МИНИСТЕРСТВО ОБРАЗОВАНИЯ
И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Орский гуманитарно-технологический институт (филиал)
федерального государственного бюджетного образовательного учреждения
высшего образования
«Оренбургский государственный университет»
(Орский гуманитарно-технологический институт (филиал) ОГУ)

Механико-технологический факультет
Кафедра программного обеспечения

СБОНИК МАТЕРИАЛОВ

Всероссийской научно-практической конференции

«АКТУАЛЬНЫЕ ПРОБЛЕМЫ АВТОМАТИЗАЦИИ УПРАВЛЕНИЯ НА ПРЕДПРИЯТИИ И В ОРГАНИЗАЦИИ»

17 ноября 2017 г.
Орск

УДК 681.51
ББК 65.050.9(4Рос)253
А 43

А 43 **Актуальные проблемы автоматизации управления на предприятии и в организации:** сборник материалов всероссийской научно-практической конференции (17 ноября 2017, Орск) /под общей редакцией доцента Е.Е.Суриной.. – Ставрополь: Логос, 2018. – 84 с.

ISBN 978-5-907078-04-8

УДК 681.51
ББК 65.050.9(4Рос)253

ISBN 978-5-907078-04-8

ФОРМИРОВАНИЕ ЕДИНОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА ПРЕДПРИЯТИЯ/ОРГАНИЗАЦИИ

РАЗВИТИЕ И ПЕРСПЕКТИВЫ БЛОКЧЕЙНА И КРИПТОВАЛЮТ

Головин Дмитрий Сергеевич,
Орский гуманитарно-технологический институт (филиал) ОГУ, г. Орск

Аннотация

Формирование представления о криптовалютах и блокчейне. Основные понятия криптовалют; актуальность использования криптовалют в современном мире.

Ключевые слова: *криптовалюта, блокчейн, финансовые технологии, цифровые валюты.*

Keywords: *crypto-currency, blockchain, financial technologies, digital currencies.*

Блокчейн – это цепочка блоков, выстроенная по определенной последовательности, заложенной в правилах. В блоках находится информация, как правило, о транзакциях; копии блоков хранятся независимо друг от друга и могут обрабатываться одновременно на множестве компьютеров. По своей сути, блокчейн – это распределённая база данных.

Криптовалюта – это цифровая валюта, которая создаётся и контролируется с помощью криптографических методов, а конкретно – блокчейна. Благодаря своим возможностям, блокчейн и криптовалюты продолжают находиться в центре внимания уже не первый год подряд.

Звучит странно, но использовать блокчейн можно и совершенно не разбираясь в его устройстве, не обязательно даже знать, что стоит за этим термином. Однако знания функционирования и распределенного хранения блоков помогут разобраться в большом разнообразии различных криптовалют, большинство из которых имеет собственные цепочки блоков.

Блокчейн создан, чтобы обеспечить финансовые транзакции без участия посредников, обезопасить переводы и хранение.

Незнакомым друг с другом людям в современном мире приходится постоянно устанавливать доверительные отношения, без которых не было бы возможности производить обмен денег на товар. Блокчейн даёт возможность понять, что техническая система в этом плане ничуть не уступает социальной.

Процесс обмена с помощью блокчейна имеет следующие характеристики:

− точность;
− понятность условий;
− безопасность;
− прозрачность.

Блокчейн помогает избавиться от вынужденного доверия к третьим лицам и все нюансы обмена товара берёт на себя.

Прорывной технологией в финансово-техническом мире является Ethereum. Это платформа для создания онлайн смарт-контрактов на базе блокчейна эфириум. Суть этой технологии в том, что за условиями выполнения финансовой сделки следит компьютерный код, и никакого участия не требуется. В Норвегии и Швеции блокчейн Эфириума уже используется для заключения страховых договоров. Подобные проекты находятся на стадии разработки в Украине, России, Дании, Германии и множестве других стран. В 2016 году Центробанк РФ запустил платформу "мастерчейн", работающую на блокчейне Ethereum. В августе 2017 года глава Ethereum foundation и глава внешэкономбанка (ВЭБ) заключили партнёрство. В октябре 2017 года Сбербанк вошёл в некоммерческий альянс Enterprise Ethereum Alliance и стал первым российским банком в нём. По мнению учёных и финансовых аналитиков, технология "умных-контрактов" влечёт за собою новую эру в финансах и технологиях.

1 декабря 2016 года президент РФ Владимир Путин поставил задачу развития цифровой экономики в России. Программу "Цифровая экономика" утвердили в июле 2017 года. Задача этой программы - интегрировать блокчейни криптовалюты во всех сферы нашей жизни. Основные два положения этой программы - институты и информационная структура. В учебных заведениях будут внедряться программы, направленные на обучение кадров для работы в сфере цифровой экономики. Развивать цифровую экономику в России хотят с помощью машинного обучения, искусственного интеллекта, "больших данных".

Перспективы развития цифровой экономики и блокчейна в России уже были чётко обозначены правительством. До 2024 года должно появиться не менее десяти высокотехнологичных компаний, управляющих цифровыми технологиями. Не менее пяти сотен средних и малых предприятий, которые будут иметь отношение к сфере цифровой экономики. Количество выпускников в сфере информационных технологий не должно быть менее восьмисот тысяч в год. Не менее сорока процентов жителей страны должны иметь цифровые навыки. Не менее десяти российских организаций будут участвовать в развитии крупных финансово-технических проектах с объемом $ 3 млн на международном уровне.

Блокчейн и криптовалюты являются общепризнанным началом новой эры в финансовом и техническом мире.

Литература:

1 Зачем России цифровая экономика [Электронный ресурс]. – Режим доступа: https://rb.ru/longread/digital-economy-in-russia/

2. Криптовалюта [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Криптовалюта

ВОЗМОЖНОСТИ СИСТЕМЫ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ «КОМПАС» И ИХ ИСПОЛЬЗОВАНИЕ В УЧЕБНОМ ПРОЦЕССЕ

Задорожный Виталий Дмитриевич,
Орский гуманитарно-технологический институт (филиал) ОГУ, г. Орск

Аннотация

В статье исследуются общие принципы использования систем автоматизированного проектирования (САПР) в учебном процессе. Дана характеристика отечественных и зарубежных САПР. Особое внимание уделено применению программного продукта «КОМПАС» Российского вендора «АСКОН».

Ключевые слова: *автоматизированное проектирование, учебный процесс, машиностроение, энергетика.*

Keywords: *computer-aided design, educational process, engineering, energy*

По различным оценкам, не менее 70% затрат в промышленности приходится на конструкторско-технологическую подготовку производства. Применение современных САПР, позволяет автоматизировать самую трудоемкую проектно-конструкторскую часть работы: разработку графики (чертежей, диаграмм, схем и т.п.) - наиболее эффективного способа представления информации [1, 45].

Развитие САПР опирается на прочную научно-техническую базу. Это - современные средства вычислительной техники, новые способы представления и обработки информации, создание новых численных методов решения инженерных задач и оптимизации. Системы автоматизированного проектирования дают возможность на основе новейших достижений фундаментальных наук отрабатывать и совершенствовать методологию проектирования, стимулировать развитие математической теории проектирования сложных систем и объектов. В настоящее время созданы и применяются в основном средства и методы, обеспечивающие автоматизацию рутинных процедур и операций, таких, как подготовка текстовой документации, преобразование технических чертежей, построение графических изображений и т.д.

Главная цель разработки САПР — повышение эффективности труда специалистов предприятия, решающих различные производственные задачи. В частности, связанные с инженерным проектированием. Повышение эффективности в данном случае может осуществляться за счет:

- снижения трудоемкости процесса проектирования на производстве;
- сокращения сроков реализации проектов;
- снижения себестоимости проектных работ, а также издержек, связанных с эксплуатацией;
- обеспечения повышения качества инфраструктуры проектирования;

- оптимизации методов проектирования [2].

Компоненты многофункциональных систем САПР традиционно группируются в три основных блока CAD, CAM, CAE. Модули блока CAD (Computer Aided Designed) предназначены в основном для выполнения графических работ, модули CAM (Computer Aided Manufacturing) - для решения задач технологической подготовки производства, модули CAE (Computer Aided Engineering) - для инженерных расчетов, анализа и проверки проектных решений [2].

Крупнейшим в мире поставщиком программного обеспечения для промышленного и гражданского строительства, машиностроения, рынка средств информации является компания Autodesk, Inc. Начиная с 1982 года компанией Autodesk был разработан широкий спектр решений для архитекторов, инженеров, конструкторов, позволяющих им создавать цифровые модели. Технологии Autodesk используются для визуализации, моделирования и анализа поведения разрабатываемых конструкций на ранних стадиях проектирования и позволяют не просто увидеть модель на экране, но и испытать её. AutoCAD, разработанный Autodesk, долгое время отвечал самым взыскательным требованиям проектировщиков. Но на сегодняшний день, обладая богатым инструментарием и возможностями адаптации к требованиям пользователя, он уже не удовлетворяет потребностям большинства проектировщиков. Этот пакет может применяться лишь при разработке очень малых и достаточно простых проектов, автоматизируя только рутинную работу кульмана и не более того. Современному проектировщику нужно гораздо больше, чем просто быстрое и красивое выполнение чертежей.

Российский рынок САПР широко представлен программными продуктами отечественных производителей. Программный комплекс «Лира» (http://www.lira.com/) является современным инструментом для численного исследования прочности и устойчивости конструкций и их автоматизированного конструирования. Одно из наиболее важных свойств этого пакета заключается в возможности расчета арматуры для железобетонных элементов (как плоских пластин, так и стержней) с учетом всевозможных загружений и комбинаций усилий и различных воздействий.

Программный комплекс «Мономах» (http://www.lira.com/) разработан для автоматизированного проектирования железобетонных конструкций многоэтажных каркасных зданий. Широкое использование в современном строительстве монолитно-каркасной технологии определило класс задач решаемых с помощью программ комплекса «Мономах». За последние годы программный комплекс «Мономах» был оценен проектировщиками как незаменимый инструмент расчета конструкций жилых и общественных многоэтажных зданий из монолитного железобетона [2].

Несомненным лидером отечественных САПР является программа «КОМПАС», разработанная российской компанией «АСКОН» с возможностями

оформления проектной и конструкторской документации согласно стандартам серии ЕСКД и СПДС. Существует в двух версиях: «КОМПАС-График» и «КОМПАС-3D», соответственно предназначенных для плоского черчения и трёхмерного проектирования.

Систематизированное применение САПР «КОМПАС» в учебном процессе Орского гуманитарно-технологического института (филиала) ОГУ заключается в следующем. На начальном этапе освоения она применяется как дополнение к «классическому» черчению в курсе «Инженерная графика». В настоящее время отработана методика сквозного применения САПР. Она основывается на поэтапном, в течение нескольких семестров, освоении системы. Например, для направлений подготовки 13.03.02 «Электротехника и электроэнергетика» и 13.03.01 «Теплоэнергетика и теплотехника» система применяется при освоении дисциплин «САПР электроснабжения», «Моделирование систем электроснабжения», «Введение в САПР энергоустановок», где наряду с использованием графической части, возможно ее использование в компьютерном моделировании. Это дает возможность создавать 3D модели изучаемых узлов и агрегатов и исследовать эти элементы без применения объектов – оригиналов (см. рисунок 1) [3].

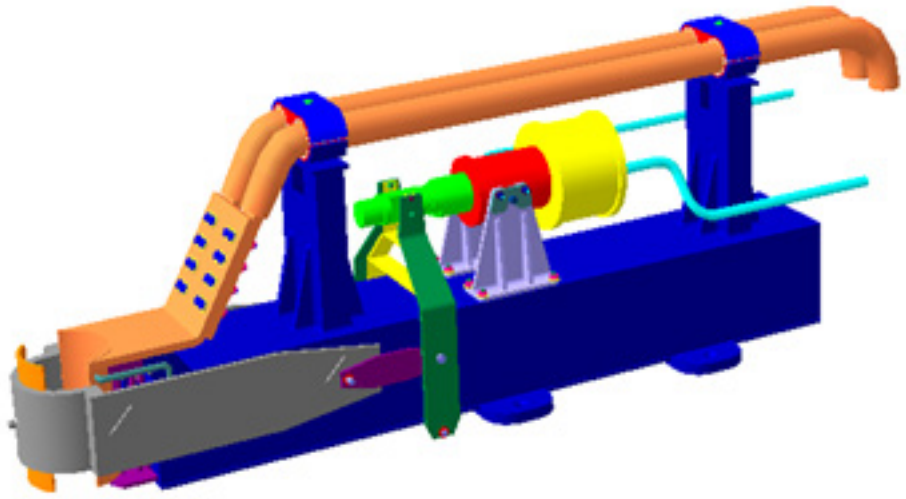


Рисунок 1 – Электрододержатель электросталеплавильной печи

Благодаря применению широкого спектра прикладных библиотек системы «КОМПАС» появляется возможность компоновать электрические схемы, энергетические установки, элементы агрегатов машиностроения.

Пример применения прикладной библиотеки «Компас-Электрик» приведен на рисунке 2.

