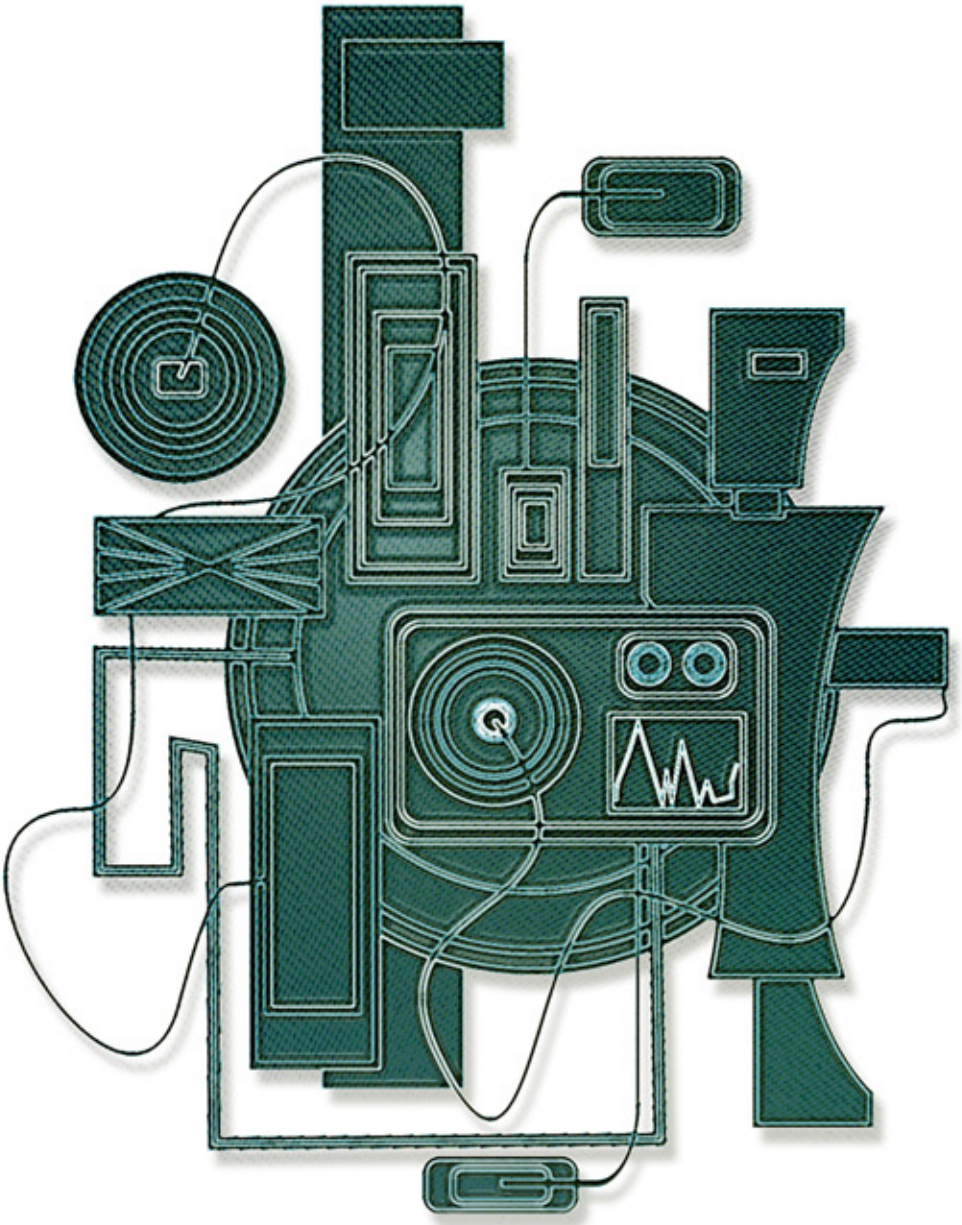
МОЛОДОЙ УЧЁНЫЙ

Международная заочная научная конференция

«Современные тенденции технических наук»



Уфа

УДК 62(01)
ББК 30
С56

С56 **Современные** тенденции технических наук: материалы междунар. заоч. науч. конф. (г. Уфа, октябрь 2011 г.). / Под общ. ред. Г.Д. Ахметовой. – Уфа: Лето, 2011. – 78 с.

ISBN 978-5-87308-042-7

В сборнике представлены материалы международной заочной научной конференции «Современные тенденции технических наук».

Предназначен для научных работников, преподавателей, аспирантов и студентов технических специальностей, а также для широкого круга читателей.

УДК 62(01)
ББК 30

ISBN 978-5-87308-042-7

СОДЕРЖАНИЕ

1. ИНФОРМАТИКА И КИБЕРНЕТИКА

2. ЭЛЕКТРОНИКА, РАДИОТЕХНИКА И СВЯЗЬ

3. АВТОМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

5. ЭНЕРГЕТИКА

6. МЕТАЛЛУРГИЯ

7. МАШИНОСТРОЕНИЕ

11. ОБЩИЕ ВОПРОСЫ ТЕХНИЧЕСКИХ НАУК

1. ИНФОРМАТИКА И КИБЕРНЕТИКА

Развитие отношений с клиентами посредством внедрения интеллектуальных систем

Алиев Камил Камандар оглы, аспирант
Липецкий государственный технический университет

Мировой кризис стал влиять в достаточной степени на рост спроса на системы, ориентированные на интеллектуальную обработку данных. Информационные системы в нашем случае требуются для анализа большого объема информации и трансформации данных для корпоративной отчетности или построения бюджетов компании. Средствами бизнес – аналитики позволяют проводить полноценный многофакторный анализ, который не достаточен для полноценного анализа данных. Здесь потребуется кластерный анализ опосредованных данных. Кластерный анализ не в полной мере отражает настоящую действительность, а именно чувствительность методов кластеризации и классификации к выбору набора параметров довольно расплывчатая.

Момент развития отношений системы и клиента начинается со сбора информации. Для этого нужно хранить и обрабатывать информацию. Данные могут добываться из разрозненных источников различными путями, в своей совокупности нередко характеризуются противоречивостью, слабой связанностью и неоднородностью. Но как это ни парадоксально, такая сырая информация имеет большую цену: плохие с точки зрения постулатов «хорошей базы данных» свойства информации – избыточность и противоречивость – позволяют, фигурально выражаясь, находить истину путем анализа противоречий лжи [1, с. 1].

Гипотетически хранить надо любую информацию, которая может быть полезна в рамках системы принятия решений. Эти сырые данные нужно объединить в единое хранилище, который представляет собой некий аппаратно-программный комплекс, гарантирующий совокупную ценность объекта. Данное предписание о целостности данных трудно отразить в системах такого уровня. Систему трудно адаптировать к предметной области. И с целью увеличения воспроизводимости данных и снижения стоимости их разработки системы проектируются те свойства объекта, которые нужны в первую очередь. Данные, для аналитической работы в необработанным виде, представляют собой многомерный куб информации.

Многомерный куб представляет собой набор функций многих переменных, заданных в кубической форме в едином пространстве. И что считать измерением, а что показателем, зависит от предметной области и целей исследования. Это своего рода некий дуализм, отражающий как направление (измерение), так и цели (показатели) [1,с. 2].

Чем больше измерений, тем больше вычислительных ресурсов требуется для анализа данных. Но с этим легко справляются приспособленные методы кластерного анализа, а именно кластеризации. Кластеризация, в общем смысле, не чувствительна к такого рода свойствам признака. Свойства исследуются при дальнейшем анализе, прибегающем совокупные методы, порой и комбинирование методов кластеризации с методами маркетинга. Методы такого совокупного анализа обеспечивают решение проблемы выбора некоторого подмножества элементов из большого исходного множества, а точнее качественной информации.

Поэтому можно сказать, что в разных задачах анализа данных приходится выбирать подмножество объектов (задача выбора прецедентов), подмножество групп объектов (задача численной таксономии или задача кластеризации данных), подмножество характеристик (задача выбора информативного пространства) и их групп (задача формирования факторов). Все это можно отнести к проблемам выбора элементов в задачах системного анализа данных, многомерного анализа данных и управления.

Развитие теории управления предприятием, инжиниринга, внутрифирменных процессов, организационных структур привело интеллектуальные системы к общему единому знаменателю – созданию систем планирования и управления внутренних ресурсов компаний. Например, ERP системы направлены на снижение внутрефирменных издержек, поиск и привлечение внутренних резервов.

Глобализация рынков, сокращение срока жизни создаваемых продуктов, усиление конкуренции привело экономические теории к созданию технологий управления взаимоотношений с клиентами (CRM). Эти стратегии направлены на максимально возможное накопление истории взаимоотношений с клиентами, касающиеся всех возможных аспектов таких взаимоотношений, обеспе-

чивающие его максимальную лояльность и удержание за счет удовлетворения его потребности в нужный момент времени в одном месте из одних рук с гарантированным качеством. Такие изменения принципов хозяйствования предприятий дали толчок созданию программных продуктов в области CRM – систем. [2, с. 1]

Возможности автоматизации деятельности аналитика в области задач анализа полученной информации, определяется наличием научно-обоснованных методик, техник и моделей работы в данном сегменте процесса анализа. Мы имеем хорошо проработанный аппарат в этой области у родственной специальности – специалистов в области маркетинга, который представлен широким спектром методик и моделей для выполнения анализа и прогнозирования ситуаций. Но рынку пока мало известно средств программного обеспечения в области информационного анализа, помогающих моделировать жизненные, социальные ситуации в зависимости от складывающихся неформальных обстоятельств, трудно поддающихся следованию объективным рыночным законам. В качестве примера: возможно, привести маркетинговое исследование возможности выхода той или иной компании, выпускающей газированную воду, на один из региональных рынков. И возможно, с точки зрения объективных законов рынка исследование покажет хорошие перспективы выхода на этот рынок у этой компании, особенно если она вооружена хорошо развитой торговой маркой в этой области.

Но аналитическое исследование тех же действий может показать совершенно обратную картину, потому что оно затронет другую сторону человеческих взаимоотношений, которая не регулируется законами рынка, этой стороной является сеть неформальных взаимоотношений субъектов. В таком исследовании уже важную роль играет категория связь объектов, их устойчивость, сила административного ресурса, оценка криминальной и политической ситуации в регионе. То есть область исследования лежит в плоскости больше социальной, чем рыночной, а здесь уже действуют другие законы и модели [2,с. 2].

Приведем конкретный пример развития отношений с клиентами посредством внедрения интеллектуальных систем. В процессе исследовательской работы над проектом «Кластерный анализ клиентской базы франчайзинговой компании» были выдвинуты следующие задачи:

1. Реализация комплекса методов кластерного анализа и проведение качественного исследования.

2. Разработка программного обеспечения иерархического метода кластеризации и метода стратегического планирования BCG Matrix.

3. Сравнительный анализ изученных методов кластеризации: метода «Кинга», метода»Форель», метода «полных связей», метода «к-средних», метода «Мак-Куина», метода «Уорда», метода «дальнего соседа» и разработанного метода кластеризации «Комбинация методов Форель и Ближайшего соседа».

4. Осуществление сегментации клиентов: использование процедуры кластерного анализа и метода стратегического планирования BCG Matrix для определения числа клиентов и их профилирования.

Целью работы является сегментация клиентов по определенным признакам, проведение интеллектуального анализа данных франчайзинговой компании, реализация методами кластерного анализа надежной системы, исследование методов кластерного анализа, сравнительный анализ методов кластеризации.

В результате проведенной работы был создан программный комплекс. Программный комплекс состоит из:

– модуля «Segmentation» – реализация комплекса методов кластерного анализа (рис. 1).

– модуля «MacrosClastering» – реализация иерархического метода «полных связей» и BCG Matrix.

Данный программный комплекс «Кластерный анализ клиентской базы франчайзинговой компании» представляет собой надежную систему и позволяет производить анализ данных, оценивать результаты с помощью визуализации данных, отчетов в графическом и текстовом виде.

Существуют другие инструменты моделирования процессов кластеризации: OSSA, MS Excel, STADIA, SPSS, STATA, STATISTICA, JMR, SYSTAT, NCSS, MINITAB 14, PRISM, Matlab, язык R (прародитель практически всех статистических пакетов). Язык R ориентируется на создание пакетов готовых решений (в различных областях).

Но в отличие от всех остальных, комплект программ «Кластерный анализ клиентской компании» открывает широкий спектр решаемых задач за счет большого количества эффективных методов кластерного анализа [3,с. 1] и использования метода BCG Matrix.

Итогом может служить тот факт, что комбинирование методов позволяет получить лучшие результаты [4,с. 2], чем одиночное использование методов кластерного анализа (кластеризации) и маркетинговых решений.

Использования метода BCG Matrix дает хорошие результаты при малом количестве признаков. Но разработанный метод «Комбинация методов Форель и Ближайшего соседа» дает наиболее лучший результат, чем метод BCG Matrix и отдельные методы кластеризации.

Основными результатами работы являются следующее:

1. Реализован комплекс методов кластерного анализа и проведен качественный анализ данных франчайзинговой компании.

2. Разработано программное обеспечение иерархического метода кластеризации и метода стратегического планирования BCG Matrix.

3. Проведен сравнительный анализ изученных методов кластеризации: метод «Кинга», метод «Форель», метод «полных связей», метод «к-средних», метод «Уорда», метод «дальнего соседа» и разработанного метода «Комбинация методов Форель и Ближайшего соседа».

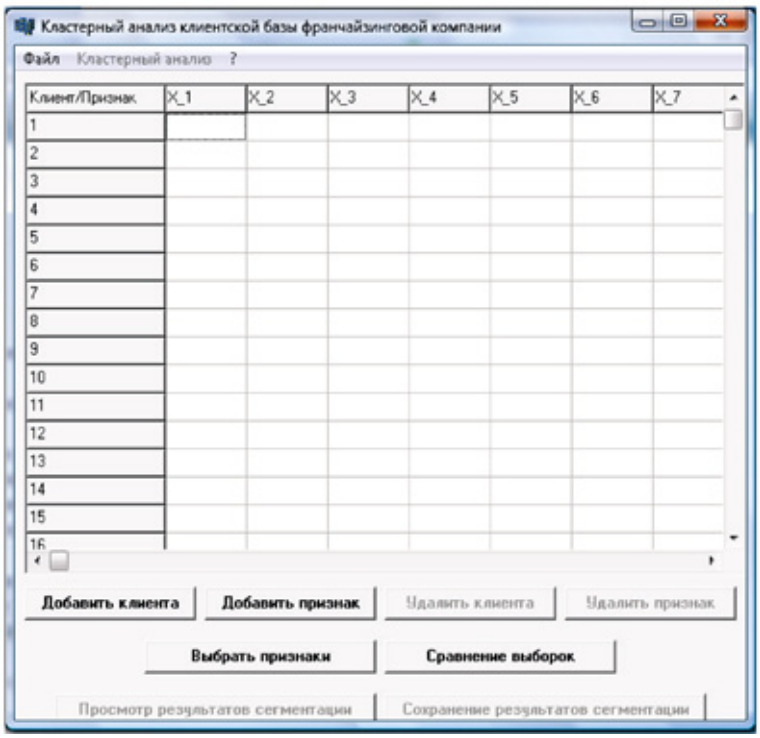


Рис. 1. Модуль «Segmentation»

4. Произведена сегментация клиентов с использованием процедуры кластерного анализа и метода стратегического планирования BCG Matrix для определения числа клиентов и их профилирования.

5. Результаты дипломной работы внедрены и используются в интеллектуальном анализе данных франчайзинговой компании ООО «Автоматизация – Л».

Таким образом, с разработкой комплекса программ «Кластерный анализ клиентской базы франчайзинговой компании» (зарегистрирован в государственном информационном фонде неопубликованных документов, номер государственной регистрации № 50200900534 программного комплекса в ФГНУ «Центр информационных технологий и систем органов исполнительной власти») является одной из систем типа CRM, применяемая для получения более «выгодных» клиентов для организации, тем самым мы определяем с помощью этой разработанной системы и разработанных методов некий прототип интеллектуальной системы, определяющая развитие отношений с клиентами посредством внедрения интеллектуальных систем.

Литература:

1. Business Intelligence и Data Mining как вклад в лояльность клиентов и рост бизнеса. http://loyaltymarketing.ru/articles/2009/12/07.html.
2. Проблемы автоматизации деятельности аналитика. http://it2b.ru/blog/arhiv/639.html.
3. Biosca, J., Lerma, J., 2008. Unsupervised robust planar segmentation of terrestrial laser scanner point clouds based on fuzzy clustering methods. ISPRS Jornal of Photogrammetry and Remote Sensing, Volume 63 (1), Pages 84–98.
4. Iyigun and A. B-I. Contour Approximation of Data: A Duality Theory, (submitted) http: // benisrael.net/DUAL-12–20–07.pdf.

Сетевые атаки. Виды. Способы борьбы

Боршевников Алексей Евгеньевич, студент
Дальневосточный федеральный университет (г. Владивосток)

В данной статье рассмотрены основные виды сетевых атак. Проведено детальное рассмотрение каждой из атак и описаны способы защиты. Статья должна послужить руководством по максимальной защите персонального компьютера подключенного к сети и личных данных пользователя этого компьютера.

Современное общество уже не может обойтись без информационных технологий. Информационные технологии проникли во все сферы жизни человека. Их неотъемлемой частью является глобальная сеть Internet. Конечно же, одной из главных задач является обеспечение безопасности обращения информации внутри сети. Одной из опасностей для безопасности являются сетевые атаки. Возникает два очевидных вопроса: «Какие виды сетевых атак бывают? Как им противостоять?»

Сетевые атаки. Виды. Способы борьбы.

Для начала установим, что такое сетевая атака. Сетевая атака – действие, целью которого является захват контроля (повышение прав) над удалённой/локальной вычислительной системой, либо её дестабилизация, либо отказ в обслуживании, а также получение данных пользователей пользующихся этой удалённой/локальной вычислительной системой.

На данный момент выделяют следующие атаки: mail-bombing, переполнение буфера, использование специализированных программ (вирусов, снифферов, троянских коней, почтовых червей, rootkit-ов и т.д.), сетевая разведка, IP-спуфинг, man-in-the-middle, инъекция (SQL-инъекция, PHP-инъекция, межсайтовый скриптинг или XSS-атака, XPath-инъекция), отказ в обслуживании (DoS- и DDoS- атаки), phishing-атаки. Рассмотрим каждую из них.

Mailbombing.

Суть данной атаки заключается в том, что на почтовый ящик посылается огромное количество писем на почтовый ящик пользователя. Эта атака может вызвать отказ работы почтового ящика или даже целого почтового сервера. Данная атака может проводиться любым хотя бы немного подготовленным противником. Простым примером программы, с помощью которой можно осуществить подобную атаку – The Unabomber. Достаточно знать адрес сервера, позволяющего анонимно отправлять почтовые сообщения, и адрес пользователя, которому эти сообщения предназначены. Количество писем, которое можно отослать для этой программы равно 12 разрядному числу. Рассмотрим способы защиты от данной атаки.

1. Давать адрес электронной почты только проверенным источникам.

2. В качестве преграды для mailbombing-а может выступать и Web-сайт провайдера, иногда настраиваемый таким образом, чтобы он автоматически определял почтовые атаки. В большинстве случаев они распознаются сервером посредством сравнения исходных IP-адресов входящих сообщений. Если количество сообщений из одного источника превышает некие разумные пределы, то все они автоматически поступают в Recycle Bin на сервере. Конечно же, ничто не мешает злоумышленнику фальсифицировать собственный IP-адрес.

Обычно к таким атакам опытные злоумышленники прибегают крайне редко.

Переполнение буфера (buffer overflows).

Атака на переполнение буфера основывается на поиске программных или системных уязвимостей, способных вызвать нарушение границ памяти и аварийно завершить приложение или выполнить произвольный бинарный код от имени пользователя, под которым работала уязвимая программа. Если программа работает под учетной записью администратора, то данная атака может позволить получить полный контроль над компьютером, на котором исполняется данная программа. [3]

Реализации атаки требует решения двух подзадач:

1. Подготовка кода, который будет выполняться в контексте привилегированной программы.

2. Изменение последовательности выполнения программы с передачей управления подготовленному коду.

Классификация атак по переполнению буфера представлена в таблице 1.

Исходя из подзадач, реализацию которых требует атака, выделяют следующие способы борьбы с атаками подобного типа:

1. Корректировка исходных кодов программы для устранения уязвимостей. Переполнение буфера происходит, прежде всего, из-за неправильного алгоритма работы программы, который не предусматривает проверок выхода за границы буферов. Также возможно применение специальных утилит автоматического поиска уязвимостей в исходном коде программы. Указанные методы и средства позволяют создавать более защищенные программы, но не решают проблему в принципе, а лишь минимизируют число уязвимостей по переполнению буфера. Данный подход ориентирован непосредственно на разработчиков программного обеспечения и не является инструментом конечного пользователя или системного администратора.

2. Использование неисполнимых буферов. Суть метода заключается в запрещении исполнения кода в сегментах данных и стека, т.е. параметры сегментов данных и стека содержат только атрибуты записи и чтения, но не

Таблица 1. Классификация атак по переполнению буфера

Подготовка кода Цель переполнения	Внедрение кода	Внедрение параметров	Не требуется
Искажение адреса возврата из функции	Атака «срыв стека»	Атака «срыв стека» с параметризацией	Атака «срыв стека» с передачей управления
Искажение указателей функций	Атака на указатели функций	Атака на указатели функций с параметризацией	Атака на указатели функций с передачей управления
Искажение таблиц переходов	Атака на таблицы переходов	Атака на таблицы переходов с параметризацией	Атака на таблицы переходов с передачей управления
Искажение указателей данных	Атака с искажением указателей данных	Атака с искажением указателей данных с параметризацией	Атака с искажением указателей данных с оригинальным кодом

исполнения. Однако ограничение на исполнение данных приводит к проблеме несовместимости. Исполняемый стек необходим для работы многим программам, так как на его основе генерируется код компиляторами, реализуются системные функции операционных систем, реализуется автоматическая генерация кода. Защита с использованием неисполнимых буферов предотвратит только атаки с внедрением кода, но не поможет при других видах атак.

3. Применение проверок выхода за границы. В основе данного метода лежит выполнение проверок выхода за границы переменной при каждом обращении к ней. Это предотвращает все возможные атаки по переполнению буфера, так как полностью исключает само переполнение. Однако, у этого решения есть существенный недостаток – значительное (до 30 раз) снижение производительности программы.

4. Применение проверок целостности. Решение, основанное на данном методе, получено благодаря проекту Synthetix. Цель Synthetix – специализация кода для увеличения производительности операционных систем. При этом вводится понятие так называемого квази-постоянства (Quasi-invariant), т.е. состояния среды, которое неизменно в определенных рамках. Такое квази-постоянство позволяет устранить ряд избыточного кода проверки выполнения различных условий. В рамках проекта реализован набор утилит, в том числе обеспечивающих контроль и защиту квази-постоянных состояний среды. К их числу относятся StackGuard и PointGuard.

Использование специализированных программ.

Рабочие станции конечных пользователей очень уязвимы для вирусов и троянских коней. Вирусами называются вредоносные программы, которые внедряются в другие программы для выполнения определенной нежелательной функции на рабочей станции конечного пользователя. В качестве примера можно привести вирус, который прописывается в файле command.com (главном интерпретаторе систем Windows) и стирает другие файлы, а также заражает все другие найденные им версии command.com.

«Троянский конь» – это не программная вставка, а настоящая программа, которая выглядит как полезное приложение, а на деле выполняет вредную роль. Примером типичного «троянского коня» является программа, которая выглядит, как простая игра для рабочей станции пользователя. Однако пока пользователь играет в игру, программа отправляет свою копию по электронной почте каждому абоненту, занесенному в адресную книгу этого пользователя. Все абоненты получают по почте игру, вызывая ее дальнейшее распространение.

Сниффер пакетов представляет собой прикладную программу, которая использует сетевую карту, работающую в режиме promiscuous mode (в этом режиме все пакеты, полученные по физическим каналам, сетевой адаптер отправляет приложению для обработки). При этом сниффер перехватывает все сетевые пакеты, которые передаются через определенный домен. В настоящее время снифферы работают в сетях на вполне законном основании. Они используются для диагностики неисправностей и анализа трафика. Однако ввиду того, что некоторые сетевые приложения передают данные в текстовом формате (telnet, FTP, SMTP, POP3 и т.д.), с помощью сниффера можно узнать полезную, а иногда и конфиденциальную информацию (например, имена пользователей и пароли).

Перехват имен и паролей создает большую опасность, так как пользователи часто применяют один и тот же логин и пароль для множества приложений и систем. Многие пользователи вообще имеют один пароль для доступа ко всем ресурсам и приложениям. Если приложение работает в режиме клиент/сервер, а аутентификационные данные передаются по сети в читаемом текстовом формате, эту информацию с большой вероятностью можно использовать для доступа к другим корпоративным или внешним ресурсам. [2]

Rootkit – программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в системе. Большинство из реализаций современных rootkit могут прятать от пользователя файлы, папки и ключи реестра, скрывать запущенные про-

граммы, системные службы, драйверы и сетевые соединения. Т.е. злоумышленник имеет возможность создавать файлы и ключи реестра, запускать программы, работать с сетью и эта активность не будет обнаружена администратором. Кроме того, rootkits могут скрывать сетевую активность путем модификации стека протоколов TCP/IP. Так, например rootkit Hacker Defender перехватывает вызовы Winsock и может обрабатывать сетевой трафик до того как он будет передан приложению. Т.е. если в системе установлен Web сервер, и соответственно открыт 80й порт, rootkit может использовать его для взаимодействия с взломщиком, в то время как другие пользователи будут без проблем работать по протоколу HTTP. [1]

Выделяют следующие способы борьбы с этими видами атак:

1. Использование антивирусных средств и регулярное обновление их сигнатур. Может решить проблему с троянскими программами, вирусами, почтовыми червями, но не решит проблему снифферов и rootkit-ов.

2. Шифрование передаваемых данных. Проблема не решает полностью проблему снифферов, однако, противник перехватывает данные, которые нельзя свободно прочитать. Для их расшифровки требуется время.

3. Использование антиснифферов (Например, AntiSniff или PromiScan).

4. Использование межсетевых экранов.

5. Использование антируткитов.

Сетевая разведка.

Сетевой разведкой называется сбор информации о сети с помощью общедоступных данных и приложений. При подготовке атаки против какой-либо сети злоумышленник, как правило, пытается получить о ней как можно больше информации. Сетевая разведка проводится в форме запросов DNS, эхо-тестирования (ping sweep) и сканирования портов. Запросы DNS помогают понять, кто владеет тем или иным доменом и какие адреса этому домену присвоены. Эхо-тестирование (ping sweep) адресов, раскрытых с помощью DNS, позволяет увидеть, какие хосты реально работают в данной среде. Получив список хостов, злоумышленник использует средства сканирования портов, чтобы составить полный список услуг, поддерживаемых этими хостами. И, наконец, злоумышленник анализирует характеристики приложений, работающих на хостах. В результате добывается информация, которую можно использовать для взлома. [2]

Способы борьбы с данной атакой:

1. Отключение эхо ICMP и эхо-ответ на периферийных маршрутизаторах. Это, однако, приведет к потере данных необходимых для диагностики сетевых сбоев.

2. Использование систем обнаружения вторжений (IDS).

IP-спуфинг.

IP-спуфинг происходит, когда злоумышленник, находящийся внутри корпорации или вне ее выдает себя за санкционированного пользователя. Это можно сделать двумя способами. Во-первых, злоумышленник может воспользоваться IP-адресом, находящимся в пределах диапазона санкционированных IP-адресов, или авторизованным внешним адресом, которому разрешается доступ к определенным сетевым ресурсам. Атаки IP-спуфинга часто являются отправной точкой для прочих атак. Классический пример – атака DoS, которая начинается с чужого адреса, скрывающего истинную личность злоумышленника.

Обычно IP-спуфинг ограничивается вставкой ложной информации или вредоносных команд в обычный поток данных, передаваемых между клиентским и серверным приложением или по каналу связи между одноранговыми устройствами. Для двусторонней связи злоумышленник должен изменить все таблицы маршрутизации, чтобы направить трафик на ложный IP-адрес. Некоторые злоумышленники, однако, даже не пытаются получить ответ от приложений. Если главная задача состоит в получении от системы важного файла, ответы приложений не имеют значения.

Если же злоумышленнику удается поменять таблицы маршрутизации и направить трафик на ложный IP-адрес, злоумышленник получит все пакеты и сможет отвечать на них так, будто он является санкционированным пользователем. [2]

Угрозу спуфинга можно ослабить (но не устранить) с помощью следующих мер:

1. Контроль доступа. Самый простой способ предотвращения IP-спуфинга состоит в правильной настройке управления доступом. Чтобы снизить эффективность IP-спуфигна, настройте контроль доступа на отсечение любого трафика, поступающего из внешней сети с исходным адресом, который должен располагаться внутри вашей сети. Если санкционированными являются и некоторые адреса внешней сети, данный метод становится неэффективным.

2. Фильтрация RFC 2827. Вы можете пресечь попытки спуфинга чужих сетей пользователями вашей сети (и стать добропорядочным «сетевым гражданином»). Для этого необходимо отбраковывать любой исходящий трафик, исходный адрес которого не является одним из IP-адресов вашей организации. Этот тип фильтрации, известный под названием «RFC 2827», может выполнять и провайдер. В результате отбраковывается весь трафик, который не имеет исходного адреса, ожидаемого на определенном интерфейсе.

3. Использование криптографической аутентификации.

Атака типа man-in-the-middle.

Для атаки типа Man-in-the-Middle злоумышленнику нужен доступ к пакетам, передаваемым по сети. Такой доступ ко всем пакетам, передаваемым от провайдера в любую другую сеть, может, к примеру, получить сотрудник этого провайдера. Для атак этого типа часто используются снифферы пакетов, транспортные протоколы и протоколы маршрутизации. Атаки проводятся с целью кражи информации, перехвата текущей сессии и полу-

чения доступа к частным сетевым ресурсам, для анализа трафика и получения информации о сети и ее пользователях, для проведения атак типа DoS, искажения передаваемых данных и ввода несанкционированной информации в сетевые сессии. [2]

Способы борьбы с данной атакой:

1) Использование шифрования данных

Инъекция.

SQL-инъекция.

SQL-инъекция – это атака, в ходе которой изменяются параметры SQL-запросов к базе данных. В результате запрос приобретает совершенно иной смысл, и в случае недостаточной фильтрации входных данных способен не только произвести вывод конфиденциальной информации, но и изменить/удалить данные. [4]

Способы защиты от данной атаки (используются исключительно администраторами ресурсов):

1. Для целых и дробных величин, перед их использованием в запросе достаточно привести величину к нужному типу.

```
$id= (int)$id; $total= (float)$total;
```

Вместо этого можно вставить систему слежения за тестированием на SQL инъекцию.

```
if ((string)$id<> (string) (int)$id) {
die ('ops');
}
```

2. Для строковых параметров, которые не используются в like, regexp и тд, экранируем кавычки.

```
$str=addslashes ($str);
```

или, лучше,

```
mysql_escape_string ($str)
```

3. В строках, которые предполагается использовать внутри like, regexp и тд, необходимо так же заэкранировать специальные символы, применяющиеся в этих операторах, если это необходимо. В противном случае, можно задокументировать использование этих символов.

PHP-инъекция.

PHP-инъекция – один из способов взлома веб-сайтов, работающих на PHP. Он заключается в том, чтобы внедрить специально сформированный злонамеренный сценарий в код веб-приложения на серверной стороне сайта, что приводит к выполнению произвольных команд. [5]

Способы борьбы с данной атакой (используются исключительно администраторами ресурсов):

1. Проверять, не содержит ли переменная $name посторонние символы:

```
<?
...
$name = $_GET ['name'];
if (strpbrk ($name, '.?/:')) die ('Blocked');
include $name. '.php';
...
?>
```

2. Проверять, что $name присвоено одно из допустимых значений:

```
<?
...
$name = $_GET ['name'];
$arr = array ('main', 'about', 'links', 'forum');
if (!in_array ($name,$arr)) $name = $arr [0];
include $name . '.php';
...
?>
```

Межсайтовый скриптинг или XSS-атака.

XSS атака – это атака на уязвимость, которая существует на сервере, позволяющая внедрить в генерируемую сервером HTML-страницу некий произвольный код, в котором может быть вообще все что угодно и передавать этот код в качестве значения переменной, фильтрация по которой не работает, то есть сервер не проверяет данную переменную на наличие в ней запрещенных знаков –, <, >, ', «. Значение данной переменной передается от генерируемой HTML-страницы на сервер в скрипт, ее вызвавший путем отправки запроса.

А далее начинается самое интересное для Злоумышленника. PHP-скрипт в ответ на данный запрос генерирует HTML-страницу, в которой отображаются значения требующихся злоумышленнику переменных, и отправляет данную страницу на браузер злоумышленника.

То есть, говоря проще, XSS атака – это атака с помощью уязвимостей на сервере на компьютеры клиентов.

XSS атака чаще всего используется для кражи Cookies (или куки, как их произносят по-русски). В них хранится информация о сессии пребывания пользователя на сайтах, что и бывает нужным злоумышленникам для перехвата управления личными данными пользователя на сайте в пределах, пока сессия не будет закрыта сервером, на котором размещен сайт. Помимо этого в Cookies хранится зашифрованный пароль, под которым пользователь входит на данный сайт, и при наличии необходимых утилит и желания злоумышленникам не доставляет особого труда расшифровать данный пароль.

Теперь опишем другие возможности XSS атак (конечно при условии их успешного проведения).

1. Возможно при открытии страницы вызвать открытие большого количества ненужных пользователю окон.

2. Возможна вообще переадресация на другой сайт (например, на сайт конкурента).

3. Существует возможность загрузки на компьютер пользователя скрипта с произвольным кодом (даже вредоносного) путем внедрения ссылки на исполняемый скрипт со стороннего сервера.

4. Зачастую происходит кража личной информации с компьютера пользователя, помимо Cookies в качестве объекта кражи выступает информация о посещенных сайтах, о версии браузера и операционной системе, установленной на компьютере пользователя, да к тому же еще и плюсуется IP-адрес компьютера пользователя.

5. XSS атака может быть проведена не только через сайт, но и через уязвимости в используемом программном обеспечении (в частности, через браузеры). Поэтому ре-

комендуется обновлять используемое программное обеспечение.

6. Также возможно проведение XSS атак через использование SQL-кода.

Как мы видим из всего вышесказанного, возможностей у XSS атак достаточно много. Злоумышленник может овладеть вашей личной информацией вплоть до получения паролей доступа к сайтам, а это очень неприятно. К тому же XSS атака наносит вред исключительно клиентским машинам, оставляя сервер в полностью рабочем состоянии, и у администрации различных серверов порой мало стимулов устанавливать защиту от этого вида атак.

Различают XSS атаки двух видов: активные и пассивные. При первом виде атаки вредоносный скрипт хранится на сервере и начинает свою деятельность при загрузке страницы сайта в браузере клиента. При втором виде атак скрипт не хранится на сервере и вредоносное действие начинает выполняться только в случае какого-либо действия пользователя, например, при нажатии на сформированную ссылку.

Способы борьбы с данным видом атак (используются исключительно администраторами ресурсов):

1. Запретить включение напрямую параметров $_GET, $_POST, $_COOKIE в генерируемую HTML-страницу.

2. Запретить загрузку произвольных файлов на сервер во избежание загрузки вредоносных скриптов.

3. Все загруженные файлы хранить в базе данных, а не в файловой системе.

XPath-инъекция.

XPath-инъекция – вид уязвимостей, который заключается во внедрении XPath-выражений в оригинальный запрос к базе данных XML. XPath (XML Path Language) – это язык, который предназначен для произвольного обращения к частям XML документа. XML (eXtensible Markup Language) – это всем известный язык разметки, с помощью которого создаются XML документы, имеющие древовидную структуру. [6]

Способы борьбы с этой атакой (используются исключительно администраторами ресурсов):

1. Проверка корректности. Независимо от приложения, среды или языка необходимо следовать следующим практическим правилам:

- Предполагайте, что все вводимые данные сомнительны.
- Проверяйте не только тип вводимых данных, но также их формат, длину, диапазон и содержимое (например, такое простое регулярное выражение как `if (/^»*^';&<> ()/)` должно находить большинство подозрительных специальных символов).
- Проверяйте данные как на стороне клиента, так и на стороне сервера, поскольку проверку на стороне клиента чрезвычайно легко перехитрить.
- Следуйте последовательной [missing word] стратегии защищенности приложения, основываясь на передовом опыте разработки защищенных приложений
- Тестируйте приложение на известные угрозы перед его выпуском.

2. Проверка данных на Web-сервере. Для защиты против XPath-внедрения и других форм внедрения кода необходимо проверять все данные, передаваемые от Web-сервера к службам системы хранения данных. Этот подход может быть очень хорош для некоторых приложений, которые, возможно, используют основанные на REST или SOAP XML-сервисы, но в других случаях он может быть не возможен. Как всегда наилучшим подходом является разумное проектирование, начиная с первоначального дизайна и до реализации приложения.

Отказ в обслуживании (DoS- и DDoS- атаки).

DoS, без всякого сомнения, является наиболее известной формой атак. Кроме того, против атак такого типа труднее всего создать стопроцентную защиту. Даже среди злоумышленников атаки DoS считаются тривиальными, а их применение вызывает презрительные усмешки, потому что для организации DoS требуется минимум знаний и умений. Тем не менее, именно простота реализации и огромный причиняемый вред привлекают к DoS пристальное внимание администраторов, отвечающих за сетевую безопасность.

