечных батарей, которые используются для повышения эффективности фотоэлектрических преобразователей. Показаны значения вырабатываемой мощности при внедрении данных систем и рациональность их использования.

**Ключевые слова:** возобновляемые источники, сервопривод, ПТММ, фотоэлектрический преобразователь.

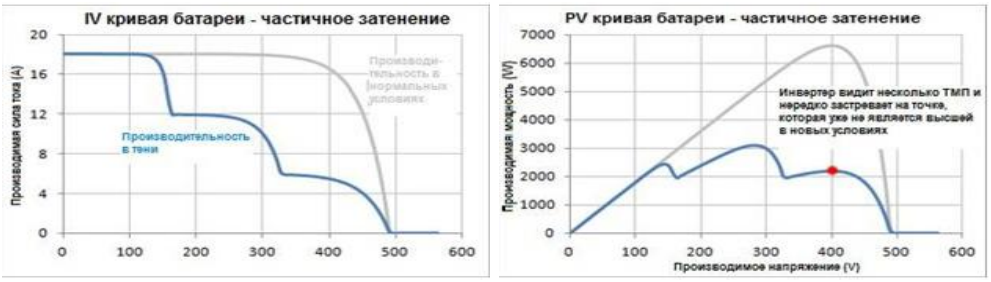
С каждым годом наблюдается усиленное развитие возобновляемых источников энергии, и эта тенденция оказывает огромное влияние на распространение и внедрение таких источников в промышленность и повседневную жизнь. С развитием силовой электроники и полупроводниковых элементов качество силовых преобразователей растет, и улучшаются их технические показатели. У фотоэлектрических преобразователей (ФЭП) относительно низкая эффективность преобразования, поэтому улучшение полной эффективности системы – важный фактор в области систем фотоэлектрических установок (ФЭУ). Это может быть частично достигнуто при помощи высокоэффективных промежуточных преобразователей с контролем точки максимальной мощности, а также внедрением систем ориентации солнечных панелей для получения как можно большей мощности от ФЭУ.

В настоящее время фотоэлемент используется во многих областях промышленности и науки. Принцип его работы и свойства достаточно хорошо известны. На данный момент КПД производимых в промышленных масштабах фотоэлементов составляет примерно 16%. У некоторых образцов этот показатель достигает 25%. КПД 46% в 2014 году получили ученые из Института солнечных энергосистем Фраунгофера в лабораторных условиях, благодаря фокусировке линзой света на фотоэлементе [1].

Существуют несколько основных необратимых потерь энергии при преобразовании в фотоэлементе [2]:
– отражение солнечного излучения от поверхности преобразователя;
– прохождение части излучения через ФЭП без поглощения в нем;
– рекомбинацией образовавшихся фото-пар, на поверхностях и в объеме ФЭП;
– внутренним сопротивлением преобразователя.

Эффективность фотоэлектрических преобразователей зависит от нескольких факторов. Структура фотоэлементов устроена таким образом, что при повышении их температуры производительность резко падает [3].

Частичное или полное затенение солнечной панели является причиной падения эффективности ФЭП. При таком режиме затененные фотоэлементы ведут себя как паразитные сопротивления, поэтому происходит падение выходного напряжения. Данную ситуацию можно обойти при помощи байпаса [4]. А также имеется возможность использования систем ориентации солнечных батарей. На рис. 1 представлены вольт-амперная и мощностная характеристики при частичном затенении.




а б

Рис. 1. Характеристики: вольт-амперная (а); мощностная (б)

Из рис. 1 видно, что при затенении происходит просадка мощности, и эффективность солнечной панели падает. Согласно формуле:

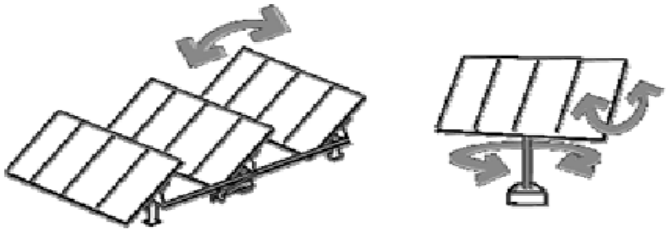
$$I_{КЗ} \sim g,$$

где $I_{КЗ}$ – ток короткого замыкания ФЭП; $g$ – количество электрон дырочных пар.

$$g = \eta \alpha J,$$

где α – показатель поглощения; η – внутренний квантовый выход; $J$ – интенсивность света.