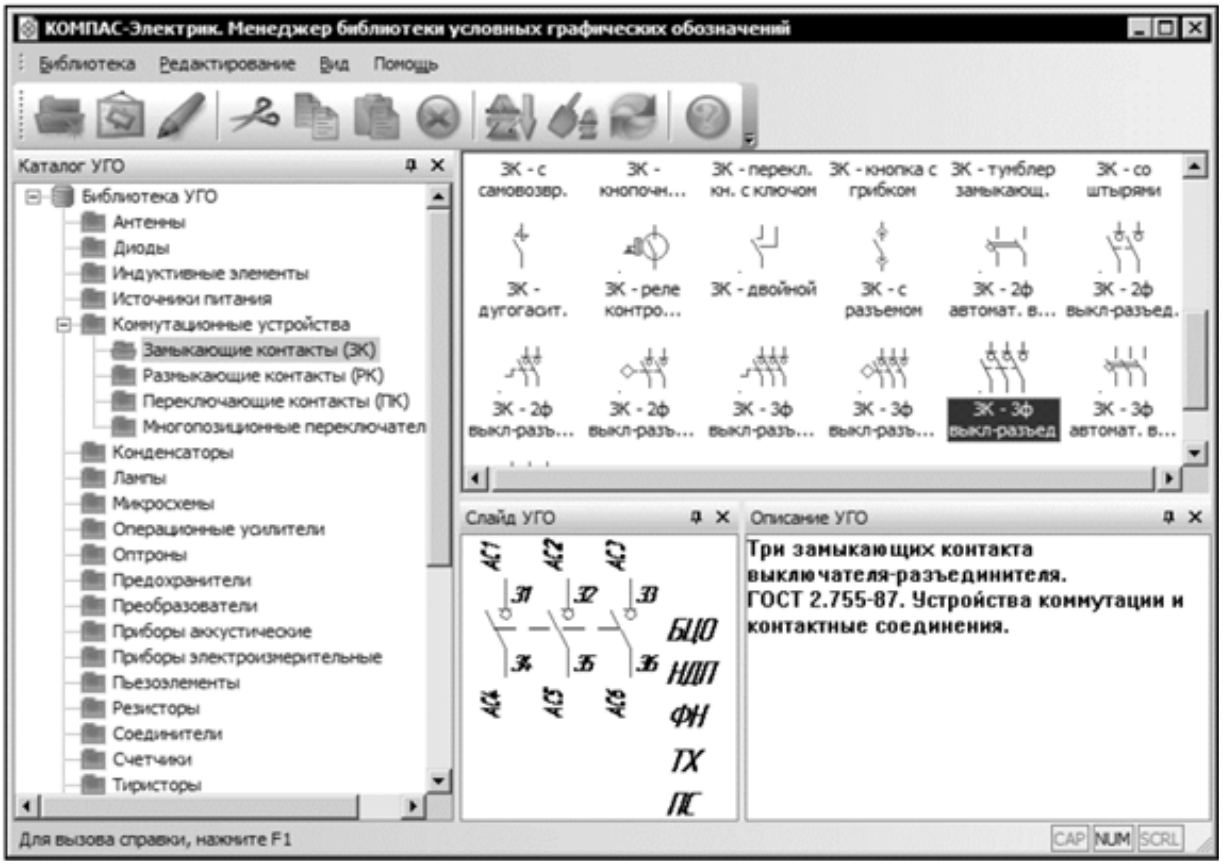


Рисунок 2 – Пример применения прикладной библиотеки САПР «КОМПАС»

Наличие большого количества прикладных библиотек в системе «КОМПАС» позволяет использовать в учебном процессе трехмерные модели как стандартных деталей, агрегатов, элементов электрических схем так и использовать их для формирования оригинальных трехмерных сборок [1,47]. Для вышеуказанных направлений подготовки бакалавров приобретенные на начальных этапах знания и умения работы с системой можно использовать при выполнении курсовых работ по дисциплинам «Электрические машины» и «Аэрогазодинамика». В процессе выполнения этих работ студенты могут формировать собственные библиотеки оригинальных элементов и деталей электро- и энергоустановок. Кроме того, система предоставляет возможность выполнять ряд расчетов, например, массо-центровочных характеристик элементов оборудования [4, 95].

Постоянная, сквозная работа с системой «КОМПАС» позволяет освоить компетенции для выполнения основных видов профессиональной деятельности выпускников, прошедших обучение по программам академического бакалавриата: научно-исследовательской и проектно-конструкторской.

Для успешного функционирования промышленных предприятий в современных условиях абсолютно необходимы передовые информационные технологий. Они позволяют не только решать широкий круг задач в сфере автоматизации финансово-хозяйственной и управленческой деятельности, но

и осуществлять комплексную автоматизацию основных технологических и производственных бизнес-процессов.

Применение системы «КОМПАС» является важным этапом в подготовке высококвалифицированных кадров для отечественной промышленности, технологическим прорывом в машиностроении и энергетике. Благодаря доступности, надежности, эффективности программного обеспечения САПР «КОМПАС» автоматизированное проектирование стало неотъемлемой частью учебного процесса. Освоение современных САПР и, прежде всего программ группы компаний АСКОН, разработанных ведущими российскими специалистами, является большим шагом вперед к новым информационным технологиям, к новому образу мышления, к новому качеству образования и новому уровню развития отечественной промышленности.

Литература

1. Задорожный В.Д. Применение систем автоматизированного проектирования в учебном процессе // Вторая региональная научная конференция «Наука и производство Урала», сб. науч. тр. – Новотроицк : НФ МИСИС. – 2006. – С. 45-48.

2. http://www.ru.wikipedia.org/-› Система автоматизированного проектирования.

3. Задорожный В.Д. Отечественная металлургия сверяет курс по КОМПАС 3D [Электронный ресурс] : Международный конкурс статей - Санкт-Петербург: АО АСКОН. – 2007.

4. Задорожный В.Д. Применение КОМПАС-3D в расчетах роликов металлургических транспортных рольгангов // Труды первой Международной научно-методической конференции «Применение программных продуктов КОМПАС-3D в высшем образовании». – Тула : ТулГУ – 2005 – с. 94-96

ЭФФЕКТИВНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ В КОРПОРАТИВНОМ УПРАВЛЕНИИ

Исаков Иван Николаевич, Блиничкин Денис Юрьевич,
Анисимов Евгений Олегович, Субботин Андрей Владимирович,
ОГТИ (филиал) ОГУ, г. Орск

Аннотация

В статье рассматриваются общие понятия, связанные с облачными вычислениями, а также применение технологии в корпоративном управлении.

Ключевые слова: *облачные вычисления, ресурсы, услуги*

Keywords: *cloud computing, resources, services*

В наши дни фактически все крупные форумы, посвященные развитию и внедрению современных ИТ-технологий, не обходятся без рассмотрения вопроса использования облачных технологий в бизнесе, госструктурах,

банковском деле. Это связано с тем, что большинство из этих направлений деятельности требуют все возрастающих вычислительных мощностей.

Это востребовало создание универсальной платформы, способной обеспечить разделение ресурсов между различными пользователями и подразделениями, а главное – обладать свойствами самоуправления и адаптации, гарантирующими необходимое масштабирование и динамизм.

Облачные технологии – это технологии обработки данных, в которых компьютерные ресурсы предоставляются Интернет-пользователю как онлайн-сервис. Актуальность облачных вычислений связана со снижением затрат, масштабируемостью и гибкостью архитектуры информационных технологий.

Использование технологии виртуализации позволяет существенно повысить эксплуатационные характеристики создаваемых информационных систем, задействовав механизмы, заложенные в аппаратной архитектуре процессоров. Сделать «прозрачной» для пользователей схему организации вычислительного процесса, что фактически позволяет любому приложению использовать вычислительные мощности, совершенно не задумываясь о технологических аспектах.

Основными преимуществами технологии облачных вычислений являются:

1) Снижение затрат на приобретение оборудования и программного обеспечения, настройку и эксплуатацию локальных центров обработки данных;

2) Высокая скорость. Большинство облачных вычислительных служб предоставляются в режиме самообслуживания и по запросу, так что даже большие объемы вычислительных ресурсов можно подготовить в кратчайший срок. Это позволяет компании избавиться от постоянного планирования загрузки.

3) Производительность. Крупнейшие облачные вычислительные службы работают в мировой сети безопасных центров обработки данных, которые регулярно обновляются до последнего поколения быстрого и эффективного вычислительного оборудования. Это обеспечивает различные преимущества по сравнению с использованием одного корпоративного центра обработки данных, включая уменьшение задержки в сети для приложений и большую экономию от масштаба.

4) Надежность. Облачные вычисления обеспечивают резервное копирование данных, аварийное восстановление и непрерывность бизнес-процессов, не требуя значительных затрат.

Национальным институтом стандартов и технологий США зафиксированы следующие обязательные характеристики облачных вычислений:

1) Самообслуживание по требованию. Потребитель самостоятельно определяет и изменяет вычислительные потребности: серверное время, скорости доступа и обработки данных, объём хранимых данных – без взаимодействия с представителем поставщика услуг;

2) Универсальный доступ по сети. Услуги доступны потребителям по сети передачи данных вне зависимости от используемого терминального устройства;

3) Объединение ресурсов. Поставщик услуг объединяет ресурсы для обслуживания большого числа потребителей в единый пул для динамического перераспределения мощностей между потребителями в условиях постоянного изменения спроса на мощности;

4) Эластичность. Услуги могут быть предоставлены, расширены, сужены в любой момент времени, без дополнительных издержек на взаимодействие с поставщиком, как правило, в автоматическом режиме;

5) Учёт потребления. Поставщик услуг автоматически исчисляет потреблённые ресурсы на определённом уровне абстракции (например, объём хранимых данных, пропускная способность и т.д.) и на основе этих данных оценивает объём предоставленных потребителям услуг.

Облачные технологии различаются по моделям развёртывания и моделям обслуживания. Моделей развёртывания насчитывается четыре:

1) Частное облако — инфраструктура, предназначенная для использования одной организацией, включающей несколько потребителей (например, подразделений одной организации). Частное облако может находиться в собственности, управлении и эксплуатации как самой организации, так и третьей стороны. Оно может физически существовать как внутри, так и вне юрисдикции владельца. Для частного облака характерно снижение стоимости оборудования за счет использования простаивающих или неэффективно используемых ресурсов, а также снижение затрат на закупки оборудования вследствие сокращения логистики.

2) Публичное облако — инфраструктура, предназначенная для свободного использования широкой аудиторией. Публичное облако может находиться в собственности, управлении и эксплуатации коммерческих, научных и правительственных организаций.

3) Общественное облако — вид инфраструктуры, предназначенный для использования конкретным сообществом потребителей из организаций, имеющих общие задачи. Общественное облако может находиться в кооперативной (совместной) собственности, управлении и эксплуатации одной или более из организаций сообщества или третьей стороны.

4) Гибридное облако — это комбинация из двух или более различных облачных инфраструктур (частных, публичных или общественных), остающихся уникальными объектами, но связанных между собой стандартизованными или частными технологиями передачи данных и приложений.

Принято выделять три основные модели обслуживания облачных технологий, которые иногда называют слоями облака.

К услугам инфраструктуры (Infrastructure as a Service – IaaS) можно отнести набор физических ресурсов: серверов, сетевого оборудования

и накопителей – предлагаемых заказчикам в качестве услуг. Услуги инфраструктуры решают задачу надлежащего оснащения ЦОД, предоставляя вычислительные мощности по мере необходимости. Частным примером услуг инфраструктуры является аппаратное обеспечение как услуга (Hardware as a Service – HaaS). Пользователь получает оборудование, на основе которого разворачивает свою собственную инфраструктуру.

Потребитель при этом не управляет базовой инфраструктурой облака, но имеет контроль над операционными системами, системами хранения, развернутыми приложениями и, возможно, ограниченный контроль выбора сетевых компонентов. В таком случае защиту платформ и приложений обеспечивает сам потребитель, а провайдер облака должен организовать защиту инфраструктуры. Для предоставления ресурсов по требованию часто используется виртуализация.

Услуги платформы (Platform as a Service – PaaS) – это модель обслуживания, в которой потребителю предоставляются приложения (созданные или приобретенные) как набор услуг, различающихся по типам. Например, рабочее место как услуга (Workplace as a Service – WaaS) позволяет использовать облачные вычисления для организации рабочих мест сотрудников, установив необходимое для работы персонала ПО. Данные как услуга (Data as a Service – DaaS) предоставляют дисковое пространство для хранения информации. Безопасность как услуга (Security as a Service – SaaS) дает возможность пользователям быстро развертывать продукты, позволяющие обеспечить безопасное использование веб-технологий.

Потребитель при этом не управляет базовой инфраструктурой облака, в том числе сетями, серверами, операционными системами и системами хранения данных, но имеет контроль над развернутыми приложениями и, возможно, некоторыми параметрами конфигурации среды хостинга. Таким образом, потребитель должен позаботиться об обеспечении защиты приложений, которые будут развернуты на предоставленных платформах.

Услуги приложений (Software as a Service – SaaS) предполагают доступ к приложениям как к сервису. Пользователь может получать доступ к ПО, развернутому на удаленных серверах, посредством Интернета, причём все вопросы обновления и лицензий на данное ПО регулируются поставщиком данной услуги. Оплата в данном случае осуществляется за фактическое использование ПО.

Приложения доступны посредством различных клиентских устройств. Потребитель не управляет базовой инфраструктурой облака, в том числе сетями, серверами, операционными системами, однако отвечает за сохранность параметров доступа и выполнение рекомендаций провайдера по безопасным настройкам приложений. Услуги приложений более всего знакомы повседневному пользователю.

Рост числа пользователей облаков разных типов, укрупнение существующих облаков и появление новых будут определять развитие

информационных, сетевых, компьютерных и телекоммуникационных технологий на ближайшие годы. Рост зоны охвата глобальных компьютерных сетей, увеличение скорости передачи информации, использование в промышленности специализированных устройств, получающих информацию из компьютерных сетей, будут способствовать развитию облачных технологий.

Литература

1 Урок на тему «Облачные технологии» [Электронный ресурс] – Режим доступа : https://infourok.ru/razrabotka-uroka-na-temu-oblachnie-tehnologii-klass-649281.html

2 Основные понятия облачных вычислений. [Электронный ресурс] – Режим доступа: http://ecm-journal.ru/docs/Osnovnye-ponjatija-oblachnykh-vychislenijj-Rukovodstvo-dlja-nachinajushhikh.aspx

3 Технология облачных вычислений. [Электронный ресурс] – Режим доступа : http://mirtelecoma.ru/magazine/elektronnaya-versiya/31/

UML-ДИАГРАММЫ В БИЗНЕС- МОДЕЛИРОВАНИИ

Кузниченко Марина Анатольевна,
Орский гуманитарно-технологический институт (филиал) ОГУ, г. Орск

Аннотация

В статье рассматриваются различные виды диаграмм языка UML, достоинства их использования при бизнес- моделировании деятельности организации.

Ключевые слова: *язык UML, диаграммы, бизнес-моделирование.*

Keywords: *language UML, diagrams, business- modeling.*

При проектировании или реинжиниринге сложных информационных систем разработчики используют различные средства моделирования бизнес-процессов организации в целом или её отдельных аспектов деятельности. Уже никого не надо убеждать в необходимости использования CASE- технологий на этом этапе работы.

Основная цель бизнес-моделирования — обеспечить взаимопонимания на всех уровнях организации, преодолеть разрыв между стратегическим видением бизнеса и практической его реализацией. С этой целью в современных средствах бизнес-моделирования используются специальные языки, понятные и легко осваиваемые и менеджерами высшего звена, включая финансовых директоров, и аналитиками, и руководителями IT-подразделений, у каждого из которых свое видение решения бизнес-задач. С помощью таких языков строятся графические модели, диаграммы, наглядно демонстрирующие шаг за шагом, как построены в компании бизнес-процессы, как организовано взаимодействие между людьми и что необходимо изменить для оптимизации архитектуры организации в целом.

Самый известный среди средств проектирования информационных систем язык UML (Unified Modeling Language), он предназначен для объектного моделирования в сфере разработки или консалтинга различного программного обеспечения (ПО). На начальном этапе следует понять, что нужно автоматизировать в архитектуре организации, а затем уже эту автоматизацию осуществлять. Бизнес-модель, в частности, помогает ответить на этот вопрос. Главное назначение бизнес-модели — дать целостную картину жизнедеятельности организации, согласовать разные точки зрения на постоянно развивающийся и меняющийся бизнес. Ценность бизнес-модели определяется тем, в какой степени она помогает отвечать на актуальные вопросы, стоящие перед организацией, насколько реально затрагивает каждого сотрудника организации.