Атаки DoS отличаются от атак других типов. Они не нацелены на получение доступа к вашей сети или на получение из этой сети какой-либо информации. Атака DoS делает вашу сеть недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения.

В случае использования некоторых серверных приложений (таких как Web-сервер или FTP-сервер) атаки DoS могут заключаться в том, чтобы занять все соединения, доступные для этих приложений и держать их в занятом состоянии, не допуская обслуживания обычных пользователей. В ходе атак DoS могут использоваться обычные Интернет-протоколы, такие как TCP и ICMP (Internet Control Message Protocol). Большинство атак DoS опирается не на программные ошибки или бреши в системе безопасности, а на общие слабости системной архитектуры. Некоторые атаки сводят к нулю производительность сети, переполняя ее нежелательными и ненужными пакетами или сообщая ложную информацию о текущем состоянии сетевых ресурсов. Этот тип атак трудно предотвратить, так как для этого требуется координация действий с провайдером. Если трафик, предназначенный для переполнения вашей сети, не остановить у провайдера, то на входе в сеть вы это сделать уже не сможете, потому что вся полоса пропускания будет занята. Когда атака этого типа проводится одновременно через множество устройств, мы говорим о распределенной атаке DoS (DDoS – distributed DoS). [2]

Угроза атак типа DoS может снижаться тремя способами:

1. Функции анти-спуфинга. Правильная конфигурация функций анти-спуфинга на маршрутизаторах

и межсетевых экранах поможет снизить риск DoS. Эти функции, как минимум, должны включать фильтрацию RFC 2827.

2. Функции анти-DoS. Правильная конфигурация функций анти-DoS на маршрутизаторах и межсетевых экранах может ограничить эффективность атак. Эти функции часто ограничивают число полуоткрытых каналов в любой момент времени.

3. Ограничение объема трафика (traffic rate limiting). Организация может попросить провайдера ограничить объем трафика. Этот тип фильтрации позволяет ограничить объем некритического трафика, проходящего по вашей сети.

Phishing-атаки.

Phishing (фишинг) – процесс обмана или социальная разработка клиентов организаций для последующего воровства их идентификационных данных и передачи их конфиденциальной информации для преступного использования. Преступники для своего нападения используют spam или компьютеры-боты. При этом размер компании-жертвы не имеет значения; качество личной информации полученной преступниками в результате нападения, имеет значение само по себе.

Приведем пример фишинг-атаки:

Пользователь получает электронную почту от support@mybank.com <mailto:support@mybank.com> (адрес – подменен) со строкой сообщения «модификация защиты», в котором ее просят перейти по адресу www.mybank-validate.info <http://www.mybank-validate.info> (имя домена принадлежит нападавшему, а не банку) и ввести его банковский PIN-код. [7]

Способы защиты от данной атаки:

- Использовать только проверенные ресурсы и пути доступа к ним.
- Использовать антивирусные средства и регулярно обновлять их сигнатуры.

Выводы.

Таким образом, были рассмотрены основные сетевые атаки и способы борьбы с ними. Данная область является наиболее развивающейся, так как идет постоянное соперничество между злоумышленниками и организациями, обеспечивающими безопасность данных. Несмотря на возможное применение комплексных мер по защите компьютера, наиболее надежным способом защиты компьютера является использование проверенных электронных ресурсов, чтение писем из проверенных источников. Т.е. наибольшую защиту от атак может обеспечить сам пользователь, соблюдая меры предосторожности.

Литература:

1. Windows под прицелом// Security Lab, декабрь 2004.
2. Кадер М. Типы сетевых атак, их описания, средства борьбы// Cisco.
3. Колищак А. Атаки на переполнение буфера// ноябрь 1999.
4. SQL-инъекция в MySQL сервере // Security Lab, декабрь 2004.
5. http://docs.php.net
6. http://www.ibm.com
7. http://os.zone.net

Обзор методов обнаружения аномалий в SQL-запросах к базам данных

Григоров Андрей Сергеевич, аспирант
Череповецкий государственный университет

Одним из способов обеспечения безопасности баз данных (БД) является использование специализированных систем обнаружения вторжений (СОВ). Под обнаружением вторжений понимается процесс выявления действий, которые способны нарушить конфиденциальность, целостность и доступность информации, хранимой в БД. Системы обнаружения вторжений являются реактивной мерой, направленной на противодействие активности злоумышленника в случаях, когда он смог преодолеть все проактивные меры.

История развития СОВ берёт своё начало в 70-х годах XX века, когда в 1972 году ВВС США был опубликован документ, в котором указывалось о необходимости развития систем компьютерной безопасности. В 1980 году Джеймс Андерсон обнародовал результаты своих исследований [1], предложив пути улучшения компьютерной безопасности на основе использования аудита и мониторинга защищаемых объектов, а в период с 1984 по 1986 год Дороти Деннинг совместно с Питером Нейманом разработали первую модель СОВ [2], ставшую основой для большинства современных систем. Следует отметить, что первые СОВ ориентировались в первую очередь на защиту от несанкционированных действий в компьютерных сетях и операционных системах, однако в дальнейшем получили развитие и другие направления. Так на сегодняшний день активно развиваются СОВ, работающие на

основе прикладных протоколов, которые используются различными программами. К таким протоколам в частности относится SQL – язык описания запросов к реляционным базам данных.

Несмотря на то, что существует достаточно большое количество методов и систем обнаружения несанкционированных действий в компьютерных сетях и операционных системах, перенос их на область баз данных в большинстве случаев оказывается невозможным. В первую очередь причина заключается в том, что действия, считающиеся вредоносными для баз данных, не всегда являются вредоносными для сети или операционной системы.

Согласно систематике СОВ, предложенной Стефаном Аксельсоном [3], выделяют три типа методов обнаружения вторжений: синтаксические методы, методы обнаружения аномалий и смешанные методы, представляющие собой композицию первых двух. К синтаксическим методам принято относить методы, базирующиеся на идее обнаружения вторжений путём сравнения SQL-запросов с шаблонами недопустимых синтаксических конструкций. Методы обнаружения аномалий, напротив, подразумевают создание шаблонов нормального поведения пользователя и последующее сравнение этих шаблонов с действиями, выполняемыми пользователями во время работы с БД.

В настоящее время большинство работ, связанных с СОВ, оценивающих адресованные к БД SQL-запросы, посвящено методам обнаружения аномалий. Предлагаемые подходы в зависимости от способа формирования и представления профиля нормального поведения можно разделить на следующие группы:

– методы, при которых профиль формируется путём синтаксического анализа текста SQL-запроса;

– методы, при которых профиль нормального поведения определяется в результате семантического анализа SQL-запроса;

– методы, учитывающие различные характеристики запроса (лексические, темпоральные, ресурсные и др.).

Синтаксические методы

В 2003 году Фредрик Валер, Дарен Мутц и Джованни Вигна из Калифорнийского университета представили новый подход для защиты веб-приложений [4]. В его основе которого лежит обучающаяся система обнаружения аномалий, использующая несколько способов обнаружения атак на БД, с которыми работают приложения. Обучение производится на базе записей из журналов приложения, которые хранят описание характерных для нормального поведения пользователя действий. Процесс обучения состоит из двух этапов. На первом этапе каждый SQL-запрос, на котором производится обучение, проходит фазу синтаксического анализа, заключающуюся в разделении текста запроса на неизменную структуру (последовательность ключевых слов), называемую *скелетом* запроса, и изменяемые параметры (строки и числа, встречающиеся в тексте). Во время обучения для каждого различного вида скелета выполняется вычисление среднестатистических показателей соответствующих ему изменяемых параметров, и полученные результаты образуют множество профайлов скелетов. Второй этап обучения заключается в определении пороговых значений для правил, определяющих принадлежность запроса к множеству нормальных или аномальных запросов. Согласно результатам экспериментов, приведённых в [4], доля ложных срабатываний для описанного метода равна 0,35%.

В работах [5, 6] Ашиш Камра и Элиза Бертино предлагают использовать обучающуюся систему обнаружения аномалий, формирующую профили нормального поведения в виде набора шаблонов SQL-запросов специального вида: каждый запрос представляется в виде вектора – *квиплета* (quiplet). Этот вектор содержит описание типа SQL-команды, множества отношений, к которым производится обращение при выполнении команды, и для каждого из этих отношений – множества используемых атрибутов. При работе системы все запросы к БД сначала передаются синтаксическому анализатору для преобразования текста SQL-запроса в квиплет. Далее проверяется принадлежность полученного квиплета множеству квиплетов, признанных допустимыми для пользователя, от имени которого производился запрос. Оценка аномальности квиплета, а, следовательно, и запроса, выполняется на основе наивного байесовского классификатора. В результате проведения опыта было показано, что доля ложно положительных срабатываний для данного метода равна 17,1%, а вероятность пропуска аномального запроса – 2,4%.

Аналогичный разработке Ашиша Камры и Элизы Бертино подход был описан в 2008 году Коломыцевым и Носок [7]. В этой работе представлен похожий механизм обнаружения аномалий, использующий наивный байесовский классификатор, за тем лишь исключением, что вектора, формирующие профили нормально поведения, содержат более общее по сравнению с вышеописанным подходом описание структуры SQL-запроса.

Син Енг Ли, Вай Луп Лоу, Пей Йен Вонг и Питер Теох взяли за основу синтаксический анализ при разработке архитектуры фреймворка DIDAFIT [8, 9], который для выявление вторжений в базы данных использует «отпечатки» транзакций, получаемые в результате анализа нормальной работы системы. Набор шаблонов создаётся путём преобразования набора допустимых SQL-запросов в набор регулярных выражений, соответствующих этим запросам. Для проверки допустимости выполнения последовательности запросов из одной транзакции предложено использовать специальный ориентированный граф, вершины которого представляют собой регулярные выражения допустимых SQL-запросов, а дуги отражают возможность выполнения одного запроса после другого.

В работе [10] Кристина Ип Чун, Михаэль Герц и Карл Левит описали DEMIDS (Detection of Misuse in Database

Systems) – систему обнаружения злоупотреблений в реляционных СУБД. DEMIDS использует журналы аудита для формирования профайлов, описывающих типичное поведение пользователей, работающих с БД. Авторы отмечают, что модели доступа пользователей (различные роли) обычно формируют несколько *рабочих областей*, включающих наборы атрибутов отношений, которые, как правило, связаны друг с другом с некоторой силой. Для описания доменной структуры базы данных и семантики отношений, а также формирования шаблонов нормального поведения в DEMIDS используется понятие *меры связанности*, которое определяет степень близости множества атрибутов относительно рабочих областей. Процесс обучения системы заключается в том, что при анализе журнала аудита для каждого SQL-запроса, встречающегося в журнале, выполняется синтаксический разбор, в результате которого определяется множество атрибутов отношений, встречающихся в запросе. Для полученного множества атрибутов вычисляется мера связанности, и если полученное значение не превышает некоторый установленный порог, то запрос признаётся характерным для нормального поведения пользователя и включается в общую базу знаний. Работа системы в режиме обнаружения аномалий заключается в выполнении синтаксического разбора запроса и сравнении полученного вектора атрибутов с сформированным профилем.

В своей работе Александр Павлов [13] предлагает подход обнаружения аномальной активности в базе данных на основе использования искусственных иммунных систем с отрицательным отбором. Описанный в работе алгоритм отрицательного отбора учитывает синтаксические особенности SQL-запросов и при обучении требует лишь наличия примеров допустимых запросов. Этап обучения заключается в выборе из случайно сгенерированного набора детекторов тех, для которых их применение к эталонным нормальным запросам не приводит к ложно положительным результатам. На этапе же обнаружения аномалий проверяется, соответствует ли предъявляемый SQL-запрос какому-нибудь из детекторов: если соответствует, то запрос признаётся аномальным. Для применения алгоритма отрицательного отбора производиться преобразование дерева синтаксического разбора запроса в вектор, атрибуты которого отражают различные характеристики структур запроса.

Семантические методы

В отличие от синтаксических методов в семантических методах акцент со структуры запроса переносится на его смысловую составляющую, то есть на то, какие данные и каким образом изменяются в результате выполнения запроса.

В 2005 году Адриан Спалка и Ян Ленхардт в [11] описали систему обнаружения аномалий в базе данных, которая в своей основе использует семантический анализ. Разработанная система работает не в режиме реального времени, когда анализ состояния базы данных производится непрерывно, а запускается по мере необходимости, например во время наименьшей загрузки СУБД. Наибольший акцент был сделан на разработку детектора аномалий в процессе роста базы данных, для создания которого было предложено два подхода. Первый подход подразумевает использовать при работе детектора аномалий информации об *эталонных значениях* атрибутов отношений, а второй – использование Δ*-отношений* (дельта-отношений), которые хранят историю изменений значений в базе данных между двумя последовательными запусками системы обнаружения аномалий. К вычисляемым эталонным значениям относятся, например, общее количество записей в таблице, количество записей с не NULL значением для указанного поля в таблице, максимальные и минимальные значения, количество записей, у которых строковое поле имеет значение не нулевой длины. Сам же процесс выявления аномалий заключается в сравнении эталонных значений в разные моменты времени. Если эталонные значения для двух последовательных вызовов системы обнаружения аномалий (СОА) значительно отличаются, то это случит сигналом о возможных аномалиях в действиях, которые были выполнены за период между запусками СОА.

В сентябре 2010 года Суну Мэтью, Михали Петропулос, Хунг Нго и Шамбху Ападхая предложили подход [12] обнаружения аномалий в поведении пользователя, ориентированный на данные, к которым производится обращение во время работы с БД. В своей работе исследователи придерживаются идеи, что наилучший способ различить нормальное поведение и аномальное – это рассмотрение в первую очередь того, к каким данным пытается получить доступ пользователь, а уже во вторую очередь – каким образом он пытается это сделать. Профайлы пользователей строятся путём вычисления для каждого запроса специального вектора, который состоит из статистических характеристик набора записей, попавших в результат выполнения запроса. Все запросы пользователя можно представить как некоторый кластер, основные характеристики которого описываются формируемыми статическими векторами. Таким образом, одним из инструментов обнаружения аномалий авторы предлагают кластерный анализ: если статистический вектор, построенный для результата выполнения запроса, относится к кластеру «нормальных» статистических векторов, то запрос признаётся нормальным, иначе запрос считает аномальным. В работе было показано, что подобный подход позволяет более эффективно, нежели синтаксические методы, обнаруживать некоторые классы атак, к числу которых, например, можно отнести атаки типа «сбор данных» (data harvesting). Однако на сегодняшний момент данное направление не достаточно изучено, а конкретные методы рассматривают лишь статистические характеристики результатов выполнения запросов и не учитывают возможные взаимосвязи в выбираемых запросом данных.

В таблице 1 представлены описанные в статье методы.

Таблица 1.

Методы обнаружения аномалий в SQL-запросах к базам данных

Название метода / авторы метода	Способ формирования профайла	Структура профайла	Механизм принятия решений
Фредрик Валер, Дарен Мутц, Джованни Вигна	Синтаксический анализ запроса	Шаблоны запросов, статистические характеристики параметров запросов.	Баесовский классификатор
Ашиш Карма, Элиза Бернито		c-, m-, f-квиплеты	
Михаил Коломыцев, Светлана Носок		c-квиплеты	
DIDAFIT Син Енг Ли, Вай Луп Лоу, Пей Йен Вонг, Питер Теох		Набор регулярных выражений, описывающих структуру текста SQL-запросов, характерных для нормального поведения.	Проверка удовлетворения текста SQL-запроса хотя бы одному из составленных регулярных выражений.
DEMIDS Кристина Ип Чун, Михаэль Герц, Карл Левит		Шаблоны векторов типичных запросов.	Сопоставление запроса и сформированного набора шаблонов.
Метод на основе искусственных иммунных систем с отрицательным отбором. Александр Павлов		Набор детекторов, покрывающий множество аномальных запросов	Если хотя бы один детектор даст положительный результат, то запрос признаётся аномальным.
Адриан Спалка, Ян Ленхардт	Семантический анализ запроса	Эталонные значения для атрибутов отношений; дельта-отношения.	Статистические функции, оценивающие отклонение от эталона.
Суну Мэтью, Михалис Петропулос, Хунг Гно		Набор векторов, содержащих статистические характеристики результатов выполнения запросов.	Кластеризация
			Оценка отклонения значений атрибутов результата выполнения запроса от эталонных значений.

Литература:

1. Anderson, James P., Computer Security Threat Monitoring and Surveillance. Technical report, James P. Anderson Company, Fort Washington, Pennsylvania, April 1980
2. Denning, Dorothy E., «An Intrusion Detection Model, « Proceedings of the Seventh IEEE Symposium on Security and Privacy, May 1986, pages 119–131
3. Stefan Axelsson. Intrusion detection systems: a survey and taxonomy. Technical Report 99–15, Chalmers Univ., March 2000.
4. Fredrik Valeur, Darren Mutz, and Giovanni Vigna, A Learning-Based Approach to the Detection of SQL Attacks. Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), 2005.
5. Ashish Kamra, Evimaria Terzi, Elisa Bertino, Detecting Anomalous Access Patterns in Relational Databases
6. Ashish Kamra, Mechanisms for Database Intrusion Detection and Response
7. Коломыцев М., Носок С., Аудит аномального поведения пользователей баз данных. Правовое, нормативное и метрологическое обеспечение системы защиты информации в Украине. Научно-технический сборник.
8. Sin Yeung Lee, Wai Lup Low and Pei Yuen Wong, Learning Fingerprints for a Database Intrusion Detection System. COMPUTER SECURITY – ESORICS 2002. Lecture Notes in Computer Science, 2002, Volume 2502/2002, 264–279.
9. Wai Lup Low, Joseph Lee, Peter Teoh, DIDAFIT: Detecting intrusions in databases through fingerprinting transactions. International Conference on Enterprise Information Systems, 2002
10. Christina Yip Chung, Michael Gertz, Karl Levitt. DEMIDS: A Misuse Detection System for Database Systems
11. A. Spalka and J. Lehnhardt. A comprehensive approach to anomaly detection in relational databases. In DBSec, pages 207–221, 2005.
12. Sunu Mathew, Michalis Petropoulos, Hung Q. Ngo, and Shambhu Upadhyaya, A Data-Centric Approach to Insider Attack Detection in Database Systems. Recent Advances in Intrusion Detection: 13th International Symposium, RAID, 2010, pp. 382–401

13. Павлов А.В. Обнаружение аномальной активности в реляционных базах данных на основе искусственных иммунных систем с отрицательным отбором. // Научно-технический вестник Поволжья. №1 2011 г. – Казань: Научно-технический вестник Поволжья, 2011. – с. 166–168

Тенденции селективного влияния социальных сетей на стабильность поведения индивидуумов и групп населения

Жалнина Екатерина Владимировна, соискатель;
Смирнов Николай Яковлевич, кандидат технических наук, доцент
Российский новый университет Ступинский филиал

В глобальной сети Internet постоянно появляются новые сервисы по созданию социальных сетей. Популярность подобных ресурсов в Сети бьет все рекорды. По сообщениям агентства Reuters, в июле текущего года сайт социальной сети MySpace стал самым посещаемым ресурсом в США, обогнав почтовую службу Yahoo!. На долю MySpace пришлось около 4,46% от общего числа посещений пользователями каких-либо сайтов, что больше, чем у Yahoo! Mail, Google и почтового сервиса Microsoft HotMail. По мнению аналитиков ComScore, популярность ресурсов по построению социальных сетей будет только расти [1].

Указанная популярность может быть использована двояко – как позитивно, так и негативно. Не снижая значимости позитивного влияния информации социальных сетей, следует обратить внимание на использование информационных ресурсов этих сетей в негативных целях. Подтверждением этому является неоднократно доказанная возможность влияния такой информации, как на отдельные личности, так и на определенные группы и слои населения. При этом используются научные достижения в области потенциального влияния на сознание, психологическую устойчивость человека, а также на восприятие, переработку информации и принятие им решений.

К настоящему времени социальные сети, по сути, являются огромной базой данных с самой разнообразной слабо структурированной информацией о сотнях миллионов людей по всему миру. В последнее время такие сети все больше открываются внешнему миру, а многие личные данные пользователей уже доступны для всех желающих [2]. Кроме того, современные социальные сети предлагают пользователям указать о себе исчерпывающую информацию, не отдавая отчет о возможных последствиях.

Влияние информационных ресурсов на определенные личности или группы людей может быть существенно усилено в случае регистрации их одновременно в нескольких социальных сетях. Дополнительной мерой влияния может являться объединение людей в определенные социальные группы (социальные маски), которые между собой не сильно пересекаются. Исходя из этого, можно сделать вывод об острой необходимости построения и применения системы противодействия негативному влиянию информации социальных сетей. При построении системы противодействия следует учитывать динамику изменений как меры и характера восприятия информации различными слоями населения, так и степень воздействия ее на определенные индивидуумы и группы.

Такие системы противодействия могут создаваться на основе анализа последствий воздействия социальных сетей. В основе различных общественных организаций и движений, как правило, лежат определенные социальные связи, причем для совместных действий в группе формируется набор связей критической массы.

Повышенный интерес к информационным ресурсам, содержащимся в социальных сетях, представляет собой слабо структурированную проблему. Данная проблема вызванасущественными проблемно-ориентированными интересами определенных групп и слоев населения, с одной стороны, и негативной направленностью с другой. Негативное проявление информационных ресурсов социальных сетей реализуется в настоящее время в направлении влияния и на социальную направленность, и на стабильность определенных государственных структур. Одним из значимых примеров такого применения социальных сетей является их целенаправленное применение в подготовке и совершении «желтых революций» и локальных социальных взрывов.

Так, в Белоруссии снова начинают «революцию через социальные сети». Зарубежные координаторы группы «Революция через социальную сеть» намерены возобновить в Белоруссии молчаливые акции протеста 21 сентября. Они призывают белорусов выйти на центральные площади городов, чтобы продемонстрировать свое недовольство действиями власти, сообщает «Независимая Газета». Цель – проверить, созрело ли население для «цветной революции» или нет.Подробный план действий опубликован в социальной сети. В блиц-опросах на улицах белорусы отмечают ухудшение уровня жизни, кое-где возникают конфликты рабочих с руководством предприятий. Однако, по мнению экспертов, до готовности к реальному массовому протесту белорусы еще не созрели [3].

Учитывая что, в целом глобальная сеть Internet управляется определенными структурами экономически развитых стран, построение системы, противодействующей определенным негативным проявлениям предполагает преодоление определенных ограничений. Эти обстоя-

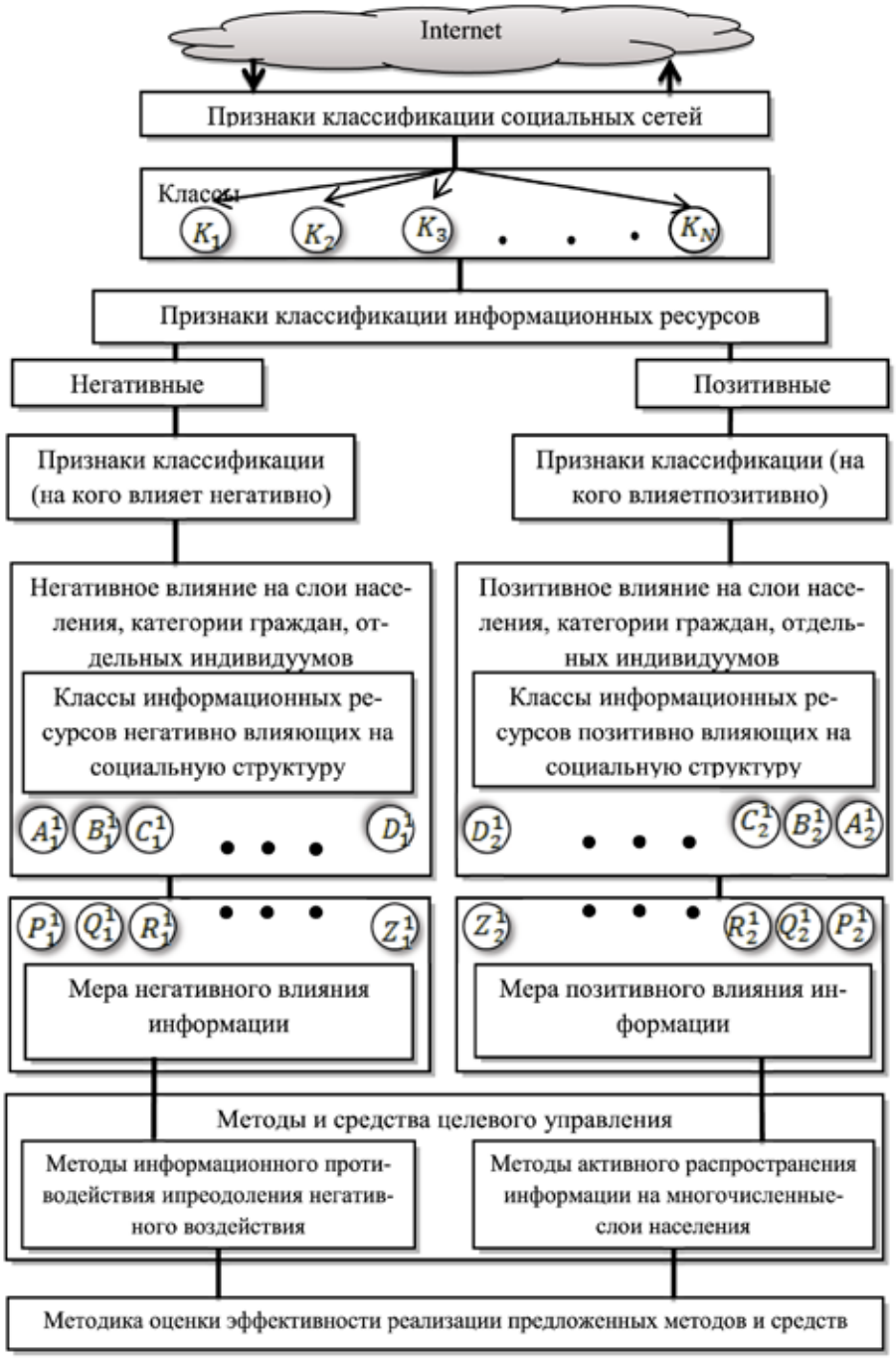


Рис. 1. Структурно-функциональная модель наблюдения, идентификации и управления информационными ресурсами социальных сетей

Обозначения: $K_{1\ldots} K_N$ – классы социальных сетей;

$A_1^1 \ldots D_1^1$ – негативно влияющие информационные ресурсы («что влияет»);

$A_2^1 \ldots D_2^1$ – позитивно влияющие информационные ресурсы («что влияет»);

$P_1^1 \ldots Z_1^1$ – социальные структуры (группы, индивидуумы) воспринимающие негативные информационные ресурсы социальных сетей («на что влияет»);

$P_2^1 \ldots Z_2^1$ – социальные структуры (группы, индивидуумы) воспринимающие негативные информационные ресурсы социальных сетей («на что влияет»).

тельства могут породить тривиальные проблемы при нейтрализации влияния разноаспектной негативной информации, выдаваемой за истинно демократичную, справедливую и достоверную. В данной работе предполагается предложить метод построения системы, позволяющий:

- осуществлять целенаправленный сбор информации и построение на этой основе эффективного мониторинга;
- идентифицировать и классифицировать информацию мониторинга, формируемого на основе альтернативных источников;

Таблица 1.

Классификация информационных ресурсов социальных сетей

№П/П	Признак	Класс, группа
1	Целевая направленностьинформации	• Позитивная; • Негативная.
2	Объект воздействия	• Население страны; • Население территории; • Население локального объекта; • Отдельные группы граждан; • Индивидуумы.
3	Мера воздействия	• Незначительная; • Слабая; • Сильная; • Чрезвычайная; • Катастрофическая.
4	Оперативность распространения	• Высокая; • Низкая.
5	Достоверность информации	• Низкая; • Высокая; • Противоречивая; • Абсолютно недостоверная (ложь); • Смешанная.
6	Полнота информации	• Низкая; • Высокая.
7	Релевантность	• Релевантная; • Нерелевантная.
8	Управляемость	• Высокая; • Низкая; • Очень низкая; • Полная неуправляемость.
9	Методы психофизического воздействия	• Информационно-психологические (использование различных типов внушения); • Нейролингвистическое программирование; • Погружение личности в виртуальную реальность.
10	Доступность	• Открытые; • Закрытые; • Смешанные.

• осуществлять многокритериальную оценку информации, негативно влияющей на определенныеобъекты;

• строить ранжированные ряды меры влияния определенных классов информационных ресурсов на различные социальные структуры;

• выбирать способ предпочтительного влияния с целью ослабления влияния негативных воздействий (Рис. 1).

При разработке метода выявлена одна из основных проблем, связанная с необходимостью классификации информационных ресурсов социальных сетей. Это объясняется слабой структуризацией информации web-сайтов, web-сервисов, web-платформ и др.

К следующей проблеме отнесена необходимость учета отличий социальных сетей от других Internet-ресурсов, заключающихся в том, что пользователи социальных сетей получают целенаправленную и оперативную информацию в режиме online, позволяющую с высокой оперативностью взаимно и одновременно информировать территориально-распределенных пользователей (операторов) и находить согласованные решения. Этому способствует создание специальных информационных структур – создание групп и сообществ по интересам, микро-блоггингов, чтение электронных средств массовой информации, а также комментарии к интернет-статьям, возможность поиска, просмотра и скачивания мультимедийных файлов, online-игр и т.д.

Предлагается следующий подход к классификации информационных ресурсов социальных сетей (Табл.1).

Одним из направлений разумной фильтрации информации социальных сетей является отражение, реализация и наблюдение конституционных и законодательных ограничений. С точки зрения коммерции

социальные сети не очень доходный бизнес. Основным источником дохода является реклама, которая зависит от посещаемости ресурса. Для увеличения доходности многие социальные сети активно внедряют инструменты электронной коммерции. В этом аспекте взаимоотношения владельцев социальной сети и государства регламентируются на основании федеральных законов «О рекламе» и «О предпринимательской деятельности», но негативный аспект, к сожалению, не регламентирован.

Представляется, что тематика социальных сетей создает реальные предпосылки применения информационных ресурсов как в целях повышения интеллектуального уровня населения, так и для организации эффективного и целенаправленного противодействия их негативному информационному влиянию и, вследствие этого, является особо актуальной.

Литература:

1. Прохоров А. Социальные сети и интернет, Компьютер Пресс, №10, 2006 г.
2. Печенкин В. Анализ социальных сетей: в ожидании чуда, Компьютерра, №42, 2005г
3. В Белоруссии снова начинают «революцию через социальные сети». Информационный портал «Росбалт», публикация от 20 сентября 2011 года.
4. Прокофьев В.Ф. Тайное оружие информационной войны: атака на подсознание. Издание второе, расширенное и доработанное. – М.: СИНТЕГ серия «Информационные войны», 2003. – 408 с.

Математическая основа алгоритма определения неисправности датчиков по их выходным данным

Кобец Кирилл Александрович, аспирант
Московская академия рынка труда и информационных технологий

Одним из факторов, определяющих достоверность результатов, получаемых при обработке результатов измерений датчиков, является наличие возможности фильтрации неточных значений. Неточные значения могут появляться в результате помех в канале связи, неисправности приемной, передающей и измерительной аппаратуры.

Неисправность датчика, как и его цепей, является частным случаем сбоев измерительного тракта. Необходимость автоматического контроля (т.е. с помощью программных или программно-аппаратных средств) исправного состояния датчика по его показаниям следует из того, что, как правило, отсутствуют дополнительные вспомогательные данные об исправности датчика, а устанавливать непосредственный контроль за измерительным оборудованием нет возможности. Неавтоматический контроль с помощью человека потребует больших материальных и ресурсных затрат. При этом именно такую неисправность сложнее всего определять автоматически. Это связано с необходимостью очень точно задать критерии корректной работы датчика, такие как возможные допуска на значения измеряемого параметра и временные интервалы для соответствующих допусков. Для определения неисправности датчиков можно использовать статистические данные, собранные при предыдущих аналогичных измерениях с помощью таких же датчиков.

При сборе статистики следует учитывать, что результаты двух различных измерений какого-либо параметра одного и того же физического процесса могут иметь различаться как по величине значений, так и по моменту времени характерных изменений в измеряемом параметре. Основными причинами таких различий как правило являются внешние воздействия на систему, в которой происходит процесс, начальные условия процесса или воздействия компонентов системы на ход процесса. Однако в целом поведение параметров физического процесса носит сходный характер.

Для статистической оценки поведения параметра удобно использовать его дисперсию [1]

$$D[X] = M\left[\left[X - M[X]\right]^2\right], \quad (1)$$

среднеквадратичное отклонение (СКО) [1]

$$\sigma_x = \sqrt{D[X]}, \quad (2)$$

а также математическое ожидание [1]

$$M[X] = \sum_{i=1}^{\infty} x_i p_i, \quad (3)$$

где

$$p_i = P(X = x_i). \quad (4)$$

Как известно

$$\sum_{i=1}^{\infty} p_i = 1. \quad (5)$$

Полагая на некотором интервале значений размера n все $p_1 = p_2 = ... = p_n$ из (5) и (3) получим

$$M[X] = \frac{1}{n}\sum_{i=1}^{n} x_i = \bar{x}, \quad (6)$$

где $\bar{x}$ – среднее арифметическое значение измеряемого параметра на интервале размера n.

Тогда из (1) и (2) следует

$$D[X] = \frac{1}{n}\sum_{i=1}^{n}\left(x_i - \bar{x}\right)^2, \quad (7)$$

$$\sigma_x = \sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(x_i - \bar{x}\right)^2} \quad (8)$$

Данные вычисления ((6), (7), (8)) следует производить на небольших интервалах, разбивая весь интервал значений параметра на k интервалов размера n. Если производить вычисления на слишком большом (в частности при $k = 1$, т.е. на всем интервале значений параметра) или слишком маленьком интервале то результаты могут оказаться некорректными. При слишком малом интервале дисперсия и математическое ожидание будут неточны, при слишком большом будут учитывать все изменения значений параметра, что не позволит обнаружить отклонения значений от ожидаемых.

При таких способах оценки точности телеизмерений математическое ожидание является лишь вспомогательным критерием. Использование его как основного наложит существенные ограничения, т.к. любое отклонение состояния системы от того, при котором рассчитывалось математическое ожидание, приведет к отклонению значений от ожидаемых. Использование дисперсии и СКО устраняет данное ограничение.

При статистическом анализе следует учитывать характер поведения измеряемого параметра физического процесса: так, например, на вибрационных параметрах как правило допускается дисперсия большей величины, чем на температурных параметрах, многие параметры предполагают изменение значений математического ожидания и дисперсии во времени. Для учета характера поведения удобно производить анализ дисперсии, СКО и математического ожидания первой [2]

$$x_i' = \frac{\Delta x_i}{\Delta t_i} = \frac{x_i - x_{i-1}}{t_i - t_{i-1}}, \quad (9)$$

и второй производной значений телеметрического параметра

$$x_i'' = \frac{\Delta x_i'}{\Delta t_i} = \frac{x_i' - x_{i-1}'}{t_i - t_{i-1}}. \quad (10)$$

Такой подход позволит отличить изменение значений параметра в результате изменения измеряемой величины от изменения в результате действия помех или прочих факторов. Без такого анализа необходимо строго оценивать временные интервалы возможных изменений статистических характеристик телеметрируемых параметров.

Для автоматического определения неисправности датчика путем анализа его показаний предлагается методика, описанная далее.

Сигнал на приемной стороне состоит из нескольких компонентов (11):

- непосредственно сигнала датчика $X_{сд}$,
- белого шума датчика $X_{шд}$,
- белого шума и помех в линии передачи данных, шума приемного и передающего устройства $X_{шл}$.

$$X_{пр} = X_{сд} + X_{шд} + X_{шл} \quad (11)$$

Белый шум присутствует в составе сигнала постоянно, но шум в линии передачи данных может компенсироваться помехоустойчивым кодированием и самим способом передачи (правильный выбор мощности, ширины полосы, модуляции сигнала). Шум датчика и шум в линии передачи, входящей в состав системы на которой проводятся измерения сложно компенсировать без использования инновационных методов: интеллектуальных датчиков, оптоволоконных бортовых линий связи и датчиков с оптическим выходом (такие методы позволяют дополнительно защитить сигнал от действия помех). Белый шум в силу своей физической природы вносит почти одинаковые искажения в принимаемый сигнал вне зависимости от внешних условий и состояний системы.

Помехи в линии связи (при их наличии) вносят сложнокомпенсируемое искажение в принимаемый сигнал, но их воздействие в большинстве случаев кратковременно.

Во время устойчивого приема сигнала $X_{пр} \approx X_{сд}$, при этом $X_{шд}$, $X_{шл} \ll X_{сд}$. При неустойчивом приеме $X_{шл}$ значительно возрастает. Как написано выше, $X_{сд}$может различаться при одинаковых характеристиках физического процесса в системе вследствие внешних воздействий на систему.

Дисперсия принимаемого сигнала, аналогично формуле (11) состоит из нескольких компонентов:

$$D[X_{пр}] = D[X_{сд}] + D[X_{шд}] + D[X_{шл}], \quad (12)$$

но для медленно меняющихся параметров $D[X_{шд}], D[X_{шл}] > D[X_{сд}]$, для быстроменяющихся параметров это условие справедливо при больших помехах в линии.