Ток короткого замыкания пропорционален количеству электрон-дырочных пар, а их количество зависит от интенсивности света. Таким образом, понятно, что производимая мощность зависит от интенсивности света, падающего на панель. Для увеличения эффективности и площади падения света вводят системы ориентации солнечных батарей. Такие системы бывают двухосевые и одноосевые. На рис. 2 представлена система ориентации солнечных батарей.



а б

Рис. 2. Система ориентации солнечных батарей: одноосевая (а); двухосевая (б)

Опыт ученых и исследователей показывает, что двухосевая система эффективнее, но ее реализация предполагает больше усилий и затрат. В [5] собраны экспериментальные данные по эффективности внедрения систем ориентации. Данные отражены в таблице. Согласно таблице: 1 вариант – неподвижная система, 2 вариант – одноосевая система, 3 вариант –

двухосевая система. Исходя из данных приведенных в таблице, двухосевая система остается самой подходящей для повышения эффективности ФЭП.

Таблица. Выработка электрической энергии

| Показатели | Значения | | |
|---|---|---|---|
| | 1 вариант | 2 вариант | 3 вариант |
| Количество вырабатываемой электрической энергии единичной площадью солнечного фотоэлемента (СФЭ) за год, Вт·ч/год | 186269,7 | 235629,13 | 252559,14 |
| Годовые затраты электрической энергии на «собственные нужды» системы слежения для единичной площади СФЭ, Вт·ч/год | – | 725,44 | 1631,85 |
| Количество вырабатываемой электрической энергии за год солнечной фотоустановкой (СФУ) с единичной площадью СФЭ и системой слежения за Солнцем за вычетом затрат энергии на «собственные нужды», Вт·ч/год | – | 234903,7 | 250927,3 |
| Увеличение выработки электрической энергии СФУ за год при использовании системы слежения за вычетом затрат энергии на «собственные нужды» системы слежения СФУ с единичной площадью СФЭ:<br>– Вт·ч/год<br>– в % | – | <br>48634<br>26,1 | <br>64657,6<br>34,7 |

Еще одним фактором, влияющим на эффективность ФЭП, является сопротивление нагрузки. Из рис. 1, б, видно, что при определенном напряжении достигается максимальная мощность. Исходя из этого, солнечные панели не напрямую подключают к нагрузке, а используют силовые преобразователи для подбора оптимального напряжения. Поиск точки максимальной мощности (ПТММ) производиться при помощи некоторых алгоритмов.

Самыми распространенными являются:

1. отклониться и наблюдать (Perturb and Observe);
2. возрастающая проводимость (Incremental Conductance);
3. нечеткий регулятор;
4. нейронный регулятор.

На рис. 2 представлена структура системы управления преобразователем. Чаще всего используется повышающий широтно-импульсный преобразователь, поскольку напряжение на выходе в основном необходимо увеличивать.

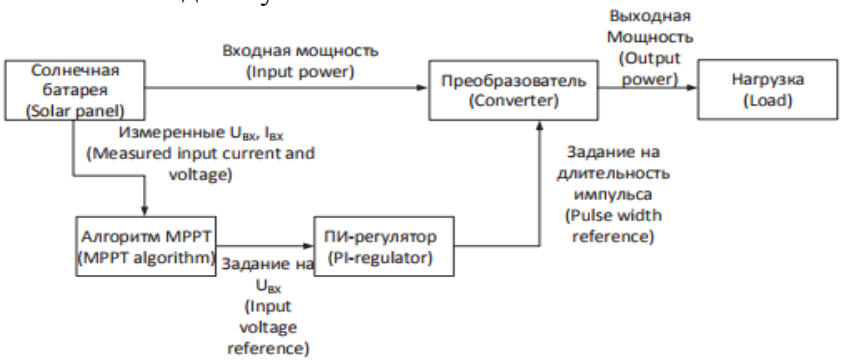



Рис. 2. Структура системы управления преобразователем

Для данной структуры реализуется один из четырех алгоритмов, представленных выше. Основной идеей всех алгоритмов является сканирование параметров системы: тока,