Язык UML имеет в своём арсенале большое множество диаграмм и их подвидов, каждая из которых предназначена осветить определённый аспект бизнес – процесса. UML создавался для того, чтобы обеспечить определение, визуализацию, документирование, а также проектирование всевозможных программных систем. С помощью UML разработчики ПО могут обеспечить полное соглашение в используемых графических обозначениях, чтобы представить общие понятия, такие как: компонент, обобщение, класс, поведение и агрегация. За счет этого достигается большая степень концентрации на архитектуре и проектировании.

Сервисы информационной системы и отношения, которые возникают между участниками бизнес- процесса, отражают диаграммы вариантов использования UML. Этот вид диаграммы наиболее наглядно отображает бизнес- процессы организации. С помощью этих диаграмм заказчик, конечный пользователь и разработчик могут совместно обсуждать функционал системы. Если диаграмма вариантов использования UML используется в процессе моделирования системы, то аналитик с её помощью решает следующие вопросы:

– определяет границы моделируемой системы от ее окружения;

– выявляет действующих лиц, а так же их взаимодействия с данной системой;

– описывает функционал системы;

– формулирует в глоссарии различные понятия предметной области, которые относятся к описанию данной системы.

На начальной стадии проектирования или реинжеринга системы выполняется полное текстовое описание, которое получается при тесном взаимодействии разработчиков с заказчиками.

Для каждого варианта использования рекомендуется создать свою диаграмму деятельности UML, она отображает разложение определенной деятельности на несколько действий. Диаграмма деятельности UML подобна блок- схеме алгоритма, поэтому она используются для того, чтобы

моделировать различные бизнес-процессы, параллельные и последовательные операции.

К статическим диаграммам относится диаграмма классов UML, которая предназначена для описания структуры системы, а также демонстрации атрибутов, методов и зависимостей между несколькими различными классами. Диаграмма классов UML призвана описать модель определенной предметной области, и в ней предусматриваются только классы прикладных объектов. В результате разработки диаграммы классов некоторые CASE – средства, например, Rational Rose, позволяют выполнить частичную кодогенерацию на язык программирования C++.

Диаграмма компонентов, в отличие от других диаграмм, описывает особенности физического представления системы. Диаграмма компонентов позволяет определить архитектуру разрабатываемой системы, установив зависимости между программными и аппаратными компонентами. Во многих средах разработки модуль или компонент соответствует файлу. Основными графическими элементами диаграммы компонентов являются компоненты, библиотеки, файлы, интерфейсы и зависимости между ними.

Для описания различных состояний объектов системы используется диаграмма состояний UML, которая представляет собой конечный автомат с простыми и композитными состояниями и переходами между ними. Конечный автомат описывает спецификацию последовательности различных состояний, через которые проходит определенный объект, или взаимодействие в ответ на некоторые события. При описании бизнес- процесса конечный автомат в диаграмме состояний UML закрепляется за исходным элементом и используется для определения поведения его экземпляров.

Диаграмма последовательности UML демонстрирует взаимодействия между несколькими объектами бизнес- процесса, которые упорядочиваются в соответствии со временем их появления. На диаграмме отображается упорядоченное во времени взаимодействие между несколькими объектами бизнес-процесса. Главными элементами в такой диаграмме выступают обозначения различных объектов, а также вертикальные линии жизни, отображающие течение времени и прямоугольники, предоставляющие деятельность определенного объекта или же выполнение им какой-либо функции.

Язык UML является объектно-ориентированным, поэтому технологии описания результатов проведенного анализа и проектирования являются семантически близкими к методам программирования на всевозможных объектно-ориентированных языках современного типа. При помощи данного языка бизнес- процессы предметной области могут быть описаны практически с любых возможных точек зрения, и точно так же описываются различные аспекты ее поведения. Все диаграммы являются наглядными и удобными для чтения даже после относительно быстрого ознакомления с его синтаксисом.

UML позволяет расширить, а также вводить собственные графические и текстовые стереотипы, что способствует его использованию не только в программной инженерии. Унифицированный язык моделирования получил достаточно широкое распространение в среде разработчиков ПО и бизнес – аналитиков.

Для того чтобы команда проектировщиков смогла добиться конечной цели для конкретного проекта, необходимо выбирать применимые возможности этого языка моделирования. Выбор используемых диаграмм UML должен быть сформулирован и обоснован в контексте конкретного проекта.

Литература

1. Андреевич Е. UML-диаграмма. Виды диаграмм UML - [Электронный ресурс]. – Режим доступа: https://www.syl.ru/article/206012/new_uml-diagramma-vidyi-diagramm-uml

---

ПРИМЕР АСУТП НА ПРЕДПРИЯТИИ «ЭРДЕНЭТ» В МОНГОЛЬСКОЙ НАРОДНОЙ РЕСПУБЛИКЕ

Лаптева Анна Владимировна,
Департамент Информационных технологий и автоматики,
Уральский федеральный университет, г. Екатеринбург,
Цогтбаатар Одхуу,
КОО «Предприятие Эрдэнэт», г. Эрдэнэт,
Лисиенко В.Г.,
Департамент Информационных технологий и автоматики,
Уральский федеральный университет, г. Екатеринбург,
Войнов Олег Юрьевич,
Департамент Информационных технологий и автоматики, Уральский федеральный университет, г. Екатеринбург,
Чесноков Ю.Н.,
Департамент Информационных технологий и автоматики, Уральский федеральный университет, г. Екатеринбург

Аннотация

Дробление полезных ископаемых, добываемых в карьере или шахте, до крупности, при которой возможно осуществление последующих стадий обработки, является первоначальной и наиболее трудоемкой операцией в общем технологическом цикле процесса сортировки и обогащения на горнодобывающем предприятии.

Предприятие имеет конусные дробилки крупного и мелкого дробления, соединенные транспортерами. В этой связи стоят задачи загрузки дробилок, измерения грансостава на выходе. Из этого следует необходимость внедрения

системы автоматического регулирования размера дробимого материала, который выполняет функции:

• измерение размеров продукта дробления;

• анализ конусных дробилок с целью выявления возможности управления размером рабочей щели.

Ключевые слова: *Дробление полезных ископаемых; система автоматического регулирования; конусная дробилка крупного дробления; руда; контроллер; гранулометр; рабочая щель; АСУ.*

Keywords: *Crushing of useful minerals; automatic control system; cone crusher is of large crushing; ore; controller; unit; working the slot; automated control system.*

Дробление полезных ископаемых, добываемых в карьере или шахте, до крупности, при которой возможно осуществление последующих стадий обработки (промывка, измельчение, сепарация и т. п.), является первоначальной и наиболее трудоемкой операцией в общем технологическом цикле процесса сортировки и обогащения.

В современных условиях одной из главных задач горно-обогатительных предприятий является сокращение энергетических затрат и эксплуатационных расходов в рудоподготовке. Наиболее энергоемким во всей технологии дезинтеграции полезных ископаемых является процесс измельчения. Поэтому основной путь экономии удельных затрат по рудоподготовке в целом – снижение крупности дробленого продукта, поступающего в измельчение.

Решение задачи снижения крупности конечного продукта и повышение производительности дробильного передела во многом обеспечивается посредствам оптимизации управлением, как самим процессом дробления, так и комплексом оборудования дробильной фабрики в целом. Для достижения данной цели необходим комплексный подход к рассмотрению ряда как технологических проблем, связанных непосредственно с конструктивными решениями применяемых схем дробления, так и проблем по оптимальному автоматизированному управлению комплектом механизмов самой дробилки, как отдельного агрегата, а также механизмов поточно-транспортной системы подачи исходного материала и уборки готового продукта.

Наиболее затратным по энергии на обогатительной фабрике является процесс измельчения руды до десятков микрон. Для оптимизации процесса измельчения возможно управлять не только им самим, но и процессом подготовки начального сырья для мельниц. Так, при снижении в питании мельниц содержания материала крупности +20 мм на 1% производительность мельниц увеличивается на 0,6%. Снижение крупности продуктов мелкого дробления на карьере «Вгепиз» в Канаде с 19 до 16 мм позволило увеличить производительность стержневых мельниц на 4,9%, снизить расход электроэнергии на 8% и стержней на 9,7%. Поэтому контроль процесса дробления является обязательным и важным элементом каждой обогатительной фабрики. Так же контроль крупности дробления позволит решить и вторую

задачу – своевременное изъятие готового продукта из замкнутого цикла, что уменьшит циркулирующую нагрузку на оборудование.

Целью работы является анализ автоматизированного измерительного комплекса, контролирующего качество выходного продукта цикла дробления, для последующей его переработки в цикле измельчения в условиях горно-обогатительного комбината КОО «Предприятие Эрдэнэт». Тема актуальна, так как существующие автоматизированные системы управления ГОК КОО «Предприятие Эрдэнэт» лишены возможности производить контроль качества продукта после процессов классификации (грохочения), в связи с чем продукт в цикл измельчения поступает неравномерный, что отрицательно сказывается на энергетических и качественных параметрах работы обогатительной фабрики в целом.

С течением времени руда становится более «бедной» по отношению к моменту начала разработки месторождения, что подразумевает увеличение объемов ее переработки для сохранения рентабельности предприятия. В связи с этим оптимизация работы каждого передела комбината и снижение энергозатрат является ключевой задачей для дальнейшей работы предприятия, что также подтверждает актуальность выбранной темы.

Оптимальные режимы предполагают работу дробилки с производительностью, равной ее пропускной способности, и при максимальном использовании мощности привода дробилки. Обеспечить такие режимы работы дробилок можно только при автоматическом управлении процессом дробления, основными задачами которого являются:

– управление процессом загрузки материала в дробилки;

– автоматическое управление режимом работы в целях получения наибольшей эффективности процесса дробления;

– управление вспомогательным оборудованием;

– автоматический контроль и защита, регистрация и учет параметров состояния оборудования, технологических параметров и общих показателей работы корпусов дробления и классификации по крупности;

– автоматический запуск и остановка основного и вспомогательного оборудования.

В состав дробильно-транспортного отделения (ДТО) входят следующие здания и сооружения [1]:

– приемный узел руды с корпусом крупного дробления ККД-1;
– корпус среднего и мелкого дробления – КСМД;
– склад крупнодробленой руды – СКДР №1;
– склад мелкодробленой руды – СМДР;
– корпус натяжных и приводных станций – КН и ПС;
– галереи ленточных конвейеров №1, 2, 3, 4, 5, 6, 7, 8, 11, 9 и 17;
– пешеходные галереи от здания АБК.

Приемный узел ККД-1 размещен в 400 м к востоку от контура рудника открытых работ.

Руда с рудника открытых горных работ автосамосвалами типа БеЛАЗ-549 грузоподъемностью 120-130 т, Катерпиллер (США) грузоподъемностью 136 т соответственно поступает на обогатительную фабрику в корпус крупного дробления ККД-1 и разгружается в приемные бункеры двух дробилок ККД 1200/130ГРЩ.

Режим разгрузки самосвалов регулируется автоматически с использованием установленных у корпуса светофоров под контролем дробильщика.

При выявлении дробильщиком в кузове автосамосвала «негабарита» или «мерзляка» (кусков руды или обледеневших глыб размером более 1000 мм) выгрузка из кузова не допускается, машина должна быть возвращена на рудник.

Перед дробилками установлены колосниковые грохоты с размером щели 150 мм. Максимальная крупность кусков исходной руды 1000 мм.

Дробленая руда крупностью 250 мм четырьмя пластинчатыми питателями В-2400 мм длиной 9,9 м подается на два параллельных конвейера №1а и 2а с шириной ленты 1600 мм, длиной 170 м, затем поступает в корпус приводных и натяжных станций, где перегружается на соответствующие конвейеры №1 и 2 с шириной ленты 1200 мм и длиной 700 м.

Руда из корпуса натяжных и приводных станций конвейерами №1 и 2 подается на конвейер №3 В = 1600 мм, длиной 102,5 м, оснащенный барабанной сбрасывающей тележкой, посредством которой разгружается в склад крупнодробленой руды.

Емкость склада составляет 65 тыс. т «живой» руды, фактически 20-25 тыс. т. Из склада ленточными питателями 1200х2000 мм руда подается на конвейеры №4, 5, 6, 6, 7, 8 В=1400 мм длиной 132,9 м (6 питателей на каждый конвейер), затем на дробилки КСД-5 шт., имеющие разгрузочную щель 27- 29мм[2].

Конусная дробилка крупного дробления (ККД), имеет гидравлическую систему регулирования размера рабочей щели, которая поднимает или опускает нижний конус с помощью гидроцилиндра [3].

Изменение твердости дробимой породы изменяет размер рабочей щели по причине недостаточной жесткости гидроцилиндра. Требуется либо частая настройка размера рабочей щели при изменении твердости дробимой породы, либо необходимо внедрение непрерывной системы автоматического регулирования (САР) рабочей щели. Выходной материал дробилки попадает на индивидуальный транспортер, что позволяет применить гранулометр в составе САР.

Дробилки КМД разгружаются на общий транспортер, что исключает возможность измерения гранулометрического состава той или иной дробилки. Кроме того, у этих дробилок изменение рабочей щели возможно только при остановке подающего транспортера и очистке дробилки от остатков дробимого материала. Рабочая щель регулируется поворотом верхнего конуса по резьбе после его расфиксации и поворотом вправо или влево, в зависимости от положения гидроцилиндра с толкателем, действующим на зубцы венца,

связанного с верхним конусом. При таком устройстве конусных дробилок классическая САР не применима. На Уралмаше дробилки такого типа получили существенную модернизацию. Конус верхний по резьбе поворачивается гидромоторами, взаимодействующими с зубчатым венцом, жестко связанным с верхним конусом. Однако угол поворота не контролируется в автоматическом режиме (отсутствуют датчики угла поворота). Необходимость расфиксации и освобождение дробилки от камней сохраняется, что затрудняет создание непрерывной САР рабочей щели. Внедрение такой САР позволило бы развить существующую АСУ ДТО.

На предприятии есть система контроля АСУ ДТО, которая выполняет функции:

– реализация завала-подпрессовки дробилок,
– выявление прохождение металла;
– контроль температуры подшипников и масла;
– контроль уровня оборотной воды в резервуарах фабрики;
– контроль за приёмом и передачей руды;
– контроль потребляемого тока электрических двигателей дробилок;
– контроль температуры электрических двигателей дробилок.

На ДТО обогатительной фабрики работают системы автоматического регулирования загрузки дробилок среднего и мелкого дробления от контроллеров Honeywell и Siemens. В качестве входного сигнала принимается аналоговый сигнал от преобразователя П848-1м, Е728-7/1, Siemens 7KG6113-2CN27-OB, которые измеряют потребляемую мощность дробилок. Системы контроля забивки течки и подпрессовки обеспечивают защиту дробилок от перегрузок. Для учета веса переработанных руд используются конвейерные весы фирмы Schenk.

Функция «оптимального управления загрузкой руды в дробилку» реализуется от контроллера PLC Simatic S7-300 [4]. Он обеспечивает управление приводами подающего конвейера, в зависимости введенного вручную значения показателя «текущая величина разгрузочной щели», автоматически формируя задание на количество подаваемой в дробилку руды (Q, т/ч).