Следовательно, для каждого параметра можно задать некоторые значения $D[X_{пр}]_{\min}$ и $D[X_{пр}]_{\max}$ на определенных интервалов времени Δt (Δt может быть велико), при которых выполнение условия (13) будет свидетельствовать о высокой точности измерений параметров физического процесса.

$$D[X_{пр}]_{\min} < D[X_{пр}] < D[X_{пр}]_{\max}. \quad (13)$$

Нарушение этого условия может свидетельствовать о высоком уровне помех в канале связи ($D[X_{пр}] > D[X_{пр}]_{\max}$) или некорректной работе измерительного оборудования

(датчика), например в результате образования ложного спая (неравенство может нарушаться как в одну, так и в другую сторону).

Дисперсии первой и второй производных тоже удовлетворяют аналогичным условиям (14), (15). Использование производных более точно позволяет идентифицировать нештатные отклонения значений измеряемых параметров.

$$D\left[X'_{np}\right]_{\min} < D\left[X'_{np}\right] < D\left[X'_{np}\right]_{\max} \quad (14)$$

$$D\left[X''_{np}\right]_{\min} < D\left[X''_{np}\right] < D\left[X''_{np}\right]_{\max} \quad (15)$$

Таким образом, оценка попадания дисперсии измеряемого параметра и дисперсии его производных, а также математических ожиданий параметров и их производных (в качестве дополнительных критериев) позволяет составить алгоритм для автоматического детектирования неисправности датчиков, а также наличия сбоев в канале передачи данных. Алгоритм может быть реализован программно (реализован в компьютерной программе) или программно-аппаратно (реализован в микроконтроллере или программируемой логической интегральной схеме). Суть алгоритма сводится к вычислению значений вышеуказанных характеристик параметра и сравнению их с граничными значениями, заданными на основе статистики предыдущих измерений аналогичного параметра. По итогам сравнений программа может сделать вывод о корректности значений параметра (или некорректности с указанием временных интервалов со сбойными значениями параметра). При этом отсутствует необходимость оператору самостоятельно анализировать значения параметров (или графики значений параметров) на предмет выявления неисправностей датчиков и их цепей.

Литература:

1. Г. Корн, Т. Корн Справочник по математике для научных работников и инженеров. М., 1973 г., 832 стр. с илл.
2. Бронштейн И.Н., Семендяев К.А. Справочник по математике для инженеров и учащихся втузов. — 13-е изд., исправленное. — М.: Наука, Гл. ред. Физ.-мат. лит., 1986. — 544 с.

Классификация методов обнаружения неизвестного вредоносного программного обеспечения

Подпружников Юрий Валерьевич, ассистент
Брянский государственный технический университет

Одной из важнейших задач компьютерной безопасности является борьба с вредоносным программным обеспечением (ВПО) и в частности подзадача его обнаружения. Все методики обнаружения можно разделить на 2 типа: методики обнаружения известного ВПО и методики обнаружения неизвестного ВПО [1]. В свете текущих тенденций развития вредоносных программ, все более актуальными становится задача создания эффективного средства обнаружения неизвестного ВПО.

Автором ведется работа по созданию подобного средства. Целью разработки является повышение эффективности обнаружения за счет совершенствования существующих методик. Был проведен анализ имеющихся методик с целью выявления их характеристик. В результате этого исследования была сформирована классификация методик, которая будет представлена в данной работе (см. рис. 1).

Методику обнаружения неизвестного ВПО можно описать с помощью следующих параметров: данные, получаемые об исследуемом ПО, способы получения этих данных, математические методы, применяемые для анализа данных, и выявляемые признаки вредоносности [2]. Комбинация этих параметров определяет основные характеристики методики: уровень ошибок первого и второго рода, ресурсоемкость, вычислительную сложность, алгоритмическую сложность (трудоемкость реализации) и др. Поэтому построенная классификация рассматривает методики в контексте каждого из этих параметров.

Классификация по характеру получаемых данных. По характеру получаемых данных методики принято разделять на структурный анализ и поведенческий анализ [3].

Структурный анализ [4] учитывает тот факт, что некоторые виды ВПО (например, вирусы) имеют отличительные особенности в структуре: расположение точки входа, специфичные последовательности команд, а также многие признаки, обнаруживаемые при так называемом эвристическом анализе. Данный вид анализа выявляет в основном косвенные признаки вредоносности, которые напрямую не указывают на вредоносность ПО, но крайне редко наблюдаются в полезном ПО.

Структурный анализ в большинстве случаев имеет высокую скорость работы (по причине небольшой вычислительной сложности). Главным минусом данного подхода является то, что не все типы ВПО имеют структурные от-

Рис. 1. Классификация методик обнаружения неизвестного ВПО

личия от полезного ПО. Таким образом, не все виды ВПО можно обнаруживать данным методом.

Также к этой категории можно отнести методики, которые анализируют бинарное подобие исследуемого ПО и известных вредоносных программ [5]. Но на практике данные методики не дают приемлемых результатов.

Поведенческий анализ [6] исследует действия, выполняемые ПО, и их последствия. Такие методики определяют вредоносность программ по тем же признакам, что и человек – по их поведению. В идеальном исполнении система, реализующая данный подход, способна защитить от любого ВПО, но на практике создать такую систему невозможно. С одной стороны слежение за всеми действиями ПО – алгоритмически сложная, ресурсоемкая и в некоторых случаях невыполнимая задача. С другой стороны, невозможно полностью формализовать понятие «вредоносное поведение». На практике такие методики следят за ограниченным набором действий, выполняемых ПО, и пытаются выявить в них ограниченный набор признаков вредоносности.

Таким образом, к плюсам поведенческого анализа можно отнести теоретическую возможность обнаружения любого типа ВПО, а также и возможность обнаружения ВПО в момент совершения вредоносного действия, а к минусам – практическую невозможность полного контроля системы, ресурсоемкость (чем больше контроль, тем сильнее замедляется работа всей системы).

Среди часто обсуждаемых проблематик поведенческого анализа можно указать вопрос полноты информации получаемой о ПО, а так же задачу анализа потока информации с различными требованиями. Вопрос полноты полученной информации в основном возникает при попытке выяснения всех возможных действий, которые может выполнять программа. Данный вопрос особо остро проявляется при обнаружении так называемых «временных бомб». Этот вид ВПО выполняет вредоносные действия только при определенных условиях, например в конкретную дату. Таким образом, при невыполнении данного условия поведенческий анализатор не сможет обнаружить такое ВПО, и оно будет беспрепятственно себя распространять.

Некоторые виды поведенческого анализа накладывают свои требования к методам анализа. Так для исследования потока исполнения (например, анализ системных вызовов на компьютере конечного пользователя) необходимы методы, которые будут его анализировать по мере поступления данных за гарантированный промежуток времени. В противном случае антивирус будет замедлять работу системы тем самым мешать пользователю.

Классификация по способу получения данных. Существующие методики обнаружения неизвестного ВПО по способу получения данных об исследуемом ПО можно разделить на две категории: методики исполняющие и не исполняющие код программы.

Методики, не исполняющие программный код, в основном применяются в структурном анализе, поэтому их основные достоинства и недостатки совпадают. Главный недостаток состоит в невозможности обнаружения ВПО, особенности которого проявляются только при исполнении кода. Главными преимуществами данного подхода являются высокая скорость, низкая ресурсоемкость и безопасность использования. Помимо того, что данные способы позволяют относительно быстро обнаруживать некоторые виды ВПО, они позволяют ускорить работу других способов. Так методика определения измененных файлов по контрольным суммам, также относящаяся к данному виду, позволяет ускорить анализ ПО с помощью других методов, например, не анализировать файл повторно, если он не был изменен.

Методики, исполняющие программный код, применяются в основном в поведенческом анализе. К таким методикам относятся сбор данных при исполнении ПО на реальной системе (например, компьютер пользователя или

«honeypot»), сбор данных при исполнении ПО на эмуляторах, а также смешанные способы. Каждый из указанных подвидов имеет свои достоинства, недостатки и области применения.

При исследовании работы ПО в реальной системе обычно контролируют ряд действий во время выполнения ПО (системные вызовы, обращение к файлам) и изменения в системе после выполнения ПО (изменения в файловой системе). Реализация данного подхода на компьютерах конечных пользователей следит за действиями программ и с одной стороны позволяет обнаружить ВПО в момент исполнения вредоносного действия, а с другой стороны замедляет работу системы.

Достоинствами данного подхода по сравнению с созданием полноценных эмуляторов являются возможность исследования ПО в «естественных условиях», высокая скорость сбора данных и относительная простота реализации. Недостатки обусловлены следующими обстоятельствами.

- Существует поведение, данные о котором невозможно собирать напрямую – возможно только косвенное их получение. В первую очередь, это относится к работе на уровне ядра системы.
- Некоторые виды ВПО используют stealth-технологии, препятствующие контролю за действиями программы, или не выполняют вредоносных действий при обнаружении контроля за собой.
- Для данного подхода к исследованию ПО не найдено приемлемое решение задачи исследования всего функционала ПО.
- Если ПО исполняется на компьютере пользователя, существует вероятность, что к моменту обнаружения оно уже нанесет ущерб пользователю.

Исследование работы ПО с помощью эмуляторов основано на эмуляции поведения системы: центрального процессора, операционной системы и пр. Фактически исследуемая программа выполняется не на реальной системе, а на специальном интерпретаторе. К достоинствам такого подхода относятся безопасность его использования, теоретическая возможность полного контроля над действиями программы, а также возможность исследования всего функционала ПО. Недостатками являются крайне высокая алгоритмическая сложность данного подхода и низкая скорость работы.

Смешанные способы в основном предполагают выполнение программы на реальном процессоре, но в изолированной среде. Таким образом, они сочетают достоинства и недостатки обоих рассмотренных выше подходов. К смешанным способам относят.

- Использование виртуальных машин. Этот довольно ресурсоемкий подход, который полностью изолирует исследуемую программу от реальной системы, но в ряде задач он оказывается быстрее эмулятора.
- Использование «песочниц» («sandbox»). Данный подход является менее ресурсоемким и более прост в реализации, чем предыдущий, но он не гарантирует полную изоляцию ПО от реальной системы.

Классификация методов анализа. Данная классификация основана на способах накопления знаний, которые используют методы анализа, и выделяет две группы методов: методы, основанные на экспертных знаниях, и различные методы машинного обучения;

Методы, основанные на экспертных знаниях**,** используются для формализации понятия «вредоносности» и знаний экспертов в области исследования вредоносных программ. Знания могут быть связаны, например, с тем, какие действия являются вредоносными (поведенческий анализ), или какие особенности структуры могут говорить о вредоносности (структурный анализ). В дальнейшем эти формализованные знания применяются для обнаружения вредоносности в анализируемых данных. Представителями данной группы методом являются.

- Метод продукционных правил [7]. Это один из самых простых в реализации, но довольно эффективный метод. В его основу положена модель представления знаний в виде конструкций «ЕСЛИ-ТО». С помощью таких правил можно указать одиночные признаки вредоносности.
- Поиск поведенческих сигнатур [6]. Данный метод разработан для поведенческого анализа. За основу взят метод продукционных правил, который был адаптирован для обнаружения вредоносных последовательностей действий (т.е. определения перехода системы в «зараженное» состояние).
- Метод, основанный на нейро-нечетких сетях [8]. В основе данного метода также лежат правила, задаваемые экспертом. Используемый в нем нечеткий логический вывод позволяет определять комплексные признаки, а элементы искусственных нейронных сетей позволяют подстраивать правила на основе известных ВПО.

Все методы данной группы довольно качественно определяют признаки, заданные экспертами, и для них характерен высокий процент обнаружения вредоносных программ, обладающих данными признаками. Тем не менее, более сложные признаки и новые техники, используемые ВПО, эти методы не определяют.

Методы машинного обучения используются для «извлечения» знаний (признаков вредоносности) на основе анализа известных ВПО. Развитию данных методов способствует наличие большого количества известных ВПО и тот факт, что основная масса нового ВПО использует сходные технологии, а иногда являются модификацией известного ВПО.

Основная задача методов машинного обучения состоит в определении зависимости между исследуемыми данными и выявляемыми признаками вредоносности. Исследования показали, что эффективность этих методов зависит от характера обнаруживаемых признаков, подбора входных данных и качества обучения, следовательно, в общем случае точность этих методов сравнить затруднительно. Однако можно выбрать наиболее подходящий метод для обнаружения конкретного признака при наличии конкретного набора данных и обучающей выборки. К методам машинного обучения относятся:

- методы, основанные на теореме Байеса [9, 3];
- метод опорных векторов [9];
- деревья решений [9, 3];
- искусственные нейронные сети [3];
- генетические алгоритмы [10] и др.

Классификация по выявляемым признакам вредоносности. В соответствии с данной классификацией выделяют два типа методик: обнаружение аномалий и обнаружение злоупотреблений.

Методы обнаружения злоупотреблений основаны на описании вредоносных действий и попытке обнаружения этих действий в исследуемом ВПО. Данный подход подобен сигнатурному поиску, используемому для обнаружения известного ВПО. Сигнатурный поиск используется для нахождения совпадений по коду программы, а методы обнаружения злоупотреблений – для поиска совпадений, например, в поведении. Многие методики данной группы относительно легко реализуются и дают приемлемые уровни ошибок первого рода. Вместе с тем, данные методы неспособны различать новые техники работы ВПО, т.е. новые признаки вредоносности. В настоящее время обнаружение злоупотреблений является наиболее распространенным подходом к обнаружению неизвестного ВПО.

Методы обнаружения аномалий основаны на описании нормальных (эталонных) особенностей программы (например, поведения) и попытке обнаружения отклонений от этого эталона. Описание эталона затрудняется наличием очень сложных программ, а также описанной выше проблемой полноты исследования программы. Данный подход алгоритмически более сложный и зачастую более ресурсоемкий, чем обнаружение злоупотреблений, однако он позволяет обнаруживать не только известные, но также и неизвестные новые признаки и техники.

Для пояснения данной классификации рассмотрим также классификацию неизвестного ВПО относительно конкретной методики, в соответствии с которой можно выделить ВПО подобное тому, на котором обучалась методика и не являющееся таковым. Иными словами, такая классификация представляет собой деление по степени подобия набора признаков вредоносности, которыми обладает ВПО, и набора признаков, обнаруживаемых методикой. Существующие методики балансируют между:

- эффективным обнаружением подобного ВПО (эффективность определяется вероятностью ошибки 1-го рода) и низким обнаружением остальных его видов (методы обнаружения злоупотреблений);
- менее эффективным обнаружением подобного ВПО, но более эффективным обнаружением остальных его видов (методы обнаружения аномалий).

Выводы. Таким образом, существует множество методик обнаружения неизвестного ВПО. Каждая из них имеет свои преимущества, недостатки и особенности использования. Но на данный момент не существует методики, которая бы полностью решали задачу обнаружения неизвестного ВПО с приемлемой эффективностью для любых видов ВПО и при любых требованиях к системе обнаружения ВПО. Теоретически объединение нескольких методик может решить эту проблему. В качестве направления для дальнейших исследований была выбрана задача эффективного синтеза методик.

Литература:

1. Salomon D. Foundations of Computer Security // Springer-Verlag, 2006. – 369 p.
2. Зегжда Д.П. Общая архитектура систем обнаружения вторжений // Проблемы информационной безопасности. Компьютерные системы. – 2001. – № 4. – С. 100–110.
3. Rabaiotti J. Counter Intrusion Software: Malware Detection using Process Behaviour Classification and Machine Learning // URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.2417&rep=rep1& type=pdf. Дата обращения: 13.05.2009.
4. Макаров В.Ф. Основные методы исследования программных средств скрытого информационного воздействия // Безопасность информационных технологий. – 2009. – № 4. – С. 11–17.
5. Kolter J. Learning to Detect Malicious Executables in the Wild // Proc. of the 10th ACM SIGKDD Intern. Conf. on Knowledge Discovery and Data Mining. – 2004. – P. 470–478
6. Туманов Ю.М.. Обнаружение вредоносных сценариев javascript на основе поведенческих сигнатур // Безопасность информационных технологий. – 2009. – № 4. – С. 63–65.
7. Ilgun K. State transition analysis: A rule-based intrusion detection approach // IEEE Transactions on Software Engineering 21 (3). – 1995. – P. 181–199
8. Нестерук Г.Ф. О применении нейронечетких сетей в адаптивных системах информационной защиты // Нейроинформатика-2005: Материалы VII всероссийской научно-технической конференции. – М МИФИ (ТУ). – 2005. – С. 163–171.
9. Kotenko I. Intrusion detection in unlabeled data with one-class Support Vector Machines // Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2004), Lecture Notes in Informatics (LNI), No. 46, Dortmund, Germany, July 2004. – P. 71–82.
10. Kim C. Effective detector set generation and evolution for artificial immune system // Proc. of International conference on computational science (ICCS 2004) . – Springer-Verlag, 2004. – P. 491–498.

Моделирование компонентов систем электропитания космических аппаратов средствами САПР

Прокудин Александр Николаевич, аспирант
Сибирский государственный аэрокосмический университет им. ак. М.Ф. Решетнева

На современных космических аппаратах (КА) системы энергообеспечения, распределения электроэнергии, системы обеспечения качества аккумулирования с учетом более высокой надежности по сравнению с другими системами занимают по массе, объему и стоимости до 30% самого КА. Поэтому проблема создания систем электропитания (СЭП) КА имеет важное, первостепенное значение, ее решение может заметно улучшить технико-экономические показатели космического аппарата в целом.

Самым современным и эффективным способом проектирования систем электропитания можно считать построение математических и компьютерных моделей компонентов системы с использованием инструментов и методов, предоставляемых системами автоматизированного проектирования (САПР).

Построенные модели компонентов СЭП позволяют проектировать, тестировать и исследовать СЭП с различными типами структур.

Основными компонентами СЭП являются: солнечная батарея, аккумуляторная батарея, стабилизатор напряжения, зарядное и разрядное устройства, нагрузка.

Силовая структура систем электропитания КА может строиться несколькими способами, которые различаются исполнением стабилизатора напряжения (СН) солнечной батареи, подключаемого либо параллельно солнечной батарее, либо последовательно с ней [2]. На рисунке 1 представлен пример параллельной структуры СЭП.

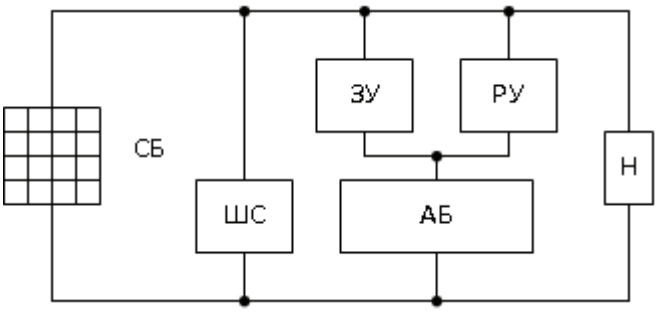


Рис. 1. Параллельная структура СЭП:
СБ – солнечная батарея, ШС – шунтовой стабилизатор,
ЗУ – зарядное устройство, РУ – разрядное устройство,
АБ – аккумуляторная батарея, Н – нагрузка

Одной из важнейших частей СЭП КА является солнечная батарея, поэтому построение адекватной модели ее работы – необходимый и важный этап в проектировании систем электропитания. В данной работе для создания модели используются средства САПР MicroCap 9.0 [3].

Солнечные батареи занимают лидирующее положение в современной космической энергетике, успешно функционируя на большинстве КА различных типов. Солнечные батареи преобразуют энергию светового излучения в электрическую энергию. Экспериментально было установлено, что вольтамперная характеристика (ВАХ) кремниевых и арсенид галлиевых фотоэлементов достаточно хорошо описывается уравнением [1]:

$$U_H = \frac{A \cdot k \cdot T}{q} \ln\left(\frac{I_\Phi - I_H}{I_0} + 1\right) - R \cdot I_H \qquad (1)$$

где U_H – напряжение на нагрузке;
I_H – ток во внешней цепи;
I_Φ – фототок;
I_O – ток насыщения;
R – последовательное сопротивление солнечного элемента (СЭ);
A – принимает значения от 1 до 3;
k – постоянная Больцмана, равная $1.38 \cdot 10^{-23}$ Дж/К;
T – абсолютная температура;
q – абсолютная величина заряда электрона, равная $1.6 \cdot 10^{-19}$ Кл.

Для ВАХ солнечной батареи справедливо выражение:

$$U_H = a_1 \ln\left(a_2\left(I_{K3} - I_H\right) + 1\right) \qquad (2)$$

где I_{K3} – ток короткого замыкания;
a_1 и a_2 вычисляются по формулам:

$$a_1 = \frac{A \cdot k \cdot T}{q} \qquad (3)$$

$$a_2 = \frac{1}{I_0} \qquad (4)$$

Реализация солнечной батареи в системе Micro-Cap имеет вид, представленный на рисунке 2.

Эта макромодель представлена в виде отдельного компонента Micro-Cap, который имеет выводы:

- *PLUS* – плюс;
- *GND* – земля;

и параметры:

- *a1* – коэффициент в выражении (2);
- *a2* – коэффициент в выражении (2);
- *Ikz* – ток короткого замыкания;
- *SEANS* – файл с расписанием интенсивности солнечного излучения на одном витке КА.

Основные элементы модели:

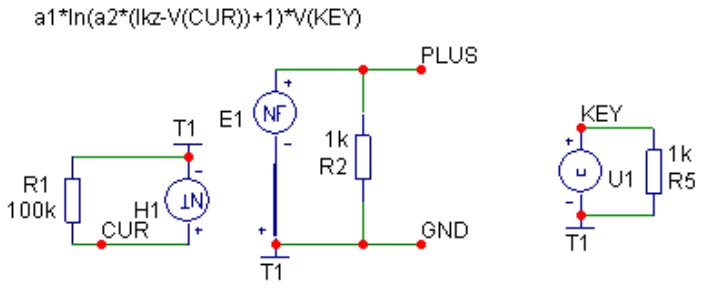


Рис. 2. Макромодель солнечной батареи

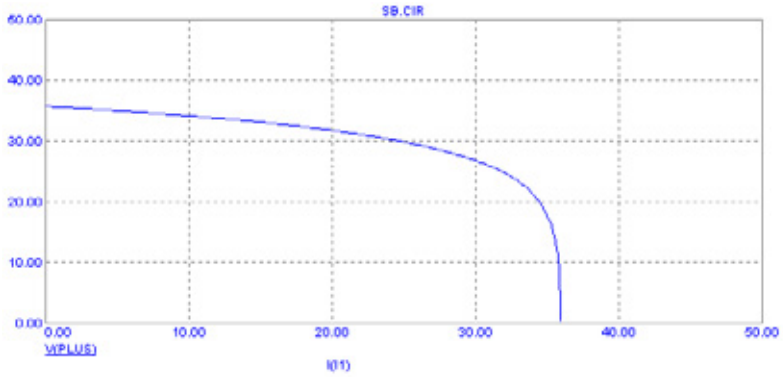


Рис. 3. Вольтамперная характеристика солнечной батареи

– *E1* – источник напряжения, задаваемый функциональной зависимостью (*NFV*). Определяет вольтамперную характеристику СБ согласно выражению (1);

– *H1* – таблично задаваемый источник напряжения, управляемый током (*NTVofI*). На выходе этого источника, в узле *CUR*, напряжение равно выходному току, если этот ток больше нуля и меньше тока короткого замыкания; нулю, если выходной ток меньше нуля; *Ikz*, если выходной ток оказался больше тока короткого замыкания;

– *U1* – источник напряжения, задаваемый пользователем (*User source*). Параметром этого источника является текстовый файл, содержащий пары значений: отсчеты моментов времени и значения напряжений в эти моменты. Этот файл может быть создан с помощью любого текстового редактора. В источнике *U1* задается коэффициент (*V (KEY)*), на который умножается ВАХ солнечной батареи. Таким образом можно регулировать интенсивность солнечного излучения на одном витке КА.

Принцип работы данной модели: источник напряжения *E1* создает разность потенциалов на выводах компонента согласно выражению (1), которая умножается на коэффициент *V (KEY)*.

Основная характеристика солнечной батареи – ВАХ, полученная с помощью данной модели имеет вид (Рисунок 3) (параметры *a1*=5, *a2*=35, *Ikz*=36).

При данных параметрах максимальная мощность СБ составляет 800 Вт, при этом оптимальное напряжение 27 В, оптимальный ток 30 А. Ток короткого замыкания 36 А, напряжение холостого хода 35.5 В.

Литература:

1. Грилихес В.А. Солнечная энергия и космические полеты [Текст] / В.А. Грилихес, П.П. Орлов, Л.Б. Попов. – М.: Наука, 1984. – 216 с.
2. Источники вторичного электропитания. / В.А. Головацкий, Г.Н. Гулякович, Ю.И. Конев и др.; Под ред. Ю.И. Конева. – М.: Радио и связь, 1990. – 280 с.
3. Разевиг В.Д. Схемотехническое моделирование с помощью MicroCap 7. – М.: Горячая линия – Телеком, 2003. – 368 с.

Моделирование системы передачи аутентифицированных командных слов

Таныгин Максим Олегович, кандидат технических наук, доцент
Юго-западный государственный университет (г. Курск)

В настоящей статье описываются математические модели, позволяющие оценить основные характеристики адаптивного алгоритма контроля подлинности и целостности сообщений ограниченной длины. Сам алгоритм подробно описан в работах [1, 2]. В основе его лежит комбинация необратимых и обратимых преобразований над информационной частью сообщения и формируемой из неё хэш-последовательности. Передаваемые сообщения буферизируются, а затем проверяются по описанному алгоритму, в результате которого отсеиваются сообщения, выданные посторонними источниками. Алгоритм предусматривает возможность варьирования соотношения длин информационной и служебной частей сообщения для обеспечения максимальной эффективности передачи, то есть является адаптивным. Поэтому необходимо в реальном масштабе времени определять характеристики канала передачи и действий злоумышленника (или активности посторонних источников). В соответствии с этими характеристиками и будут изменяться параметры передачи.

Одной из наиболее легко обнаруживаемых, но при этом, одной из самых информативных характеристик канала является количество получаемых посторонних командных слов, то есть слов, выданных не легальным источником, а посторонним, является. Увеличение числа посторонних командных слов (ПКС) неизбежно ведёт к повышению вероятности формирования из командных слов буфера более чем одной цепочки командных слов и необходимости повторной передачи всего пула. В тоже время длина проверочных полей (которая напрямую влияет на вероятность записи в буфер посторонних командных слов) должна быть адекватна состоянию канала передачи, так как мы не можем допустить излишней информационной избыточности. Следует срезу отметить, что классификация слов на легальные и посторонние производится лишь после получения пула команд, а до этого момента все слова получаемые источником слова имеют один уровень достоверности. Но вместе с тем, исследование вероятностных характеристик работы приёмника ведётся с учётом того, что каждая полученная команд уже априорно классифицирована.

Представим выдачу ПКС как случайный пуассоновский процесс, то есть процесс без предыстории, в котором вероятность получения очередного ПКС не зависит от того, сколько и за какой период было получено ПКС до него. Аналогично представим и процесс получения приёмником легальных командных слов (ЛКС). Пусть вероятность $P_{ПКС}$ получения ПКС в K раз больше вероятности $P_{ЛС}$ получения ЛКС:

$$P_{ПКС} = K \times P_{ЛКС} \quad (1)$$

Пусть к определённому моменту времени приёмник получил $n_{ЛКС}$ ЛКС. Тогда количество полученных $N_{ПКС}$ ПКС будет распределено по пуассоновсому закону:

$$p(N_{ПКС}) = \frac{(K \cdot n_{ЛКС})^{n_{ПКС}} \times e^{-K \cdot n_{ЛКС}}}{n_{ПКС}!} \quad (2)$$

где: $K \times n_{ЛКС}$ – математическое ожидание числа полученных ПКС,
$p(n_{ПКС})$ – вероятность получения ровно $N_{ПКС}$ ПКС.

Вероятность записи каждого случайно сформированного ПКС в буфер на какой-либо ярус определится длиной поля синхронизации:

$$p_{зап} = 2^{-L} \quad (3)$$

где L – длина поля синхронизации в битах.

При размещении $n_{ПКС}$ ПКС по ярусам буфера часть из них будет отсеяна посредством проверки содержимого поля синхронизации. Число $n_{П}$ посторонних командных слов, попавших на определённый ярус ПКС, распределится о биномиальному закону:

$$p(n_{П}) = C_{n_{ПКС}}^{n_{П}} \cdot (p_{зап})^{n_{П}} \cdot (1 - p_{зап})^{n_{ПКС} - n_{П}} \quad (4)$$

Объединяя с (1) получим вероятность того, что на определённый ярус запишется ровно $n_{П}$ ПКС:

$$p(n_{П}) = \sum_{i=^{n_{П}}}^{\infty} \left\{ \left[C_i^{n_{П}} \cdot (p_{зап})^{n_{П}} \cdot (1 - p_{зап})^{i - n_{П}} \right] \times \frac{(K \cdot n_{ЛКС})^{i} \times e^{-K \cdot n_{ЛКС}}}{i!} \right\} \quad (5)$$

Пусть предельная ёмкость одного яруса составляет N. Тогда вероятность того, что число ПКС, попавших на определённый ярус, превысит или будет равно N (ситуация переполнения буфера по одному ярусу), составит:

$$p_{\text{прев}} = \sum_{j=N}^{\infty} \sum_{i=j}^{\infty} \left\{ \left[C_i^j \cdot (p_{\text{зап}})^j \cdot (1 - p_{\text{зап}})^{i-j} \right] \times \frac{(K \cdot n_{\text{ЛКС}})^i \times e^{-K \cdot n_{\text{ЛКС}}}}{i!} \right\} \quad (6)$$

Ниже на рисунке 1 приведены графики при зависимости $p_{\text{прев}}$ от $n_{\text{ЛКС}}$ при различных значениях L, K и N (для наглядности и удобства анализа данные приведены в логарифмическом масштабе).

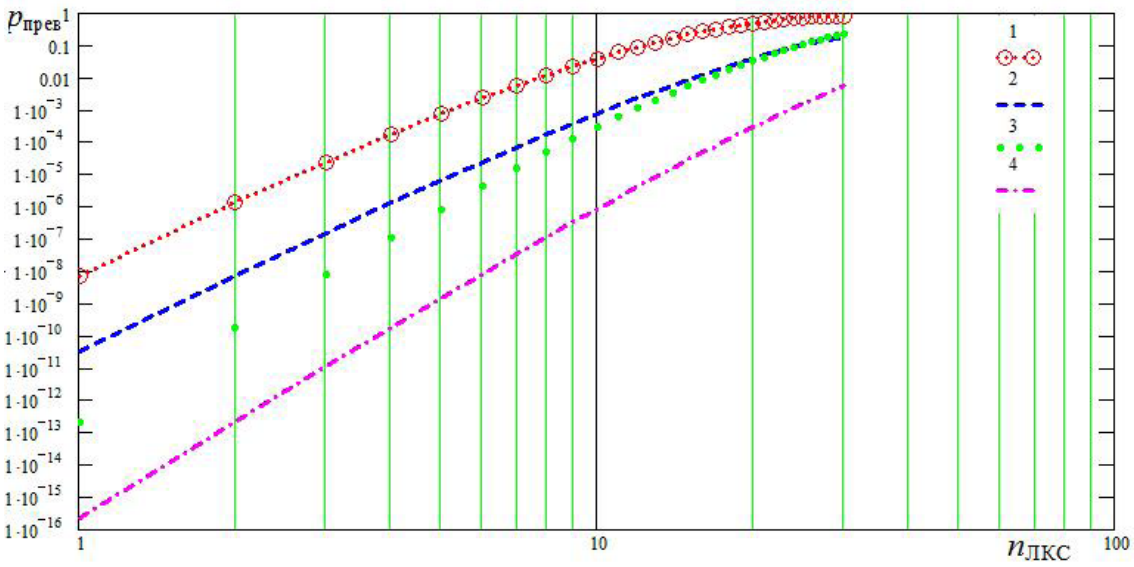


Рис. 1. Зависимость вероятности переполнения буфера по одному из русов от числа полученных легальных командных слов (логарифмическая шкала):
1) L = 3, K =3, N = 8 2) L = 4, K =3, N = 8
1) L = 3, K =2, N = 10 2) L = 4, K =2, N = 10

Видно, что на большей части график представляет собой прямую. То есть при малых значениях $n_{\text{ЛКС}}$ зависимость между ней и $p_{\text{прев}}$ можно выразить соотношением

$$p_{\text{прев}} \approx C1 \times (n_{\text{ЛКС}})^{C2},$$

где C1 и C2 — константы, которые в основном определяются величиной коэффициента K.

Проведённые расчеты показали, что изменение параметра K практически нивелируется обратно пропорциональным изменением вероятности записи ПКС в буфер $p_{\text{зап}} = 2^{-L}$. То есть кривая $p_{\text{прев}}$ при каких-либо значениях L и K практически идентична кривой $p_{\text{прев}}$ при значениях $(L+1)$ и $2 \cdot K$. Поэтому в дальнейших расчетах мы использовали в качестве параметра одно значение — произведение $2^{-L} \cdot K$.

График зависимости $p_{\text{прев}}$ от $n_{\text{ЛКС}}$ и N при фиксированных значения произведения $2^{-L} \cdot K$ приведён на рисунке 2.

Однако с практической точки зрения больший интерес представляют не соотношения межу числом полученных команд и вероятностью переполнения буфера, а соотношения между параметрами L, K, N и M — размера пула командных слов (глубина буфера и максимальное число получаемых ЛКС) и достигаемой при этом соотношении вероятности переполнения какого-либо яруса буфера. При реализации адаптивной системы передачи командных слов эта вероятность может быть важна при выборе длины поля синхронизации (так как параметры K, N и M можно считать условно неизменными). То есть, если при каких-то значениях параметра мы обнаружили неоднократное переполнение буфера по ширине (частота переполнений превысила теоретически рассчитанный пример), это свидетельствует о высокой интенсивности выдачи ПКС. Следовательно, для возврата частоты переполнений в приемлемый диапазон, необходимо либо повысить длину поля синхронизации L, либо изменить параметры N и M. И наоборот, если переполнений не происходит, мы можем увеличить длину пула (если необходимо выдавать протяжённые серии ЛКС), уменьшить его ширину (для повышения скорости обработки содержимого буфера) и уменьшить длину поля синхронизации (для уменьшения информационной избыточности).

Если проанализировать графики на рисунке 2, то можно обнаружить, что при фиксированных вероятностях переполнения буфера наблюдается линейное соотношение между шириной буфера N и числом полученных ЛКС (или глубиной буфера M). То есть любой зафиксированной частоте переполнения буфера, длине поля синхронизации и интенсивности выдачи ПКС соответствует определённое соотношение между шириной и глубиной буфера. Иными словами: $N \approx \alpha \cdot M$, где α — функция от параметра $2^{-L} \cdot K$ и наблюдаемой частоты переполнения буфера, которая при большом числе циклов передачи практически равна вероятности переполнения.

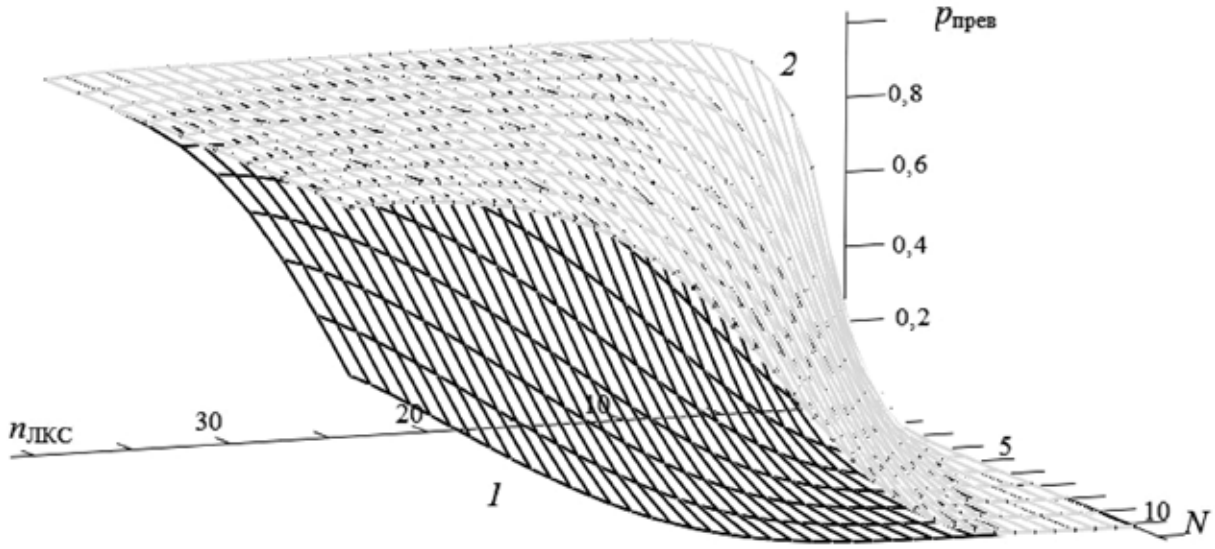


Рис. 2. Зависимость вероятности переполнения буфера по одному ярусу от числа полученных ЛКС и ширины буфера *N*:
1) $2^{-L} \cdot K = 0{,}25$; 2) $2^{-L} \cdot K = 0{,}5$.

Таким образом, зафиксировав все значения вероятности переполнения буфера в интересующих нас диапазонах изменения *N* и *M*, мы имеем возможность варьировать соотношение между длиной буфера и его шириной, добиваясь требуемого уровня частоты переполнения буфера при таком фиксированном параметре передачи, как интенсивность выдачи посторонних командных слов. При этом достаточно хранить в памяти устройства набор коэффициентов α при различных *L* и *K*, чтобы оперативно изменить соотношение *N* /*M*.