напряжения, мощности солнечной панели. Исходя из этих данных, необходимо увеличивать или уменьшать скважность преобразователя. Например, увеличивая скважность, замечаем, что если мощность увеличивается, то продолжаем увеличивать скважность. При уменьшении мощности, уменьшаем скважность. Описание и результаты реализации алгоритмов в модели описаны в [6]. На рис. 3 представлены результаты из [6].

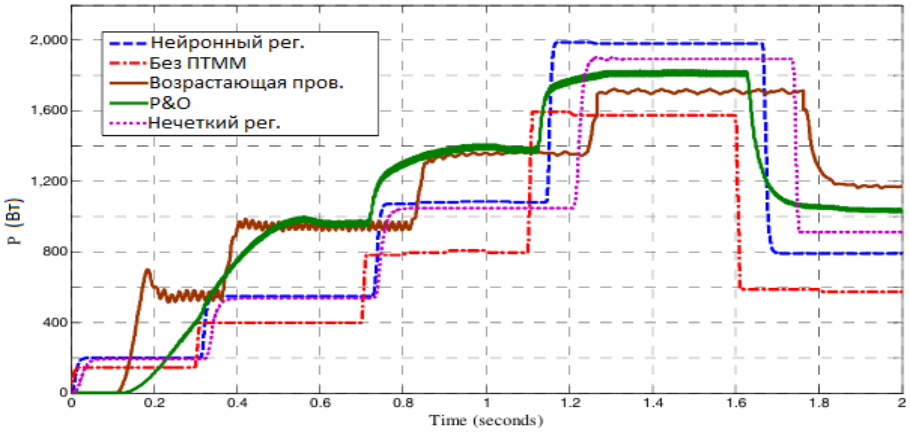



Рис. 3. Результат работы алгоритмов ПТММ

Из рис. 3 видно, что самым эффективным алгоритмом управления является внедрение нейронного регулятора. Прирост эффективности составляет 25%. Нечеткий регулятор увеличивает эффективность на 20%. Остальные алгоритмы повышают эффективность до 8–15%. Самым оптимальным методом управления является внедрение нечеткого регулятора, поскольку по сравнению с нейронным регулятором реализация становиться легче как в аппаратной части, так и в программной. По сравнения с традиционными алгоритмами прирост эффективности заметно больше.

Таким образом, внедрение систем ориентации солнечных батарей и алгоритмов поиска точки максимальной мощности дают возможность увеличить эффективность фотоэлектрической станции. Единственным недостатком реализации подобных систем является их дороговизна. Увеличение мощности ФЭУ повлекут за собой увеличение затрат.

**Литература**

1. Tibbits T.N.D., Beutel P., Grave M., Karcher C., Oliva E., Siefer G., Wekkeli A., Schachtner M., Dimroth F., Bett A.W., Krause R., Piccin M., Blanc N., Muñoz-Rico M., Arena C., Guiot E., Charles-Alfred C., Drazek C., Janin F., Farrugia L., Hoarau B., Wasselin J., Tauzin A., Signamarcheix T., Hannappel T., Schwarzburg K., Dobrich A. New efficiency frontiers with wafer-bonded multi-junction solar cells // Proceedings of the 29th European Photovoltaic Solar Energy Conference. – 2014. – P. 1975–1978.
2. Википедия [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/%D0%A4%D0%BE%D1%82%D0%BE%D1%8D%D0%BB%D0%B5%D0%BC%D0%B5%D0%BD%D1%82, своб.
3. Джумаев А.Я. Анализ влияния температуры на рабочий режим фотоэлектрической солнечной станции // Технические науки – от теории к практике. – №5 (42). – 2015. – С. 33–40.
4. Прохоров А.И. Проблемы эксплуатации солнечной электростанции при частичном затенении // Электротехнические и компьютерные системы. – 2011. – № 3. – С. 365–366.
5. Ахметшин А.Т., Ярмухаметов У.Р. Повышение эффективности солнечных фотоэлектрических установок для децентрализованного электроснабжения сельскохозяйственных потребителей // Вестник ИрГТУ. – 2015. – № 8(103). – С. 150–156.
6. Jain S., Vaibhav A., Goyal L. Comparative analysis of MPPT techniques for PV in domestic applications // Proceedings of the 6th IEEE Power India International Conference. – 2014. – P. 1–6.