Имеется возможность построения САР рабочей щели ККД.

При разработке такой системы необходимо решаются задачи:

• найти метод измерения размеров продукта дробилки;

• исследовать конусные дробилки с целью выявления возможности управления размером рабочей щели;

• составить структурную схему системы регулирования;

• выбрать оборудование для реализации этой схемы.

Литература

1. Технологическая инструкция по обогащению медно-молибденовых руд на обогатительной фабрике совместного Монголо-Российского КОО «Предприятие Эрдэнэт» – 2008.

2. Круглов В. Н. Проведение промышленных испытаний и модернизация системы оценки крупности дробленой руды «ГРАНИКС» // УГТУ-УПИ. Отчет о научно-исследовательской работе. – 2014.

3. Критерии для сравнения конусных дробилок. Режим доступа: http//www.maxi-exkavator.ru/articles/crusher/~id=1830.

4. Старостин А. А., Лаптева А. В. Технические средства автоматизации и управления. – Екатеринбург: Изд-во Урал. ун-та, 2015. – 168 с.

ИСТОРИЯ СТАНОВЛЕНИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА В РОССИИ

Муллабаев Виктор Наилович,
Орский гуманитарно-технологический институт (филиал) ОГУ, г.Орск

Аннотация

В статье представлен обзор этапов развития информационного общества в России, показаны возможности информационно-коммуникационных технологии в управлении государством и предоставлении государственных услуг обществу.

Ключевые слова: *электронное правительство, информационно-коммуникационных технологии, Электронная Россия, многофункциональный центр.*

Keywords: *e-government, information and communication technologies, Electronic Russia, multifunctional center*

Началом формирования информационного общества в современной России считается принятие Государственной думой документа Концепция информационной политики в 1998 году и разработка в 1998-1999гг. Концепции федеральной целевой программы (ФЦП) «Развитие информатизации в России на период до 2010 года». В 2000 году Россия подписала Окинавскую хартию глобального информационного общества, которая обязывала стран участниц способствовать устранению цифрового неравенства, развитию информационной экономики, электронного государства, электронной демократии, электронного правительства. В этих и предыдущих документах были определены стратегические направления движения России к информационному обществу. После 2000 г. в России началась административная реформа, которая предполагала существенную перестройку ключевых административных процедур в органах власти. Стандартом качества административной процедуры является административный регламент, который должен содержать название услуги, описание ожидаемого результата, процесс

оказания услуги, максимальные сроки ожидания выполнения, требования к инфраструктуре доступа к услуге, ссылки на нормативные акты, регулирующие предоставление услуги. Для реализации административных процедур в электронном виде на основе информационных систем в 2002 году была принята ФЦП «Электронная Россия 2002-2010», где были отмечены следующие направления:

• внедрение технологий электронного взаимодействия органов исполнительной власти с населением и организациями для предоставления государственных услуг, создание единой системы информационно-справочной поддержки населения и организаций для получения государственных услуг;

• создание стандартов электронного взаимодействия органов исполнительной власти и населения для оказания и получения государственных услуг;

• создание единой информационно-справочной системы с перечнем государственных услуг и описания процедур оказания этих услуг.

Основными исполнителями ФЦП «Электронная Россия» являлись Министерство экономического развития для проведения административной реформы и Министерство информационных технологии и связи отвечающий за технологическую инфраструктуру и ИТ-отрасль. При реализации первого этапа ФЦП (2002-2005гг) было поставлено много целей. Сюда входило: создание современной инфраструктуры информационно-коммуникационных технологии (ИКТ), совершенствование нормативно-правовой базы в сфере ИКТ, запуск пилотных проектов в регионах РФ по внедрению ИКТ-решений, поддержка и развитие национальной промышленности в области ИКТ, совершенствование взаимодействия государства с гражданами и организациями на основе ИКТ, создание средств межведомственного взаимодействия для федерального правительства на основе ИКТ, подготовка и переподготовка кадров для работы с ИКТ, решение проблемы информационного неравенства. В силу ряда как технических, так и организационных трудностей не удалось осуществить все цели. Так, например, отсутствовал закрепленный в нормативных правовых актах механизм реализации комплексной межведомственной программы. Здесь необходимо было учитывать не только интересы различных органов исполнительной власти федерального уровня, но и координировать работу с органами исполнительной власти регионального уровня и, особенно, с органами местного самоуправления.

Несмотря на все недостатки на первом этапе ФЦП (2002-2005 гг) были разработаны и внедрены ряд как инфраструктурных, так и инновационных проектов, среди которых можно отметить следующие информационные системы:

- системы принятия и поддержки управленческих решении;
- веб-сайты и порталы правительства РФ и различных органов исполнительной власти;

- многофункциональные центры (МФЦ) для оказания государственных услуг на местах;
- системы по проведению государственных закупок.

Подводя итоги по первому этапу можно отметить стремление органов власти на облегчение, прежде всего работы государственных служащих и сокращение собственных издержек на реализацию типовых процедур взаимодействия с гражданами и бизнесом. Поэтому на начальном этапе основной упор был сделан на формирование системы межведомственного электронного взаимодействия (СМЭВ).

Но поскольку, большинство государственных услуг граждане получают на региональном и муниципальном уровнях, то трудно реализовать государственное управление без активного участия регионов. Поэтому в 2006 г. ФЦП «Электронная Россия 2002-2010» была серьезно пересмотрена в сторону уменьшения прочих поставленных мероприятий и 17 июля 2006 правительством РФ была принята Концепция региональной информатизаций. Целью концепции был анализ социально-экономических проблем и потребностей региона и нахождение путей их решения на основе использования ИКТ. В 2007-2008гг. были разработаны первые типовые программно-технические комплексы для предоставления государственных услуг и решения задач государственного управления на региональном уровне.

В 2008 г. после преобразования Мининформсвязи в Минкомсвязи и полной смены руководства отрасли, ФЦП «Электронная Россия 2002-2010» была вновь пересмотрена и отмечены такие недостатки как излишне ведомственный характер Программы, отрицательно влияющий на качество взаимоотношении государства и общества. Поэтому в третьем релизе ФЦП «Электронная Россия» количество программных мероприятии еще более уменьшилось и в качестве основной цели было поставлено формирование инфраструктуры электронного правительства, призванной повысить качество взаимоотношений государства и общества, оперативность предоставления государственных и муниципальных услуг, эффективность межведомственного взаимодействия на основе использования ИКТ. Единый портал государственных услуг – сайт ogic.ru был запущен 1 января 2009 г., который работал в тестовом режиме и предоставлял в основном справочно-нормативную информацию. В августе 2009 года Правительство России определило компанию «Ростелеком» в качестве единственного исполнителя мероприятий программы «Электронная Россия» по проектированию и созданию инфраструктуры электронного правительства. В число данных мероприятий также было включено обеспечение предоставления государственных услуг в электронном виде через сеть Интернет. Новый единый портал государственных услуг от «Ростелекома» - сайт gosuslugi.ru вместо старого ogic.ru заработал в конце 2009 г. Сервис авторизации с личным кабинетом пользователя начал работать на портале с 1 апреля 2010 года. Это предоставило пользователям возможность регистрироваться на сайте и отправлять документы и заявления на оформление различных услуг.

27 июля 2010 г. был принят федеральный закон № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», который определяет принципы и процедуру предоставления государственных и муниципальных услуг, обязанности органов власти, права заявителей, условия и порядок оплаты услуг. По новому закону запрещается федеральным органам власти требовать у получателей услуг сведения, которые есть в распоряжении других ведомств. Необходимыми документами, государственные структуры должны обмениваться друг с другом в электронном виде без участия получателя услуг. Для этого разработана единая система межведомственного электронного взаимодействия (СМЭВ), связывающая воедино информационные системы государственных и региональных ведомств. Новая схема межведомственного взаимодействия служит для сокращения сроков предоставления государственных услуг, упрощения самой процедуры для потребителей услуг, уменьшения финансовых затрат граждан и юридических лиц и снижения коррупционных рисков. По закону № 210-ФЗ предполагаются разные способы обращения граждан за электронными государственными слугами – через веб-порталы, многофункциональные центры (МФЦ) по оказанию государственных услуг, специализированные информационные киоски (инфоматы) и с помощью «Универсальных электронных карт» (УЭК).

Итоги реализации ФЦП «Электронная Россия» на конец 2010 года показали невысокую эффективность исполнения программы. Главными причинами этого, считается недостаток финансирования, несовершенство нормативных актов, ведомственная разобщенность и недостаточное понимание органов власти в тонкостях проводимых мероприятиях. Несмотря на все недостатки в реализации ФЦП «Электронная Россия», есть и положительные результаты, среди которых появление большого внимания общества к вопросам информатизации в сфере управления государством. Граждане считают, что Интернет как средство общения с государством гораздо удобнее, чем очередь в приемной госучреждения. За восемь лет своего существования ФЦП «Электронная Россия» создала хорошую основу для перехода государственных структур в «бесконтактный» формат взаимодействия с обществом. После её завершения были сформулированы новые стратегические цели развития на ближайшую перспективу. Информационные технологии будут играть немаловажную роль в достижении этих целей. По мнению Минкомсвязи, главными итогами ФЦП «Электронная Россия (2002-2010 гг.)» стало создание системы межведомственного электронного взаимодействия (СМЭВ) и единого портала государственных услуг ЕПГУ. Эти проекты уже активно востребованы обществом. Например, на портале ЕПГУ ежемесячно регистрируется более 1,5 млн новых пользователей и летом 2017 года их количество достигло 50 миллионов. В это же время, количество доступных федеральных услуг в электронном виде на ЕПГУ стало более 350. Из наиболее популярных услуг можно отметить проверку судебной и налоговой задолженностей, штрафов ГИБДД, получение выписки с индивидуального лицевого счета в Пенсионном

фонде РФ, регистрацию автотранспортных средств в ГИБДД, получение водительских удостоверений, оформление загранпаспортов.

Для совершенствования достигнутых решений по ФЦП «Электронная Россия (2002-2010 гг.)» и выполнения новых мероприятий по информатизации общества 20 октября 2010 г. принята государственная программа «Информационное общество (2011-2020 гг.)». Проект программы «Информационное общество» включает следующие направления: создание электронного правительства, повышение качества жизни граждан, преодоление цифрового неравенства, обеспечение безопасности в информационном обществе, сохранение культурного наследия и развитие рынка ИКТ. При этом основную часть программы (25-30%) занимает создание электронного правительства. Минкомсвязи отказалось от так называемого отраслевого подхода. Если ранее, в стратегии развития информационного общества, были прописаны такие направления, как ИКТ в образовании, ИКТ в здравоохранении, ИКТ в культуре и т. д., то в программе «Информационное общество» все они объединены в одно направление повышения качества жизни граждан. Основа программы: результаты должны приносить реальную, ощутимую пользу населению. Повышение качества жизни должно выражаться в простых и доступных электронных услугах, которыми граждане пользуются почти ежедневно: получение больничного листка, запись на прием через интернет, доступный по цене широкополосный Интернет, возможность оплаты штрафа с мобильного телефона и другое. Все направления оформлены в виде четырех подпрограмм:

- Информационно-телекоммуникационная инфраструктура информационного общества;
- Информационная среда;
- Безопасность в информационном обществе;
- Информационное государство.

По программе «Информационное общество (2011-2020 гг.)» правительству Российской Федерации поручено обеспечить достижение следующих показателей:

а) уровень удовлетворенности граждан РФ качеством предоставления государственных и муниципальных услуг к 2018 году - не менее 90 процентов;

в) доля граждан, имеющих возможность получения государственных и муниципальных услуг в электронной форме, к 2018 году - не менее 70 процентов;

Ответственным исполнителем программы правительство назначило Министерство связи и массовых коммуникаций Российской Федерации. Главными показателями успешной реализации Программы станут рост индекса Российской Федерации в международном рейтинге стран по уровню развития информационных и телекоммуникационных технологий и увеличение количества граждан, пользующихся государственными услугами в повседневной жизни. По государственной программе доля населения РФ,

пользующаяся электронными государственными услугами к 2020 году должна увеличиться с 11% (данные 2010 года) до 85%.

Литература

1. Электронная Россия ФЦП — [Электронный ресурс]. — Режим доступа: http://www.tadviser.ru/index.php/Статья:Электронная_Россия_ФЦП

2. Электронное правительство России — [Электронный ресурс]. — Режим доступа: http://www.tadviser.ru/index.php/Статья:Электронное_правительство_России

3. Стырин Е.М. История формирования электронного правительства в России — [Электронный ресурс]. — Режим доступа: https://www.eos.ru/eos_delopr/eos_delopr_intesting/detail.php?ID=78993

4. Информационное общество ГП — [Электронный ресурс]. — Режим доступа: http://www.tadviser.ru/index.php/Статья:Информационное_общество_ГП

КОМПЛЕКСНЫЕ РЕШЕНИЯ ПРОГРАММИРОВАНИЯ ЧПУ ОБРАБОТКИ ПО 3D МОДЕЛИ

Сергиенко Светлана Николаевна,
Орский гуманитарно-технологический институт (филиал) ОГУ, г .Орск,
Кочковская Светлана Сергеевна,
Орский гуманитарно-технологический институт (филиал) ОГУ, г. Орск

Аннотация

В статье исследуются общие принципы программирования на станках с числовым программным управлением. Дана характеристика отечественных и зарубежных САПР. Уделено внимание применению программного модуля «КОМПАС ЧПУ»

Ключевые слова: *автоматизированное проектирование, управляющие программы, станки с ЧПУ*

Keywords: *computer-aided design, control programs, CNC machines*

В связи с применением вычислительной техники для автоматизации проектирования на сегодняшний день предлагается ряд способов кодирования и языков, позволяющие описывать конструктивно-технологические характеристики детали. Однако методы описания структуры изделий и технологических процессов разработаны еще не достаточно.

Алгоритмизация решения более сложных технологических задач в первую очередь основаны на синтезе и анализе структуры, функции и характеристик сложных объектов и процессов. В связи с этим все большее значение для развития методов автоматизированного проектирования приобретают системные исследования объектов и процессов проектирования.

Основу этих исследований составляет представление о конструкции детали.

Эксплуатация станков с ЧПУ возможна при наличии не только соответствующего технологического процесса, но и обеспечивающих его исполнение управляющих программ (УП). Поэтому программирование обработки для станков с ЧПУ отличается трудоемкостью и сложностью, требует от технолога высокой профессиональной подготовки, знания не только ряда технологических дисциплин, но и основ программирования, некоторых разделов математики.

Программирование технологических процессов для станков с ЧПУ — качественно новый этап, на котором выполняется значительная часть работы, перенесенная из сферы непосредственного производства в область его технологической подготовки. Так, действия квалифицированного рабочего, обрабатывающего заготовку на обычном станке, заменяются на станке с ЧПУ автоматической работой станка по управляющей программе, содержащей подробную информацию о последовательности и характере функционирования его исполнительных механизмов. Требования к квалификации оператора станка снижаются, так как задачи формообразования теперь решает технолог-программист на этапе подготовки УП.