Литература:

1. Таныгин М.О. Верификация данных, передаваемых между устройством и программным обеспечением // Электронные средства и систем управления: материалы докладов Международной научно-практической конференции: в 2 т.Т.2 – Томск: В-Спектр, 2011. – с. 49–52.
2. Tanygin M.O. Method of Control of Data Transmitted Between Software and Hardware // Комп'ютерні науки та інженерія: материали IV Міжнародної конференції молодих вчених CSE–2010 – Львів: Видавництво Львівскої політехніки, 2010. – с. 344–345.

Работа выполнена при поддержке гранта Президента РФ для государственной поддержки молодых российских ученых – кандидатов наук (Конкурс – МК-2010). Шифр МК-3642.2010.

Облачные технологии

Широкова Екатерина Алексеевна, преподаватель
Пензенский автомобильно-дорожный колледж

Последнее время все чаще можно услышать термин «облачные технологии» и «облачные вычисления». Так что же такое «облачные технологии»? Википедия дает такое описание: «*Облачные вычисления (англ. cloud computing) – технология распределённой обработки данных, в которой компьютерные ресурсы и мощности предоставляются пользователю как интернет-сервис*» [1].

Термин «Облако» (cloud) используется как метафора, основанная на изображении Интернета на диаграмме компьютерной сети, или как образ сложной инфраструктуры, за которой скрываются все технические детали. Широко распространенное формальное определение облачных вычислений было предложено Национальным институтом стандартов и технологий США: «*Облачные вычисления представляют собой модель для обес-*

печения по требованию удобного сетевого доступа к общему пулу настраиваемых вычислительных ресурсов (например, сетей, серверов, систем хранения данных, приложений и услуг), которые можно быстро выделить и предоставить с минимальными управленческими усилиями или минимальным вмешательством со стороны поставщика услуг» [1].

Что же не считают облачными вычислениями? Во-первых, это автономные вычисления на локальном компьютере. Во-вторых, это «коммунальные вычисления» (utility computing), когда заказывается услуга исполнения особо сложных вычислений или хранения массивов данных. В-третьих, это коллективные (распределённые) вычисления (grid computing). На практике границы между всеми этими типами вычислений достаточно размыты. Однако будущее облачных вычислений всё же значительно масштабнее коммунальных и распределённых систем.

Для того чтобы понять что такое «облако» стоит начать с истории данного вопроса. Необходимо понять: действительно ли эта технология находится в разряде новых идей или эта идея не так уж и нова.

1. История и ключевые факторы развития

Идея того, что сейчас мы называем облачными вычислениями, впервые была озвучена Джозефом Карлом Робнеттом Ликлайдером (J.C.R. Licklider) в 1970году, когда он был ответственным за разработку ARPANET (Advanced Research Projects Agency Network). Идея Линклайдера заключалась в том, что каждый человек будет подключен к сети, из которой он будет получать не только данные, но и программы. Другой ученый Джон Маккарти (John McCarthy) говорил о том, что вычислительные мощности будут предоставляться пользователям как услуга (сервис) [2]. На этом развитие облачных технологий было приостановлено до 90-х годов. Ее развитию поспособствовали ряд факторов [2]:

Стремительное развитие сети Интернет, а именно пропускной способности. Хотя в начале 90-х глобальных прорывов в области облачных технологий не произошло, сам факт «ускорения» Интернета дал толчок к скорейшему развитию технологии.

В 1999 году появилась компания Salesforce.com, которая предоставила доступ к своему приложению через сайт. Эта компания стала первой компанией, предоставившей свое программное обеспечение по принципу «программное обеспечение как сервис» (SaaS).

В 2002 году Amazon запустила свой облачный сервис, где пользователи могли хранить информацию и проводить необходимые вычисления.

В 2006 году Amazon запустила сервис Elastic Compute cloud (EC2), где пользователи могли запускать свои собственные приложения. Таким образом, сервисы Amazon EC2 и Amazon S3 стали первыми сервисами облачных вычислений.

Свой вклад в развитие облачных вычислений внесла компания Google со своей платформой Google Apps для веб-приложений в бизнес секторе.

Развитие аппаратного обеспечения (а именно создание многоядерных процессоров и увеличение емкости накопителей информации) и технологий виртуализации (в частности программного обеспечения для создания виртуальной инфраструктуры, например, Xen-виртуализация) способствовало не только развитию, но и большей доступности облачных технологий.

2. Облачные технологии в настоящее время

Итак, еще раз обратимся к определению, которое дает Википедия. Облачные вычисления (англ. cloud computing) — технология распределённой обработки данных, в которой компьютерные ресурсы и мощности предоставляются пользователю как интернет-сервис. Предоставление пользователю Интернет-услуг — ключевое понятие. Однако, под Интернет-сервисом стоит понимать не только доступ к сервису через Интернет, но и так же доступ через обычную сеть с использованием веб-технологий.

Из истории и определения видно, что основой создания и стремительного развития послужили крупные интернет сервисы, такие как Google, Amazon и др, а так же технический прогресс. Более подробно остановимся на влиянии программного и аппаратного развития [2].

Развитие многоядерных процессоров привело к увеличению производительности при тех же размерах оборудования, снижению стоимости оборудования, а как следствие эксплуатационных расходов, снижению энергопотребления облачной системы, что для большинства Центров Обработки Данных (ЦОД) является большой проблемой при наращивании мощностей. Увеличение емкостей носителей информации, и как следствие снижение стоимости хранения 1Мб информации привело к безграничному увеличению объемы хранимой информации, снижению стоимости обслуживания хранилищ информации при значительном увеличении объемов хранимых данных. Развитие технологии многопоточного программирования привело к эффективному использованию вычислительных ресурсов многопроцессорных систем, гибкому распределению вычислительных мощностей «облака». Развитие технологии виртуализации привело к возможности создания виртуальной инфраструктуры, гибкому масштабированию и наращиванию систем, снижению расходов на организацию и сопровождение систем, доступности виртуальной инфраструктуры через сеть Интернет. Увеличение пропускной способности сети привело к увеличению скорости обмена данными, снижению стоимости Интернет трафика, доступности облачных технологий. Все эти факторы привели к повышению конкурентоспособности облачных технологий в сфере Информационных Технологий.

Как и у любой технологии, облачные технологии имеют как свои достоинства, так и недостатки. К основным достоинствам можно отнести следующие [2]:

Доступность – «облака» доступны всем и везде, где есть Интернет и с любого устройства, где есть браузер.

Низкая стоимость – снижение расходов на обслуживание (использование технологий виртуализации), оплата лишь фактического использование ресурсов облака пользователем (позволяет экономить на покупке и лицензировании программного обеспечения), аренда «облака», развитие аппаратной части вычислительных систем.

Гибкость – неограниченность вычислительных ресурсов (виртуализация).

Надежность – специально оборудованные ЦОД имеют дополнительные источники питания, регулярное резервирование данных, высокая пропускная способность Интернет канала, устойчивость к DDOS атакам.

Безопасность – высокий уровень безопасности при грамотной организации, однако, при халатном отношении эффект может быть противоположным.

Большие вычислительные мощности – пользователь может использовать все доступные в «облаке» вычислительные мощности.

При всех своих достоинствах облачные технологии имеют ряд серьезных недостатков [2]:

Постоянное соединение с сетью – для работы с «облаком» необходимо постоянное подключение к сети.

Программное обеспечение – пользователю доступно только то программное обеспечение, которое есть в «облаке», а так же пользователь не может настраивать приложения под себя.

Конфиденциальность – в настоящее время нет технологии, обеспечивающей 100% конфиденциальность данных.

Надежность – потеря информации в «облаке» означает невозможность ее восстановления.

Безопасность – хотя «облако» является достаточно надежной системой, но в случае проникновения злоумышленника, ему будет доступен огромный объем данных.

Дороговизна оборудования – для создания своего «облака» необходимы значительные материальные ресурсы.

Облачные технологии имеют обширный спектр услуг, которыми может воспользоваться пользователь для решения конкретных задач [6]. Ниже приведены основные виды предоставляемых услуг облачными системами [1][2][5].

Все как услуга (Everything as a Service) – при таком подходе пользователю будет доступно все от программно аппаратной части до управления бизнес процессами, включая взаимодействие между пользователями. Все что требуется от пользователя – это доступ в сеть Интернет.

Инфраструктура как услуга (Infrastructure as a Service) – пользователю доступна только компьютерная инфраструктура (как правило, виртуальные платформы, связанные в сеть), которую он сам настраивает под свои нужды.

Платформа как услуга (Platform as a Service) – пользователю доступна компьютерная платформа с установленной операционной системой и, возможно, программным обеспечением.

Программное обеспечение как услуга (Software as a Service) – пользователю доступно программное обеспечение, развернутое на удаленных серверах, доступ к которому осуществляется через сеть Интернет. Такой вид услуги подразумевает оплату только лишь за фактическое пользование программным обеспечением, а все вопросы по лицензированию и обновлению программного обеспечения лежат на поставщике данной услуги.

Аппаратное обеспечение как услуга (Software as a Service) – пользователю предоставляется оборудование на правах аренды, которое он может использовать в своих целях. Данный вид услуги очень похож на услуги «Инфраструктура как сервис» и «Платформа как сервис», за исключением того, что пользователь имеет доступ только лишь к оборудованию, на которое он сам устанавливает все программное обеспечение.

Рабочее место как услуга (Workplace as a Service) – компания организует рабочие места для своих сотрудников, устанавливая и настраивая все необходимое программное обеспечение.

Данные как услуга (Data as a Service) – пользователю предоставляется дисковое пространство для хранения информации.

Безопасность как услуга (Security as a Service) – позволяет пользователям развертывать продукты, обеспечивающие безопасность веб-технологий, переписки, локальной системы.

Облачные сервисы, предоставляющие те или иные виды услуг, в свою очередь делятся на три категории: публичные, частные и гибридные [2][5].

Публичное «облако» – ИТ-инфраструктура, которую используют множество компаний и сервисов. Пользователи при этом не могут управлять и обслуживать данное «облако», вся ответственность по этим вопросам лежит на владельце «облака». Абонентом может стать любая компания, а так же любой индивидуальный пользователь. «Облака» такого типа предлагают легкий и доступный в цене способ развертывания веб-сайтов или бизнес-систем с большими возможностями масштабирования, которые не доступны в «облаках» других типов. Примеры: онлайн сервисы Amazon EC2 и Simple Storage Service (S3), Google Apps/Docs, Salesforce.com, Microsoft Office Web.

Частное «облако» – безопасная ИТ-инфраструктура, контролируемая и эксплуатируемая одной компанией. Абонент может управлять «облаком» самостоятельно, либо поручить это внешнему подрядчику. Сама инфраструктура может размещаться в помещениях самой компании, либо у внешнего оператора, либо частично у оператора и частично у компании.

Гибридное «облако» – ИТ-инфраструктура, использующая лучшие стороны публичного и частного типов «облаков». Такой тип в основном используется, когда организация имеет сезонные периоды активности. Т.е. часть

мощностей частного «облака» перебрасывается на публичное «облако», если оно не справляется с текущими задачами. Кроме этого доступ к ресурсам компании организован через публичное «облако».

3. Современные тенденции и перспективы развития

Сегодня облачные вычисления — это то, чем почти каждый пользуется ежедневно. Подыскав в интернете подходящий сервис для ежедневного пользования, большинство из которых бесплатны или стоят относительно дёшево, пользователь избавляет себя от необходимости покупать более новые компьютеры для обеспечения высокой производительности, от сложностей в настройке сложных систем и покупки дорогих программных пакетов.

Облачные технологии развиваются стремительно и охватывают все больше и больше сфер деятельности. Например, почтовые клиенты. Ещё недавно у большинства пользователей был установлен тот или иной почтовый клиент приёма, отправки и обработки электронной почты, сейчас роль почтового клиента выполняет Gmail, а в качестве гибких и удобных альтернатив такие сервисы как Yahoomail, Webmail, Hotmail и другие [7]. Более того, в последнее время среди достаточно крупных мировых порталов наметилась тенденция по переносу почтовых систем на готовые площадки вроде Gmail [4][7]. В данном случае пользователь изначально получает знакомый ему интерфейс.

Похожая ситуация наблюдается и с офисными пакетами. Онлайн редакторы Zoho Writer или Документы Google могут выполнять те же самые функции, что и обычные офисные пакеты, более того, многие такие редакторы не только могут форматировать и сохранять документы, но и импортировать и экспортировать их в другие форматы [3]. Табличные редакторы Editgrid или Google могут легко заменить Exel. И это далеко не полный список всех доступных сервисов, доступных всем тем, у кого есть доступ к сети Интернет.

Можно заметить, что «облака» завоевали популярность. К тому же сами технологии постоянно совершенствуются. По мнению европейских экспертов, первоначально необходимо развитие методик регулирования юридических вопросов, связанных с аспектами функционирования систем, а так же методов планирования и анализа эффективности [7].

Одной из ключевых особенностей является возможность удаленного доступа к сервисам, однако, встает вопрос о хранении данных. Более того, хранимая информация может подпадать под законы страны, в которой находится физическое хранилище (еще хуже, если используется распределенное хранилище) [6]. В связи с этим, эксперты призывают государства начать задумываться о решении юридических аспектов работы облачных систем. Еще одним важным фактором развития является создание экономических моделей использования ИТ-услуг. Кроме юридических и экономических аспектов выделяют и ряд технических проблем, требующих пристального внимания. Самой важной считается проблема безопасности. Споры по этой теме ведутся уже давно, но пока нет единого мнения, которое устраивало бы всех. Кроме этого необходимо разрабатывать систему управления системами, которая бы смогла обеспечить более гибкую масштабируемость, совершенствовать системы хранения и управления данными и многие другие [7].

Заключение

В самом общем смысле, исходя из всего выше сказанного, облачными технологиями можно назвать технологии, которые позволяют клиентским рабочим местам использовать внешние вычислительные ресурсы, емкости для хранения информации и др.

Действительно, облачные технологии предоставляют практически безграничные возможности благодаря своим сервисам, начиная с простого хранения информации и заканчивая предоставлением сложных безопасных ИТ-инфраструктур. Кроме предоставления конечным пользователям вычислительных мощностей, облачные технологии предоставляют новые рабочие места для ИТ-специалистов, которые способны настраивать и сопровождать «облака». И т.к. сами технологии достаточно молоды, продолжаются исследования возможности их применения в различных областях жизни.

Главная трудность в развитии облачных технологий состоите не в решении технических вопросов, а в выборе взаимовыгодного пути развития. Именно поэтому многие коммерческие и государственные организации участвуют в обсуждении концепций и выбирают стратегии развития ИТ-систем.

Литература:

1. http://ru.wikipedia.org — статья «Облачные вычисления»
2. http://habrahabr.ru — статья «Облачные вычисления, краткий обзор или статья для начальника»
3. http://www.crn.ru — статья «ИТ «в облаке»: 100 лучших вендоров»
4. http://www.cnews.ru — по материалам статей «ИТ-директора боятся «облаков»« и «Cloud Computing: при чем тут виртуализация?»
5. http://www.xakep.ru — статья «Заоблачные вычисления: Cloud Computing на пальцах»
6. http://it.sander.su — статья «Облачные технологии и распределенные вычисления»
7. http://www.bureausolomatina.ru статья «Будущее облачных технологий: европейский взгляд»

2. ЭЛЕКТРОНИКА, РАДИОТЕХНИКА И СВЯЗЬ

Анализ регулярных и нерегулярных погрешностей несимметрично-полосковых линий передач

Абдулаева Ума Алиевна, кандидат технических наук, ст.преподаватель
Дагестанский государственный технический университет (г. Махачкала)

Анализ конструкции ГИС СВЧ показывает, что можно выделить четыре основные группы погрешностей: микрогеометрии, разброс электрических и магнитных параметров конструкционных материалов, формы. Каждая группа включает в себя несколько видов. Погрешности, приведенные в табл. рис. 5.1. в [1] называются конструктивно-технологическими погрешностями. Для микрополосковых линий (МПЛ) наиболее характерны погрешности I, II, III групп: погрешности геометрии, погрешности микрогеометрии, разброс электрических и магнитных параметров материалов.

По своему характеру эти погрешности могут быть регулярными и нерегулярными. Регулярные погрешности характеризуются отклонением от номинальных параметров конструкции строго постоянным в пределах одного образца, но случайным в пределах партии ГИС СВЧ, а нерегулярные – случайным колебаниям конструкционных параметров.

В практических конструкциях присутствуют все приведенные в [1] конструкторско-технологические погрешности одновременно и вероятностные параметры электрических характеристик полосковых линий определяются их совокупным влиянием.

Для определения закона распределения волнового сопротивления МПЛ, выполненный из материала с неоднородной диэлектрической и магнитной проницаемостью, и имеющей разброс геометрических размеров, необходимо воспользоваться выражением:

$$z_0 = z_{od}\sqrt{\mu_{эфф} / \varepsilon_{эфф}}\ , \qquad (1)$$

где $\mu_{эфф}$ – эффективная магнитная проницаемость; $\xi_{эфф}$ – эффективная диэлектрическая проницаемость; $z_{эфф}$ – волновое сопротивление МПЛ с воздушным диэлектрическим заполнением.

Известно, что для случайной величины, которая является дифференцируемой функцией системы случайных величин $x_1, ..., x_n$, плотность вероятности определяется так:

$$f(y) = \int_{-\infty}^{\infty} \dots \int_{-\infty}^{\infty} f(\psi, x_2, ..., x_n)\left|\frac{d\psi}{dy}\right| dx_2 \dots dx_n\ ,$$

где $\psi = x_1 = \varphi(y, x_2, ..., x_n)$.

На графиках на рис. 1 приведены пределы изменения z_0 и ожидаемый процент выхода годных при допуске на $z_{01} \pm 10\%$.

Сравнение полученных данных для МПЛ, имеющих только регулярные погрешности, показывает, что появление нерегулярных погрешностей резко ухудшает параметры партии МПЛ. Увеличивается разброс значений волнового сопротивления, уменьшается вероятность выхода годных.

Для несимметричной полосковой линии (рис. 2) равномерное уменьшение размеров проводников выразится через смещение:

$$\delta n_j = \begin{cases} dh \\ d\text{n} \\ -\text{dw} \\ -\text{dt} \end{cases}$$

dh – поверхности заземленного проводника;
dn – нижней поверхности полоскового проводника;
– dw – краев полоскового проводника;
– dt – нижней и верхней поверхностей полоскового проводника.

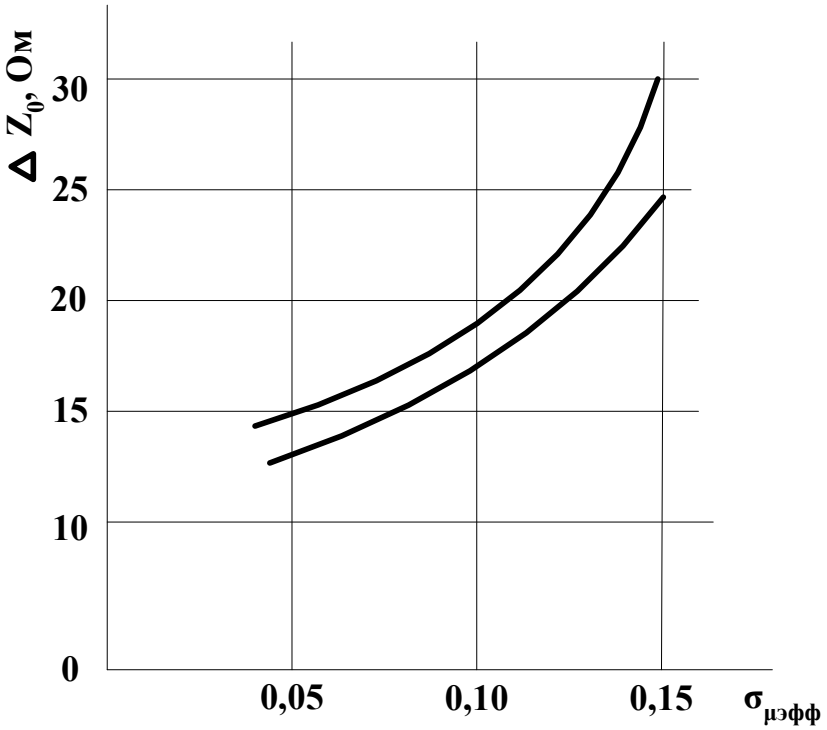


Рис. 1. Вероятностные параметры для партии МПЛ, имеющих совокупные регулярные погрешности

Тогда из выражения

$$\alpha_n = \frac{1}{2\mu_0 z_0}\sum R_{sj}\frac{dL}{dn_j} \qquad (2)$$

получаем:

$$\alpha_n = \frac{1}{2\mu_0 z_0}\left[\left(\frac{dL}{dh} - 2\frac{dL}{dw} - 2\frac{dL}{dt}\right)R_{s1} + R_{s2}\frac{dL}{dh}\right] \qquad (3)$$

где R_{S1} и R_{S2} – поверхностные сопротивления многослойного полоскового и заземленного проводников, Ом; μ – магнитная проницаемость среды, Н/м; dL – бесконечно малое приращение индуктивности, обусловленное бесконечно малым равномерным уменьшением размера dn всех проводников в направлении, перпендикулярном их поверхности, z_0 – волновое сопротивление полосковой линии.

В свою очередь $R_{S1} = \left(\pi f \mu_1 \rho_1\right)^{1/2}$ и $R_{S2} = \left(\pi f \mu_2 \rho_2\right)^{1/2}$,

где μ_1, μ_2, ρ_1, ρ_2 – величины, характеризующие магнитную проницаемость и удельное сопротивление материала проводника и заземленных пластин, f – рабочая частота.

Так как коэффициент потерь

$$K = 1 + K_\lambda (K_ш - 1),$$

где K_λ – частотная поправка,

$K_ш$ – коэффициент шероховатости $K_ш = \cos ec(\alpha/2)$ внешней поверхности полоскового проводника K_1, его внутренней поверхности K_2 (рис. 2) и поверхности заземленного проводника K_3 в общем случае одинаковы, имеем

$$\alpha_n = \frac{1}{2\mu_0 z_0}\left[\frac{R_{S1}}{2}\left(\frac{dL}{dh} - 2\frac{dL}{dw} - 2\frac{dL}{dt}\right)\left(K_1 + K_2\right) + K_3 R_{s2}\frac{dL}{dh}\right] \qquad (4)$$

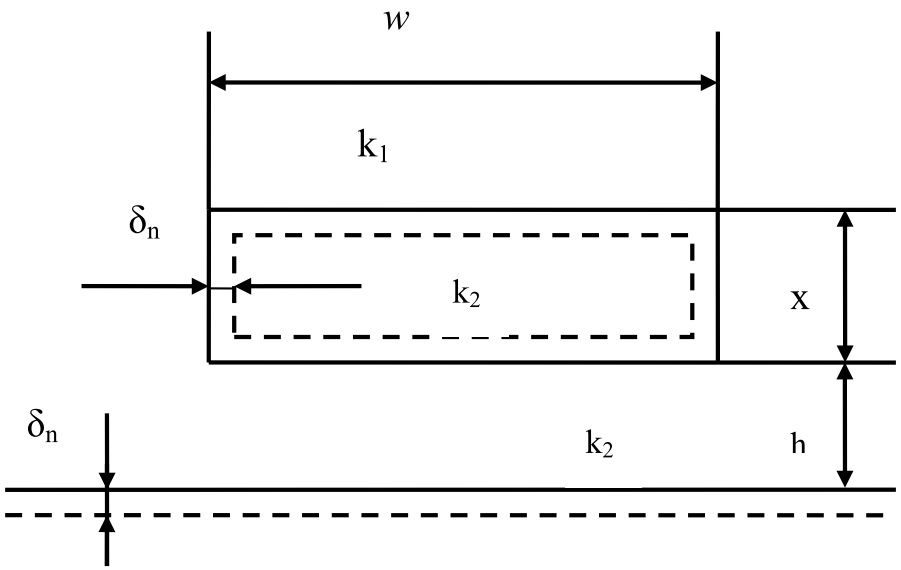


Рис. 2. Несимметричная полосковая линия (НПЛ)

Для расчета затухания в НПЛ по [2] в качестве исходных данных кроме геометрических размеров необходимо знать рабочую длину волны, шероховатость поверхности диэлектрика и внешней поверхности полоскового проводника, удельное сопротивление токонесущих поверхностей и толщину поверхностных слоев металла (адгезионного и защитного).

Для НПЛ возможна нестабильность ширины полоскового проводника, расстояния между полосковым проводником и заземленной поверхностью.

Нестабильностью или нерегулярностью геометрических размеров называют их непостоянство по длине полосковой линии передачи. Возможно плавное и сосредоточенное изменение размеров. А также следует различать регулярное отклонение геометрических размеров от расчетной величины. Нестабильность и регулярные отклонения геометрических размеров могут быть вызваны технологическими погрешностями.

При заданных значениях волнового сопротивления геометрические размеры несимметричных полосковых линий можно найти из следующего выражения:

$$z_0 = \frac{1}{2\pi}\left(\frac{\mu}{\varepsilon}\right)^{1/2} \ln\frac{8h}{w} \qquad (5)$$

где $\mu=1{,}26*10^{-6}$; $\varepsilon=8{,}85*10^{-12}*\varepsilon_{эфф}$; $w \leqslant h$.

Для рассмотрения воздействия регулярных отклонений геометрических размеров на величину волнового сопротивления и значения КСВН примем $w/h=x$.

При регулярном отклонении геометрических размеров для каждой конкретной полосковой линии

$$x = x_n + \Delta x,\ z_0 = z_{0n} + \Delta z_0$$

где x_n и z_{0n} – номинальные (расчетные) значения параметров полосковой линии.

Величины x_n и z_{0n} характеризуют приращение этих параметров в результате воздействия регулярных отклонений геометрических размеров. Для определения величины приращения Δx и Δz_{0n} характеризуют приращение этих параметров в результате воздействия регулярных отклонений геометрических размеров.

Для определения величины приращения Δz_0 при известном Δx следует вычислить разность:

$\Delta z_0 = z_0(x_n) - (x_n+\Delta x)$.

В случае же, когда отклонения размеров полосковых линий регулярны, а в пределах партии изделий подчиняются закону нормального распределения, волновое сопротивление, характеризующее партию полосковых линий, будет описываться вероятностными закономерностями. Для их определения необходимо найти плотность вероятности логарифма отношения двух случайных величин h и w, имеющих нормальные законы распределения вероятностей.

После некоторых преобразований имеем

$$W_1(z_0)=\frac{k\sqrt{1-R^2}\sigma_1\sigma_2\exp\left(\frac{z_0}{a}\right)}{k^2\sigma_1^2-2Rk\sigma_1\sigma_2\exp\left(\frac{z_0}{a}\right)+\sigma_2^2\exp\left(\frac{2z_0}{a}\right)}*$$

$$*\left\{1+\sqrt{\frac{\pi}{2(1-R^2)}}*\frac{k\sigma_1(w\sigma_1-Rh\sigma_2)+\sigma_2(h\sigma_2-Rw\sigma_1)\exp\left(\frac{z_0}{a}\right)}{\sigma_1\sigma_2\left[k^2\sigma_1^2-2Rk\sigma_1\sigma_2\exp\left(\frac{z_0}{a}\right)+\sigma_2^2\exp\left(\frac{2z_0}{a}\right)\right]^{1/2}}\right\}* \quad (5)$$

$$*\exp\left\{-\frac{\left[kh-w\exp\left(\frac{z_0}{a}\right)\right]^2}{2\left[k^2\sigma_1^2-2Rk\sigma_1\sigma_2\exp\left(\frac{z_0}{a}\right)+\sigma_2^2\exp\left(\frac{2z_0}{a}\right)\right]}\right\}$$

Здесь $z_0=a\ ln\ k_y$, σ_1, σ_2 – средние квадратические отклонения случайных величин h и w; R – коэффициент корреляции между ними.

Для нормированных значений случайных величин $\sigma_1/h=\gamma_1$; $\sigma_2/w=\gamma_2$; $h/w=g$ выражение (5) можно переписать:

$$W_{1n}(z_0)=\frac{kg\sqrt{1-R^2}\gamma_1\gamma_2\exp\left(\frac{z_0}{a}\right)}{\alpha*\pi*k^2\gamma_1^2g^2-2Rk\gamma_1\gamma_2g\exp\left(\frac{z_0}{a}\right)+\gamma_2^2\exp\left(\frac{2z_0}{a}\right)}*$$

$$*\left\{1+\sqrt{\frac{\pi}{2(1-R^2)}}*\frac{k\gamma_1(\gamma_1-R\gamma_2)+\gamma_2(\gamma_2-R\gamma_1)\exp\left(\frac{z_0}{a}\right)}{\gamma_1\gamma_2\left[k^2\gamma_1^2g^2-2Rk\gamma_1\gamma_2g\exp\left(\frac{z_0}{a}\right)+\gamma_2^2\exp\left(\frac{2z_0}{a}\right)\right]^{1/2}}\right\}* \quad (6)$$

$$*\exp\left\{-\frac{\left[kg-\exp\left(\frac{z_0}{a}\right)\right]^2}{2\left[k^2\gamma_1^2g^2-2Rk\gamma_1\gamma_2g\exp\left(\frac{z_0}{a}\right)+\gamma_2^2\exp\left(\frac{2z_0}{a}\right)\right]}\right\}$$

На рис. 3 приведены кривые распределения, построенные из (6) в предположении, что k=8, R=0.

При одновременном присутствии одинаковых по величине погрешностей размеров $\gamma_1=\gamma_2$ большее влияние на волновое сопротивление оказывает погрешность ширины полоскового проводника, а не толщина диэлектрика.

Более общим случаем является нестабильность геометрических размеров в пределах полосковой линии [1]. Модель полосковой линии со случайно распределенными вдоль ее длины неоднородностями, вызванными нестабильностью геометрических размеров, приведена на рис. 4.

На рисунке 4 E – э.д.с. генератора, питающего линию; z_0 – волновое сопротивление линии; Γ_i – коэффициент отражения от i-той неоднородности (всего в линии n неоднородностей); l_{0i} – расстояние от входа линии до i-той неоднородности; l_i – расстояние между неоднородностями. Анализ свойств волноводного тракта с малыми случайными неоднородностями выполнен в [2], и может быть использован для статически неоднородных полосковых линий.

Результирующий коэффициент отражения на входе полосковой линии

$$\acute{\Gamma}_0=\sum_{i=1}^{n}\Gamma_{oi}e^{if_{0i}} \quad (7)$$

где $(\Gamma i)_0$ – собственный коэффициент отражения i-той неоднородности, пересчитанный на вход линии.

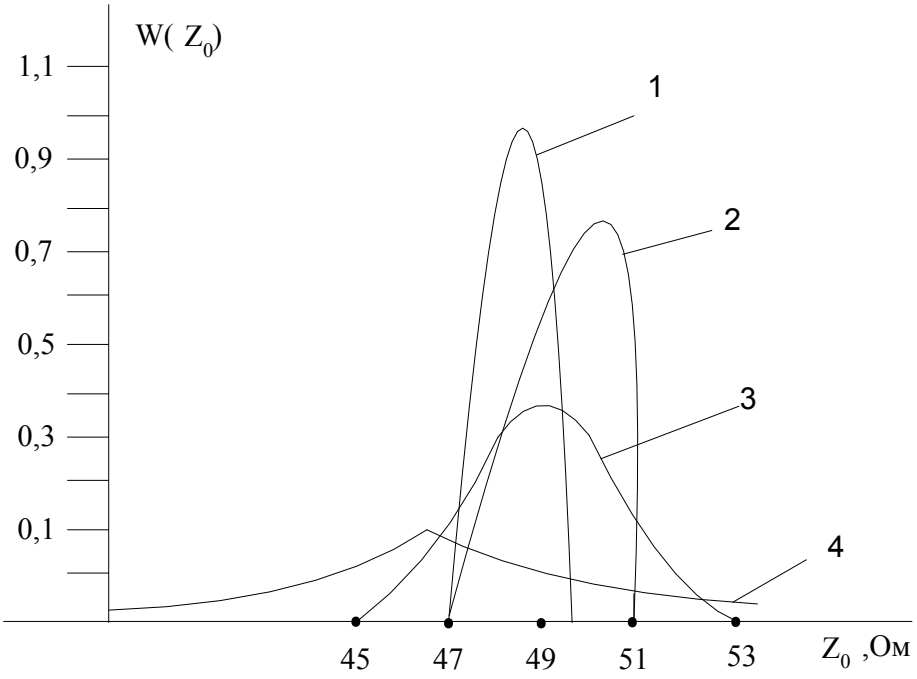


Рис. 3. кривые распределения волнового сопротивления для γ=0,01, g=1;
кривые построены для 1 – γ_2=0,01; 2-γ_2=0,02; 3 – γ_3=0,05; 4 – γ_4=0,2.

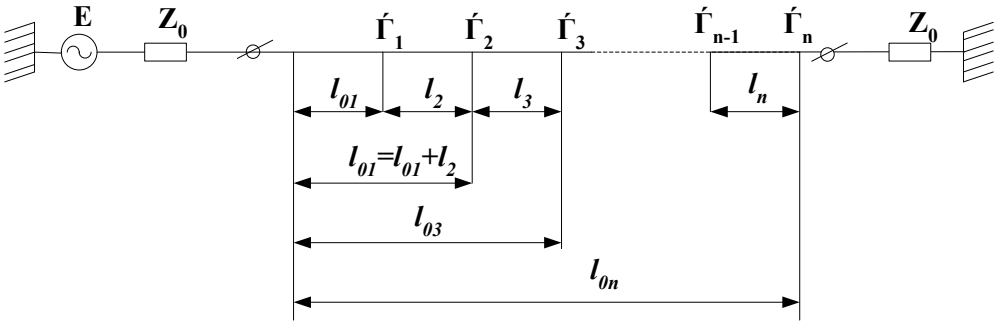


Рис. 4. Модель полосковой линии со случайно распределенными вдоль нее неоднородностями.

Литература:

1. Бушминский И.П., Морозов Г.В. конструирование и технология пленочных элементов СВЧ — микросхем. М., 1978.
2. Перец Р.И. Статические характеристики тракта СВЧ: — Антенны. 1973, №17.

Организация беспроводного информационного взаимодействия в специализированном измерительно-вычислительном комплексе

Колготин Павел Вячеславович, аспирант
Пензенский государственный университет

Разнообразие задач и ситуаций, в которых применяется автоматизированный сбор информации, обуславливает широкий спектр типов и принципов функционирования датчиков с интеллектуальными возможностями

первичной обработки и передачи информации. Совокупность интеллектуальных сенсоров, модулей беспроводной связи и вычислительно-аналитических модулей является основой для построения инфраструктуры распределенной системы сбора и обработки информации. Одно из представлений распределенной системы сбора и обработки информации в рамках концепции построения контрольно-измерительной сети (КИС) для сетей связи специального назначения описывается в [1]. Основными узлами сети являются измерительно-вычислительные комплексы (ИВК). Для ИВК предлагается организовать информационное взаимодействие с помощью приемо-передатчиков, осуществляющих передачу данных по инфракрасному (ИК) каналу между модулями комплекса. ИК канал для данной распределенной системы выбран в связи с определенными требованиями:

1. Информационная безопасность. ИВК предназначен для использования на специальных объектах, где особые требования к побочным электромагнитным излучениям и наводкам, соблюдению контролируемой зоны для информационных сигналов.

2. Расширяемость и масштабируемость. При развертывании ИВК необходимо учитывать возможность расширения и усложнения объекта мониторинга в процессе построения инфраструктуры ИВК.

3. Мобильность. Функциональность ИВК не должна зависеть от пространственно-временной привязки активных сенсорных узлов.

4. Оперативность. Необходимо обеспечить постоянную готовность системы для информационного обмена и возможность быстрой передачи большого массива данных.

5. Экологичность. Излучение беспроводных модулей ИВК не должно оказывать отрицательного влияния на организм человека.

Беспроводные системы передачи данных по радиоканалу (Bluetooth, Zigbee, WiFi, и т.п.) не удовлетворяют, как минимум, требованиям 1 и 5, поскольку имеют возможность перехвата радиоизлучения за пределами контролируемой зоны (КЗ) [2], также они оказывают негативное влияние на человека при интенсивном длительном воздействии.

В свою очередь, система информационного взаимодействия на основе ИК канала (СИВИК) удовлетворяет всем предъявленным требованиям и поэтому речь далее пойдет о ней. В СИВИК предлагается использовать ненаправленное излучение (большой угол расхождения излучения), что позволит принимать и передавать информационные и управляющие сигналы в пределах помещения с учетом переотражений. Это повышает мобильность системы. Расширяемость и масштабируемость предполагается обеспечивать за счет добавления в СИВИК новых приемо-передающих ИК-модулей (далее просто ИК-модулей). Известно [3], что ИК-диоды, как и светодиоды, позволяют модулировать световой поток сигналами с частотой до сотен мегагерц и наводки от всех элементов блока, в котором установлен ИК-диод, приводят к тому, что световой поток постоянно включенного ИК-диода оказывается промодулирован высокочастотными колебаниями, незаметными для глаза, но которые могут быть обнаружены с помощью специальной аппаратуры. Однако информационные сигналы, передаваемые в этом ИК диапазоне, не подвержены влиянию электромагнитных помех (наводок) и сами не являются источником помех для аппаратуры и информационных сетей связи, находящихся поблизости. При этом недостатки, связанные с ограничением распространения радиоволн ИК диапазона пределами помещения, скорее являются достоинствами с точки зрения информационной безопасности, так как перехват информационных сигналов вне контролируемой зоны возможен только через открытые оптические участки КЗ (например, окна), но разместив на «опасных» участках элементы зашумления, можно исключить такую возможность. Излучение в предлагаемом для использования диапазоне не влияет на человеческий организм, поэтому такое решение вполне оправдано.