**Шустов Илья Владимирович**
Год рождения: 1994
Университет ИТМО, факультет систем управления и робототехники, кафедра электротехники и прецизионных электромеханических систем, студент группы № Р4245
Направление подготовки: 13.04.02 – Электроэнергетика и электротехника
e-mail: ivshustov7394@gmail.com

**УДК 681.5.033.5**

# СИНТЕЗ СИСТЕМЫ УПРАВЛЕНИЯ СЛЕДЯЩЕГО ЭЛЕКТРОПРИВОДА С УПРУГИМИ СВЯЗЯМИ

**Шустов И.В.**
**Научный руководитель – к.т.н., доцент Толмачев В.А.**

Работа выполнена в рамках темы НИР № 617026 «Технологии киберфизических систем: управление, вычисления, безопасность».

Описана методика синтеза четырехконтурной системы управления углом поворота следящего электропривода с упругими связями. Предложен новый способ расчета коэффициента передачи пропорционального регулятора внутреннего контура скорости, позволяющий при больших коэффициентах соотношения масс расширить полосу пропускания системы управления и уменьшить динамические ошибки слежения за сигналом задания в типовых режимах работы.
**Ключевые слова:** следящий электропривод, прецизионное приборостроение, подчиненное регулирование, система наведения, оптический телескоп, упругий механизм.

Среди тенденций развития техники можно выделить, с одной стороны, повышение требований к точности воспроизведения электроприводом заданных законов движения, а с другой стороны, уменьшение массогабаритных показателей приводимых в движение механизмов. Повышение требований к точности электропривода почти всегда обуславливает необходимость повышения его быстродействия. Уменьшение массогабаритных показателей механизмов, как правило, является причиной усиления упругих связей между их звеньями. При сочетании этих факторов уменьшение динамических нагрузок и усталостных напряжений в звеньях механизмов, повышение производительности и качества технологических процессов возлагаются на систему управления электропривода. К настоящему времени проработаны вопросы построения систем управления электроприводов с упругими связями на основе структур с подчиненным регулированием [1–3] и с регуляторами состояния [1, 4]. Методики их настройки соответствуют современным методам теории автоматического управления.

В практических задачах широко распространен случай, когда механическая подсистема электропривода может быть представлена двухмассовой моделью [1]. Характерным примером такой системы является безредукторный следящий электропривод угломестной оси опорно-поворотного устройства (ОПУ) системы наведения телескопов траекторных измерений [5].

Структурная схема энергетической подсистемы безредукторного следящего электропривода угломестной оси ОПУ приведена на рис. 1.

На рис. 1 введены следующие обозначения: $K_{\text{ШИП}}$ – коэффициент усиления силового преобразователя; $c_e$, $\beta$ и $T_e$ – коэффициент противоЭДС, жесткость механической характеристики и электромагнитная постоянная электродвигателя соответственно; $J_1$ и $J_2$ – моменты инерции масс; $c_{12}$ – коэффициент крутильной жесткости; $u_y$ – управляющий сигнал информационной подсистемы; $\omega_0$ – управляющий сигнал силового преобразователя

эквивалентный скорости холостого хода электродвигателя; $p$ – оператор дифференцирования.