При подготовке УП перерабатывается большой объем технологической информации. В ряде случаев поиск и нахождение оптимальных решений возможны лишь при широком использовании в процессе программирования электронно-вычислительных машин. Методы и организация подготовки УП на предприятиях зависят от доступа к ЭВМ, наличия и совершенства специального программно-математического обеспечения (ПМО), типизации технологических процессов, серийности изделий, профессионального уровня работников технологических служб. Развитие и широкое распространение в промышленности средств вычислительной техники, применение ЭВМ для управления участками станков и создание автоматизированных рабочих мест — все это создает предпосылки для полного перехода на автоматизиро¬ванную подготовку УП для станков с ЧПУ. При этом неизбежно слияние систем автоматизации программирования (САП) изготовления изделий с системами автоматизации их проектирования (САПР), что связано с решением насущного вопроса производства — комплексной автоматизации проектирования и изготовления.

На сегодняшний день существуют ряд прикладных программ, которые могут в автоматическом режиме построить алгоритм программы обработки неплоских деталей посредством 3D моделирования. Детали, которые проходят обработку на станках с числовым программным управлением рассматриваются с точки зрения объектов геометрии, основу которого составляет создание управляющих программ. Числовое программное управление это компьютеризированная система управления, которая способна считывать информацию специализированного языка программирования и управляющая приводами станка и оснастки. Интерпретатор CNC (Computer Numerical Control) системы это перевод входного языка в команды управления главным

приводом, приводом подач и так далее. Системы ЧПУ описываемые CNC, сформированы на микропроцессоре с операционной памятью, с операционной системой, у которой имеется собственный микроконтроллер. Программа может быть загружена с внешних носителей.

Управляющие программы для станков с ЧПУ могут создаваться следующими способами:

— с помощью стойки станков ЧПУ, так называемого цехового программирования;

— программирование на персональном компьютере с последующей передачей на стойку станка.

Как правило, второй вариант оказывается более приемлемым и действенным. Программирование происходит при помощи кода. Кодирование можно производить в любом текстовом редакторе.

В качестве языка программирования ЧПУ чаще всего используют G код, который обозначается как код ИСО 7-бит. Программы, написанные с использованием данного кода, имеют жесткую структуру, которые состоят из кадров. Каждый кадр заканчивается символом перевода строки и имеет номер (на первую строку программы выше сказанное не распространяется). Ошибки в написании программ обработки могут повлечь за собой различные сбои в работе станка. Поэтому надежнее было бы проводить визуализацию созданной программы обработки, прежде чем загрузить ее в работу. В этом случае программист может обнаружить ошибку, сымитировав процесс обработки при помощи симулятора, тем самым предотвратив выход из строя дорогостоящего оборудования. Такая симуляция получила название «бэкплот». Она дает возможность распознать ошибку при простом просмотре кода управляющей программы.

В качестве примера можно привести программный продукт «CIMCO» (рисунок 1)., который достаточно широко используют машиностроительные предприятия нашего региона. На рисунке изображена обработка детали с ошибочными кадрами перемещения инструмента. Однако, твердотельное моделирование позволяет проводить демонстрацию процесса удаления материала более полно, что позволяет рассмотреть деталь со всех сторон, тем самым увидеть все ее элементы, и правильность обработки без зарезов и столкновений [1]

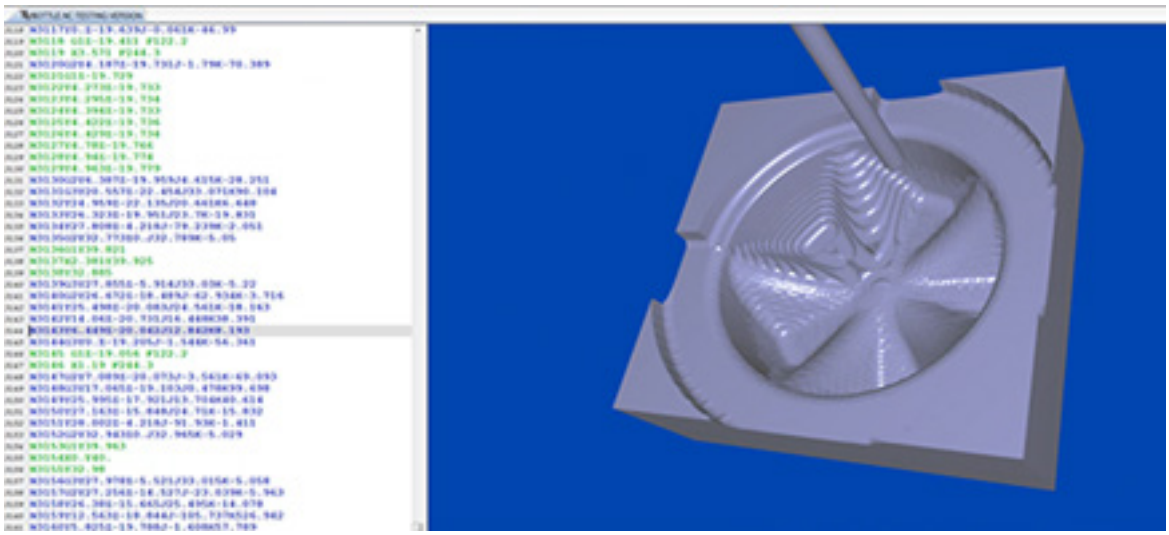


Рисунок 1 – Фрезерная верификация

В качестве альтернативы данному программному продукту можно предложить модуль «КОМПАС-ЧПУ», позволяющий создать 3D модель и технологический процесс обработки на металлорежущих станках с ЧПУ с последующей визуализацией обработки.

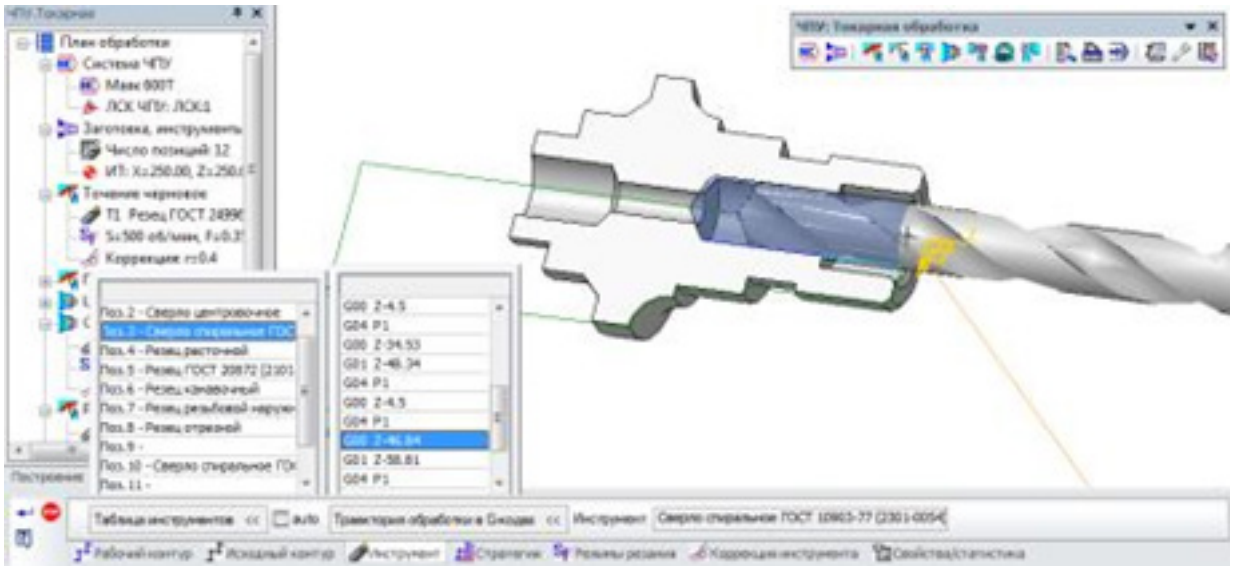


Рисунок 2 – Модуль ЧПУ системы «КОМПАС»

Для предприятия это означает сокращение срока подготовки изделий к производству — нет необходимости экспортировать данные из КОМПАС-3D в CAM-системы, нет потерь времени на конвертацию и исправление ошибок при некорректной передаче. Упрощается и работа инженера-технолога — он использует одну 3D-систему, не отвлекаясь на сторонние приложения, и уверен в точности данных, на основе которых разработана управляющая программа [2].

Работа приложения в составе КОМПАС-3D позволяет в автоматическом режиме перестраивать управляющую программу для станка с ЧПУ в случае изменения геометрии детали.

Литература

1. Малюх В.Н. Введение в современные САПР. – М.: ДМК Пресс, 2014. 192 с.ил ISBN 978-5-94074-986-8.
2. http://kompas.ru//-›Модуль ЧПУ токарная обработка.

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ И ОРГАНИЗАЦИИ

ОСОБЕННОСТИ УСТАНОВКИ СИСТЕМЫ УПРАВЛЕНИЯ КОНТЕНТОМ MODX

Богданова Вера Сергеевна, Подсобляева Ольга Валерьевна,
Орский гуманитарно-технологический институт (филиал) ОГУ, г. Орск

Аннотация

В статье рассмотрена структура системы управления пакетами, которая дает возможность администраторам сайтов управлять содержимым, шаблонами, дополнениями и даже самими сайтами удаленно. Все работает из единого интерфейса внутри Менеджера системы. Подробно описаны этапы и особенности установки систему управления контентом MODx.

Ключевые слова: *Инструмент управления содержимым, программирование, сайт, установка*

Keywords: *Instrument of management of contents, programming, website, installation*

MODx имеет открытый исходный код и открытую лицензию. Система написана на языке программирования PHP, для хранения данных использует СУБД MySQL, и является платформой для разработки web-приложений.

Данная система, является мощным инструментарием для развертывания и защиты сайта, web-приложения.

Имеется возможность создания пользователей и различных вариантов их группировок, отделенных от администрирования сайта. При этом есть возможность разрешить одним пользователям просмотр одних ресурсов, а другим пользователям будут доступны другие ресурсы и возможности. Аутентификация производится через встроенную систему пользователей, службу каталогов Active Directory, OpenID, и любую другую систему, которая может использовать MODx API.

Инструмент управления содержимым дает полный контроль над всеми элементами сайта, например, позволяет копировать, удалять, редактировать как отдельные документы, так и целые папки с их содержимым.

MODx имеет особую систему шаблонов, благодаря которой программный код полностью отделен от разметки страницы, без подключения для этого дополнительных плагинов, модулей, расширений. В отличие от других систем, требующих подробного изучения темизации, в MODx пользователь работает с HTML напрямую, что позволяет без дополнительных усилий полностью контролировать вывод информации

Архитектура MODx полностью соответствует требованиям безопасности. Каждый ввод данных фильтруется, и каждое обращение к базе данных выполняется через специально-подготовленные запросы, которые устраняют возможность SQL инъекции.

Система управления пакетами, дает возможность администраторам сайтов управлять содержимым, шаблонами, дополнениями и даже самими сайтами удаленно. Все работает из единого интерфейса внутри Менеджера системы.

К основным преимуществам можно отнести:

– полный контроль над выводом HTML-кода, разделение логики работы CMS и дизайна;

– возможность создавать программный код в сниппетах, модулях и плагинах, а также подключать параметры Template Variable (TV) для создания дополнительных полей;

– поддержка AJAX, MooTools, prototype;

– графический web-установщик;

– поддержка PHP 4.3.11 и выше;

– кросс-браузерность и кросс-платформенность работы;

– возможна установка на IIS, Apache, Nginx, Lighttpd и Zeus web -сервера;

– возможно размещение в «облаке» через Amazon Elastic Compute Cloud;

– полный контроль над всеми метаданными и структурой URL для поисковой оптимизации;

– совместимость с MVC (Model-View-Controller);

– контроль доступа и назначение прав для доступа к менеджеру сайта ACL;

– возможность настройки менеджера под нужды заказчика;

– репозиторий готовых расширений.

Для установки данной системы на локальный сервер необходимо на официальном сайте MODx скачать архив с последней версией системы. В папке «home» на локальном сервере создать папку с названием сайта латинскими буквами, в которой создается корневая папка «www». Затем следует извлечь файлы архива в папку «www» и переименовать файл ht.access в .htaccess, для поддержки дружественных URL.

После изменений в корневой папке локального сервера, его требуется перезапустить.

Для продолжения установки MODx следует в адресной строке браузера, ввести название сайта, которое совпадает с названием созданной папки. В окне предупреждения нужно перейти по ссылке «install now», после чего будет предложено выбрать язык установки. Из выпадающего списка следует выбрать русский язык. Затем на следующем шаге нужно выбрать пункт «New Installation» нажать кнопку «Next».

На следующей странице, изображенной на рисунке 1, необходимо сделать подключение к базе данных. Для этого следует заполнить поля с данными о пользователе и базе данных, в поле «метод соединения» выбрать

SET NAMES и указать кодировку utf8_general_ci. После подключения к базе данных становятся доступны поля для настройки панели администратора, где указываются логин и пароль суперадминитратора, а так же выбирается язык, который будет использоваться MODx по умолчанию.

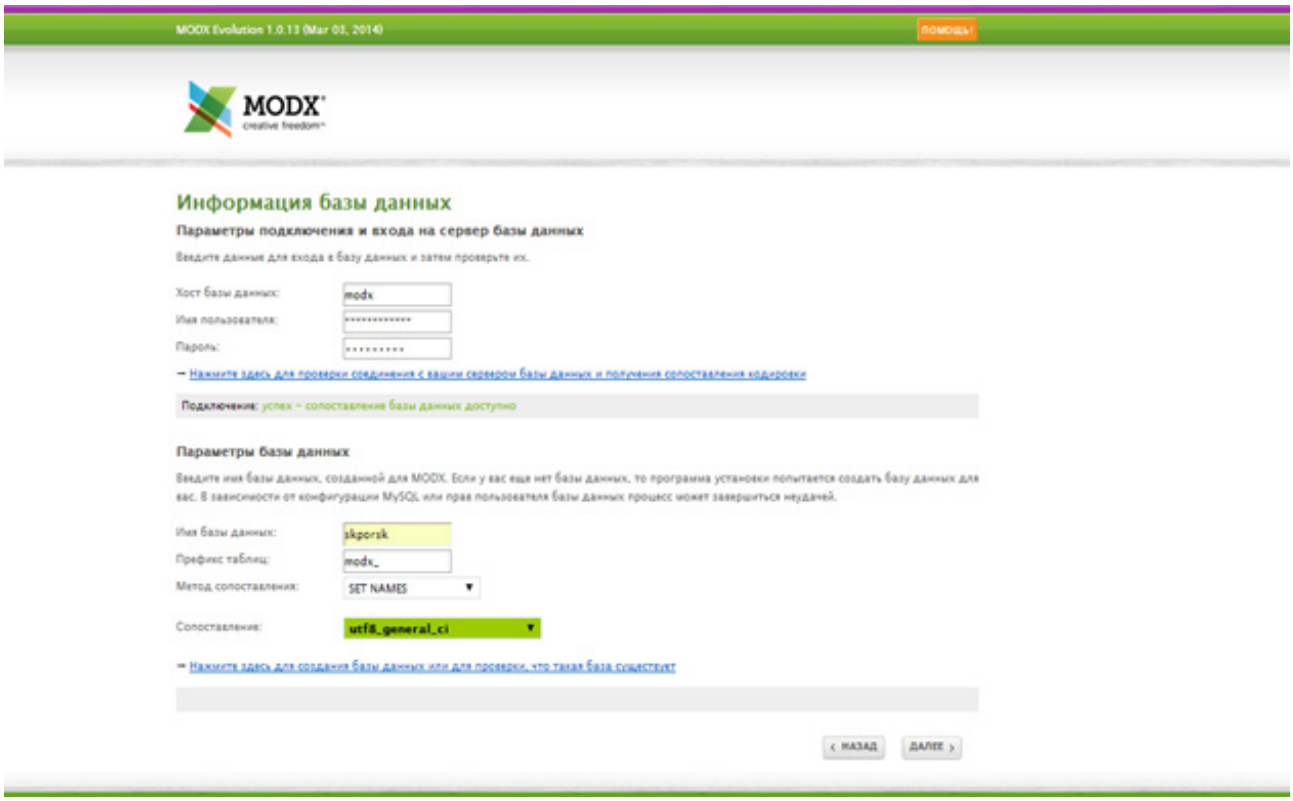


Рисунок 1 – Окно подключения к базе данных.