Оперативность предлагается обеспечить как за счет увеличения количества ИК-модулей, так и за счет выбора оптимальной топологии, реализации быстрых и надежных протоколов взаимодействия, способа кодировки сообщений.

Для построения СИВИК предлагается следующая топология (Рис. 1).

Каждый ИК-модуль осуществляет генерацию кодированной последовательности электрических импульсов и модуляцию ими светового потока с длиной волны 0,84–0,96 мкм. Используется набор ИК-диодов с разной длиной волны, чтобы увеличить плотность светового потока в широком диапазоне чувствительности фотоприемника с учетом «окна прозрачности» [4]. В зависимости от местоположения и доступности получателя пакета данных взаимодействие может осуществляться непосредственно между ИК-модулями отправителя и получателя по кратчайшему пути, либо при отсутствии такой доступности – через ближайшие ИК-модули. Причем важно так расположить центральный ИК-модуль, подсоединенный к вычислительно-аналитическому модулю, чтобы для него были индивидуально доступны несколько ИК-модулей. Чем больше двухсторонних связей между ИК-модулями в соответствии с топологией на рис. 1, тем более надежна работа СИВИК. Соответственно, повышается оперативность, а это, как было отмечено, важное требование для системы.

Для доставки информационных пакетов до нужного ИК-модуля сигнала может ретранслироваться, т.е. каждый ИК-модуль может выступать в роли центрального узла, подсоединенного к какому-либо элементу ИВК, и в роли ретранслятора (см. рис. 1). Существует два типа ретрансляторов: ИК-модуль без буфера и ИК-модуль с буфером. Первый осуществляет коммутацию пакета следующим образом. По каналу приходит пакет – ретранслятор принимает заголовок пакета в буфер и, проанализировав информацию в заголовке, начинает передавать пакет из буфера в канал, одновременно продолжая прием прихо-

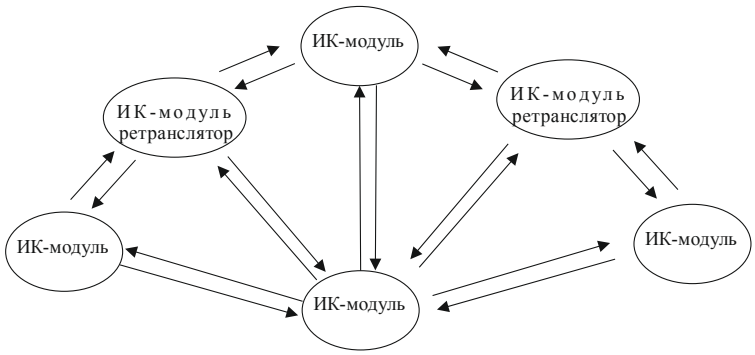


Рис. 1. Топология построения СИВИК

дящего пакета. Теперь буфер становится очередью, на вход которой поступают данные из канала, в который приходит пакет, а данные из хвоста поступают для передачи далее в канал (длина очереди равна длине заголовка пакета). Тем самым обеспечивается минимальная задержка при передаче пакета. Ретранслятор второго типа принимает в буфер весь пакет, проводит проверку пакета на наличие ошибок и, если они не обнаружены, начинает передачу пакета далее в канал при этом, если на вход приходит еще один пакет, то он принимается даже, если отправка предыдущего еще не закончилась.

Время доставки пакета в сети вычисляется по формуле:

$$t_{\text{доставки}} = \frac{L_{\text{пакета}} \cdot 8}{V} + \left(\frac{L_{\text{заг}} \cdot 8}{V} + t_{\text{обр.}}\right) N_{\text{мод}} + \left(\frac{L_{\text{пакета}} \cdot 8}{V} + t_{\text{обр.}}\right) N_{\text{мод. с буф.}} +$$

$$+ t_{\text{ср. ож. маркера 1}} + \ldots + t_{\text{ср. ож. маркера n}} \frac{(L_{\text{ср. дл. оч.1}} + \ldots + L_{\text{ср. дл. оч. n}}) \cdot 8}{V},$$

где $L_{заг}$ – длина заголовка пакета в байтах; V – скорость передачи информации в сети (бит/с); $t_{обр.}$ – время анализа заголовка ИК-модулем; $L_{пакета}$ – длина пакета в байтах; $N_{мод}$ – количество ИК-модулей, преодолеваемых пакетом на пути от отправителя к приёмнику; $N_{мод\ с\ буф}$ – количество ИК-модулей с буфером, преодолеваемых пакетом на пути от отправителя к приёмнику; $t_{ср.\ ож.\ маркера\ k}$ – среднее время ожидания маркера k-ым узлом; $L_{ср.\ дл.\ оч.k}$ – средняя длина очереди на k-ом узле.

Первое слагаемое данного выражения – время, затраченное узлом сбора на передачу пакета; второе – задержка на ИК-модулях без буфера; третье – на ИК-модулях с буфером. Как видно из данного выражения, задержка ИК-модулях без буфера пропорциональна длине заголовка пакета, а задержка ИК-модулях с буфером – длине пакета. На тех участках, где присутствуют большие помехи используются ИК-модули с буфером. ИК-модули без буфера можно применять там, где желательно иметь большую скорость передачи сообщений и нет серьезных помех.

Предлагается использовать частотное разделение каналов на передачу и прием. При этом диапазон частот, выделенный на передачу и прием, можно разделить на подканалы, организуя многоканальную систему. Адреса узлов ИВК распределяются так, чтобы каждому каналу в СИВИК соответствовал определенный адресный интервал. Тогда процесс коммутации пакета будет совсем простым: достаточно только определить в какой адресный интервал попадает адрес получателя пакета (он указан в заголовке пакета на рис. 2). Такой способ коммутации очень прост и эффективен.

Поле «CRC» содержит код CRC для обнаружения ошибки при передаче сообщения, что повышает надежность работы сети (если с помощью данного кода обнаруживается ошибка, то получатель пакета посылает отправителю запрос на повторную передачу, если же ошибок нет, то получатель посылает отправителю подтверждение приема пакета). В поле «Длина» записывается длина пакета. Поле «адрес отправителя» может и не присутствовать. Так, например, если получателю пакета не нужно знать, кто отправил пакет, это поле в заголовке пакета можно опустить. В поле «флаги» указывается, какие поля присутствуют в заголовке, а какие нет. Кроме поля «адрес отправителя» в заголовке могут присутствовать и другие необязательные поля, например, если сообщение разбито на несколько кадров, то в заголовке должны указываться идентификатор пакета и порядковый номер кадра в сообщении. Возможность исключения из заголовка ненужных полей в некоторых случаях позволяет сократить длину пакета, а следовательно уменьшить трафик.

При проектировании СИВИК стала проблема обеспечения работы системы в режиме реального времени. Метод доступа к каналу передачи данных играет решающую роль при большой загрузке СИВИК.

Для обеспечения более надежной работы СИВИК, был выбран вариант с децентрализованным управлением (централизованное управление ненадежно, т.к. при выходе из строя центрального узла управления выходит из строя вся сеть).

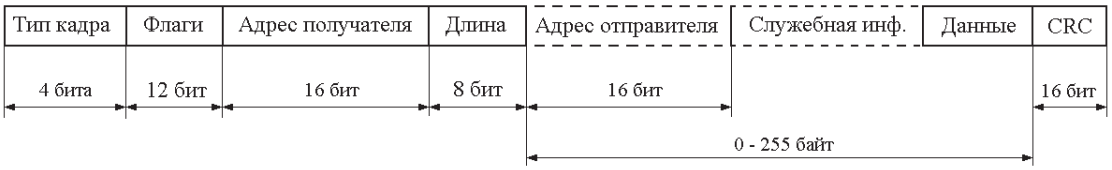


Рис. 2. Формат заголовка пакета данных

Теперь стояла задача разработать такой метод доступа к каналу передачи данных, который бы обеспечивал наилучшую работу сети в реальном масштабе времени, т.е. нужно обеспечить приоритетный доступ к среде передачи данных.

Все известные децентрализованные методы управления (случайных доступ; круговая передача маркера; управление, используемое в сети CAN и др.) не удовлетворяли поставленной задаче. Каждый метод имеет свои достоинства и существенные недостатки, и в итоге ни один не удовлетворял поставленной задаче. Из сложившейся ситуации был только один выход – был выбран маркерный метод доступа, причем стратегия передачи маркера задается с помощью программы, которая выполняется на узлах сбора (сенсорах). Т.е. на узле сбора имеется специализированный процессор, который и выполняет программу, описывающую алгоритм передачи маркера. К тому же, в состав узла сбора уже входит специализированный процессор для управления работой сенсоров, его можно использовать и с целью передачи маркера в СИВИК. Для этого в процессор достаточно ввести дополнительные прерывания: одно возникает при приходе маркера в нужный ИК-модуль, по этому прерыванию запускается программа пересылки сообщений, другое – при окончании передачи сообщений (истекло время передачи сообщений, больше нет сообщений для передачи). Таким образом, один процессор выполняет управление оконечной и передачей информации в опорной сети. Теперь стратегию передачи маркера можно выбирать в зависимости от решаемой сетью задачи и даже менять стратегию в процессе работы системы: достаточно только загрузить новые программы управления маркером в опорные узлы.

При передаче инфракрасного сигнала возникают помехи: солнечный свет, отражение и лампы дневного света [5]. Есть возможность снизить риск зашумления последовательности – кодировать один информационный символ последовательностью нулей и единиц. Кодовая последовательность – это набор нулей и единиц (чипов), с помощью которого кодируют один символ (бит) для дальнейшей передачи. Сам сигнал представляет собой последовательность кодовых последовательностей. Основными свойствами кодовых последовательностей являются очень хорошие автокорреляционные и взаимнокорреляционные свойства. От кодовой последовательности зависит помехоустойчивость системы. При одинаковых длинах свойства последовательностей могут кардинально отличаться.

Выигрыш в качестве связи зависит от длинны последовательностей и от их характеристик, в первую очередь – взаимных свойств и способа модуляции [6]. Следовательно, выбор оптимального ансамбля сигналов сводится к поиску такой структуры кодовых последовательностей, в которой центральный пик автокорреляционной функции (АКФ) имеет наибольший уровень, а боковые лепестки АКФ и максимальные выбросы взаимнокорреляционной функции (ВКФ) по возможности минимальны. Выбор и анализ характеристик оптимальной кодовой последовательности является темой отдельной статьи, поэтому в данном материале не рассматривается. Важен обозначенный принцип отбора кодовой последовательности.

Таким образом, предложенный вариант построения беспроводной системы информационного взаимодействия на основе ифракрасного канала может являться основой для разработки действующей модели с целью её использования в специализированном измерительно-вычислительном комплексе с учетом требований предъявляемых к распределенным системам подобного рода.

Литература:

1. Колготин, П.В. Автоматизация процесса испытаний новой аппаратуры на сетях связи специального назначения / П.В. Колготин // Труды международного симпозиума «Надежность и качество 2010», Пенза, том.2 стр. 402–405
2. Хорев, А.А. Классификация и характеристика технических каналов утечки информации, обрабатываемой ТСПИ и передаваемой по каналам связи / Хорев А.А. // Специальная техника, №2, 1998 г. http://ess.ru/publications/articles/tspi/tspi.htm
3. Freeman. Защита компьютерной информации от утечки по ПЭМИН http://www.support17.com/component/content/39.html?task=view
4. Шрайбер, Г. Инфракрасные лучи в электронике. Москва: ДМК, 2003 г.
5. Ипатов, В. Широкополосные системы и кодовое разделение сигналов. Принципы и приложения. Москва: Техносфера, 2007 г.
6. Малыгин, И.В. Коды, коды, коды http://cxem.net/sprav/sprav111.php

3. АВТОМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

Исследование режимов функционирования испытательного стенда «Искусственные легкие» в системе MATLAB

Иванов Андрей Михайлович, аспирант; Оневский Павел Михайлович, кандидат технических наук, доцент;
Третьяков Александр Александрович, кандидат технических наук, доцент
Тамбовский государственный технический университет

Рассматривается моделирование функционирования в системе Matlab комплекса «Искусственные легкие», предназначенного для имитации процессов дыхания человека при испытании индивидуальных дыхательных аппаратов изолирующего типа.

Индивидуальные дыхательные аппараты (ИДА) для защиты органов дыхания изолирующего типа с химически связанным кислородом используются в различных областях в экстремальных ситуациях: на земле и под землей, в космосе и на транспорте, на воде и под водой.

В настоящее время испытательный стенд «Искусственные легкие» (ИЛ) является основным инструментом для определения характеристик ИДА, что не требует привлечения людей-добровольцев.

Недостатками существующих зарубежных и отечественных стендов «Искусственные легкие» (ИЛ) являются невозможность изменения формы дыхательной кривой и реализации математическим и программным обеспечением автоматизированной системы управления установки дыхательного коэффициента меньше 1 (т.е. при снижении производительности регенеративного патрона ИДА). Поэтому создание автоматизированного испытательного стенда, позволяющего реализовать значение дыхательного коэффициента в диапазоне 0.8–1.2 является актуальной задачей. Решение данной задачи невозможно без проведения имитационных исследований с использованием современных средств моделирования.

Испытательный стенд ИЛ состоит из четырех основных блоков: блок подачи диоксида углерода и азота, блок имитации дыхания, блок имитации потребления кислорода (по массе и объему), блок управления [1, с. 591].

Блок имитации дыхания создает пульсирующий поток газовой дыхательной смеси (ГДС), аналогичный потоку, формируемому легкими человека. Блок работает поочередно в режиме вдоха и выдоха.

Аналогично в двух режимах работает блок имитации потребления кислорода путем сброса части ГДС в атмосферу через соответствующие клапаны. Подача смеси диоксида углерода и азота в имитатор дыхания происходит на стадии вдоха.

Для проведения имитационных исследований функционирования стенда при различных психофизиологических состояниях человека необходимо использовать математическую модель потребления кислорода пользователем ИДА.

Основными входными параметрами модели являются: легочная вентиляция $W_л$ (дм^3/мин), глубина дыхания $V_д$ (дм^3), частота дыхания n (мин$^{-1}$).

Исходный режим для имитационного моделирования:

– глубина дыхания $V_д$=1.75 дм^3;
– частота дыхания n = 20 мин$^{-1}$;
– подача диоксида углерода W_{CO2} (0) = 1.1 дм^3/мин;
– коэффициент дыхания, $K_д$ = 1;
– объем системы ИЛ, $V_{ил}$ = 10 дм^3.

Задачей исследования является обеспечение заданной концентрации диоксида углерода на входе в ИДА (т.е. на выдохе из ИЛ) и определение кривых дыхания, реализующих данную концентрацию, путем автоматизации процессов управления стендом ИЛ.

Основные соотношения математической модели:

– подача диоксида углерода за такт вдоха-выдоха:

$$V_{CO_2}(0) = W_{CO_2}(0) / n, \text{ дм}^3;$$

– потребление кислорода за такт вдоха-выдоха:

$$V_{O_2}(0) = W_{CO_2}(0) / K_д, \text{ дм}^3.$$

Состав ГДС в испытательном стенде перед первым циклом вдоха-выдоха принимался равным атмосферному: C_{CO_2} ИЛ = 0.2%; C_{O_2} ИЛ = 21%; C_{N_2} ИЛ = 100 – C_{CO_2} – C_{O_2} = 78.8 %.

Объемы газов, поступающих в насос ИЛ для схемы с имитацией потребления кислорода по массе и объему:

$$V_{CO_2}\text{ИЛ} = C_{CO_2}\text{атм} \cdot V_д / 100, \text{ дм}^3,$$

$$V_{O_2}\text{ИЛ} = C_{O_2}\text{атм} \cdot V_д / 100 - V_{O_2}, \text{ дм}^3,$$

$$V_{N_2}\text{ИЛ} = C_{N_2}\text{атм} \cdot V_д / 100, \text{ дм}^3,$$

где C_{CO_2} атм, C_{O_2} атм, C_{N_2} атм – объемные доли газов в атмосферном воздухе, %.

На выдохе соответственно имеем:

$$C_{CO_2}^{\text{выд}} = (V_{CO_2}(0) + C_{CO_2}\text{ИЛ} \cdot V_{ИЛ}/100 + V_{CO_2} ИЛ) \cdot 100/(V_{CO_2}(0) + V_{ИЛ} + V_{\text{д}}),$$

$$C_{O_2}^{\text{выд}} = (C_{O_2}\text{ИЛ} \cdot V_{ИЛ}/100 + V_{O_2} ИЛ) \cdot 100/(V_{CO_2}(0) + V_{ИЛ} + V_{\text{д}}),$$

$$C_{N_2}^{\text{выд}} = 100 - C_{CO_2}^{\text{выд}} - C_{O_2}^{\text{выд}},$$

где $C_{CO_2}^{\text{выд}}$, $C_{O_2}^{\text{выд}}$, $C_{N_2}^{\text{выд}}$ – объемные доли газов на выдохе, %.

Далее полученные значения $C_{CO_2}^{\text{выд}}$, $C_{O_2}^{\text{выд}}$, $C_{N_2}^{\text{выд}}$ подставляются вместо C_{CO_2} ИЛ, C_{O_2} ИЛ, C_{N_2} ИЛ и так далее для других циклов.

На рис. 1 представлена модель стенда ИЛ, реализованная с помощью пакета моделирования динамических систем Simulink, входящий в состав пакета прикладных программ Matlab.

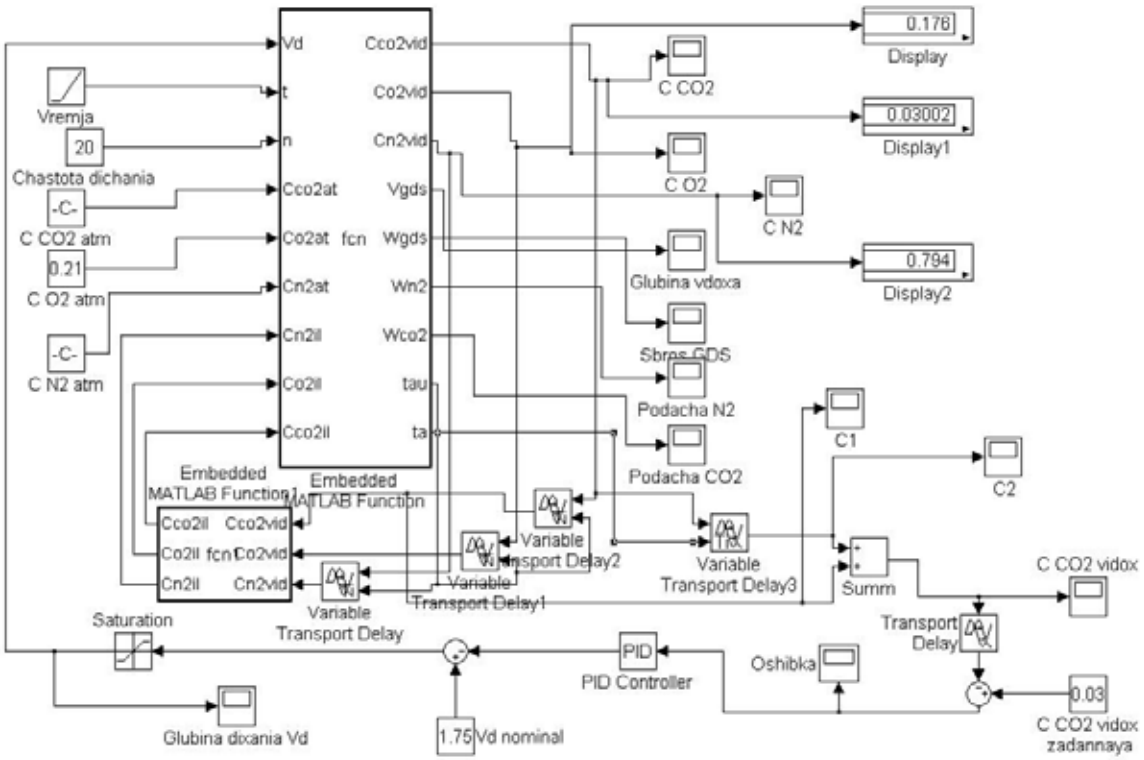


Рис. 1. Simulink-модель стенда ИЛ

На рис. 2–4 представлены результаты имитационных исследований. Они характеризуют переходные режимы работы стенда ИЛ для различных заданных концентраций диоксида углерода на входе в ИДА.

На рис. 3, 4 показаны кривые дыхания, реализующие заданные концентрации диоксида углерода.

Результаты моделирования показывают, что испытательный комплекс выходит на номинальный режим работы (C_{CO_2}=0,03) менее чем за 5 минут с точностью до 0,1%, что подтверждается результатами испытаний реального стенда при «ручном» управлении. С увеличением концентрации диоксида углерода на выходе из блока имитации дыхания уменьшается глубина и частота дыхания. Минимальная частота дыхания ограничивалась величиной 15 min^{-1}.

Автоматизация процессов управления стендом ИЛ повысит точность воспроизведения реальных дыхательных процессов, присущих человеку в различных психофизиологических состояниях.

Полученные результаты могут быть использованы при принятии оптимальных проектных решений на всех этапах разработки и сопровождения ИЛ.

Литература:

1. Гудков, С.В. Совершенствование методики испытания изолирующих дыхательных аппаратов с химически связанным кислородом / С.В. Гудков, Д.С. Дворецкий, А.Ю. Хромов // Вестник ТГТУ. 2009. Том 15. № 3. С. 589–597.

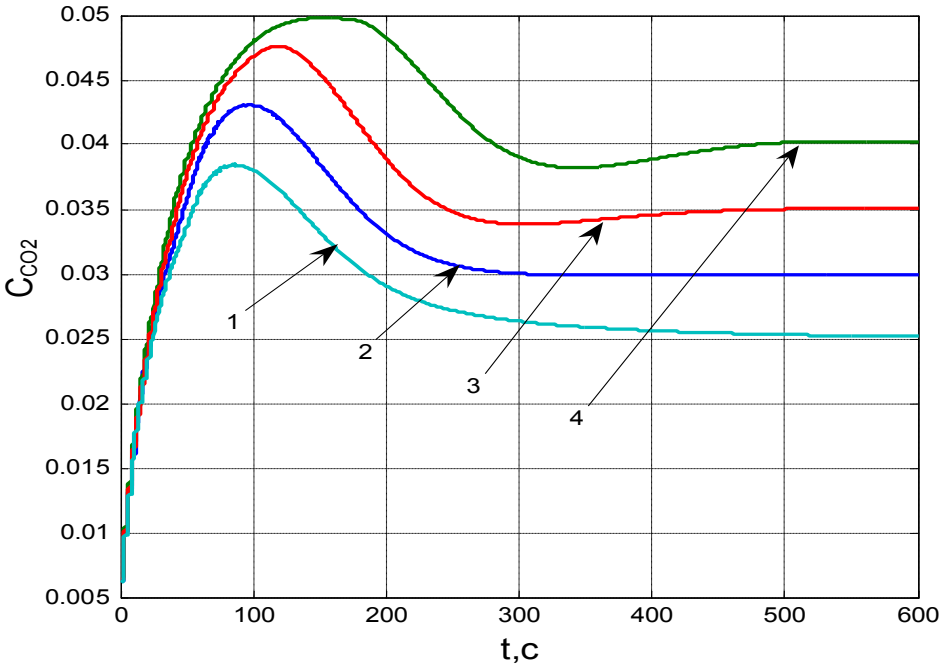


Рис. 2. Концентрация CO_2 в искусственных легких

1 - $C_{CO_2}^{зад}$ =0.025,2 - $C_{CO_2}^{зад}$ =0.03,3 - $C_{CO_2}^{зад}$ =0.035,4 - $C_{CO_2}^{зад}$ =0.04

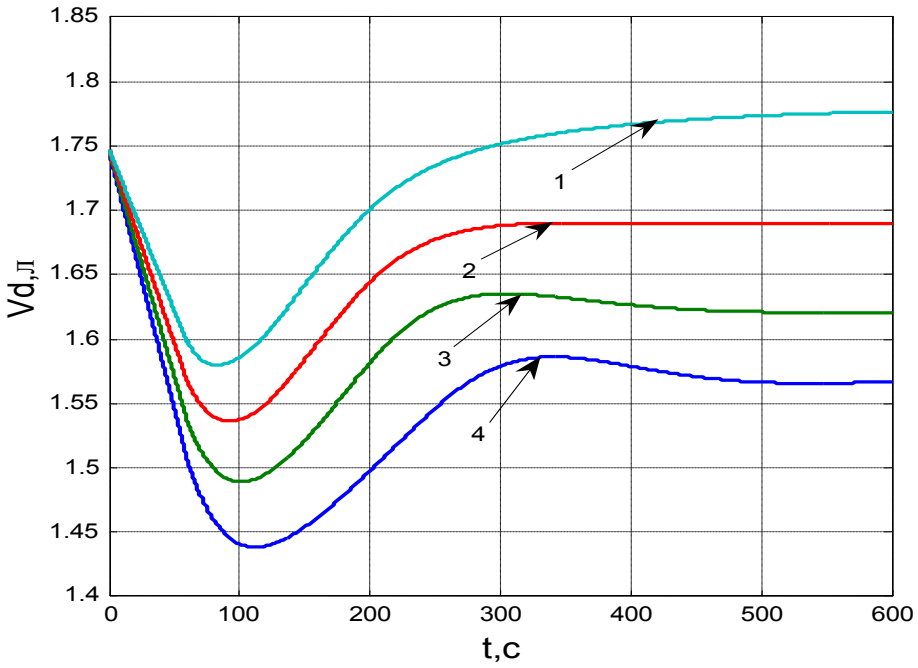


Рис. 3. Глубина дыхания $V_д$, [л]

1 - $C_{CO_2}^{зад}$ =0.025,2 - $C_{CO_2}^{зад}$ =0.03,3 - $C_{CO_2}^{зад}$ =0.035,4 - $C_{CO_2}^{зад}$ =0.04

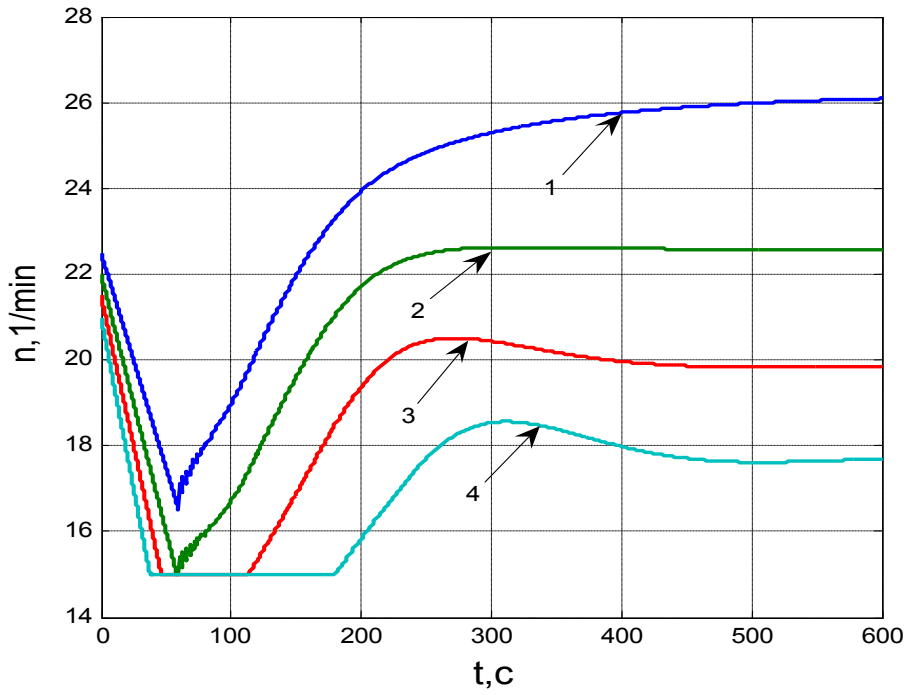


Рис. 4. Частота дыхания *n* [1/min]

1 - $C^{зад}_{CO_2}$ =0.025,2 - $C^{зад}_{CO_2}$ =0.03,3 - $C^{зад}_{CO_2}$ =0.035,4 - $C^{зад}_{CO_2}$ =0.04

Применение алгоритмов с элементами искусственного интеллекта к решению задачи исключения ложных срабатываний автоматической пожарной сигнализации

Малышев Константин Сергеевич, аспирант
Нижегородский государственный технический университет (Дзержинский политехнический институт)

В настоящее время ложные срабатывания автоматических систем противопожарной защиты наносят большой ощутимый экономический ущерб. Отвлечение пожарных подразделений на ложный вызов, не позволяет вовремя ликвидировать настоящие возгорания. Особенно большое количество ложных срабатываний в настоящее время происходит на промышленных объектах. Это связано, прежде всего, с присутствием т.н. «ложных факторов пожара», которые по физическому воздействию на чувствительные элементы пожарных извещателей сходны с опасными факторами пожара, однако не вызваны пожаром. К подобным факторам можно отнести пыль, выделение тепла в ходе технологического процесса, высокая влажность и т.д. В настоящее время для работы большинства систем противопожарной защиты используются классические пороговые алгоритмы, формирующие сигнал о возгорании по информации автоматических извещателей лишь одного типа (задымление, повышение температуры, увеличение УФ или ИК излучения и т.д.). Как следствие, данный подход не позволяет надежно отличать воздействие на чувствительный элемент пожарного извещателя факторов пожара или сходных факторов вызывающих ложное срабатывание.

В работе для определения факта пожара предложено использовать информацию о динамике развития контролируемого фактора для определения причины вызвавшей его. При использовании традиционных алгоритмов формирования сигнала о возгорании учитывается только текущее значение контролируемого параметра (температура среды, задымление) и не учитываются его предыдущие значения. В предлагаемом варианте система поддержки принятия решений обрабатывает информацию от пожарных извещателей с использованием алгоритма искусственных нейронных сетей и определяет уровень достоверности сигнала «Пожар», формируемого приемно-контрольным прибором. Используя данный алгоритм, удастся надежно отличить факт возгорания от влияния сходных факторов, даже при их одновременном воздействии.

Обучение искусственных нейронных сетей производится на данных динамической модели развития типовых очагов пожара (горение твердых, жидких, газообразных веществ, а так же тление). Обобщающие способности ИНС в

данном случае позволяют распознавать не только динамику типовых, но также и более сложных «реальных» пожаров. В настоящее время исследования проводятся при помощи искусственной нейронной сети типа LVQ (квантизация обучающих векторов). Они представляют из себя самоорганизующиеся искусственные нейронные сети в дополнение к соревнующемуся слою которых добавляется линейный слой, который можно обучить реагировать на различные комбинации классов, формируемых соревнующимся слоем.

Отдельным вопросом для рассмотрения является разработка алгоритма обучения искусственной нейронной сети, поскольку обучающая выборка даже для небольшого количества извещателей весьма велика и процесс обучения при помощи традиционных алгоритмов осуществляется недопустимо длительное время. Для решения данной задачи разработан специализированный стохастический эволюционный алгоритм обучения, который существенно сокращает время обучения.

Использование комбинации приведенных алгоритмов для построения интеллектуальной экспертной системы детектирования пожара позволит существенно сократить количество ложных срабатываний. Данный подход целесообразно применять на объектах повышенной опасности. В этом случае незначительные затраты на установку дополнительных электронных модулей и применение данных алгоритмов к обработке информации от них с лихвой перекроют возможные потери в случае ложного срабатывания системы.

В настоящее время применение данных алгоритмов несколько ограничивается стоимостью электронных компонентов для реализации интеллектуальных вычислений в реальном масштабе времени (нейропроцессоры). Однако динамика развития производства данных устройств позволяет с уверенностью сказать, что в ближайшее время появятся бюджетные варианты нейропроцессоров с требуемыми параметрами.

5. ЭНЕРГЕТИКА

Индикатор правильности чередования фаз

Мальцев Максим Сергеевич, аспирант
Иркутский государственный университет путей сообщения

Назначение и конструкция

Индикатор правильности чередования фаз (далее индикатор) предназначен для определения чередования фаз А, В, С сети трехфазного переменного тока напряжением 380 В частотой 50 или 60 Гц.

Индикатор состоит из корпуса, выполненного из электроизоляционного материала, с вынесенным щупом и соединительными проводами. Соединительные провода снабжены зажимами с изоляцией на конце, которая окрашена в черный и красный цвет. Длина соединительных проводов в сумме должна быть не менее 1 м. На торцевой части корпуса находятся элементы световой индикации.

Размер корпуса не нормируется, определяется удобством пользования.

Эксплуатационные испытания

1. При испытаниях изоляции индикаторов напряжение прикладывается между щупом и временным электродом, наложенным на корпус.

2. Нормы и периодичность электрических испытаний приведены в табл. 1 и 2.

Правила пользования

Перед началом использования индикатор проверить визуально. При обнаружении внешних повреждений корпуса или изоляции соединительного провода, пользоваться индикатором запрещается.

При использовании индикатора необходимо помнить, что отсутствие индикации не является обязательным признаком отсутствия напряжения. Поэтому применение индикатора не отменяет обязательного пользования указателями напряжения.

Подсоединить зажимы к проводам в следующем порядке:

– черный к нулевой шине;

– красный к любому фазному проводу.

Коснуться щупом к любой из оставшихся двух фаз. Если светодиоды мигают поочередно с частотой примерно 2–4 Гц, то щуп подключен к фазе А, красный зажим к фазе В. В случае неправильного чередования светодиоды мигают одновременно с частотой более 25 Гц и с малой интенсивностью.

При работе индикатор необходимо держать за корпус и не допускать касания щупом двух токоведущих частей, находящихся под разными потенциалами.

Таблица 1.

Нормы электрических приемо-сдаточных испытаний средств защиты

Наименование средств защиты	Напряжение электроустановок, кВ	Испытательное напряжение, кВ	Продолжительность испытания, мин.
Индикатор правильности чередования фаз	До 1	3	5

Таблица 2.

Нормы и сроки эксплуатационных электрических испытаний средств защиты

Наименование средств защиты	Напряжение электроустановок, кВ	Испытательное напряжение, кВ	Продолжительность испытания, мин.	Периодичность испытаний
Индикатор правильности чередования фаз	До 1	2	5	1 раз в 12 мес.

6. МЕТАЛЛУРГИЯ

Прогнозная модель электропотребления предприятием металлургического профиля. Алгоритм отбора значимых факторов

Бажинов Алексей Николаевич, инженер-программист;
Ершов Евгений Валентинович, доктор технических наук, профессор
Череповецкий государственный университет
Рыбинская государственная авиационная технологическая академия имени П.А. Соловьева

Рассмотрен один из подходов к решению задач автоматического исследования данных – деревья решений; введено понятие значимости входных атрибутов и формула ее расчета; приведены результаты практического применения этого метода в задаче выявления значимых факторов для прогнозирования электропотребления металлургическим предприятием.

Ключевые слова. *Деревья решений; значимость; входные атрибуты модели; электропотребление; металлургия.*

Проблема прогнозирования электропотребления предприятием металлургического профиля представляет собой сложную многопараметрическую задачу, имеющую вероятностную составляющую [6, с. 117]. Объём фактического использования электроэнергии обусловлен не только управленческими решениями, структурой портфеля заказов промышленного предприятия, но и типом дня (рабочий день или выходной), погодными условиями, временем суток и многими другими факторами. Причинная связь электропотребления с каждым из этих параметров довольно сложна и не имеет однозначного формального описания линейной моделью. В то же время применение нелинейных регрессионных моделей проблематично. Для этого требуется явное задание характера нелинейности еще до проведения анализа, что является серьезным ограничением [5, с. 41].

Таким образом, учитывая специфичность и сложность задачи, можно сделать вывод от том, что хорошо зарекомендовавшие себя в случае с регрессионной моделью методы[1] отбора значимых входных признаков не могут быть применены [1, с. 345].

Одним из наиболее перспективных подходов к решению задач автоматического исследования данных, лишенному рассмотренных выше недостатков, является дерево решений – способ представления правил в иерархической, последовательной структуре, где каждому объекту соответствует единственный узел, дающий решение [2, с. 94]. Под правилом понимается логическая конструкция, представленная в виде «если ... то ...».

На сегодняшний день существует значительное число алгоритмов, реализующих деревья решений: CART, C4.5, NewId, ITrule, CHAID, CN2 и др. [3, с. 29].

Большинство из известных алгоритмов являются «жадными алгоритмами». Если один раз был выбран атрибут, и по нему было произведено разбиение на подмножества, то алгоритм «не может» вернуться назад и выбрать другой атрибут, который дал бы лучшее разбиение. Поэтому на этапе построения нельзя сказать даст ли выбранный атрибут, в конечном итоге, оптимальное разбиение [3, с. 72].

В работе за основу взят алгоритм C4.5[2] построения дерева решений, для которого количество потомков у узла не ограничено, решающий только задачи классификации, так как «не умеет» работать с непрерывным целевым полем [2, с. 308].

Для решения поставленной задачи необходимо, во-первых, внести изменения в процедуру разбиения по значениям непрерывного типа; во-вторых, что самое главное, ввести понятие «значимости» входных атрибутов и определить формулу для её расчетов.

Ниже приведён алгоритм разбиения по значениям непрерывного типа:

1. Упорядочить все значения по возрастанию.
2. Разбить исходное множество T на два – T_1 и T_2. На первой итерации в T_1 попадает только первый элемент,

[1] Процедура Forward Selection (прямой отбор), процедура Backward Elimination (обратное исключение), процедура Stepwise, процедура Best Subsets (лучшие подмножества).

[2] C4.5 – алгоритм построения дерева решений, количество потомков у узла не ограничено. Не умеет работать с непрерывным целевым полем, поэтому решает только задачи классификации.