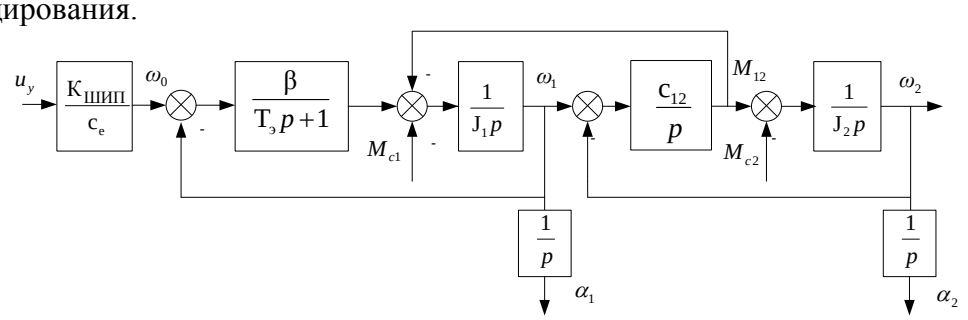



Рис. 1. Структурная схема энергетической подсистемы электропривода

Наиболее распространенным решением для следящих электроприводов систем наведения телескопов является подчиненная четырехконтурная система управления углом поворота [2], состоящая из контура регулирования момента, двух контуров регулирования скорости и внешнего контура регулирования угла поворота. Ее достоинствами являются простота и определенность выбора параметром регуляторов, простота наладки системы на реальном объекте и удобство ограничения внутренних координат. Структурная схема четырехконтурной системы управления приведена на рис. 2.

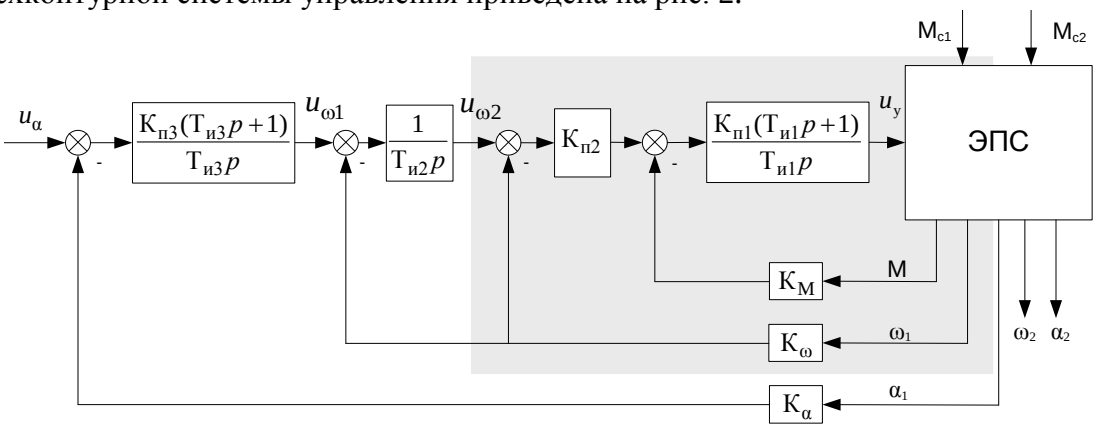



Рис. 2. Структурная схема системы управления

На рис. 2 введены следующие обозначения: $u_\alpha$ – требуемый угол поворота; $u_{\omega1}$ и $u_{\omega2}$ – сигналы задания для внешнего и внутреннего контуров регулирования скорости; $K_{п1}$ и $T_{и1}$ – коэффициент передачи и постоянная интегрирования регулятора момента; $K_{п2}$ и $T_{и2}$ – коэффициент передачи и постоянная интегрирования регуляторов скоростной подсистемы; $K_{п3}$ и $T_{и3}$ – коэффициент передачи и постоянная интегрирования регулятора угла поворота; $K_M$, $K_\omega$, $K_\alpha$ – коэффициенты датчиков момента, скорости и угла; $M$, $M_{c1}$, $M_{c2}$ – моменты двигателя и нагрузок на опорах оси; $\omega_1$, $\alpha_1$ и $\omega_2$, $\alpha_2$ – скорости и углы поворота первой и второй масс соответственно; ЭПС – энергетическая подсистема привода.