Все настройки возможно будет изменить в дальнейшем из панели администратора.

Для продолжения установки необходимо установить галочку о принятии лицензии и нажать кнопку «установить».

В конце папка Install будет удалена, для обеспечения безопасности сайта.

На рисунке 2 изображено завершение установки системы.

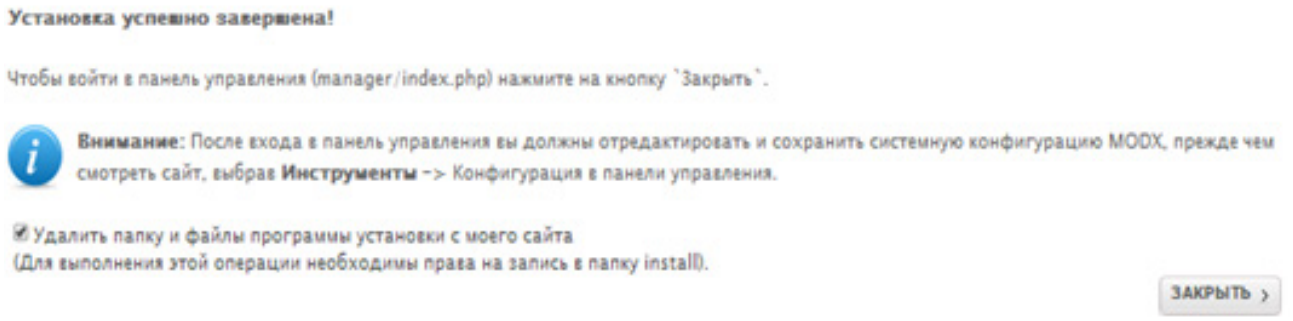


Рисунок 2 - завершение установки MODx.

Система MODx включает в себя управление такими элементами как шаблоны, параметры (TV), чанки, сниппеты, плагины.

Шаблон - это обычная HTML-разметка, описывающая структуру и дизайн отображения страницы и ее элементов, содержащая ссылки на CSS-документы и другие объекты, определяющие ее визуальное отображение. Шаблон может содержать вызовы сниппетов, чанков, параметров (TV).

Каждый из загруженных или созданных шаблонов можно подключать как к отдельному ресурсу, так и к группе ресурсов.

Параметры (TV) - это динамические элементы шаблона, получающие значения из различных источников данных, обозначенных при создании параметра. Существуют и предопределенные параметры, которые для конкретного ресурса имеют свои значения, например, предопределённый параметр [*pagetitle*] содержит заголовок страницы. Параметры могут иметь различный тип данных и разное значение на различных страницах сайта.

Для того чтобы использовать параметр нужно вставить в шаблоне или в области контента выражение [*Name*], где Name- имя присвоенное параметру.

Чанк-это фрагмент HTML кода, который многократно используется при создании сайта.

Например, если какая-то часть кода HTML повторяется несколько раз, но вносить изменения требуется сразу везде, где встречается этот повторяемый фрагмент кода, то создается чанк, где в качестве содержимого используется этот повторяемый код. После чего, вместо этих повторяемых блоков, можно вставить вызов, созданного чанка. Таким образом, при необходимости внести какие-то изменения в повторяемые блоки, эти изменения вносятся в созданный чанк. Чанки не могут прямо содержать исполняемый код, однако могут включать в себя вызовы сниппетов, параметров (TV), обеспечивающих динамическую логику.

Использование чанка может осуществляется в шаблоне, в области контента, в коде другого чанка, в параметре (TV). Для вызова чанка следует указать его имя, помещенное в двойные фигурные скобки.

Сниппет — это PHP код, который может быть вызывать из шаблона, обеспечивающий динамическую логику. Сниппеты позволяют отделить бизнес-логику от структуры и представления данных на web-странице. Сниппеты могут принимать параметры и выводить какой-либо результат. В месте вызова сниппета, вставляется его результат. С помощью сниппетов можно создать генерацию динамического меню, вывод ресурсов или контента по какому-либо условию, форму обратной связи.

Вызов осуществляется по имени сниппета, помещенного между квадратными скобками с восклицательными знаками, если же будут указываться параметры, то после имени сниппета, вместо восклицательного знака, ставиться вопросительный знак.

Так же при вызове сниппета, можно отправлять ему на обработку различные значения параметров. Обычно, у каждого сниппета имеется свой

набор поддерживаемых параметров, от которых зависит выводимый сниппетом результат. В качестве параметров можно использовать чанки, или другие сниппеты.

Для того чтобы передать некоторые значения параметров следует использовать конструкцию: [!Имя_сниппета? &параметр=`значение`!].

В комплекте с MODx идут такие полезные сниппеты, как Ditto, eForm, UltimateParent, Wayfinder, AjaxSearch.

Плагины - это интерактивные PHP-скрипты. Запускаются при наступлении события, которое они отслеживают.

Для каждого шаблона можно добавить дополнительные поля, которые затем можно выводить на странице с помощью специальных плейсхолдеров. Это дает небывалую гибкость в разработке.

Элементы можно изменять, и создавать новые.

Все это делает MODx отличной платформой для создания разнообразных web-сайтов.

Литература

1. Галатенко, В. А. Основы информационной безопасности / В. А. Галатенко. – М. : Интернет-университет информационных технологий – www.INTUIT.ru, 2014. – 208 с.

2. Галатенко, В. А. Стандарты информационной безопасности / В. А. Галатенко. – М. : Интернет-университет информационных технологий – www.INTUIT.ru, 2010. – 264 с.

3. Lonely, R. Алгоритм шифрования данных с открытым клю-чом RSA [Эл. ресурс] / R. Lonely.– URL :www.rusdoc.ru/material/raznoe/rsa.shtml

4. Антивирусная защита компьютерных систем : курс лекций для Интернет-университета информационных технологий от лабора-тории Касперского – М. : Интернет-университет информационных технологий –www. INTUIT.ru, 2011. – URL : www.intuit.ru/department/security/antiviruskasp/

5. Вирусы и средства борьбы с ними : курс лекций для Интер-нет-университета информационных технологий от лаборатории Кас-перского – М. : Интернет-университет информационных технологий – www.INTUIT.ru, 2011. – URL : www.intuit.ru/department/security/viruskasper/

6. Мэйволд, Э. Безопасность сетей : курс лекций для Интернет-университета информационных технологий / Э. Мэйволд. – М. : Ин-тернет-университет информационных технологий – www.INTUIT.ru, 2012. – URL :www.intuit.ru/department/security/netsec/

7. Кобб, М. Безопасность IIS : курс лекций для Интернет-университета информационных технологий / М. Кобб, М. Джост. – М. : Интернет-университет информационных технологий – www.INTUIT.ru, 2013. – URL:www.intuit.ru/department/internet/iissecurity/

8. Малюк, А. А. Информационная безопасность : концептуаль-ные и методологические основы защиты информации : уч. пособие для вузов / А. А. Малюк. – М. : Горячая линия – Телеком, 2014. – 280 с.

СТЕГАНОГРАФИЧЕСКОЕ СОКРЫТИЕ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ BITMAP ФАЙЛОВ

Зияутдинов Владимир Сергеевич, Воронин Илья Васильевич, Селищев Олег Владимирович, Золотарева Татьяна Александровна
Липецкий государственный педагогический университет имени П.П.Семенова-Тян-Шанского, г. Липецк

Аннотация

В статье рассматривается алгоритм стеганографического сокрытия информации и приводится программный продукт, реализующий данный алгоритм с использованием несжатых графических файлов.

Ключевые слова: *стеганография, защита информации, сокрытие информации, сообщение, контейнер*

Keywords: *steganography, protection of information, withholding information, message, container*

Задача защиты информации от несанкционированного доступа была поставлена и решалась человечеством очень давно. Два основных направления, существующие и в наше время, для решения этой задачи были определены еще в древнем мире. Это стеганография и криптография. [2]

В отличии от криптографии, целью которой является шифрование информации и превращение ее в нечитаемый вид с последующей передачей по открытому каналу, целью стеганографии является сокрытие факта передачи информации. Существует много различных стеганографических методов сокрытия информации, но всех их объединяет тот факт, что сокрытие сообщения происходит путем встраивания в обычный объект, который не привлекает внимания, после чего данный объект передается любым открытым способом.

Главными определениями в стеганографии являются сообщение и контейнер. Сообщение – это засекреченные данные, наличие которых надлежит спрятать. Контейнер – это открытая информация, которую возможно применить для сокрытия сообщения. В мире цифровых технологий контейнерами могут являются любые мультимедийные файлы. Пустой контейнер – это контейнер, не содержащий секретных сведений. Заполненный контейнер – контейнер, в котором расположены секретные сведения. [3]

Одним из основных условий для применения стеганографических методов сокрытия информации является то, что заполненный контейнер должен быть неотличим от пустого контейнера. Для этого необходимо разобраться в структуре файла-контейнера и выбрать места для закладки сообщения.

В качестве сообщения будет использоваться обычный текстовый файл с расширением txt, в качестве файла-контейнера будет использован графический файл с расширением bmp. Файлы формата BMP (BitMap) являются стандартным типом файлов Windows для хранения растровых изображений

без сжатия. В современных BMP-файлах цвет каждого пиксела (точки) представляется 24-мя битами (бит/пиксель), данный параметр называется глубиной цвета. Этот параметр задает количество цветов, которое может принять каждая точка изображения. Например, монохромное изображения в данном формате имеет глубину цвета в 1 бит/пиксель, что соответствует двум цветам. Таким образом, 24-битное изображение может содержать 2^{24} = 16 777 216 цветов. Каждый цвет пиксела кодируется в формате RGB, что соответствует интенсивности красного, синего и зеленого цвета.

Различные исследования показали, что человеческий глаз не различает такое большое количество оттенков, что позволяет использовать bmp файлы в качестве стеганографических контейнеров. Человеческое зрение имеет низкую чувствительность к колебаниям в оттенках синего цвета. Именно поэтому внедрение информации часто производят используя B-составляющие RGB-структур [1]. Но использование только синей составляющей негативно сказывается на размере информации, скрываемой в контейнере.

При разработке программы были учтены исследования доказывающие, что человеческий глаз плохо отслеживает изменение в младшем бите R-составляющей, 2-х младших битах G-составляющей и 4-х битах B-составляющей 24-битного изображения (рис. 1).

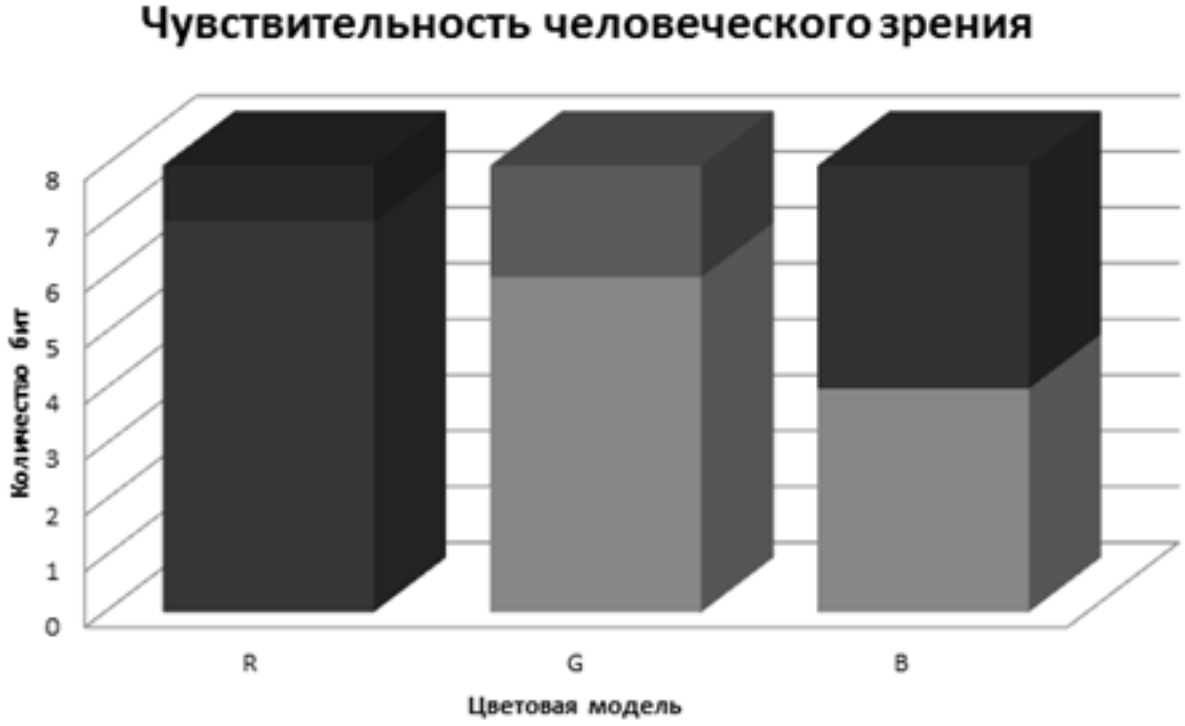


Рис. 1. Чувствительность человеческого зрения к изменениям различных цветов

Используя данные сведения можно увеличить объем передаваемой информации в одном контейнере без значительного ухудшения сокрытия информации. В таблице 1 представлен сравнительный анализ различных методов.