остальные – в T_2. На следующей итерации первый элемент из T_2 попадает в T_1 и т.д.

3. Вычислить индекс $Gini_{split}$ для каждого из разбиений множества T. Выбрать то разбиение, для которого индекс $Gini_{split}$ минимален. Используются следующие соотношения:

$$Gini(T) = 1 - \sum_{i=1}^{n} p_i^2 \quad (1)$$

$$Gini_{split}(T) = \frac{N_1}{N} Gini(T_1) + \frac{N_2}{N} Gini(T_2) \quad (2)$$

где p_i – вероятность нахождения примера класса i во множестве T, N – количество примеров во множестве T (N_1 и N_2 – во множестве T_1 и T_2 соответственно)[4, с. 204].

4. Дальнейшее разбиения узла прекращается при выполнении одного из условий:

– в узле содержится достаточное количество примеров (настроечный параметр);

– узел содержит примеры одного класса;

– количество нераспознанных примеров меньше минимального количества примеров в узле (настроечный параметр).

Теперь введем понятие «значимости» входного атрибута. Под значимостью атрибута будем понимать показатель, характеризующий, насколько сильно выходное поле зависит от данного входного.

Формула для расчета значимости имеет вид:

$$Z_m = \frac{\sum_{j=1}^{k_m} \left(E_{m,j} - \sum_{i=1}^{n_{m,j}} E_{m,j,i} \cdot \frac{N_{m,j,i}}{N_{m,j}} \right)}{\sum_{l=1}^{g} \sum_{j=1}^{k_l} \left(E_{l,j} - \sum_{i=1}^{n_{l,j}} E_{l,j,i} \cdot \frac{N_{l,j,i}}{N_{l,j}} \right)} \cdot 100\% \quad (3)$$

где g – количество входных атрибутов, k_l – количество узлов, которые были разбиты по атрибуту l, $E_{l,j}$ – энтропия родительского узла, разбитого по атрибуту l, $E_{l,i,j}$ – энтропия дочернего узла для j-го, разбитого по атрибуту l, $N_{l,j}$, $N_{l,i,j}$ – количество примеров в соответствующих узлах, $n_{l,j}$ – количество дочерних узлов для j-го родительского.

Вычисление показателя значимости для атрибутов возможно только после построения дерева классификационных правил.

Технологические процессы потребления электроэнергии подчиняются циклическим, функциональным и случайным тенденциям, из которых наиболее прогнозируемые циклические зависимости (как правило, суточные, недельные и годичные).

Циклические зависимости составляют 70–80 % всех отклонений в процессе потребления электроэнергии [6, с. 46]. Наиболее существенными циклическими факторами практически во всех производственных процессах являются: величины фактического потребления электроэнергии в предыдущие периоды, время суток, день недели, долгота светового дня.

Закономерности функционального характера являются вторым из основных изучаемых факторов при прогнозировании, их долевое участие составляет приблизительно 10–15 % от всего объема отклонений. В эту группу включаются отклонения, объясняемые известными и относительно предсказуемыми факторами производства: температурой воздуха или теплоносителя, значениями и прогнозами параметров, являющихся основными производственными факторами, определившими профиль и величины фактического потребления электроэнергии (объем поставок сырья, объем самого производства) и т.д.

И, наконец, случайные тенденции составляют третью, завершающую компоненту прогноза: их долевое участие в общем процессе невелико, но амплитуда отклонений может быть довольно значительна. Очевидно, что назвать такие отклонения «истинно случайными» будет неверно: каждое отклонение может быть впоследствии объяснено вполне закономерными причинами.

Дерево решений, построенное на основе исходных данных потребления электроэнергии одним из крупных предприятий металлургического профиля, получилось сильноветвистым. На рисунке 1 приведена лишь одна его ветвь (значения всех параметров указаны в условных единицах измерения).

Дальнейшие вычисления показали, что основными факторами, определяющими достоверность прогноза, являются следующие (табл. 1).

В задачах краткосрочного прогнозирования электропотребления распределение значимости параметров, а возможно и их состав, будет иным.

Таким образом, для целевого метода прогнозирования основными влияющими факторами являются автокорре-

Таблица 1.

Значимость основных факторов для прогнозной величины электропотребления в задаче суточного прогнозирования

№ параметра	Параметр	Значимость, %
1	Потребление электроэнергии в предыдущий день	47
2	Объём производства в предыдущий день	18
3	Потребление электроэнергии два дня назад	13
4	Статус дня	12
5	Среднесуточная температура воздуха	7
6	Долгота дня	3

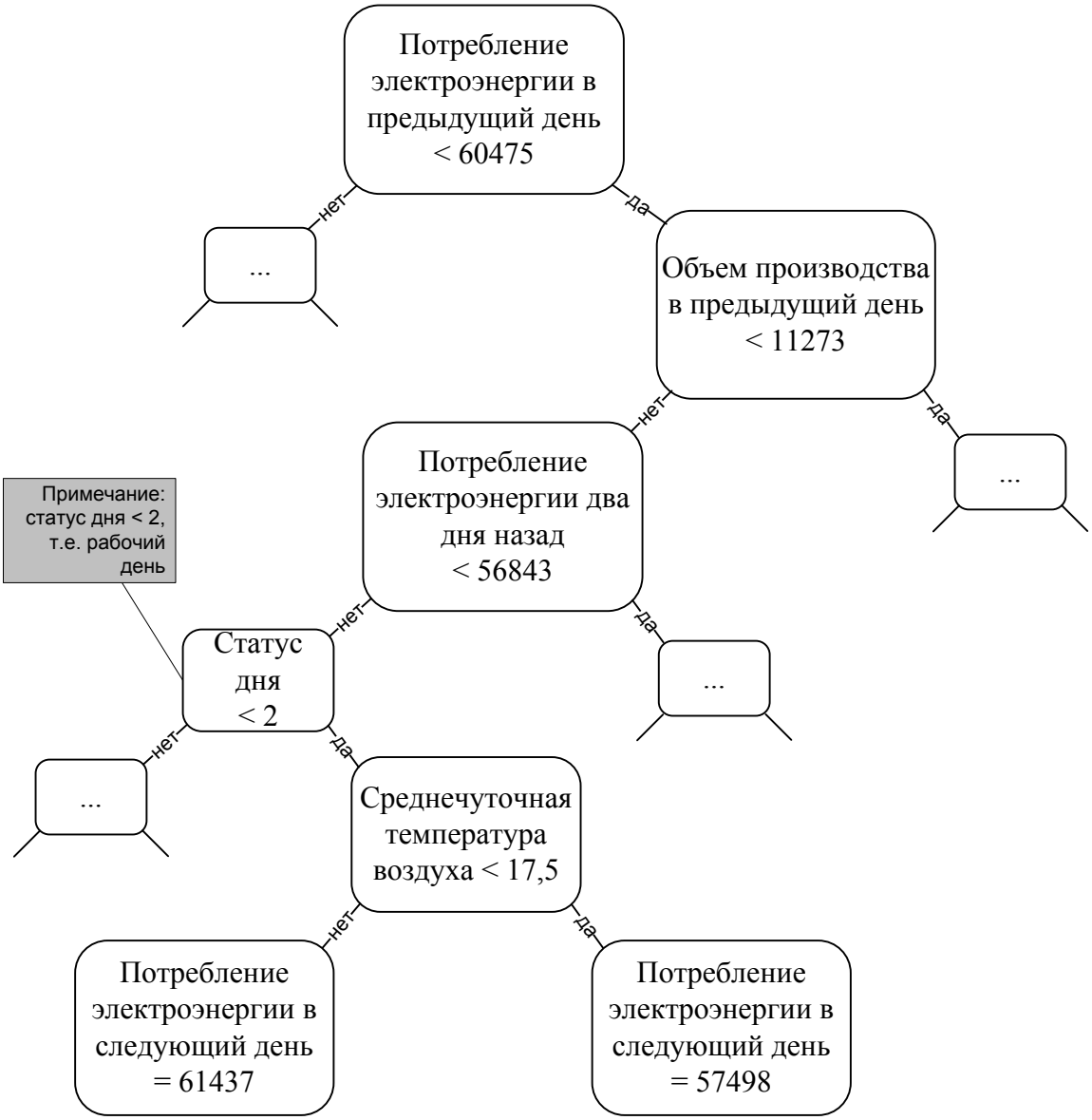


Рис. 1. Ветвь дерева решений в задаче прогноза электропотребления металлургическим предприятием

ляционные: потребление электроэнергии в предыдущий день и два дня назад, а также статус дня и объем производства в предыдущий день.

Из выбранных основных входных данных наименьшей точностью обладает статус дня: все возможные состояния описываются набором всего из 5-ти значений: рабочий день, рабочий день по 6-ти дневной неделе, рабочий день по приказу руководителя предприятия, выходной день, праздничный день. В сочетании с достаточно высокой степенью значимости этого параметра ошибка в его значении может привести к принципиально неверному прогнозу. Поэтому следует отметить, что улучшение качества метода прогнозирования в первую очередь должно быть направлено на введение в модель дополнительных данных, таких как графики работы подразделений, объемы выпуска по цехам и прочее. Однако, дублирование информации в составе избыточного признака не просто не улучшает качество модели, но и порой, наоборот, ухудшает его.

К примеру, при добавлении к существующему набору входных параметров группы энергоресурсов, сопутствующих электроэнергии в металлургическом производстве, наблюдалось ухудшение основных показателей качества прогнозирования. К этой группе относятся следующие показатели: кислород технологический, азот компримированный, сжатый воздух, вода техническая оборотная и т.д.

Детальный анализ ситуации выявил мультиколлинеарность между этими параметрами и электропотреблением. В доказательство сказанного, исследуем увеличение стоимости кислорода технологического. Как видно из рис. 2, основную долю (21 % из 24 %) в увеличении стоимости занимают энергозатраты – в большей степени электроэнергия. Аналогичная ситуация имеет место и по другим параметрам указанной группы.

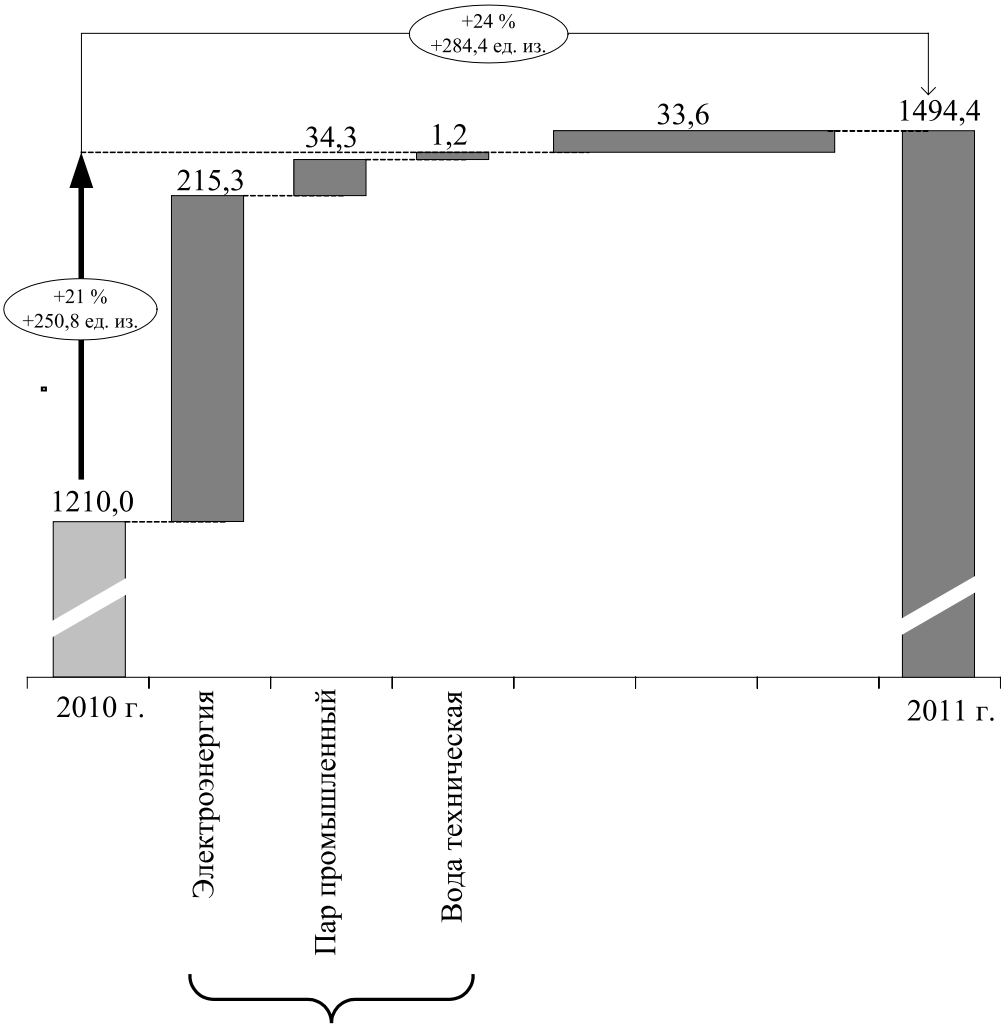


Рис. 2. Увеличение стоимости кислорода технологического в 2011 году к 2010 году (в условных единицах измерения)

Проведенный выше анализ применимости деревьев принятия решений для задачи отбора значимых параметров для прогнозирования объёмов потребления электроэнергии показал, что данный метод применим для решения таких задач в рамках крупных потребителей электроэнергии, работающих в секторе свободной торговли. Изложенный подход не претендует на полную замену высококвалифицированного труда эксперта-энергетика предприятия. Однако, используя средства и методы по детальной обработке и всестороннему анализу больших массивов данных, эксперт предприятия может выйти на качественно иной уровень прогнозирования, своевременно реагируя на изменения в структуре суточного энергопотребления с помощью инструмента для составления более точных заявок на длительный срок – неделя, месяц.

Литература:

1. Айвазян С.А., Мхитарян В.С. Прикладная статистика и основы эконометрики, М.: Юнити, 1998. с. 1005
2. Коршунов Ю.М. Математические основы кибернетики. М.: Энергоатомиздат, 1987. с. 496
3. Ларичев О.И., Мошкович Е.М. Качественные методы принятия решений. Вербальный анализ решений. М.: Наука. Физматлит, 1996. с. 208
4. Левитин А.В. Алгоритмы: введение в разработку и анализ, М.: Вильямс, 2006. С. 576
5. Никифоров Г.В., Олейников В.К., Заславец Б.И. Энергосбережение и управление электропотреблением в металлургическом производстве. М.: Энергоатомиздат, 2003. С. 480.
6. Цымбал В.П. Математическое моделирование металлургических процессов. М. – Металлургия, 1986. с. 239

Исследование перемещений металла в очаге деформации при пилигримовой прокатке тонкостенных труб

Раскатов Евгений Юрьевич, кандидат технических наук, доцент
Уральский федеральный университет имени первого Президента России Б.Н. Ельцина (г. Екатеринбург)

Описана математическая модель и приведены результаты перемещений металла в мгновенном очаге при пилигримовой прокатке труб.

Ключевые слова: *Моделирование, обжатия, калибровка, расчетная модель, гильза, подача, напряжения*

A efforts of the metal displacement in the deformation zone during pilger rolling thin-walled tubes

Evgeny Raskatov, Candidate of Technical Sciences, associate professor at the Metallurgical and rotary machines Department
Urals Federal University of the first Russian President Boris Yeltsin

The mathematical model is described and the results of the displacement of the metal in an instantaneous deformation zone for pilger rolling tubes are mentioned.

Key words: *Model-based analysis, cobbing, grooving, computational model, shell, batch, stress*

Использование непрерывнолитых заготовок круглого сечения обеспечивает существенные преимущества пилигримового способа производства бесшовных труб. Однако непрерывнолитые заготовки имеют внешние и внутренние дефекты, в осевой зоне слитка образуются ликвация, пористость, раковины. В связи с этим, при пилигримовой прокатке очень важно создать благоприятную схему напряженно-деформированного состояния металла в очаге деформации, что предотвратит образование рванин на поверхности труб и обеспечит интенсивную проработку литой структуры металла, то есть получить трубы высокого качества. При этом особенно важно оценить закономерности обжатия и течения металла как по длине очага деформации, так и по ширине калибра в зависимости от величины подачи, особенно в местах выпуска калибров.

Исследование течения металла в очаге деформации пилигримовой прокатки труб усложняется тем, что в каждый момент времени рабочий конус валков соприкасается с металлом не по всей поверхности очага деформации (рис. 1), а какой-то сравнительно небольшой частью, то есть имеет место мгновенный очаг деформации [1].

Моделирование процесса прокатки тонкостенных труб в пилигримовом стане выполнялось с использованием программного продукта ANSYS v10.0 [2]. Расчет выполнялся с использованием метода конечных элементов в объемной постановке.

Упор сделан на определение закономерностей течения металла на первом участке, где бойковой частью валка осуществляется интенсивная деформация гильзы, и полирующем участке калибра валка, на котором раскатывается объем металла, смещенный на первом участке деформации. Материал трубы в очаге деформации испытывает упругопластические деформации, которые достигают конечных значений. Поскольку их уровень высок, то при описании модели материала трубы в очаге деформации учтена не только физическая, но и геометрическая нелинейность. Для материала трубы принята упругопластическая модель Прандтля-Рейса. Принимается, что трение на всей поверхности контакта валков с трубой подчиняется закону сухого трения Кулона, а коэффициент трения постоянен на всей контактной поверхности. Исследовался процесс пилигримовой прокатки тонкостенной трубы из стали 14ХГС диаметром 325 мм из гильзы диаметром 500 мм, причем диаметр дорна равен 300 мм. Скорость вращения валков составляла 45 об/мин.

Моделирование процесса пилигримовой прокатки проводили для калибровки валков, имеющей центральный угол бойкового участка 110 градусов, полирующего участка – 65 градусов, участка выпуска – 45 градусов и холостого участка 110 градусов. Величина подачи составляла 10, 20, 30 мм. Температура прокатываемого материала гильзы принята постоянной и равной 1050°С.

На рис. 2 изображена расчетная модель прокатываемой трубы с калибром валка перед прокаткой.

В силу симметрии рассматривается четверть предельного сечения трубы с калибром валка. Учитывается деформация гильзы по трем направлениям на основе трехмерной объемной модели. В качестве кинематических граничных условий задавалось отсутствие нормальных перемещений по плоскостям симметрии гильзы и валков.

На рис. 3 и 4 показан характер изменения обжатия гильзы в зависимости от угла поворота валка соответственно для подач 10 и 30 мм. На рисунках дан характер обжатия, по высоте линии 1 (рис. 1). Обозначение линии, например, 10–70 – означает, что подача 10 мм, а угол поворота валка 70 градусов. Из рис. 3 следует, что при по-

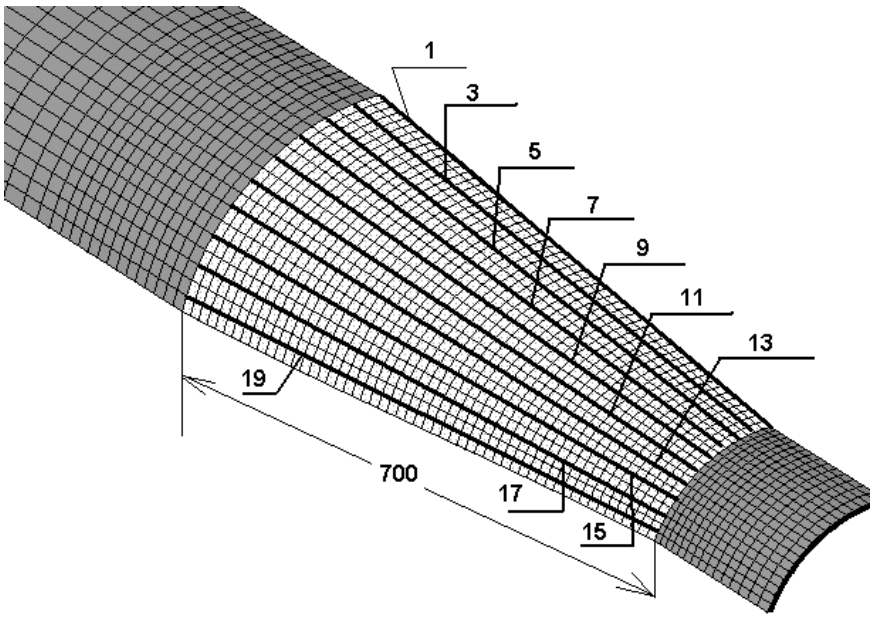


Рис. 1. Расчётная модель очага деформации

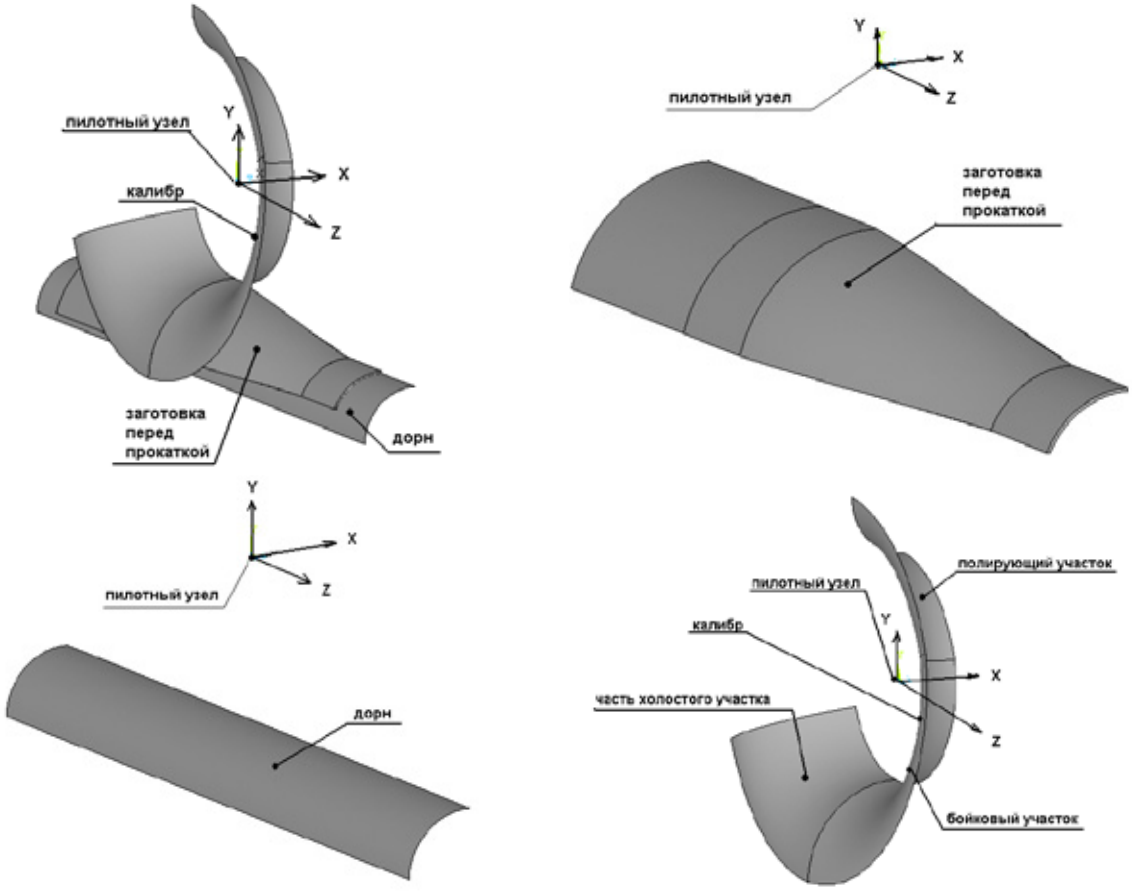


Рис. 2. Расчётная модель прокатываемой трубы в пилигримовых валках

даче гильзы в валки величиной 10 мм волна металла образуется практически для угла поворота валка 120 градусов, затем на полирующем участке она обжимается и при угле поворота валка 130 градусов волна не наблюдается. При подаче 30 мм волна образуется до угла поворота валка равного 130 градусов, затем она обжимается и исчезает при угле поворота валка 140 градусов.

Рис. 5 и 6 характеризуют обжатия по нормалям по линиям 1, 5, 9, 13 и 17 контакта калибра с гильзой (рис. 1), соответственно для двух углов поворота валка 80 и 100

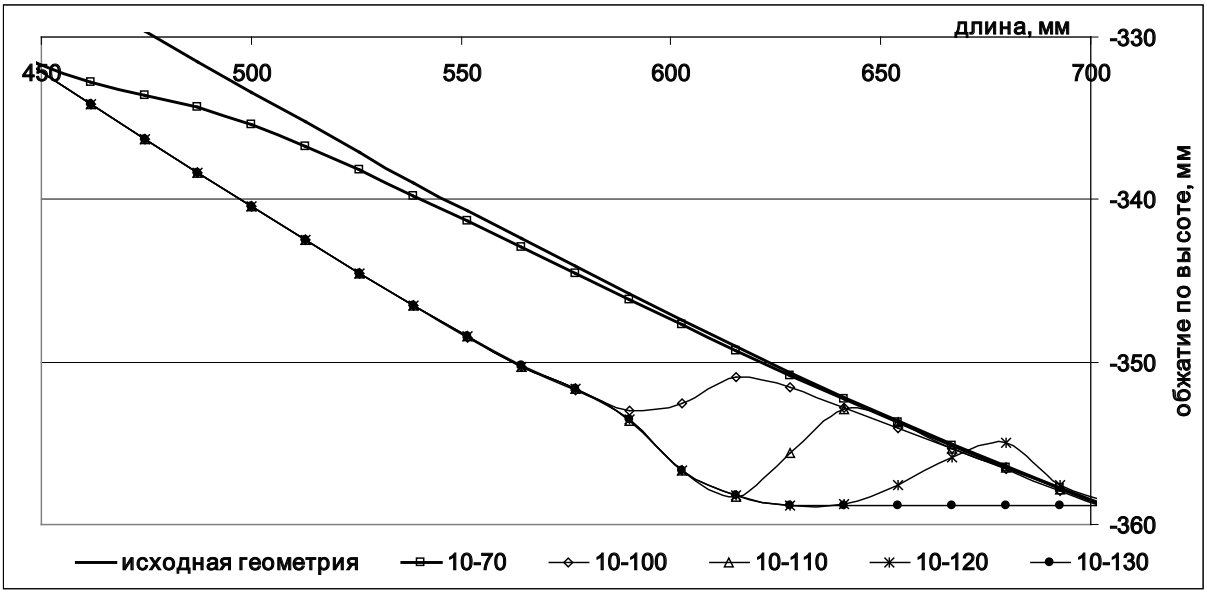


Рис. 3. Характер обжатия по высоте части линии 1 в зависимости от угла поворота. Подача 10 мм

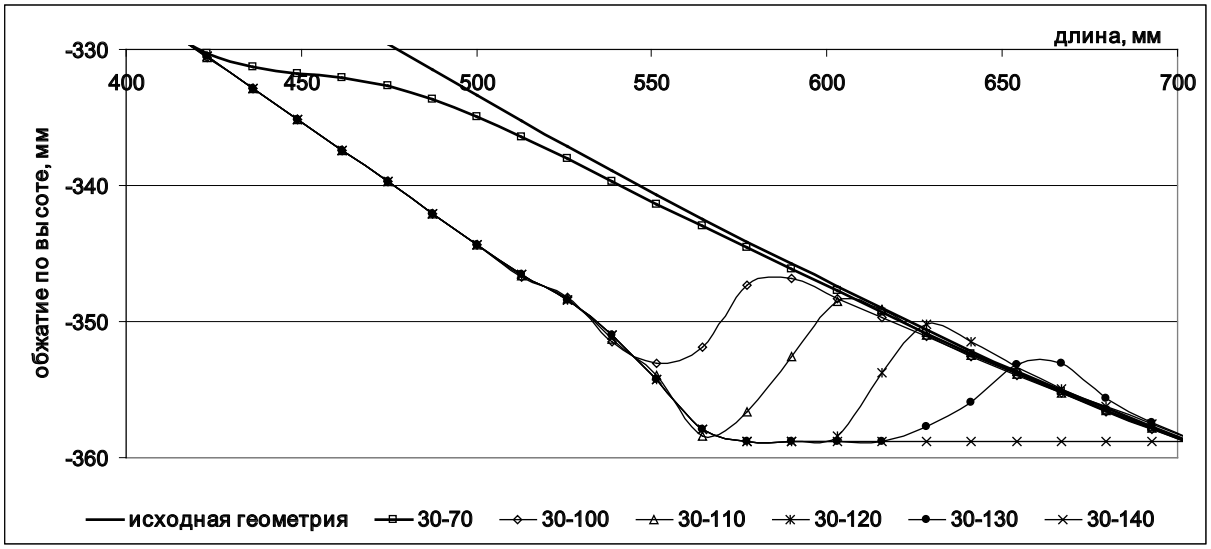


Рис. 4. Характер обжатия по высоте части линии 1 в зависимости от угла поворота. Подача 30 мм

градусов. Для подачи гильзы в валки 10 мм для этих же углов поворота приведены эпюры нормальных напряжений – SX. Калибровка валков 110–65–45–140. Из рисунков следует, что по периметру гильза обжимается неравномерно, причем наибольшее обжатие имеет место на участке по линии 9. На этом же участке возникают наибольшие нормальные напряжения, которые с величины 325 МПа при угле поворота валка 80 градусов возрастают до 720 МПа при угле поворота валков 110 градусов.

Заключение

В результате теоретического исследования перемещений металла в очаге деформации, определен уровень обжатий и области возникновения максимальных нормальных напряжений, а также характер обжатия гильзы валками при пилигримовой прокатке стальных тонкостенных труб.

Литература:

1. Тетерин П.К. Теория периодической прокатки. М: Металлургия, 1978.
2. ANSYS. Structural Analysis Guide. URL: http://www.cadfem.ru

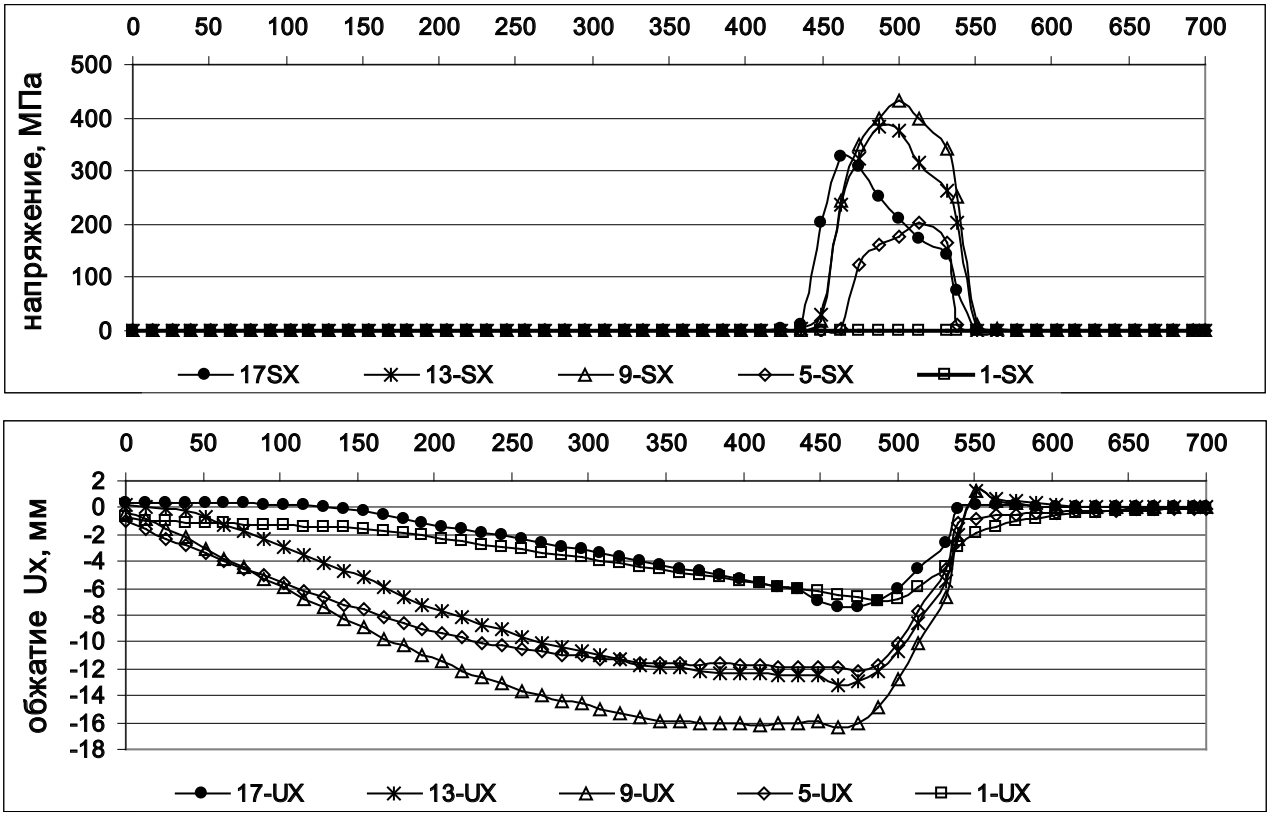


Рис. 5. Контактные нормальные (SX) напряжения по линиям 1, 5, 9, 13 и 17 контакта калибра с заготовкой. Характер обжатия по нормали (UX) по линиям 1, 5, 9, 13 и 17 контакта калибра с заготовкой. Угол поворота 80 градусов

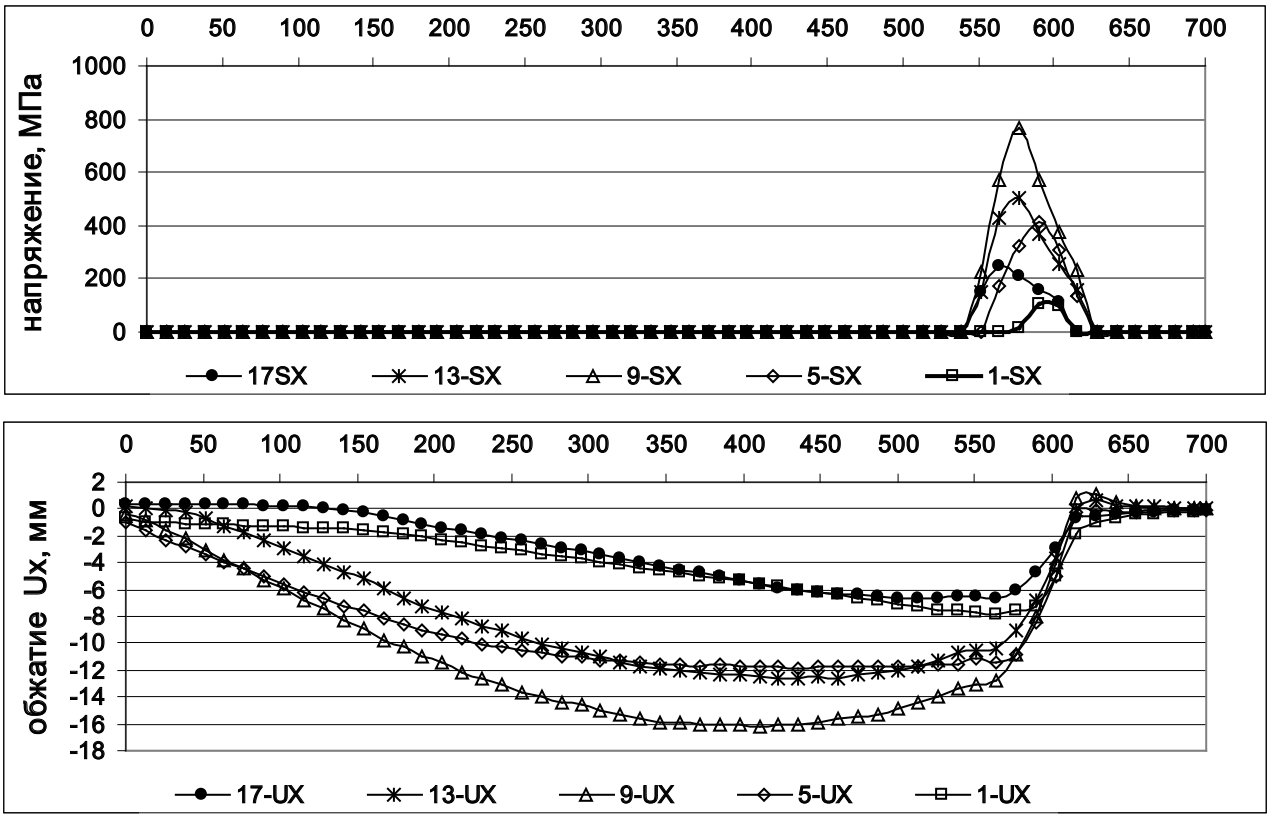


Рис. 6. Контактные нормальные (SX) напряжения по линиям 1, 5, 9, 13 и 17 контакта калибра с заготовкой. Характер обжатия по нормали (UX) по линиям 1, 5, 9, 13 и 17 контакта калибра с заготовкой. Угол поворота 110 градусов

7. МАШИНОСТРОЕНИЕ

Агрономические и агроэкологические аспекты систем обработки почвы

Данатаров Агахан, кандидат технических наук; Ашыров Сердар Чашемович, ст.преподаватель
Туркменский сельскохозяйственный университет (г. Ашгабат)

It is established that influence of aeration drainage on vodno-air, salt and thermal modes of soil is shown in increase of water conductivity soil and especially arable sole horizon that the weight provides effective redistribution in thickness of a file of a ground on all its depth. Active regulation of a moisture, salts and heat in soil with presence of aeration drainage has effective influence on productivity of a cotton and especially on old irrigated heavy soils of an arid zone. Results of experimental check have confirmed analytical assumptions of efficiency of application of aeration drainage on cotton systems.