Контур регулирования момента содержит пропорционально-интегральный (ПИ) регулятор и настраивается на технический оптимум. Коэффициент передачи пропорционального (П) регулятора внутреннего контура скорости (выделен цветом на рис. 2) выбирается так, что его полоса пропускания ограничивается на уровне, определяемом резонансной частотой механизма $\Omega_0$ и коэффициентом соотношения масс $\gamma$ по формуле:

$$\omega_{ср} = \frac{\Omega_0}{\gamma^{3/4}},$$

где

$$\Omega_0 = \sqrt{\frac{c_{12}\gamma}{J_2}}\ ,\ \gamma = \frac{J_1 + J_2}{J_1} = \frac{J_\Sigma}{J_1}.$$

Внешний контур регулирования скорости настраивается на технический оптимум с использованием интегрального регулятора. Настройка контура угла поворота на симметричный обеспечивается ПИ-регулятором.

Быстродействие всей системы при этом определяется полосой пропускания внутреннего контура регулирования скорости.

Описанная настройка внутреннего контура регулирования скорости при коэффициенте соотношения масс больше девяти соответствует апериодической переходной характеристике [1]. Однако эта настройка не обеспечивает наилучшего быстродействия среди прочих настроек, соответствующих апериодическим переходным характеристикам. Таким образом, существует возможность повышения быстродействия внутреннего контура регулирования скорости и, следовательно, всей системы в целом. Выигрыш в быстродействии по отношению к системе, настроенной по методике [2], будет тем больше, чем больше коэффициент соотношения масс [1]. Синтезу системы управления, позволяющей получить этот выигрыш, и была посвящена данная работа.

На рис. 3 приведена структурная схема внутреннего контура регулирования скорости с двухмассовой механической подсистемой, в которой контур регулирования момента представлен передаточной функцией, соответствующей системе, настроенной на технический оптимум с некомпенсируемой постоянной времени $T_{\mu 1}$.

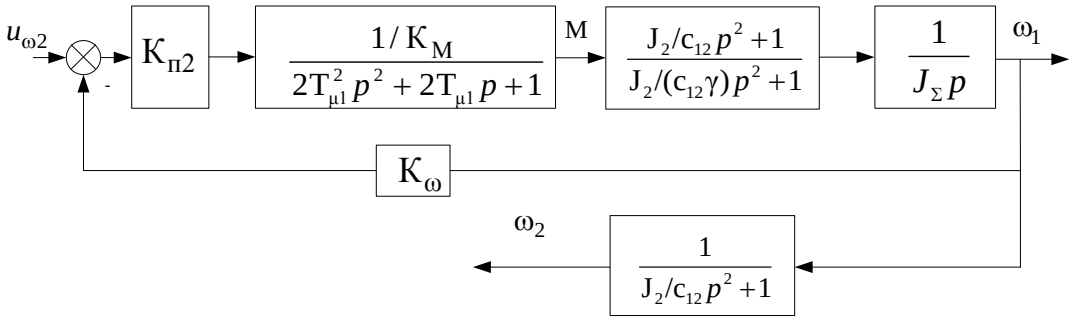



Рис. 3. Структурная схема внутреннего контура регулирования скорости

Передаточная функция системы, приведенной на рис. 3, может быть представлена выражением

$$\frac{\omega_2(p)}{u_{\omega 2}(p)} = \frac{D(p, K_{2n})}{Q(p, K_{2n})},$$

где $D(p, K_{n2})$ – характеристический полином замкнутого внутреннего контура регулирования скорости, полученный при пренебрежении малой постоянная времени $T_{\mu 1}$ и при замене переменной через среднегеометрический корень $p=p\omega_0$:

$$D(p, K_{2n}) = p^3 + a_1(K_{n2}) p^2 + a_2(K_{n2}) p + 1, \quad (1)$$

где коэффициенты $a_1(K_{n2})$, $a_2(K_{n2})$, $\omega_0(K_{n2})$ определяются параметрами энергетической подсистемы электропривода, коэффициентами передачи датчиков и коэффициентом передачи П-регулятора внутреннего контура скорости:

$$a_1(K_{2n}) = \gamma\left(\frac{K_M \Omega_0 J_\Sigma}{K_\omega K_{2n}}\right)^{-2/3},\ a_2(K_{2n}) = \left(\frac{K_M \Omega_0 J_\Sigma}{K_\omega K_{2n}}\right)^{2/3},\ \omega_0(K_{n2}) = \sqrt[3]{\frac{K_{2n} K_\omega \Omega_0^{\,2}}{K_M J_\Sigma}}.$$

Характеристический полином (1) можно разложить на множители:

$$p^3 + a_1(K_{n2}) p^2 + a_2(K_{n2}) p + 1 = (p + \alpha)(p + \beta + j\omega)(p + \beta - j\omega), \quad (2)$$

где $\alpha$ и $\beta \pm j\omega$ – вещественный и комплексно-сопряженный корни характеристического уравнения.