Таблица 1. Зависимость объема скрываемой информации от объема контейнера при замещении различных битов исходного контейнера

Размер файла / Метод	1 440 000 байт (800*600 пикселей)	2 764 800 байт (1280x720 пикселей)
Замена младшего B-бита	60 000 байт	115 200 байт
Замена всех младших битов	180 000 байт	345 600 байт
Замена предложенных битов	420 000 байт	806 400 байт

В качестве исходного файла используется 24-битовый bmp файл, имеющий следующую структуру:

1. На заголовок отводится 14 байт, из них 2 байта на принадлежность файла к формату BMP, эти данные постоянны и они могут использоваться для определения факта отнесения файла к данному формату. В следующих 4 байтах содержится информация о размере файла, данная информация понадобится для определения возможности кодировки сообщения. Далее следуют два блока по 2 байта, которые не используются в определении формата файла, но они могут использоваться для внесения служебной информации при сокрытии информации. Последний блок в заголовке объемом 4 байта используется для определения адреса начала растрового массива, эта информация будет использоваться для определения начального адреса изменяемых данных.

2. Далее идет информационный 40-ка байтовый заголовок массива растровых данных. Сюда входит информация о ширине и высоте изображения, глубина цвета и другая информация.

3. Далее идет растровый массив. Он не имеет фиксированного значения, т.к. в нем хранится информация о каждом пикселе изображения (интенсивность каждой составляющей цветовой модели RGB). Объем растрового массива можно вычислить по формуле:

$$V_{р.м} = ширина * высота * глубинацвета$$

Именно данные растрового массива подвергаются изменению и в него записывается передаваемая информация. Помимо этого для правильной работы алгоритма, необходимо учитывать количество внедренной информации, оно будет записываться в неиспользуемое поле в заголовке файла. Блок схема работы алгоритма представлена на рисунке 2.

Рис. 2. Блок схема работы программы

Основной технической особенностью bitmap файлов является тот факт, что при хранении информации в 24-битовом файле каждому пикселю соответствует три последовательных байта, которые хранят информацию об интенсивности основных цветов в последовательности BGR, а не RGB. Эту особенность необходимо учитывать при замене младших битов.

Многие программы обнаружения стегановставок ориентированы на выявление текстовой информации в младших битах каждого байта изображения. Другими словами производится поиск ASCII кодов символов, применяемых для написания сообщения. Для скрытия присутствия данных символов был разработан алгоритм замены символов, которые применяются при написании сообщения, на неприменяемые при письме (рис. 3).

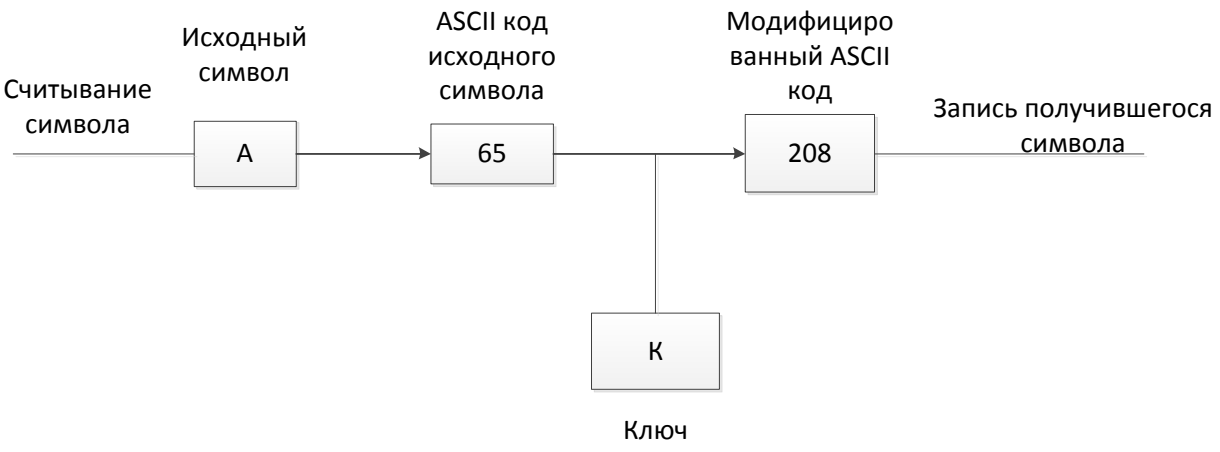


Рис. 3. Процесс модификации исходного символа

При этом ключ можно использовать заранее согласованный между получателем и отправителем сообщения, или вставлять его в передаваемое изображение, например в строку заголовка.

Предложенный алгоритм стеганографического преобразования был реализован в виде Windows приложения (рис. 4). Данное приложение обладает дружественным, интуитивно понятным интерфейсом и позволяет производить кодировку и раскодировку информации предложенным методом.

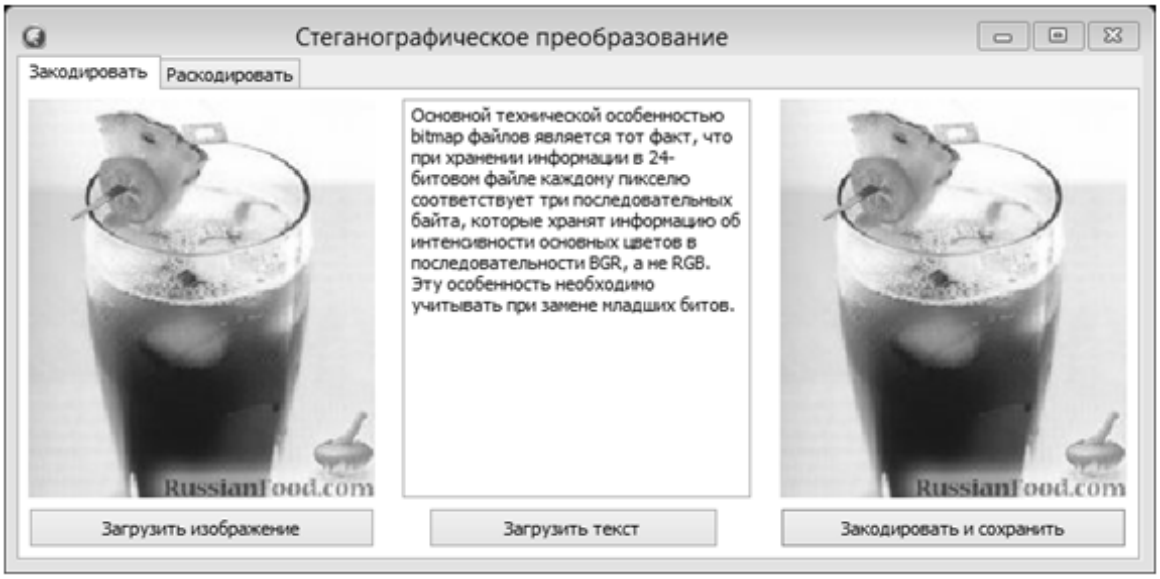


Рис. 4. Окно разработанного приложения

Исследование работы алгоритма на выявление стеганографических вставок человеческим глазом проводилась на группе людей, которым предлагалось из двух изображений (обработанное программой и исходный вариант) выбрать изображение, в котором, по их мнению, присутствуют скрытые данные. Исследования показали, что люди не могут определить изображение со скрытой информацией, процент правильных ответов носит случайный характер.

Литература:

1. Watson A. The cortex transform: rapid computation of simulated neural images // Computer Vision, Graphics, and Image Processing. 1987. Vol. 39. № 3. P. 311-327.

2. Коробейников А.Г., Математические основы криптографии. Учебное пособие// СПб ГИТМО (ТУ), 2002, 41 с.

3. Скрыпкин В.В., Воронин И.В. Сравнительный анализ стеганографических методов защиты информации, передаваемой при помощи растровых изображений // Информационные технологии в процессе подготовки современного специалиста: Межвузовский сборник статей. – Липецк: ФГБОУ ВПО «ЛГПУ», 2015. – Выпуск 19. С. 94-100.

ОСНОВНЫЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Мурзаков Александр Владимирович,
Орский гуманитарно-технологический институт (филиала) ОГУ, г. Орск

Аннотация

В статье рассматриваются понятие информационной безопасности, её основные составляющие, способы обеспечения информационной безопасности в организации.

Ключевые слова: *информационная безопасность, защита информации, доступность, конфиденциальность, целостность.*

Keywords: *information security, information security, accessibility, confidentiality, integrity.*

Появление новых информационных технологий и развитие мощных компьютерных систем хранения и обработки информации повысили уровни защиты информации и вызвали необходимость в том, чтобы эффективность защиты информации росла вместе со сложностью архитектуры хранения данных.

В реальной деятельности любой организации защита экономической информации становится обязательной. Разрабатываются всевозможные документы по защите информации; формируются рекомендации по защите информации; действует Федеральный Закон о защите информации, который рассматривает проблемы защиты информации и задачи защиты информации, а также решает некоторые уникальные вопросы защиты информации.

Таким образом, угроза защиты информации сделала средства обеспечения информационной безопасности (ИБ) одной из обязательных характеристик информационной системы.

На сегодняшний день существует достаточно много систем хранения и обработки информации, где в процессе их проектирования фактор информационной безопасности хранения конфиденциальной информации имеет особое значение. К таким информационным системам можно отнести, например, банковские или юридические системы безопасного документооборота и другие информационные системы, для которых обеспечение защиты информации является жизненно важным для защиты информации в информационных системах.

Другими словами, вопросы защиты информации в информационных системах решаются для того, чтобы изолировать нормально функционирующую систему от несанкционированных управляющих воздействий и доступа посторонних лиц или программ к данным с целью хищения.

Под информационной безопасностью следует понимать защищенность информации от случайных и преднамеренных воздействий естественного

или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации.

Целью ИБ является обезопасить ценности системы, защитить и гарантировать точность и целостность информации, минимизировать разрушения, которые могут иметь место, если информация будет модифицирована или разрушена.

На практике важнейшими являются три аспекта информационной безопасности: доступность, целостность и конфиденциальность. Доступность - возможность за разумное время получить требуемую информационную услугу. Целостность - ее защищенность от разрушения и несанкционированного изменения. Конфиденциальность - защита от несанкционированного прочтения. Именно доступность, целостность и конфиденциальность являются равнозначными составляющими ИБ.

Нарушение каждой из трех категорий приводит к нарушению ИБ в целом. Так, нарушение доступности приводит к отказу в доступе к информации, нарушение целостности приводит к фальсификации информации и, наконец, нарушение конфиденциальности приводит к раскрытию информации.

Выделение этих категорий в качестве базовых составляющих информационной безопасности обусловлено необходимостью реализации комплексного подхода при обеспечении режима ИБ. Кроме этого, нарушение одной из этих категорий может привести к нарушению или полной бесполезности двух других. Например, хищение пароля для доступа к компьютеру (нарушение конфиденциальности) может привести к его блокировке, уничтожению данных (нарушение доступности информации) или фальсификации информации, содержащейся в памяти компьютера (нарушение целостности информации).

Обеспечение ИБ не одноразовый акт. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования и развития системы защиты, непрерывном контроле ее состояния, выявлении ее узких и слабых мест и противоправных действий.

ИБ может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты на всех этапах обработки информации. Наибольший эффект достигается тогда, когда все используемые средства, методы и меры объединяются в единый целостный механизм - комплексную систему защиты информации.

На практике выделяют следующие направления ИБ:

− правовая защита - это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;

− организационная защита - это регламентация деятельности и взаимоотношений исполнителей на нормативно-правовой основе исключающая или ослабляющая нанесение какого-либо ущерба исполнителем;

– инженерно-техническая защита - это использование различных технических средств, препятствующих нанесению ущерба коммерческой деятельности

Защита информации строится на следующих принципах: построение системы информационной безопасности; принцип обеспечения надежности системы защиты информации; непрерывность развития системы управления информационной безопасностью.

Построение системы ИБ в организации требует к себе системного подхода, который предполагает оптимальную пропорцию между организационных, программных, правовых и физических свойств ИБ РФ, подтвержденной практикой создания средств защиты информации по методам защиты информации, применимых на любом этапе цикла обработки информации системы.

Для любой концепции ИБ, тем более, если используются методы защиты информации в локальных сетях и компьютерных системах, принцип непрерывного развития является основополагающим, ведь ИБ постоянно подвергается все новым и новым с каждым разом еще более изощренным атакам, поэтому её обеспечение в организации не может быть разовым актом, и созданная однажды технология защиты информации, будет постоянно совершенствоваться вслед за ростом уровня взломщиков.

Один из методов достижения ИБ - обеспечение средств борьбы с вредоносным ПО. Например, программы для защиты информации и система защиты информации от вирусов. Целесообразность построения системы защиты информации заключается в превышении суммы ущерба при взломе системы защиты информации на предприятии над стоимостью разработки средства защиты компьютерной информации, защиты банковской информации и комплексной защиты информации.

Важно знать, что характерной особенностью электронных данных является возможность легко и незаметно искажать, копировать или уничтожать их. Поэтому необходимо организовать безопасное функционирование данных в любых информационных системах, т.е. защищать информацию.

Наибольший ущерб информации наносят неправомерные действия самих сотрудников и компьютерные вирусы. Для защиты информации в компьютерах и информационных сетях широко используются разнообразные программно-технические средства защиты. Они включают различные системы ограничения доступа на объект, сигнализации и видеонаблюдения.

К наиболее практикуемым способам защиты информации относится её кодирование, предполагающее использование криптографических методов ~~защиты информации. Оно не спасает от физических воздействий, но в~~ остальных случаях служит надёжным средством. Другой метод предполагает использование устройств, ограничивающих доступ к объектам и данным.

Комплексно мероприятия по обеспечению сохранности и защиты информации, объектов и людей включают организационные, физические,

социально-психологические мероприятия и инженерно-технические средства защиты.

Литература

1. Гришина, Н. В. Информационная безопасность предприятия. Учебное пособие / Н.В. Гришина. - М.: Форум, 2015

2. Организация безопасной работы информационных систем: учебное пособие / Ю.Ю. Громов, Ю.Ф. Мартемьянов, Ю.К. Букурако и др.; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». - Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2014. - 132 с.: ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=277794, коэффициент книгообеспеченности 1.

3. Сурина, Е.Е. Современные проблемы и задачи обеспечения информационной безопасности СИБ – 2017: Международная научно-практическая конференция (г. Москва, 18 апреля 2017 г.) [Текст]: сборник статей / Московский финансово-юридический университет МФЮА. – М.: МФЮА, 2017. ISBN 978-5-94811-232-9, с. 79-86

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ (ПРЕДПРИЯТИЯ) И ПУТИ ИХ РЕШЕНИЯ.

Сенаторов Вячеслав Владимирович,
Орский гуманитарно-технологический институт, филиал ОГУ, г. Орск,
Юхимчук Виктор Александрович,
Орский гуманитарно-технологический институт, филиал ОГУ, г. Орск

Аннотация

В статье говорится о том, какие угрозы в сфере информационных технологий могут возникнуть и стоит опасаться. А также как обезопасить себя или свою организацию от информационных угроз.