Key words: *Influence of aeration drainage On a vodno-salt mode of soil and productivity of a cotton.*

Изучение причин возникновения процессов уплотнения почв на орошаемых землях осуществлялось с учетом работ Н.Д. Прянишникова (1929), А.Н. Соколовского (1956), А.Н. Костякова (1961), О.Г. Грамматикати (1969), Н.А. Качинского (1970), В.С. Казакова (1984), В.В. Медведева (1988, 1994), Б.Б. Шумакова (1993, 1995), А.Г. Бондарева (1990, 1998), Ф.Р. Зайдельмана (1996, 2003), Н.С. Скуратова (2001), Д.А. Черняховского (2003), Ю.П. Добрачева (2004), В.Н. Богословского (2004), Н.А. Пронько (2001, 2009), Ю.П. Танделова (2007) и многих других ученых, посвященных различным аспектам ухудшения состояния мелиорируемых земель.

Уменьшение деградации почв и повышение их качества является основой экологической интенсификации агротехнологий. Качество почвы, так же как и урожайность, является сложным понятием, которое трудно определить или измерить. Качество почвы трактуется как способность поддерживать биологическую продуктивность, сохранять окружающую среду, развитие здоровых растений и животных. Не взирая на обширность этого определения, можно согласиться, что поддержание продуктивности растений через оптимальные резервы питательных веществ в почве, способность ее сохранять влагу и благоприятную структуру для роста корней являются теми свойствами, которые влияют на ее экологию. Снижение качества почвы в результате антропогенного воздействия может быть определено как ее деградация. Водная и ветровая эрозии, химическая деградация и ухудшение физических свойств почв главные виды ее деградации. Продуктивность сельского хозяйства, выбор технологий производства, разработка системы машин, а также направления агроинженерных исследований обусловлены острой необходимостью сохранения основных ресурсов с.-х. производства – почвы, воды, воздуха и энергии [1].

Для решения данной проблемы 1989–1994 гг. в ТуркменНИИГиМ по теме «Технология нарезки аэрационного дренажа и эффективность его работы в условиях аридной зоны» разработана технология улучшения водно-воздушного, солевого, питательного и теплового режимов с последующим получением гарантированных урожаев, отвечающая требованиям водосберегающих ресурсов и снижению экологической напряженности в аридной зоне. Влияние аэрационный дренаж (АД) на водно-воздушный режим почвы проявляется прежде всего в подпахотном горизонте, где влагоемкость почвы по результатам опытов повышалась на 30% (глубина 30–50 см). Влагоемкость в пахотном слое (глубина 0–35 см) увеличивалась лишь на 6%. Наблюдения в последующие три года показали, что зона рыхления постепенно уплотняется, однако исходных показателей плотность все же не достигала, отмечено также увеличение порозности на 27–30% сразу после АД и 5,5–16% на третий год после АД.

Как показали наблюдения, порозность улучшилась в результате увеличение числа крупных водопроводящих и воздухопроводящих пор, а это способствовало увеличению водопроницаемости почвогрунта более 100 раза [2]. Эффективность АД по водопроницаемости почвы, наблюдается при нарезке дрен на расстоянии в пределах от 0,6–0,9 м. Под воздействием АД почва более активно аэрировалась. Температура почвы на глубине 0,6 м при междренном расстоянии 0,9 м в среднем меньше было на 4,4% (в целом по глубине 9%) по сравнению с контрольным вариантом.

Нарезка АД существенно отразилась на основных фазах развития хлопчатника. Фенологические наблюдения показали, что на участках АД и сплошным рыхлением всходы хлопчатника, начало бутонизации, цветение, плодообразование и созревание опережают на 1–4 дня. Данные показатели по контрольному варианту, что в конечном итоге отражается на росте растений, их урожайности [2]. Установлено, что связи с увеличением междренного расстояния коэффициент фильтрации грунта

уменьшается и приближается по величине к водопроницаемости пахотного горизонта. Однако, при уменьшении расстояния между кротовинами до 0,6–0,9 м действие АД стабилизируется, в чем можно убедиться, анализируя кривые зависимости изменения коэффициента фильтрации.

Следовательно, при нарезке АД обеспечивает следующие преимущества по сравнению с первоначальным состоянием почвы: в результате понижения ГВ повышается способность почв накапливать влагу атмосферных осадков в течение вегетационного периода, и, таким образом, растения лучше обеспечиваются влагой; корни глубже проникают (до 150 см) почву; мощное развитие корней улучшает структуру почвы; кротовинах накапливается вода; благодаря улучшению микроклимата увеличивается вегетационный период на 12 дней; дает возможность возделывания разных культур; переходит некапилярной порозности в капилярную; становиться хорошая водо- и воздухопроницаемость почвогрунтов. Концентрация свежего органического вещества обособленной прослойкой в нижней части пахотного слоя оказывает огромное окультуривающее действие на этот слой и подпочву: сдерживается минерализация органического вещества и потеря минеральных форм от промывания, усиливается накопление гумуса и улучшается его качественный состав, питательные вещества в глубоких слоях почвы становятся доступными для растений; увеличивается период, в течение которого можно обрабатывать почву; повышаются другие агрохимические показатели плодородия почвы; снижается кислотность, увеличивается сумма поглощенных оснований, содержание подвижного фосфора и обменного калия. В результате проведения кротования-рыхления почвы, рыхление почвы происходит на всю глубину V – образной формы, щирина которой по верху составляет 65–70 см. При этом средняя комковатость почвы составляет 30–60 мм. Кротовые дрены оформлены в монолите грунта с плотностью склета 18–22 г/см^3, влажностью 8–12%.

Таким образом, можно сделать вывод о том, что воздействие АД на водно-воздушный, солевой и тепловой режимы почвы проявляется в повышении водопроводимости почвенного и особенно подпахотного горизонта, что обеспечивает эффективное масса перераспределение в толще массива грунта на всю его глубину. Активное регулирование влаги, солей и тепла в почве с наличием АД оказывает эффективное воздействие на урожайность хлопчатника и особенно на староорошаемых тяжелых почвах аридной зоны. Результаты экспериментальной проверки подтвердили аналитические предположения об эффективности применения АД на хлопковых системах.

Литература:

1. Борисенко, И.Б. Совершенствование ресурсосберегающих и почвозащитных технологий и технических средств обработки почвы в острозасушливых условиях Нижнего Поволжья. Диссертация доктора технических наук. Волгоград 2006. С. 4–402.
2. Данатаров, А., Байджанов Г. Мелиоративная и экономическая эффективность аэрационного дренажа. «Молодой ученый» ежемесячный научный журнал. Чита. 2010. №8. с. 83–91.

Технологии и техника для рыхления-кротования переуплотненных почв

Данатаров Агахан, кандидат технических наук; Ашыров Сердар Чашемович, ст.преподаватель
Туркменский сельскохозяйственный университет (г. Ашгабат)

Stability of aeration drainage was defined by means of laboratory-field methods: the laboratory; the field; laboratory-field. The description ways the device of aeration drainage differ not only character of application and efficiency. At observance of technology of cutting of aeration drainage, and also service regulations of aeration drainage, efficiency and duration of its action on heavy soils of an arid zone has made 4 years.

Key words: *инженерное конструирование; экологическая безопасность; обработка почв*

Внедрение интенсивных технологий с ипользованием энергонасыщенных и тяжелых агрегатов увеличило уплотнение почвогрунтов и ускорило образование почвенной уплотненной подошвы. Этот процесс усугубляется увеличением количества операций применением повышенных доз удобрений и пестицидов. Наиболее распространенным способом борьбы с почвенной подошвой является механическое рыхление на глубину 50 см [4].

Повышение плодородия почв – основное условие устойчивости земледелия и внедрения интенсивных технологий. На современном уровне сельскохозяйственной науки и производства понятие плодородие почв подкреплено определенными качественными и количественными показателями и становиться фактором управляемым. В числе важнейших показателей плодородия, таких, как глубина пахотного слоя, кислотность почвенной среды, запасы подвижных элементов питания, на первом месте

стоит содержание в почве гумуса и свежего органического вещества, его качественное состояние. В управлении процессами создания и разложения гумуса решающая роль принадлежит внесению навоза и других форм органических удобрений, накоплению в почве корневых и пожнивных остатков, системе обработки почвы, регулирующей активность биологических процессов, соотношение интенсивных аэробных и замедленных анаэробных условий разложения. Важно, чтобы сочетание всех условий обеспечивало близкий к бездифицитному или положительный баланс гумуса. По примерным расчетам, на тяжело- и среднесуглинистых почвах при содержании 2% гумуса (примерно 50 т гумуса в пахотном слое на 1 га пашни) ежегодно разлагается в среднем под культурами севооборота около 2% общего запаса гумуса, или одна тонна. Примерно половина этого (0,5 т) восполняется за счет корневых и пожнивных остатков. Вторую половину должно пополнить внесение органических удобрений. Принимая, что 1 т навоза дает при разложении около 50 кг гумуса, для пополнения дефицита в 500 кг необходимо вносить 10 т навоза на каждый гектар севооборотной площади. На песчаных землях разложение идет быстрее в севооборотах с многолетними травами, пожнивными и сидеральными культурами, увеличивается количество поступающих в почву корневых и пожнивных остатков. Частое и в малых дозах внесение навоза при поверхностной заделке способствует интенсивной минерализации почвы, а в больших дозах при глубокой заделке усиливет его мелиорирующее воздействие на плодородие почв. Там где нет возможности вносить необходимое количество органических удобрений, целесообразно использовать растительные остатки. В исследованиях последних лет установлен ряд положений, которые могут быть приняты в качестве теоретических основ для изучения и формирования зональных систем обработки почвы [5].

В естественных условиях плодородие почв в основном обеспечивается за счет гумификации органического вещества, поступающего в почву с отмершими растениями, с остатками микроорганизмов и животных, а также корневых выделений и корней. В процессе обработки при наличии аэрации влаги и тепла активизируется разложение органического вещества и в большем количестве выделяется CO_2. Это имеет большое значение и в процессе растворимости различных веществ в почве. Образовавщаяся в процессе разложения органического вещества CO_2 при наличии вода растворяет фосфаты, что способствует увеличению доступности фосфора для питания растений. Следовательно, если нет микроорганизма, то нет CO_2, соответственно нерастворимое соединения фосфорный кислоты не может переходит в растворимое состояние.

Целесообразность строительства беструбчатых кротовых дрен в минеральных почвах определяется не только их гранулометрическим составом, но и генетическим типом почв и их структурой. Чем водопрочнее структура и выше агрегированность почв, тем продолжительности действия кротовых дрен. Для количественной оценки продолжительности действия кротовых дрен в минеральных почвах в СНГ используют способ Ф.Р. Зайдельмана, позволяющий судить о сроке действия земляной дрены по водопрочности микроагрегатов размером 3–5 мм. Качественная диагностика устойчивости кротовых дрен возможна по микроагрегатному составу почв способом С.В. Астапова [1]. Методы определения срока действия кротовых дрен минеральных почвах освещены Ф.Р. Зайдельмана [3].

Характер разрушения кротовин, как показали раскопки, наблюдается в первую очередь в верхнем своде, ослабленном вследствие прохода нож-стойки. Кротователь новой конструкции позволил нарезать скошенные дрены смещенными относительно нож-стойки. При этом стенки кротовин имели плотное сложение (1,5–1,74 г\см^3), т.к. разрушение и смежные грунта в процессе формирования кротовин происходит к центру проходки. Практически наружные стенки кротовин имели плотность грунта равную монолиту, а внутренние стенки были уплотнены от 1,5 – до 1,6 г\см^3.

Раскопки дрен позволили прийти к выводу, что в почвах с тяжелым механическим составам (50–60% глины), основной приток к дренам происходил через наружные стенки, т.к. коэффициент фильтрации грунта в междренном пространстве был менее чем в монолите. Однако, благодаря наличию двух спаренных кротовин, интенсивность поступления воды в дрены была значительно больше чем в одиночные дрены. Следует отметить, что при данной конструкции АД количество воды, отводимой дренажем по сравнению с притоком воды непосредственно через щель в дрену, уменьшилась (до 0,08–0,27 м\сут.) и практически определялось фильтрационными способностями грунта. Благодаря такой конструкции АД, схема притока воды к дренам значительно изменилась, что позволило снизить градиент напора, а следовательно, и предотвратить суффозионный вынос частиц грунта.

Устойчивость кротовых дрен определялась с помощью лабораторно-полевых методов: лабораторным (Р.Ф. Астапова) [1]; полевым (М.Н. Глотова) [2]; лабораторно-полевым (Ф.Р. Зайдельмана) [3]. Описание способы устройство АД различаются не только характером применения и эффективностью. При соблюдении технологии нарезки АД, а также правил эксплуатации АД, эффективность и продолжительность действия его на тяжелых почвах аридной зоны составила 4 года.

Литература:

1. Астапов, С.В. Устойчивость кротовых дрен при закладке кротового дренажа. – В кн.: Кротовый дренаж. – М.: 1943. – с. 79–97.
2. Глотов, М.Н. Кротовый дренаж и его применение. В. кн.:Кротовый дренаж.– М.:1943.с. 8–7.

3. Зайдельман, Ф.Р. Режим и условия мелиорации заболоченных почв. 2-е изд., перераб. и дополн. – М.: Колос. 1975. 308 с.
4. Панов, И.М., Сучков, И.В., Ветохин, В.И. Вопросы теории взаимодействия рабочих органов глубокорыхлителей с почвой. В. кн.: Исследование и разработка почвообрабатывающих и посевных машин НПОВИСХОМ: М.1988. – с. 30–56.
5. Применение комбинированно-ярусной системы обработки почвы в интенсивном земледелии. НПО «Подмосковье» М. ВО «Агропромиздат» 1988. с. 3–29.

11. ОБЩИЕ ВОПРОСЫ ТЕХНИЧЕСКИХ НАУК

Инновации в организации учебного процесса с учетом формирования профессиональных компетенций

Борисенко Ирина Геннадьевна, ст. преподаватель
Сибирский федеральный университет (г. Красноярск)

Рассматриваются инновации в организации учебного процесса и методическом обеспечении при преподавании начертательной геометрии на основе компетентностного подхода с учетом формирования профессиональных компетенций по государственным стандартам высшего профессионального образования третьего поколения.

Ключевые слова: *профессиональные компетенции, компетентностный подход, высшее профессиональное образование, начертательная геометрия, компьютерные технологии, рабочая тетрадь.*

С 70-х годов прошлого века в США и ряде стран Европы широко используется идея и термин «компетентность». К областям развития компетентности отнесены учеба, работа, забота о здоровье, культура, политика, охрана окружающей среды и.т. д. Симпозиум «Ключевые компетенции для Европы», проведенный Советом Европы в Берне в 1996 году определил идеи интегрированного развития компетентности.

Российское общество сегодня предъявляет все более высокие требования к подготовке специалистов, приближения уровня их профессиональной подготовки к международным требованиям, а это требует совершенствования всей системы высшего образования.

Концепция модернизации российского образования определяет компетентностный подход, как одно из важных концептуальных положений разработки государственных образовательных стандартов высшего профессионального образования третьего поколения с учетом предыдущего опыта и рекомендаций Болонской декларации, принятой в 1999 году. В декларации сформулирован ряд целей, достижение которых, по мнению участников Болонского процесса, позволят создать единое взаимосвязанное Европейское пространство высшего образования [2].

Определение понятия «профессиональная компетентность» в системе образования предложенное Ю.Г. Татур: «Компетентность специалиста – это проявление на практике его стремлений и способности (готовности) реализовать свой потенциал знаний, умения, опыт личные качества и др. для успешной творческой (продуктивной) деятельности в профессиональной и социальной сфере, осознавая социальную значимость и личную ответственность за результат своей деятельности, необходимость ее постоянного совершенствования» [11]. Однако споры по осмыслению определения понятий «компетенции», «профессиональная компетентность» ведутся до сих пор, что обусловлено, прежде всего, особенностями структуры деятельности специалистов различных профессиональных областей. Однако, объединяющей характеристикой данного понятия остается степень сформированности у специалистов единого комплекса знаний, умений и навыков, а также ответственности и ценностного отношения в профессиональной и социальной деятельности [7].

Компетентностный подход является основой разработки профессиональных стандартов нового поколения и требует переориентации всего образовательного процесса «на студентоцентрированный характер» [1].

Основными единицами профессиональных стандартов должны стать две основные группы компетенций – надпрофессиональные (ключевые) и профессиональные, формирование которых будет способствовать усилению фундаментальной подготовки бакалавров и специалистов [1]. Актуальной является проблема развития самообразовательной деятельности студентов, являющейся основой формирования их профессиональных компетенций [7].

В процессе обучения общепрофессиональным дисциплинам, при разработке методического сопровождения используются различные предметно знаковые системы, оказывающие поддержку преподавателю путем создания и реализации соответствующих средств и условий для достижения результата – приобретения компетентностей.

При внедрении новых образовательных стандартов с учетом формирования у обучающихся профессиональных и надпрофессиональных компетентностей методическая деятельность преподавателя направлена на то, чтобы объединить в единый комплекс содержание, методы, формы обучения, основой которого является учебник для повышения эффективности обучения студентов, в первую очередь за счет увеличения интенсивности самостоятельной работы [8].

Постоянно растущий объем предлагаемых студентам знаний при уменьшении часов аудиторных занятий требует оптимизации времени учебного процесса.

Начертательная геометрия, являющаяся «грамматикой языка техники» [10], как писал В. И Курдюмов: «... так как она учит нас правильно читать чужие и излагать наши собственные мысли, пользуясь в качестве слов одними только линиями и точками, как элементами всякого изображения. Кроме этого, изучение ее является лучшим средством развития нашего воображения, а без достаточно развитого воображения немыслимо никакое серьезное техническое творчество, т.е. проектирование» [10], составляет основу инженерного образования, формирующего базовые знания, необходимые для дальнейшего изучения графических и специальных дисциплин. Рассматривая проблему повышения качества при обучении начертательной геометрии, одной из общепрофессиональных инженерных дисциплин, нельзя исключить такие важные составляющие процесса как деятельность и творческое саморазвитие личности [4].

Для реализации задач, которые ставит современное общество пред высшей школой и учитывая изложенные выше проблемы на кафедре начертательной геометрии (НГЧ) Сибирского федерального университета (СФУ) проводится поиск и внедрение новых форм обучения.

Эффективность изучения начертательной геометрии и инженерной графически в значительной степени можно повысить за счет использования новых информационных технологий, наибольшую же эффективность принесет использование трехмерной компьютерной графики и анимации. На кафедре разработаны методические материалы с использованием трехмерной графики. Мультимедийное обеспечение лекций не только дает возможность разнообразить иллюстративный материал, но, благодаря использованию новых технологий, преобразивших традиционную форму обучения, становится более привлекательной, позволяет студентам представить и понять сложный теоретический материал. Лекции проходят более разнообразно, вызывая повышенный интерес аудитории, что формирует повышение познавательной активности студентов. Использование анимации и электронных слайдов способствует повышают у студентов осознание отображения различных пространственных объектах на плоскости, развитию пространственного мышления и повышают уровень усвоения рассматриваемого материала.

Одним из важнейших средств обучения графическим дисциплинам, получивших в последнее время общее признание у преподавателей и обучающихся, является рабочая тетрадь, издаваемая типографским способом. Тетрадь, содержащая графические условия предлагаемых задач, разработана на основе учебного пособия, в котором подробно объясняется методика решения задач с указанием страниц основных понятий как в рабочей тетради [6], так и в учебном пособии (курс лекций) [5]. Таким образом, студенты имеют возможность по ссылке на страницу в тетради быстро посмотреть и вспомнить те понятия, которые уже встречались ранее. Если возникает необходимость более подробно рассмотреть теоретические вопросы, то могут обратиться к учебнику на ту страницу, ссылка на которую указана в пособии. Студенты учатся пользоваться учебной литературой и приобретают навык необходимости использования литературы, как способа расширения круга знаний.

В настоящее время около 80% поступающих в технические вузы, к сожалению, не изучали в школе черчение, плохо знают геометрию, не обладают пространственным представлением, не умеют организовать самостоятельную работу. Поэтому использование рабочей тетради на практических занятиях приобретает особое значение. Оно способствует синхронному решению максимального количества задач на доске и в тетради, так как полностью исключается неточность копирования студентами исходных данных, а также экономится время студента при самостоятельном решении задач дома, даёт возможность преподавателю постоянно контролировать процесс обучения и уровень усвоения материала.

При коллективном решении задач в аудитории создается атмосфера творчества, диалога, происходит общение как между студентами и преподавателем, так и между студентами по заданной тематике, что формирует такие качества как коммуникабельность и сотрудничество, являющиеся надпрофессиональными компетенциями.

Наряду с «традиционными» предлагаются задачи, имеющие несколько вариантов решений, что исключает возможность дублирования решений задач, так как одно и то же графическое решение у нескольких студентов становится практически невозможным. Причем, перед студентами ставится задача не только найти, но и выбрать более рациональный путь её решения. Это ведет к развитию индивидуализации и творческого начала, формирует познавательную активность студентов.

Как показала практика, применение в процессе обучения трехмерной компьютерной графики, анимации, использование рабочей тетради, разработанной в совокупности с учебным пособием, способствует более продуктивному усвоению студентами специальных терминов и понятий, приобретению практических умений и навыков, формированию у обучающихся умений и навыков самоконтроля, развитию пространственного мышления.

В результате повысилась эффективность самостоятельной работы студентов, как при подготовке к практическим занятиям, так и при подготовке к экзаменам, а также их успеваемость, не смотря на слабую первоначальную подготовку.

Разработка современного методического сопровождения, использование новейших технических, компьютерных и других интерактивных средств в преподавании начертательной геометрии, инженерной графики и других инженерных дисциплин, позволяет внедрять активные методы обучения с целью повышения его эффективности, развития познавательной и творческой деятельности об-

учающихся, подготовки их к самостоятельной профессиональной деятельности [9]. Все это, в совокупности, способствует развитию компетентности будущего квалифицированного специалиста и бакалавра отвечающего требованиям интенсивно развивающейся экономики и общества в целом.

Литература:

1. Байденко, В.И. Выявление состава компетенций выпускников вузов, как необходимый этап проектирования ГОС ВПО нового поколения. Метод. пособие., М.: 2006, – 55 с.
2. Болонский процесс и его значение для России. Интеграция высшего образования в Европе /под ред. К. Пурсиайнена и С.А. Медведева. – М.: РЕЦЭП, 2005. – 199 с.
3. Громкова, М.Т. Андрагогика : теория и практика образования взрослых [Текст] : учеб. пособие для системы доп. проф. образования: учеб. пособие для студентов вузов / М.Т. Громкова. – М.: ЮНИТИ – ДАНА, 2005. – 495 с.
4. Грачева, С.В., Виткалов, В.Г. Инновационный подход к проведению практических занятий по начертательной геометрии // Сб: Совершенствование подготовки учащихся и студентов в области графики, конструирования и стандартизации. – Саратов. 2001. – С. 102–104.
5. Дергач В.В. Начертательная геометрия: курс лекций / В.В. Дергач, А.К. Толстихин, И.Г. Борисенко. – Красноярск, Сибирский федеральный ун-т; 2011. – 127 с.
6. Дергач В.В. Начертательная геометрия: рабочая тетрадь / сост: В.В. Дергач, И.Г. Борисенко, А.К. Толстихин. – Кр-ск: ИПЦ СФУ, 2009. – 55 с.
7. Звягинцева, Н.Ю. Компетентный подход в обучении будущего педагога // Научный журнал «Синергетика образования», выпуск 15, Армавир, 2009.
8. Зеер, Э.Ф. Психология профессионального образования [Текст] : учеб. пособие / Э.Ф. Зеер. – М. ; Воронеж, 2003. – 480 с.
9. Зимняя, И.А. Культура, образованность, профессионализм специалиста [Текст] / И.А. Зимняя // Проблемы качества, его нормирования и стандартов в образовании. – М. : Исследовательский центр проблем качества подготовки специалистов, 1998. – С. 156.
10. Курдюмов, В.И. Курс начертательной геометрии «Проекции ортогональные» Издательство Петербургского института инженеров путей сообщения, СПб, 1985
11. Татур, Ю.Г. Компетентностный подход в описании результатов и проектировании стандартов высшего профессионального образования: Материалы ко второму заседанию методологического семинара. Авторская помощь. – М.: Исследовательский центр проблем качества подготовки специалистов, 2004.

Агромелиоративные мероприятия для повышения плодородия почв

Данатаров Агахан, кандидат технических наук, докторант;
Ашыров Сердар Чашемович, ст. преподаватель
Туркменский сельскохозяйственный университет имени С.А. Ниязова

На основе теоретических и экспериментальных исследований разработаны оптимальные параметры аэрационного дренажа и глубокорыхлителя. Обоснована технология нарезки аэрационного дренажа и рыхления подпахотного слоя глубокорыхлителем, которая позволяет улучшить агротехнические показатели работы используемого оборудования при наименьших затратах. Технико-экономические расчёты показали, что нарезка аэрационного дренажа позволяет снизить расходы по эксплуатации техники до 30%, обеспечить оптимальной водно-воздушной режим почв в условиях аридной зоны и повысить урожайность хлопчатника до 10 ц/га.

On the basis of theoretical and experimental researches optimum parameters of drainage aeration and chisel plow are developed. The technology of cutting drainage aeration and loosening of subsurface by means of chisel plow which allows to improve work agrotechnical indicators used equipment at the least expenses is proved. Technical and economic calculations have shown, that cutting drainage aeration allows to reduce expenses on technics operation up to 30%, to provide optimum of soils water-air regime in the conditions of arid zone and raise cotton productivity up to 10 centner\hectares.

Кардинальным направлением развития современных аграрных технологий и техники является снижение затрат на единицу продукции при сохранении экологических показателей. Одним из инструментов анализа и проектирования ресурсосберегающих технологий и почвообрабатывающих орудий может служить система свойств и ха-

рактеристик состояния почвы. Свойства почвы – это своего рода отклик на управляющее воздействие. Одно из средств управления состоянием почвы – почвообрабатывающее орудие [3].

Концентрация свежего органического вещества обособленной прослойкой в нижней части пахотного слоя оказывает огромное окультуривающее действие на этот слой и подпочву: сдерживается минерализация органического вещества и потеря минеральных форм от промывания, усиливается накопление гумуса и улучшается его качественный состав, питательные вещества в глубоких слоях почвы становятся доступными для растений; увеличивается период, в течение которого можно обрабатывать почву; повышаются другие агрохимические показатели плодородия почвы; снижается кислотность, увеличивается сумма поглощенных оснований, содержание подвижного фосфора и обменного калия.

Основное назначение кротового или аэрационного дренажа (АД) – улучшения водно-воздушного, солевого и теплового режимов тяжелых почвогрунтов с целью повышения плодородия и урожайности сельскохозяйственных культур. Технология устройства АД должно призвана для обеспечения эффективности и долговечности его работы. Но до настоящего времени такой дренаж применялся и изучался лишь в зоне осушения в качестве кротового дренажа (КД), т.е. для отвода излишних вод. Принцип, которого дренажа заключается в следующем. Тонкий лемех с имеющимся на его основании специальным устройством, формует при движении лемеха устойчивый туннель. Это достигается за счет использования торпедообразного расширителя. Формирование кротовин происходит в процессе блокированного резания массива грунта. По теории Ю.А. Ветрова [4] процесс разрушения грунта возможно рассматривать как блокированное, полублокированное или свободное резание в зависимости от условий резания.

Сохранение естественной структуры грунта вокруг дрены обеспечивает достаточную водозахватную способность и эксплуатационную надежность. Для удовлетворения изложенных требований нами были разработаны специальные, универсальные рыхлители-кротователи новой конструкции, защищенные авторским свидетельством №1751263 [1].

Технология нарезки АД разработана с учетом грунтовых условий и биологических требований к развитию корневой системы хлопчатника, которая основана на разрыхления подпахотных слоев и нарезке в монолите грунта перпендикулярно основному дренажу водоаккумулирующих кротовых спаренных дрен на глубину 600 мм и на расстояния 900 мм. Оценку прочности грунта проводили протативными прибором, основные конструктивные данные которого приведены в работе Ю.А. Ветрова [4]. В работе применялись разные методы лабораторных и полевых исследований.

Скорость перемещения рабочего органа принимались в пределах 0,25 м/с. Устойчивость кротовых дрен определялась с помощью лабораторно-полевых методов: лабораторным (Р.Ф. Астапова) [2]; полевым (М.Н. Глотова) [5]; лабораторно-полевым (Ф.Р. Зайдельмана) [7]. При соблюдении технологии нарезки АД, эффективность и продолжительность действия его на тяжелых почвах аридной зоны составила 4 года.

Установлено, что при нарезка АД в аридной зоне позволяет улучшить водно-воздушный режим почвы за счет перераспределения влаги нижележащие подпахотные горизонты и ее аккумуляции в грунтовом массиве 0–60 см по глубине. В результате проведения кротования-рыхления почвы, рыхление почвы происходит на всю глубину V-образной формы, ширина которой по верху составляет 65–70 см. При этом средняя комковатость почвы составляет 30–60 мм. Кротование дрены сформованы в монолите грунта с плотностью скелета 1,5–1,7 г/см^3, влажность 8–12%.

Следовательно, для нарезки АД и рыхления подпахотного уплотненного слоя теоретически и экспериментально исследованы и разработаны оптимальные параметры АД и глубокорыхлителя (НАД-2–60), на ней также можно установить приспособление для внесения органоминеральных жидких удобрений. Обоснована технология нарезки АД и рыхления подпахотного слоя глубокорыхлителем; которая позволяет улучшить агротехнические показатели работы орудий при наименьших затратах [6]. Технико-экономические расчеты показали, что нарезка АД позволяет снизить эксплуатационные расходы до 30%, обеспечить оптимальной водно-воздушной режим почвы в аридной зоне и повышает урожайность хлопчатника до 10 ц\га.

Литература:

1. А.с. 1751263 /СССР/. Устройство для нарезки кротовин /Хоммадов К., Данатаров А. – Москва. 1992. Бюл.№28.
2. Астапов С.В. Устойчивость кротовых дрен при закладке кротового дренажа. – В кн.: Кротовый дренаж. – М.: 1943. – с. 79–97.
3. Ветохин, И.В. Систематизация свойств и характеристик состояния почвы как элемент теории проектирования почвообрабатывающих орудий и технологий почвы Техніко-технологічні аспекти розвитку та випробування нової техніки і технологій для сільського господарства України Збірникнаукових праць Випуск 13 (27) Книга 2 Дослідницьке 2009 с. 30–38.
4. Ветров Ю.А. Резание грунтов землеройными машинами. – М.: Машиностроение. 1971. – 360 с.
5. Глотов М.Н. Кротовый дренаж и его применение. В кн.: Кротовый дренаж. – М.: 1943. – с. 8–71.

6. Данатаров, А. Аэрационный дренаж в условиях аридной зоны Международный научно-практический журнал №6. Проблемы освоения пустынь. Ашхабад.1998. с. 91–95.
7. Зайдельман Ф.Р. Режим и условия мелиорации заболоченных почв. 2-е изд., перераб. и дополн. – М.: Колос. 1975. 308 с.

Аналог проблемы Гольдбаха-Эйлера для группы z_m

Оразов Мамед, кандидат физико-математических наук, докторант
Туркменский сельскохозяйственный университет имени С.А. Ниязова (г. Ашхабад)

В данной работе рассматривается задача, аналогичная проблеме Гольдбаха–Эйлера для группы классов вычетов по модулю m, принадлежащих некоторым заданным подмножествам группы z_m (z_m – группа, образованная множеством приведенных классов вычетов по заданному модулю m). Исходя из того, что все простые числа за исключением простых делителей m, находятся в примитивных классах вычетов по модулю m, то вопрос о представлении классов вычетов по модулю m в виде суммы двух примитивных классов вычетов можно рассматривать как аналог бинарной проблемы Гольдбаха для группы z_m. Получена точная формула для числа представлений натурального числа n в виде суммы двух примитивных классов по модулю m.

In the given work the problem similar to problem Гольдбаха–Эйлера for group of classes of deductions on module m, belonging to some set subsets of group z_m (z_m – the group formed by set of resulted classes of deductions on set module m) is considered. Recognising that all simple numbers except for simple dividers m, are in primitive classes of deductions on module m the question on representation of classes of deductions on module m in the form of the sum of two primitive classes of deductions can be considered as analogue of binary problem Гольдбаха for group z_m. The exact formula for number of representations of natural number n in the form of the sum of two primitive classes on module m is received.

Здесь мы рассмотрим аналогичную задачу проблемы Гольдбаха–Эйлера для группы классов вычетов по модулю m. А именно задачу о представлении класса вычетов по модулю m в виде суммы нескольких классов вычетов по модулю m принадлежащих некоторым заданным подмножествам группы z_m.

Гольдбах (1742 г.) высказал предположение (бинарная проблема Гольдбаха), что любое число ≥ 4 можно представить в виде суммы двух простых чисел.

В курсе теории чисел доказывается, что множество приведенных классов вычетов представляет собой группу, то есть для множества приведенных классов вычетов по любому модулю m выполняются все условия группы. Эта группа является коммутативной и конечной группой.

Так как все простые числа за исключением простых делителей m находятся в примитивных классах по модулю m, причем имеются в каждом классе вычетов по модулю m, то вопрос о представлении классов вычетов по модулю m в виде суммы двух примитивных классов вычетов можно рассматривать как аналог проблемы Гольдбаха–Эйлера для группы z_m.

В отличие от классической проблемы Гольдбаха–Эйлера этот ее аналог для группы z_m решается полностью.

Пусть n – целое число. Обозначим через $r(n) = r_m(n)$ число представления натурального n в виде суммы двух примитивных вычетов по модулю m, то есть число решений сравнения

$$x + y \equiv n(mod\ m)$$

в примитивных вычетах x и y.

Имеем:

$$r(n) = \sum_{\substack{x,y\ mod\ m \\ x+y\equiv n(mod\ m) \\ (x,m)=(y,m)=1}} 1 = \sum_{\substack{x=1 \\ (x,m)=1}}^{m} \sum_{\substack{y=1 \\ (y,m)=1 \\ y\equiv n-x(mod\ m)}}^{m} 1 = \sum_{\substack{x=1 \\ (x,m)=(n-x,m)=1}}^{m} 1 = \sum_{\substack{x=1 \\ (x(n-x)\,m)=1}}^{m} 1 =$$

$$= \sum_{x=1}^{m} \sum_{d\,(x(n-x)\,m} \mu(d) = \sum_{d/m} \mu(d) \sum_{\substack{x=1 \\ x(n-x)\equiv o(d)}}^{m} 1 = \sum_{d/m} \mu(d) \frac{m}{d} \omega(d,n),$$

где $\omega(d,n)$ – число решений сравнения $x(n-x) \equiv o(\mathrm{mod}\, d)$; $\mu(d)$ – функция Мёбиуса определяется равенством

$$\mu(d)=\begin{cases}1, \text{если } d=1\\ (-1)^t, \text{если } d=p_1,p_2\dots p_t\end{cases}$$

$p_1, p_2, \dots, p_t$ – различные простые числа.

В силу мультипликативности функции $\omega(d,n)$ по первому аргументу, отсюда следует

$$r(n)=m\prod_{P/d}\left(1-\frac{\omega(p,n)}{p}\right).$$

Из определения функции $\omega(d,n)$ следует, что

$$\omega(p,n)=\begin{cases}2, & \text{если } p\nmid n\\ 1, & \text{если } p/n\end{cases}$$

Поэтому

$$r(n)=k\prod_{p\setminus(k,n)}\left(1-\frac{1}{p}\right)\cdot\prod_{\substack{p/k\\ p\neq n}}\left(1-\frac{2}{p}\right)=\;=k\prod_{p/k}\left(1-\frac{1}{p}\right)\cdot\prod_{\substack{p/k\\ p\neq n}}\left(1-\frac{2}{p}\right)\left(1-\frac{1}{p}\right)^{-1}=\varphi(k)\prod_{\substack{p/k\\ p\neq n}}\frac{p-2}{p-1}.$$

Таким образом, мы получили точную формулу для числа представлений натурального числа n в виде суммы двух примитивных классов вычетов по модулю m.

Литература:

1. Маршал Холл. Теория групп.-М.: Иностранная литература, 1962.
2. Бухштаб А.А. Теория чисел.- М.: Просвещение, 1966.
3. Гельфонд А.О., Линник Ю.В. Элементарные методы в аналитической теории чисел.- М., 1962.

О нулях преобразований Лапласа некоторых неубывающих функций

Оразов Мамед, кандидат физико-математических наук, докторант
Туркменский сельскохозяйственный университет имени С.А. Ниязова (г. Ашхабад)

В работе доказывается, что если полуплоскости сходимости преобразование Лапласа некоторой неубывающей функции близко к экспоненте преобразования Лапласа другой неубывающей функции и допускает аналитическое предложение в некоторую вертикальную полосу левее абсциссы сходимости, то оно не обращается в нуль в области, подобной области Валле-Пуссена, свободной от нулей дзета-функции.

In the work it is proved that if in a half plane of convergence the transformation of Laplasa of some nondecreasing function is close to an exponent of transformation of Laplasa of other nondecreasing function and supposes analytical continuation in some vertical strip more to the left of a convergence abscis thus it does not turn tto zero in the area similar to area of Valle-Pussen free from zeta-function zero.