Вводя понятие степени колебательности $\mu = \omega/\beta$, приведем равенство (2) к виду:

$$p^3 + a_1(K_{n2})p^2 + a_2(K_{n2})p + 1 = (p+\alpha)(p+\beta+j\beta\mu)(p+\beta-j\beta\mu).$$

Подставляя вместо коэффициентов $a_1(K_{n2})$ и $a_2(K_{n2})$ их выражения, раскрывая скобки в правой части уравнения и приравнивая коэффициенты при одинаковых степенях оператора дифференцирования $p$, получим систему уравнений:

$$\gamma\left(\frac{J_\Sigma\Omega_0K_M}{K_{n2}K_\omega}\right)^{-2/3} = 2\beta+\alpha,\ \left(\frac{J_\Sigma\Omega_0K_M}{K_{n2}K_\omega}\right)^{2/3} = 2\alpha\beta+\beta^2(1+\mu^2),\ 1=\alpha\beta^2(1+\mu^2). \quad (3)$$

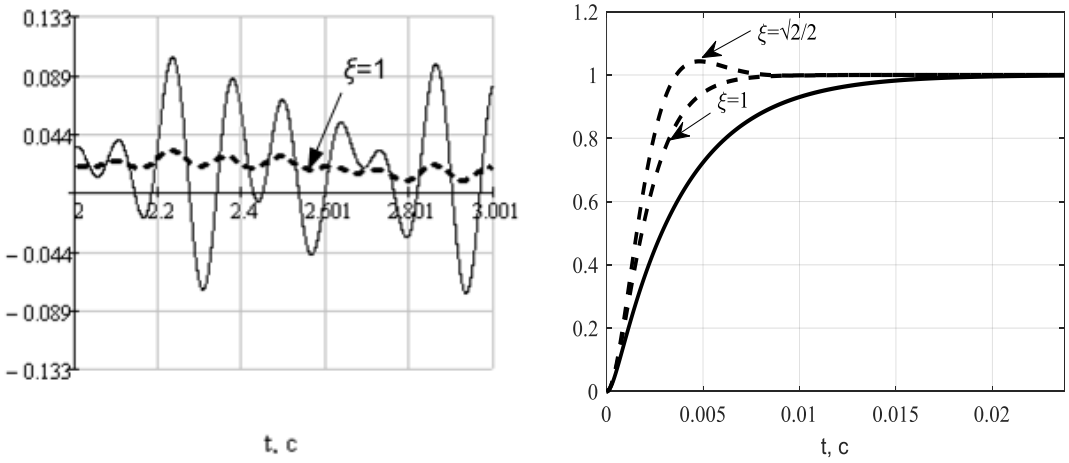
Из системы (3) можно исключить вещественный корень $\alpha$:

$$\gamma\left(\frac{J_\Sigma\Omega_0K_M}{K_{n2}K_\omega}\right)^{-2/3} = 2\beta+\frac{1}{\beta^2(1+\mu^2)},\ \left(\frac{J_\Sigma\Omega_0K_M}{K_{n2}K_\omega}\right)^{2/3} = \beta^2(1+\mu^2)+\frac{2}{\beta(1+\mu^2)}. \quad (4)$$

Систему уравнений (4) можно упростить, если перейти от степени колебательности к параметру затуханию по формуле $\mu = \sqrt{1-\xi^2}/\xi$:

$$\gamma\left(\frac{J_\Sigma\Omega_0K_M}{K_{n2}K_\omega}\right)^{-2/3} = 2\beta+\frac{\xi^2}{\beta^2},\ \left(\frac{J_\Sigma\Omega_0K_M}{K_{n2}K_\omega}\right)^{2/3} = \frac{\beta^2}{\xi^2}+\frac{2\xi^2}{\beta}. \quad (5)$$

При условии, что параметры энергетической подсистемы и параметр затухание $\xi$ заданы, в системе уравнений (5) остается только два неизвестных параметра: $K_{n2}$ и $\beta$. Решая уравнение (1) по формуле Кардано, можно найти аналитическую зависимость $\beta(K_{n2})$, тогда для оценки коэффициента передачи П-регулятора внутреннего контура скорости можно использовать любое из уравнений системы (5).




а б

Рис. 4. Переходные характеристики (а); ошибки слежения (б)

На рис. 4, а, представлены переходные характеристики внутреннего контура регулирования скорости, на рис. 4, б, – графики ошибок слежения четырехконтурной системы управления за задающим сигналом, изменяющимся с постоянным ускорением 10 град./с. Сплошные кривые соответствует системе, настроенной по методике [2], пунктирные кривые – системе, настроенной с учетом предлагаемых в данной работе корректив. Результаты моделирования соответствуют параметрам, приведенным в таблице.

Таблица. Результаты моделирования при разных параметрах затухания

| $R_ф$, Ом | $L_ф$, мГн | $c_M$, Нм/А | $c_e$, Нм/рад/с | $J_1$, Нм$^2$ | $J_2$, Нм$^2$ | $c_{12}$, Нм/рад |
|---|---|---|---|---|---|---|
| 2,3 | 12 | 62,5 | 40 | 3 | 520,4 | $4{,}44\times10^8$ |

По результатам моделирования установлено, что при настройке системы управления по предлагаемой методике при параметре затухания $\xi = 1$ полоса пропускания внутреннего контура скоростной подсистемы по отношению к [2] может быть расширена в 1,83 раза. Это,

в свою очередь, приводит к расширению полосы пропускания системы управления в целом и к снижению в несколько раз динамических ошибок слежения в типовых режимах работы (рис. 4, б).

В работе описан новый способ расчета коэффициента передачи П-регулятора внутреннего контура скорости четырехконтурной системы управления угла поворота следящего электропривода системы наведения телескопов траекторных измерений. Представленный метод синтеза системы управления позволяет достичь максимального быстродействия при заданном для внутреннего контура регулирования скоростной подсистемы параметре затухания. К достоинствам метода следует также отнести удобство отладки системы на реальном объекте и ограничение ее внутренних координат.

**Литература**

1. Борцов Ю.А., Соколовский Ю.Г. Автоматизированный электропривод с упругими связями. – 2-е изд., перераб. и доп. – СПб.: Энергоатомиздат. Сантк-Петербург. от-ние, 1992. – 288 с.
2. Толмачев В.А. Синтез следящего электропривода оси опорно-поворотного устройства // Изв. вузов. Приборостроение. – 2008. – Т. 51. – № 6. – С. 68–72.
3. Тарарыкин С.В., Тютиков С.С., Салахутдинов Н.В., Анисимов А.А. Методика проектирования цифровых полиномиальных регуляторов электромеханических систем // Вестник ИГЭУ. – 2005. – № 3. – С. 24–35.
4. Дроздов В.Н., Абдуллин А.А. Управление объектом с упругими связями // Вестник Санкт-Петербургского Государственного Университета Технологии и Дизайна. Серия 1, Естественные и технические науки. – 2012. – № 2. – С. 36–39.
5. Васильев В.Н., Томасов В.С., Шаргородский В.Д. Состояние и перспективы развития систем прецизионного электропривода комплексов высокоточных наблюдений космических объектов // Изв. вузов. Приборостроение. – 2008. – Т. 51. – № 6. – С. 5–12.

**СОДЕРЖАНИЕ**

# АЛЬМАНАХ НАУЧНЫХ РАБОТ МОЛОДЫХ УЧЕНЫХ УНИВЕРСИТЕТА ИТМО
## Том 1

В авторской редакции
Редакционно-издательский отдел Университета ИТМО
Дизайн обложки Н.А. Потехина
Зав. РИО Н.Ф. Гусарова
Редактор Л.Н. Точилина
Подписано к печати 19.11.2018
Заказ № 4141
Тираж 100 экз.