Классическая постановка задачи о распределении простых чисел в натуральном ряду состоит в исследовании асимптотического поведения функции $\pi(x)$ означающий число простых чисел, не превосходящих x

Известные в настоящее время асимптотические формулы для $\pi(x)$ имеют вид

$$\pi(x) = li\ x + R(x), \text{ где } li\ \text{x} = \int_2^x \frac{du}{\ln u}$$

интегральный логарифм, а $R(x)$ – остаточный член, оценка которого связана с распределением нулей дзета функции Римана $\varsigma(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$.

Введем обозначение

$$L_f(s) = \int_0^{\infty} e^{-su} f(u) du$$

преобразование Лапласа функции $f(u)$ определенной для всех неотрицательных u и интегрируемой на каждом конечном отрезке $[0, u]$, $u \in U$.

Тогда из тождества Эйлера следует:

$$sL_g(s) = \Phi(s) \exp sL_f(s) \tag{1}$$

при $f(x) = \pi(e^x)$, $g(x) = [e^x]$.

Таким образом, задача о распределении простых чисел является частным случаем следующей общей задачи: заданы две функции вещественного аргумента $f(x)$ и $g(x)$, преобразования Лапласа которых связаны соотношением (1), причем функция $\Phi(s)$ устроена достаточно хорошо. Считая асимптотику функции $g(x)$ известной, найти асимптотику функции $f(x)$.

В дальнейшем мы будем считать что при

$$x \to +\infty, g(x) = ce^x + \mathrm{O}\left(e^{\alpha x}\right), \tag{2}$$

где $0 < \alpha < 1$, c – положительная константа.

Отсюда следует, что преобразование Лапласа $L_g(s) = \int_0^{\infty} e^{-su} g(u) du$

абсолютно сходится в полуплоскости $\mathrm{Re}s > 1$.

Пусть $s = \delta + it, \delta = \mathrm{Re}\, s, \quad t = \mathrm{Im}\, s.$ и в условиях (1) и (2) $f(x)$ неубывающая функция, и $\Phi(1 + t) \neq 0$ для $t \in R$. Тогда функция $L_g(s)$ не обращается в нуль на прямой $\sigma = 1$.

Теорема 1. Пусть $f(x)$ и $g(x)$ – функции определенные при $x \geq 0$, причем $f(x)$ – неубывающая функция,

$sL_g(s) = \Phi(s) \exp sL_f(s),$

где функция $\Phi(s)$ – такова, что $1/\Phi(s)$ ограничена в полуплоскости

$\sigma > a, \quad 0 < a < 1)$. Тогда, если $g(x) = Ce^x + \mathrm{O}\left(e^{ax}\right),$

то функция $F(s) = \exp sL_f(s)$ не обращается в нуль в области

$$\sigma \geq 1 - \frac{c}{\ln|t|}, \quad |\mathrm{t}| > 3,$$

где c – положительная константа, зависящая только от a.

Литература:

1. Landau E. Über den verlauf der zahlentheorethen Funktion. Arch. Math. und Phys. 5 (1903), 86-91.
2. Ингам А.Е. Распределение простых чисел.- ОНТИ, 1936.
3. Тичмарч Е. Теория дзета функции Римана, ИЛ, 1953.

Условия нулевой плотности множеств натуральных чисел в арифметических прогрессиях, представимых в виде $p+a^m$

Оразов Мамед, кандидат физико-математических наук, докторант
Туркменский сельскохозяйственный университет имени С.А. Ниязова (г. Ашхабад)

Рассматривается задача о представлении натуральных чисел, при надлежащих заданному классу вычетов по некоторому модулю и представимых в виде суммы $u+v$, *где* u,v – *члены двух заданных последовательностей натуральных чисел. В 1934 году Н.П.Романов доказал теорему о положительной плотности множеств натуральных чисел представимых в виде* $p+a^m$ *где* p – *пробегает простые числа,* m – *натуральные число. В данной работе рассматривается анолагичная задача на случай, когда представимые числа принадлежат арифметической прогрессии по заданному модулю* k. *Кроме того полечены достаточные условия для того, чтобы числа некоторых арифметической прогрессии представимые виде* $p+a^m$, *имели нулевую асимптотическую плотность.*

The problem about representation of natural numbers is considered at ought to the set class of deductions on some module and representable in a kind u+v where u and v members of two set sequences of natural mumbers. In 1934 N.P.Romanow has proved the theorem of positive density of sets of natural numbers representable in a kind $p+a^m$ *where r-runs simple numbers, m-natural numbers, and* $\geqslant 2$ *the set integer. In the given work the similar problem on a case when representable numbers belong to an arithmetic progression on the set module to is considered. Besides sufficiens are treated that numbers of some arithmetic progressions representable in a kind* $p+a^m$ *had zero asymptotic density.*

Пусть $N_a(x,k,l)$ – число натуральных чисел $n \equiv l(\mathrm{mod}\, k)$ представимых в форме $p+a^m$ и не превосходящих x,

$$c(k,l,a) = \sum_{d \in M_k} \frac{\mu(d)}{\delta(d)},$$

где $\delta(d) = \delta_a(d)$ – показатель числа a по модулю d,

$$M_k = \bigcup_{m=1}^{\delta(k)} \{d/(a^m - l,k)\},$$

c (k,l,a) – плотность множеств натуральных чисел в арифметических прогрессиях, представимых в виде $p+a^m$.

После несложных рассуждений получаем

$$N_a(x,k,l) \;<<\; c(k,l,a)\cdot x + \mathrm{O}(\ln x)$$

В связи с этим представляет интерес исследование вопроса о положительности суммы

$$c_1(k,l,a) = \sum_{\substack{m=1 \\ (a^m - l,k)=1}}^{\delta(k)} 1 = \delta(k)\, c(k,l,a)$$

Введём функцию $\omega(d) = \sum_{\substack{x=1 \\ x(x-l)\equiv o(d)}}^{d} 1$ (число решений сравнения $x(x-l) \equiv o(\mathrm{mod}\, d)$) как известно, мультипликативна при $d = p$ (p – простое число) имеем:

$$\omega(p) = \begin{cases} 2, & \text{если } p \nmid l, \\ 1, & \text{если } p / l \end{cases}$$

Поэтому

$$c_1(k,l,a) = k \prod_{p/k}\left(1 - \frac{\omega(p)}{p}\right) = k \prod_{p/(k,l)}\left(1 - \frac{1}{p}\right)\cdot\prod_{\substack{p/k \\ p\nmid l}}\left(1 - \frac{2}{p}\right) = k\frac{\varphi(k,l)}{(k,l)} \prod_{\substack{p/k \\ p\nmid l}}\left(1 - \frac{2}{p}\right).$$

Отсюда видно, что если k четно / поскольку мы предполагаем существование первообразного корня по модулю k, это означает, что $k = 2q^{\alpha}$, где q – нечетное простое число, $\alpha \geq 1$ – целое /, а l – нечетно, то $c_1(k,l,a) = 0.$ Таким образом справедлива.

Теорема. Если $k = 2q^{\alpha}$, где q – нечетное простое число, $\alpha \geq 1$ – целое, то во всех классах вычетов, порожденных нечетными числами, множество чисел вида $p + a^m$, где a – первообразный корень по $\mathrm{mod}\, k$ имеет нулевую асимптотическую плотность; во всех остальных классах вычетов по $\mathrm{mod}\, k$ плотность чисел вида $p + a^m$ положительно.

Литература:

1. Romanov N.P. Uber einige Sartze der additiven Zahlentheorie, Math. Ann.109 (1934).668–678.
2. Selberg S. A generalization of a theorem of Romanoff, Kong. Norse vid.Selsc. For handl. 35, 17 (1962), c. 91–95
3. Файнлейб А.С., Оразов М. Бинарные аддитивные задачи с показательной функцией. Литовский математический сборник. 1978.№4. с. 187–198.

Теорема Карамата и её применение в аддитивных задачах

Оразов Мамед, кандидат физико-математических наук, докторант
Туркменский сельскохозяйственный университет имени С.А. Ниязова (г. Ашхабад)

Пусть U и V две последовательности натуральных чисел, $\mathbf{N_U(x)}$ *и* $\mathbf{N_V(x)}$ *их подсчитывающие функции. Введем обозначение*

$$M_U(x) = \max_{1 \leq a \leq x} \sum_{\substack{a \leq u \leq x \\ u-a \in U}} 1$$

Доказывается, что при наличии достаточно хорошей оценки $M_U(x)$ *асимптотическая плотность суммы последовательностей U и V определяется асимптотикой свертки.*

$$\int_0^x N_U(x-y)\,dN_V(y).$$

Let the U and V are two sequences of natural numbers, where $N_U(x)$ *and* $N_V(x)$ *are their calculating functions. Let us introduce the notation*

$$M_U(x) = \max_{1 \leq a \leq x} \sum_{\substack{a \leq u \leq x \\ u-a \in U}} 1$$

It is proved that while presence of sufficient positive estimate $M_U(x)$ *the asymptotic density of the sum of sequences of U and V is defined by asymptotic compression*

$$\int_0^x N_U(x-y)\,dN_V(y).$$

Теорема. (Карамата[2]). Пусть $f(t)$ – неубывающая функция, определенная для всех $t \geq 0, f(0) = 0,$ $L_f(s) = \int_0^{\infty} e^{-su}\,df(u)$, причем интеграл сходится при $s > 0$. Тогда, если по крайней мере одна из функций $f(t)$ или $L_f\left(\frac{1}{t}\right)$ – правильно меняющаяся функция порядка α (в смысле Карамата), то при $\mathbf{t \to \infty}$

$$f(t) \sim \frac{1}{\Gamma(\alpha+1)} L_f\left(\frac{1}{t}\right).$$

Лемма 1. Пусть $\boldsymbol{f(t)}$ *и* $\boldsymbol{g(t)}$ – неубывающие правильно меняющиеся функции порядков соответственно α и β. Тогда при $\mathbf{t \to \infty}$

$$\int_0^t f(t-u)dg(u) \sim \frac{\Gamma(\alpha+1)\Gamma(\beta+1)}{\Gamma(\alpha+\beta+1)} f(t)g(t).$$

Доказательство. Положим $h(t) = \int_0^t f(t-u)dg(u)$; функция h(t) неубывающая, так как $h(t) = \iint\limits_{\substack{u+\vartheta \le t \\ u,\vartheta>0}} df(u)dg(\vartheta)$ и $L_h(s) = L_f(s)L_g(s)$.

Согласно теореме Карамата [2], при $t \to \infty$

$$L_h\left(\frac{1}{t}\right) = L_f\left(\frac{1}{t}\right)L_g\left(\frac{1}{t}\right) \sim \Gamma(\alpha+1)\Gamma(\beta+1)f(t)g(t),$$

откуда следует, что $L_h\left(\frac{1}{t}\right)$ – правильно меняющаяся функция порядка $\alpha+\beta$. Вторично применяя теорему Карамата [2], получаем

$$h(t) \sim \frac{1}{\Gamma(\alpha+\beta+1)} L_h\left(\frac{1}{t}\right) \sim \frac{\Gamma(\alpha+1)\Gamma(\beta+1)}{\Gamma(\alpha+\beta+1)} f(t)g(t).$$

Пусть $\boldsymbol{U}$ и $\boldsymbol{V}$ две возрастающие последовательности натуральных чисел, $N_U(x)$ и $N_V(x)$ – их подсчитывающие функции. Введем обозначение

$$M_U(x) = \max_{1 \le a \le x} \sum_{\substack{a \le u \le x \\ u,u-a \in U}} 1.$$

Теорема 1. Имеют место соотношения:

$$N(n \le x, n = u+\vartheta) = \int_0^x N_U(x-y)dN_V(y) - \theta M_U(x)N_V^2(x); \quad (1)$$

$$N(n \le x, n = u+\vartheta) = \int_0^x N_U(x-y)dN_V(y) - \theta_1 M_U(x)N_V^2(x), \quad (2)$$

где $0 \le \theta \le \theta_1 \le 1$.

Доказательство. Применим неравенство Романова-Эрдеша к множеству целых точек (u,ϑ), где $u \in U,\ \vartheta \in V,\ u+\vartheta \le x$. Тогда

$$P = \sum_{\substack{u+\vartheta \le x \\ u \in U, \vartheta \in V}} 1 = \sum_{\substack{\vartheta \le x \\ \vartheta \in V}} \sum_{\substack{u \le x-\vartheta \\ u \in U}} 1 = \sum_{\substack{\vartheta \le x \\ \vartheta \in V}} N_U(x-\vartheta) = \int_0^x N_U(x-y)dN_V(y) \quad (3)$$

и

$$R = \sum_{\substack{u,u' \in U \\ \vartheta,\vartheta' \in V \\ u+\vartheta = u'+\vartheta' \le x \\ u' \le u, \vartheta \le \vartheta'}} 1 \le \sum_{\substack{\vartheta < \vartheta' \le x \\ \vartheta,\vartheta' \in V}} \sum_{\substack{u-u' = \vartheta'-\vartheta \\ u,u' \in U \\ u' < u \le x}} 1 == M_U(x) \sum_{\substack{\vartheta < \vartheta' \le x \\ \vartheta,\vartheta' \in V}} 1 = \frac{1}{2} M_U(x)N_V^2(x). \quad (4)$$

Так как $P - 2R \le N_1 \le N \le P$, то отсюда следует

$$N = P - 2\theta R, \quad N_1 = P - 2\theta_1 R, \quad 0 \le \theta \le \theta_1 \le 1.$$

Заменяя P, R полученными для них выражениями, получаем формулы (1), (2).

Теорема 1. показывает, что при наличии достаточно хорошей оценки $M_U(x)$ асимптотическая плотность суммы последовательностей $\boldsymbol{U}$ и $\boldsymbol{V}$ определяется асимптотикой свертки $\int_0^x N_U(x-y)dN_V(y)$.

Большинство последовательностей, рассматриваемых в аддитивной теории чисел, обладает правильно меняющимися подсчитывающими функциями. В этой ситуации из теоремы 1. следует

Теорема.2. Если $N_U(x)$ и $N_V(x)$ – правильно меняющиеся функции порядков соответственно α и β, причем

$$N_V(x) = 0\left(\frac{N_U(x)}{M_U(x)}\right), \quad (5)$$

то при $x \to \infty$

$$\left.\begin{aligned} N(n \le x, n = u+\vartheta) \\ N_1(n \le x, n = u+\vartheta) \end{aligned}\right\} \sim \frac{\Gamma(\alpha+1)\Gamma(\beta+1)}{\Gamma(\alpha+\beta+1)} N_U(x)N_V(x). \quad (6)$$

Доказательство. По лемме 1. в условиях теоремы 2.

$$\int_0^x N_U(x-y)dN_V(y) \sim \frac{\Gamma(\alpha+1)\Gamma(\beta+1)}{\Gamma(\alpha+\beta+1)} N_U(x)N_V(x). \quad (7)$$

Из условия (5) вытекает

$$M_U(x)N_V^2(x) = o\big(N_U(x)N_V(x)\big). \quad (8)$$

Подставляя (7) и (8) в (1) и (2), получаем утверждение теоремы.

Таким образом, если $M_U(x) = o\big(N_U(x)\big)$, то справедливость асимптотической формулы (6) обеспечивается уже просто редкостью последовательности $\boldsymbol{V}$. Арифметическая природа членов этой последовательности не играет никакой роли.

Литература:

1. Шнирельман Л.Г. Об аддитивных свойствах чисел.- Изв. Донского политехнического института,1 ч, 1930, 3-28.
2. Karamata J. Journal für die reine und angewandt the Mathem. 104 (1931), 27-40
3. Барбан М.Б. Метод «большего решета» и его применения в теории чисел.- УМН, 21, 1 (1966), 51-102
4. Левин Б.В., Файнлейб А.С. Применение некоторых интегральных уравнений к вопросам теории чисел.- УМН 22, №3 (35), 1967, 119-128.

Аналоги неравенств Романова-Шнирельмана и Романова Ердоша для аддитивной группы

Оразов Мамед, кандидат физико-математических наук, докторант
Туркменский сельскохозяйственный университет имени С.А. Ниязова (г. Ашхабад)

В работе рассматривается задача об оценке снизу плотности представимых чисел в бинарной аддитивной задаче о сложении последовательностей натуральных чисел U и V в случае, когда U и V подмножества аддитивной абелевой группы G. Показано, что наряду с тождеством Романова для группы G справедливы также аналоги неравенств Романова-Шнирельмана и Романова-Эрдеша.

The work considers the issue of lower-bound estimate of density of represented numbers in a binary additive task on addition of sequences of natural number U and V in case where U and V are a subset of additive Abelian group G. It has been shown that along with Romanoff identical equation for group G analogues of Romanoff-Shnirelmann and Romanoff-Erdos inequalities are also correct.

В1934 году Н.П.Романов [1] заметил, что оценки снизу плотности представимых чисел в бинарной аддитивной задаче о сложении последовательностей U и V можно свести к верхней оценки выражения

$$R = \sum_{\substack{u-u'=\vartheta'-\vartheta>0 \\ (u,\vartheta)\,(u',\vartheta')\in W}} 1$$

Основой для такого сведения является тождество

$$\sum_n r^2(n) = P + 2R \text{ (тождество Романова)}, \quad (1)$$

где $r(n) = \sum_{\substack{u+v=n \\ u\in U, v\in V}} 1$, $P = \sum_{\substack{u+v\le x \\ u\in U, v\in V}} 1$

При таких обозначениях величин R и P из (1) с помощью неравенства Коши-Буняковского получаем неравенства $N \ge \frac{P^2}{P+2R}$, (неравенства Романова-Шнирельмана) и $N_1 \ge P - 2R$ (неравенства Романова-Ердоша)

(здесь N-число целых чисел промежутка $[1,x]$, представимых в виде $\boldsymbol{u+v}$, $\mathbf{N_1}$ – число целых чисел промежутка $[1, x]$, однозначно представимых в виде $\boldsymbol{u+v}$,Отметим прежде всего, что тождество Романова можно обобщить на любую адди-

тивную группу. Пусть G – аддитивная абелева группа, U и V – какие-либо подмножества группы G, W – некоторое конечное множество пар (u, v), где $u \in U, v \in V$. Для каждого $g \in G$ обозначим через $r(g)$ – число представлений элемента G в виде суммы $u + v$, где $(u, v) \in W$.

Тогда $$\sum_{g \in G} r^2(g) = \sum_{g \in G} \sum_{\substack{u+v=u'+v'=g \\ (u,v),(u',v') \in W}} 1 = \sum_{g \in G} r(g) + \sum_{\substack{u-u'=v'-v \neq 0 \\ (u,v),(u',v') \in W}} 1 = P + R,$$

где $P = \sum_{g \in G} r(g)$ – число пар множества W, $R = \sum_{\substack{u-u'=v'-v \neq 0 \\ (u,v),(u',v') \in W}} 1$.

Заметим для дальнейшего, что наряду с тождеством Романова для аддитивной группы G справедливы также аналоги неравенств Романова-Шнирельмана и Романова-Эрдеша. Действительно, в силу неравенств Коши

$$\left(\sum_{g \in G} r(g) \right)^2 \leq \sum_{\substack{g \in G \\ r(g) > 0}} 1 \cdot \sum_{g \in G} r^2(g)$$

Отсюда и из тождества Романова следует

$$\sum_{\substack{g \in G \\ r(g) > 0}} 1 \geq \frac{\left(\sum_{g \in G} r(g) \right)^2}{\sum_{g \in G} r^2(g)} = \frac{P^2}{P + R}$$

(аналог неравенства Романова-Шнирельмана). Далее,

$$\sum_{\substack{g \in G \\ r(g)=1}} 1 \geq \sum_{g \in G} r(g)\big(2 - r(g)\big) = P - R$$

(аналог неравенства Романова-Эрдеша). В интересующем нас случае для величины P и R получаем следующие оценки:

$$P = \varphi(k)\delta(k),$$

$$\text{и } R = \sum_{\substack{m,m'=1 \\ m \neq m'}}^{\delta(k)} \varphi(k) \prod_{p \nmid (a^{m'} - a^m)} \frac{p-2}{p-1}$$

Литература:

1. Romanow N.P. Über limge satze der additiven Zahlentheorie, Math. Ann., 109 (1934), 669-678.
2. Шнирельман Л.Г. Об аддитивных свойствах чисел.- Изв. Донского политехнического института,1 ч, 1930, 3-28.
3. Erdöş P. On additive properties of aquares of primes, Konikl Nederland Aad. Amst., 41.1 (1938), 37-41.

Оценки снизу для числа представлений в задачах аддитивной теории чисел

Оразов Мамед, кандидат физико-математических наук, докторант
Туркменский сельскохозяйственный университет имени С.А. Ниязова (г. Ашхабад)

В работе рассматривается задача о представлений натурального числа в виде суммы членов двух заданных последовательностей U и V, одно из которых является достаточно редкой. В широком классе задач число представлений натурального числа в виде суммы $u + v$, ($u \in U, v \in V$.) принимает лишь значение 0 и 1. Несмотря на это, в данной работе доказано, что число представлений не является ограниченным во многих из таких задач.

In the work the following problem is considered about notation of the natural number in the form of the sum of the members of two preset sequences u and v, one of them is quite rare. In the wide class of problems the represent able number of the natural number in the form of the sum of u+ v, ($u \in U, v \in V$.) takes only the value of 0 and 1. In addition in the present work it is proved that the represent able number is not a limited one in the many problems like that.

Число представлений натурального числа в виде суммы членов двух последовательностей, одна из которых является достаточно редкой, для большинства натуральных чисел в широком классе задач принимает лишь значение 0 и 1. Несмотря на это, как будет показано в данной работе, число представлений не является ограниченным во многих из таких задач. Мы получили здесь Ω – теоремы для числа представлений, дающие нижние оценки максимального порядка роста этого числа.

Лемма 1. Пусть U и T – произвольные последовательности натуральных чисел, $V = a^T$, где $a \geq 2$ – заданное целое число, $1 \leq D \leq x$, D – целое число, взаимно простое с a,

$$r(n) = \sum_{u+\vartheta=n} 1.$$

Тогда имеет место неравенство: $\max\limits_{n\leq x} r(n) \geq \dfrac{D}{x} N_V\left(\dfrac{x}{2}\right) \min\limits_{(l,D)=1} \sum\limits_{u\leq\frac{x}{2}, u\equiv l(D)} 1$
$u\in U$

Доказательство. Имеем $\sum\limits_{\substack{n\leq x \\ n=O(D)}} r(n) \leq \max\limits_{n\leq x} r(n) \sum\limits_{\substack{n\leq x \\ n=O(D)}} 1 \leq \dfrac{x}{D} \max\limits_{n\leq x} r(n)$ (1)

С другой стороны,

$$\sum_{\substack{n\leq x \\ n=0(D)}} r(n) = \sum_{\substack{u+\vartheta\leq x \\ u+\vartheta\equiv 0(D)}} 1 \geq \sum_{\vartheta\leq\frac{x}{2}} \sum_{\substack{u\leq\frac{x}{2} \\ u\equiv -\vartheta(D)}} 1 \geq N_V\left(\frac{x}{2}\right) \min_{(l,D)=1} \sum_{\substack{u\leq\frac{x}{2} \\ u\equiv l(D)}} 1, \quad (2)$$

так как $(\vartheta, D) = 1$ при $\vartheta \in V$. Сопоставляя (1) и (2.), получаем утверждение леммы.

Теорема 1. Пусть $a \geq 2$ – целое число, T – произвольная возрастающая последовательность натуральных чисел, $m \geq 1$. Тогда при $x \geq \max\left(a^{t_1+1}, u_1 + a^{t_2}\right)$ справедливо неравенство:

$$\max_{n\leq x} \sum_{\substack{u+a^t=n \\ \omega(u)=m \\ t\in T}} 1 > c(m) \frac{(\ln\ln x)^m}{\ln x} N_T\left(\frac{\ln x}{\ln a}\right) \frac{\varphi(a)}{a}.$$

Приведём несколько следствия теоремы

Следствие 1. Если $N_T(x) = \psi(x) \cdot \dfrac{x}{(\ln x)^m}$, $\psi(x) \to \infty$, $\psi(x) \to \infty$, то число решений уравнения $u + a^t = n$ $(\omega(n) = m, t \in T)$ не ограничено по $\mathbf{n}$.

Следствие 2.

$$\sum_{\substack{pq+a^r=n \\ p,q,r-\text{простые}}} 1 = \Omega(\ln\ln n).$$

Действительно, положим в теореме 1. $m = 2$ и возьмем в качестве T последовательность простых чисел. Тогда согласно теореме 1

$$\max_{n\leq x} \sum_{\substack{hq+a^r=n \\ p,q,r-\text{простые}}} 1 > c(a) \ln\ln x. \quad (3)$$

Следствие 3.

$$\sum_{\substack{pq+a^{q^r}=n \\ p,q,r-\text{простые}}} 1 = \Omega(\ln\ln\ln n)\cdot$$

Действительно, полагая в теореме 1. $m=1$ и беря в качестве T последовательность чисел имеющих ровно два простых делителя с учетом кратности, получаем

$$\max_{n\le x} \sum_{\substack{pq+a^{q^r}=n \\ p,q,r-\text{простые}}} 1 > c(a)\frac{\ln\ln x}{\ln x}\cdot\frac{\ln x\cdot\ln\ln\ln x}{\ln\ln x} = c(a)\ln\ln\ln x.$$

Отсюда, так же, как и выше, следует наше утверждение.

Литература:

1. Romanow N.P. Über limge satze der additiven Zahlentheorie, Math. Ann., 109 (1934), 669-678.
2. Selberg S.Note on the distribution of the interes $ax^2+by^2+c^{z^2}, A>ch$. Math. Naturwid., 50, 2 (1949), 65-69.

О некоторых задачах теории мультипликативных функций

Оразов Мамед, кандидат физико-математических наук, докторант
Туркменский сельскохозяйственный университет имени С.А. Ниязова (г. Ашхабад)

Работа посвящена задачам, где изучается асимптотическое поведение суммы значений мультипликативных функций. Устанавливается связь между такими суммами по простым числам и натуральным числам. Результаты, полученные в работе, основаны на исследовании аналитических свойств указанных сумм и имеют приложения в теории свободных нормированных полугрупп.

Work is devoted problems where it is studied асимптотическое behavior of the sum of values of multiplicative functions. Connection between such sums on simple numbers and natural numbers is established. The results received in work, are based on research of analytical properties of the specified sums and have appendices in the theory free normative semi groups.

Пусть $\gamma(n)$ и $\beta(n)$ – неотрицательные мультипликативные функции. Определим функции $f(x)$ и $g(x)$ следующим образом:

$$f(x)=\sum_{\gamma(p)\le x}\beta(p), \quad g(x)=\sum_{\gamma(n)\le x}\beta(n)$$

(p – простые числа, n – натуральные числа). Введем обозначения:

$$M_f(s)=s\int_1^\infty \frac{f(x)}{x^{s+1}}dx \qquad M_g(s)=s\int_1^\infty \frac{g(x)}{x^{s+1}}dx$$

Учитывая определения функции $f(x)$ и $g(x)$, имеем

$$M_f(s)=s\int_1^\infty \frac{f(x)}{x^{s+1}}dx=\int_1^\infty x^{-s}df(x)=\sum_{\gamma(p)\ge 1}\frac{\beta(p)}{\gamma(p)^s};$$

$$M_g(s)=s\int_1^\infty \frac{g(x)}{x^{s+1}}dx=g(1)+\int_1^\infty x^{-s}dg(x)=\sum_{\substack{n=1 \\ \gamma(n)\ge 1}}^\infty \frac{\beta(n)}{\gamma(n)^s}$$

Откуда

$$M_f(s)=\sum_p \frac{\beta(p)}{\gamma(p)^s}-\sum_{\substack{p\\ \gamma(p)<1}} \frac{\beta(p)}{\gamma(p)^s}$$

$$\mathrm{M_g(s)}=\sum_{\mathrm{n=1}}^{\infty}\frac{\beta(\mathrm{n})}{\gamma(\mathrm{n})^{\mathrm{s}}}-\sum_{\gamma(\mathrm{n})<1}\frac{\beta(\mathrm{n})}{\gamma(\mathrm{n})^{\mathrm{s}}}$$

Предположим, что ряд $\sum_{n=1}^{\infty}\frac{\beta(n)}{\gamma(n)^s}$ сходится в полуплоскости $\sigma>1$.

Начиная с этого момента, мы предполагаем также, что $\gamma(n)\geq 1$ для всех натуральных n. Так как все члены ряда

$$\sum_{n=1}^{\infty}\frac{\beta(n)}{\gamma(n)^s}$$

неотрицательные числа, то отсюда следует, что ряд для $M_g(s)$

(а следовательно и ряд для $M_f(s)$) при $\sigma>1$ сходится абсолютно. Доказывается следующие теоремы:

Теорема 1. Пусть $\beta(n)$ и $\gamma(n)-$ неотрицательные мультипликативные функции, причем $\gamma(n)\geq 1$ для всех n.

$$\sum_{\gamma(n)\leq x}\beta(n)=cx+O\left(\frac{x}{(\ln x)^{2+\varepsilon}}\right),\quad c\neq 0,\ \varepsilon>0,$$

Тогда если ряды

$$\sum_p\sum_{r=2}^{\infty}\frac{\beta(p^r)\ln\gamma(p^r)}{\gamma(p^r)} \quad \text{и} \quad \sum_p\frac{\beta^2(p)\ln\gamma(p)}{\gamma^2(p)}$$

сходятся и $\sum_{r=1}^{\infty}\frac{\beta(p^r)}{\gamma(p^r)}<1$, для всех p, то $\sum_{\gamma(p)\leq x}\beta(p)\sim\frac{x}{\ln x}$

Рассмотрим несколько следствий теоремы 1.

Следствие 1. Пусть $\beta(n)$ – неотрицательная мультипликативная функция $\sum_{\gamma(n)\leq x}\beta(n)=cx+O\left(\frac{x}{(\ln x)^{2+\varepsilon}}\right),\quad c\neq 0,\ \varepsilon>0.$

Если ряды $\sum_p\sum_{r=2}^{\infty}\frac{\beta(p^r)\ln p^r}{p^r}$ и $\sum_p\frac{\beta^2(p)\ln p}{p^2}$

сходятся и $\sum_{r=1}^{\infty}\frac{\beta(p^r)}{p^2}<1$ для всех простых p,

то

$$\sum_{p\leq x}\beta(p)\sim\frac{x}{\ln x}.$$

В частности, этим условиям удовлетворяет функция $\beta(n)\equiv 1$. Поэтому отсюда следует закон простых чисел.

Следствие 2. Пусть $\gamma(n)-$ мультипликативная функция, $\gamma(n)\geq 1$ для всех неотрицательных n.

$$\sum_{\gamma(n)\le x} 1 = cx + O\left(\frac{x}{(\ln x)^{2+\varepsilon}}\right), \quad c \neq 0,\ \varepsilon > 0.$$

Тогда если ряды

$$\sum_p \sum_{r=2}^{\infty} \frac{\ln\gamma(p^r)}{\gamma(p^r)} \quad \text{и} \quad \sum_p \frac{\ln\gamma(p)}{\gamma^2(p)}$$

сходятся и

$$\sum_{r=1}^{\infty} \frac{1}{\gamma(p^r)} < 1 \quad \text{для всех простых } p,$$

то

$$\sum_{\gamma(p)\le x} 1 \sim \frac{x}{\ln x}.$$

Теорема 2. Пусть $\beta(n)$ и $\gamma(n)$ – неотрицательные, вполне мультипликативные функции, $\gamma(p) > \max(1, \beta(p))$ при всех простых p.

$$\sum_{\gamma(n)\le x} \beta(n) = cx + O\left(\frac{x}{(\ln x)^{2+\varepsilon}}\right), \quad c \neq 0,\ \varepsilon > 0, \qquad (1)$$

Тогда если ряд

$$\sum_p \frac{\beta^2(p)\ln\gamma(p)}{\gamma^2(p)}$$

сходится, то

$$\sum_{\gamma(p)\le x} \beta(p) \sim \frac{x}{\ln x}.$$

Теорема 3. Пусть $\beta(n)$ и $\gamma(n)$ – неотрицательные мультипликативные функции, $\gamma(p) > \max(1, \beta(p))$ для всех простых p и выполнено условие (1).

Тогда

$$\sum_{\gamma(p)\le x} \beta(p) \sim \frac{x}{\ln x}.$$

Литература:

1. Файнлейб А.С. Некоторые асимптотические формулы для сумм мультипликативных функций и их приложения.- Литовский матем. сборник, 7, №13, 1967, 535–545.
2. Ингам А.Е. Распределение простых чисел. – ОНТИ, 1936.
3. Титчмарш Е.К. Теория дзета-функции Римана. – ИЛ, 1953.

Непрерывные аналоги закона распределения простых чисел

Оразов Мамед, кандидат физико-математических наук, докторант
Туркменский сельскохозяйственный университет имени С.А. Ниязова (г. Ашхабад)

Работа содержит достаточные условия, которым должно удовлетворять преобразование Меллина неубывающей функции $f(x)$, чтобы была справедлива асимптотическая формула $f(x) \sim x/\ln x$ при $x \to \infty$. Из полученных результатов, в частности, при $f(x) = \pi(x)$ здесь содержится асимптотический закон распределения простых чисел.

Work contains sufficient conditions with which should satisfy transformation Mellin of not decreasing function $f(x)$ that it was fair Asymptotic formulae $f(x) \sim x/\ln x$ at $x \to \infty$. From the received results, in particular, at $f(x) = \pi(x)$ here contains asymptotic the law of distribution of simple numbers.

Пусть $f(x)$ – неубывающая функция, определенная при $x \geq 1$

$$M_f(s) = s\int_1^{\infty} \frac{f(x)}{x^{s+1}}dx, \quad F(s) = e^{M_f(s)}$$

Поставим вопрос о том, какие минимальные ограничения на функцию $F(s)$ обеспечивают асимптотическую формулу

$f(x) \sim \dfrac{x}{\ln x}$ – аналог закона простых чисел.

В работе доказывается следующая лемма.

Лемма 1. Пусть интеграл $M_f(s)$ сходится при $\sigma > 1$, $F(s) = e^{M_f(s)}$. Если производная $F'(s)$ равномерно продолжима на прямую $\sigma = 1$, исключая точку $s = 1$,

$$F(s) = o\left(\frac{1}{(\sigma - 1)^{4/3}}\right)$$

при $\sigma \to 1 + 0$, то функция $F(s)$ не обращается в нуль в замкнутой полуплоскости $\sigma \geq 1$.

Мы воспользовались тем, что из равномерной продолжимости $F'(s)$ следует равномерная продолжимость $F(s)$, так как при $1 < u_1 < u_2$

$$F(u_2 + it) - F(u_1 + it_1) = \int_{u_1}^{u_2} F'(u + it)du = O(u_2 - u_1),$$

что влечет за собой равномерную продолжимость функции $F(s)$, и следовательно, оценку

$$F(\sigma + 2it_1) = O(1), \quad (\sigma \to 1 + 0, \ t_1 \neq 0).$$

Далее из равенства $F(s) = e^{M_f(s)}$ следует

$$\frac{F'}{F}(s) = M'_f(s) = -\int_1^{\infty} x^{-s} \ln x df(x) = -\int_1^{\infty} x^{-s} d\left(\int_1^x \ln u df(u)\right).$$

Функция $h(x) = \int_1^x \ln u df(u)$ очевидно неубывающая.

Применим к ней сформулированную ниже теорему Икеара.

Теорема. (Теорема Икеара [2]). Пусть $h(x)$ неубывающая функция, определенная при $x \geq 1$.

Если функция

$$\int_1^{\infty} x^{-s} dh(x) - \frac{1}{s-1}$$

равномерно продолжима на прямую $\sigma = 1$, то $h(x) \sim x$ при $x \to \infty$.

В нашем случае

$$\int_1^{\infty} x^{-s} dh(x) - \frac{1}{s-1} = -\frac{F'}{F}(s) - \frac{1}{s-1},$$

так что из предыдущего вытекает, что условия теоремы Икеара выполнены. Согласно этой теоремы

$$h(x) = \int_1^x \ln u df(u) \sim x, \qquad (x \leftarrow \infty).$$

Отсюда следует

$$f(x) - f(2) = \int_2^x \frac{1}{\ln u} dh(u) = \frac{h(x)}{\ln x} - \frac{h(2)}{\ln 2} + \int_2^x \frac{h(u)}{u \ln^2 u} du,$$

откуда

$$f(x) = \frac{h(x)}{\ln x} - \frac{h(2)}{\ln 2} + f(2) = O\left(\int_2^x \frac{du}{\ln^2 u}\right) \sim \frac{x}{\ln x}.$$

Теорема доказана.

Литература:

1. Ингам А.Е. Распределение простых чисел.– ОНТИ, 1936.
2. Райков Д.А. Обобщение теоремы Икеара-Ландау.– Матем. сб. 8 (45), №3, 1938, 559–568.
3. Постников А.Г. Упрощение элементарного доказательства А.Сельберга асимптотического закона распределения простых чисел.– УМН, т.х., 1955, №4.

Научное издание

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ ТЕХНИЧЕСКИХ НАУК

Международная заочная научная конференция
г. Уфа, октябрь 2011 г.

Материалы печатаются в авторской редакции

Дизайн обложки: *Е.А. Шишков*
Верстка: *П.Я. Бурьянов*

Подписано в печать 24.10.2011. Формат 60x90 $^{1}/_{8}$.
Гарнитура «Литературная». Бумага офсетная.
Усл. печ. л. 8,6. Уч.-изд. л. 5,6. Тираж 300 экз.

Отпечатано в типографии «Лайм»
450059, г. Уфа, ул. Новосибирская, д. 2