Ключевые слова: *Информация, информационная безопасность, угроза, защита.*

Keywords: *Information, information security, threat, protection.*

Приватная информация на данный момент представляет собой огромный интерес не только для конкурирующих организаций (предприятий). Именно она становится причиной посягательства со стороны злоумышленников.

Множество проблем связано с неполноценной защиты от угроз, в результате чего для организации (предприятия) это может повлечь большие проблемы. Даже единичный случай халатности не только рабочего персонала, но и разработчиков, может принести организации (предприятия) денежные убытки и потери клиентской базы.

Угрозам подвергается информация о статусе и деятельности организации (предприятия). Деятельность по защите, охраняемой обладателями информации, в первую очередь, связана с предотвращением утечки конфиденциальной информации.

Выделяют основные виды конфиденциальной информации:

- Служебная тайна
- Адвокатская тайна
- Коммерческая тайна
- Профессиональная тайна
- Врачебная тайна
- Налоговая тайна
- Персональные данные и другие

Виды и особенности информационных угроз.

Потеря охраняемой информации происходит из-за нарушения работы с конфиденциальной информации. Мы разделим каналы утечки информации на несколько групп:

I. К первой группе относят каналы, образующиеся за счет дистанционного скрытого видеонаблюдения, фотоматериалов, чтения данных с помощью электронных носителей.

II. Во вторую группу включают наблюдение за информацией в процессе её обработки с целью запоминания и последующего хищения носителей.

III. К третьей группе относят несанкционированное подключение к специальной аппаратуре или к устройствам системы или линиям связи. Тем самым злоумышленники выводят из строя механизмы защиты и получают доступ ко всей информации.

IV. К четвертой группе относится незаконное получение информации путем подкупа или шантажа должностных лиц, знакомых, работающих в данной деятельности.

Обеспечение информационной безопасности организации (предприятия).

Важнейшим процессом защиты систем достигается целым комплексом организационных мер. В их составе антивирусная система, защита межсетевого экранирования и электромагнитного излучения. Системы защищают информацию на электронных носителях, передаваемые по каналам связи данные, разграничивают доступ к разноплановым документам, создают запасные копии и восстанавливают конфиденциальную информацию после повреждений.

Полноценное обеспечение информационной безопасности на предприятии должно быть стандартизировано и находиться под полным контролем круглогодично, в реальном времени в круглосуточном режиме.

При этом система учитывает весь жизненный цикл информации, начиная с момента появления и до полного её уничтожения или потери значимости для предприятия.

К способам защиты информации можно отнести:

- организация охраны организации;
- меры защиты, включающие контроль доступа в помещения;
- тщательный подбор персонала;

Более подробнее можно рассмотреть такой вид защиты электронной информации как криптографическая защита информации. Она представляет собой защиту информации с помощью ее криптографического преобразования.

Одним из самых распространенных средств защиты электронной информации в организациях является использование электронной подписи. Электронная подпись — это информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Сертифицированные средства криптографической защиты, полученные в удостоверяющем центре, не только подтверждают действительность электронной подписи, но и обеспечивают безопасность электронной информации.

Основные определения и критерии классификации угроз

Угроза - это потенциальная возможность определенным образом нарушить информационную безопасность.

Попытка реализации угрозы называется атакой, а тот, кто предпринимает такую попытку, - злоумышленником. Потенциальные злоумышленники называются источниками угрозы.

Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении).

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется окном опасности, ассоциированным с данным уязвимым местом. Пока существует окно опасности, возможны успешные атаки на ИС.

Наиболее значимые атаки последнего года

27 июня 2017 года началось массовое распространение новой модификации программы. На этот раз вирус использует те же уязвимости системы, что и WannaCry

WannaCry червь -шифровальщик, отличительной особенностью которого является функция саморазмножения, обычно отсутствующая у классических шифровальщиков.

Для заражения этим шифровальщиком не надо ничего делать, достаточно иметь уязвимое подключение к интернету. При заражении компьютера с операционной системой Windows появляется окно с требование оплатить на bitcoin кошелек минимальную сумму в 300$ для возврата доступа к не поврежденной файловой системе.

Рисунок 1 - Окно вируса WannaCry

Обратите внимание на рисунок 1 — от пользователя не требуется никакой реакции. За счет чего это стало возможным? Тут все просто — авторы WannaCry воспользовались утечкой из ShadowBrokers, в результате которой миру стали известны множество ранее неизвестных уязвимостей и способов проведения атак. Среди них была и уязвимость ETERNALBLUE и связанный с ней бэкдор DOUBLEPULSAR.

Первая позволяла через уязвимый SMB получать удаленный доступ к компьютеру и незаметно устанавливать на него программное обеспечение. Так и устанавливается шифровальщик WannyCry. Компания Microsoft еще в марте выпустила соответствующий патч для данной уязвимости, но, как показывает опыт, многие администраторы по разным причинам не удосужились его установить на свои компьютеры.

Уязвимость ETERNALBLUE присутствует на всех версиях Windows, исключая Windows 10. Учитывая наличие в мире большого числа уже неподдерживаемых компанией операционных систем семейства Windows (Windows XP, Windows 8, Windows Server 2003) и масштаб атаки, Microsoft пошла на беспрецедентный шаг и выпустила патчи и для этих ОС.

Литература

1. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — М.: КноРус, 2013.
2. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. — М.: ДМК, 2014.
3. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. — М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013.
4. Васильков, А. В. Безопасность и управление доступом в информационных системах / А.В. Васильков, И.А. Васильков. - М.: Форум, 2015.
5. Гафнер, В. В. Информационная безопасность / В.В. Гафнер. - М.: Феникс, 2014.
6. Гришина, Н. В. Информационная безопасность предприятия. Учебное пособие / Н.В. Гришина. - М.: Форум, 2015.
7. Чипига, А. Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. - М.: Гелиос АРВ, 2013.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ НА ПРЕДПРИЯТИИ. ПРИЧИНА УТЕЧКИ ИНФОРМАЦИИ.

Якунин Илья Алексеевич,
Орский гуманитарно-технологический институт (филиал ОГУ), г. Орск,
Мельников Александр Евгеньевич,
Орский гуманитарно-технологический институт (филиал ОГУ), г. Орск
Стародубцев Евгений Николаевич,
Орский гуманитарно-технологический институт (филиал ОГУ), г. Орск
Быков Евгений Александрович,
Орский гуманитарно-технологический институт (филиал ОГУ), г. Орск

Аннотация

В статье рассматривается защита персональных данных на предприятии. Приведены базовые классы защиты, мероприятия по обеспечению безопасности данных и подсистемы, осуществляющие эти мероприятия. Разбираются основные причины утечки информации и принципы организационной защиты информации.

Ключевые слова: *информация, система, безопасность, защита*

Keywords: *information, system, security, protection*

В настоящее время человек в своей повседневной рабочей среде постоянно находится в некой информационной сети. Вся информация, которая собрана на работника какого-либо предприятия, всевозможные отчёты и сводки, приказы и документы, всё это является важнейшими данными для каждой организации.

И каждая организация, в свою очередь, заботится об информационной безопасности всех своих данных. А в особенности, защитой персональных данных каждого работника. Так в чем же заключается обеспечение информационной защиты данных. Сначала нужно понять, что представляет собой информационная безопасность на предприятии и система защиты информации. Какие существуют угрозы повреждения или утечки данных. И какими средствами осуществляется защита информации.

Информационная безопасность на предприятии представляет собой комплекс мер по защите и поддержанию системы, обеспечивающей защиту информационных данных от различных воздействий естественного или искусственного характера, которые, впоследствии, могут нанести ущерб всей информационной системе организации. А разнообразные организационные и технические меры, направленные на обеспечение безопасности всех видов данных, являются системой защиты персональных данных на предприятии.[1]

В соответствии с федеральным законом от 27.07.2006 N 152-ФЗ персональные данные – это информация, свойственная физическому лицу, идентифицирующая его однозначно.

Так, в базе персональных данных предприятия хранится такая информация о сотруднике, как: ФИО, дата рождения, образование, профессия, семейное положение, номер трудовой книжки и т.д. Состав данных выбирается предприятием индивидуально, исходя из законодательных и нормативно-правовых актов.

Категории персональных данных представлены на рисунке 1.

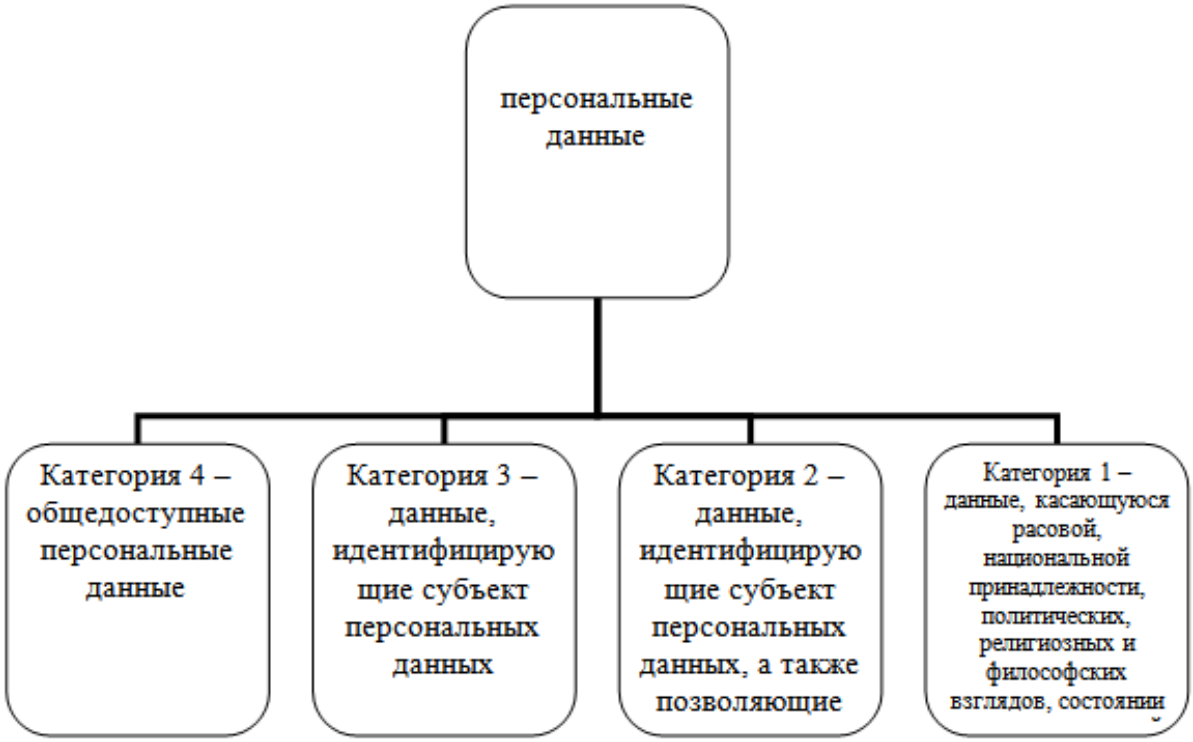


Рисунок 1 – Категории персональных данных

Так же в зависимости от объёма и категории, хранимых данных информационная система требует один из следующих классов защиты:

Класс 4 – информационные системы, нарушение безопасности, которых не влечет негативных последствий для субъекта.

Класс 3 – системы, нарушение безопасности, которых могут повлечь несущественным последствиям для субъекта.

Класс 2 – системы, нарушение безопасности, которых приведет к негативным последствиям для субъекта.

Класс 1 – системы, нарушение безопасности, которых приведет к серьёзным негативным последствиям для субъекта.

Зависимость классов защиты представлены в таблице 1.

Таблица 1 – Зависимость класса защиты от объёма и категории данных.

Объем/Категория	Объем 3(<1000, организация)	Объем 2(<1000-100000, отрасль, город)	Объем 3(>100000, субъект Федерации)
Категория 4(обезличенные, общедоступные)	Класс 4	Класс 4	Класс 4
Категория 3(идентификационные)	Класс 3	Класс 3	Класс 2
Категория 2(идентификационные и еще)	Класс 3	Класс 2	Класс 1
Категория 1(медицинские, социальные)	Класс 1	Класс 1	Класс 1

В соответствии с Постановлением Правительства РФ от 17 ноября 2007 г. № 781, а также документом ФСТЭК «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных», мероприятия по безопасности данных при обработке формируются в зависимости от класса информационных систем с учетом возможного возникновения угроз безопасности в отношении персональных данных. Такие мероприятия включают в себя:

- определение угроз безопасности при обработке персональных данных в информационной системе, а также формирование моделей угроз;

• разработку на основе таких моделей угроз системы защиты, обеспечивающей устранение этих угроз, методами защиты персональных данных соответствующего класса защиты;

• проверку готовности средств защиты информации (далее СЗИ) к применению и составление заключений о возможности их эксплуатации;

• установку и ввод в эксплуатацию СЗИ в соответствии с эксплуатационной и технической документацией;

• обучение лиц, которые будут эксплуатировать СЗИ, правилам работы с ними;

• контроль за применением СЗИ, учет эксплуатационной и технической документации к ним, носителей персональных данных;

• учет лиц, допущенных к работе с персональными данными в информационной системе;

• контроль над соблюдением условий использования СЗИ, предусмотренных эксплуатационной и технической документацией;

• проведение расследований и составление заключений по фактам несоблюдения условий хранения носителей ПДн, использования СЗИ, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн; а также принятие мер по предотвращению возможных опасных последствий подобных нарушений;

• описание системы защиты персональных данных.

• Мероприятия по техническому обеспечению безопасности ПДн при их обработке в ИСПДн включают:

• мероприятия по размещению, специальному оборудованию, охране и организации режима допуска в помещения, где ведется работа с ПДн;

• мероприятия по закрытию утечки ПДн по техническим каналам при их обработке в информационных системах;

• мероприятия по защите ПДн от несанкционированного доступа (далее НСД) и определению порядка выбора средств защиты персональных данных при их обработке в ИСПДн.

Для осуществления мероприятий по защите персональных данных при обработке в информационных системах от несанкционированного доступа и неправомерных действий пользователей могут включать в себя следующие подсистемы:

1) Подсистема управления доступом, регистрации и учета осуществляется. Как правило, реализуется с помощью программных средств блокирования несанкционированного доступа, сигнализации и регистрации. Эти программные средства защиты самих операционных систем, СУБД и прикладных программ. Они выполняют функции защиты самостоятельно или в комплексе с другими средствами защиты и направлены на исключение или затруднение выполнения несанкционированных действий пользователей или нарушителей. К ним относятся специальные утилиты

и программные комплексы защиты, в которых реализуются функции диагностики (тестирование файловой системы), регистрации (журналирование действий и операций), сигнализации (предупреждение об обнаружении фактов несанкционированных действий или нарушения штатного режима функционирования информационной системы персональных данных).

2) Подсистема обеспечения целостности также реализуется преимущественно средствами самих операционных систем и СУБД. Работа данных средств основана на расчете контрольных сумм, уведомлении о сбое в передаче пакетов сообщений, повторе передачи непринятых пакетов.

3) Подсистема антивирусной защиты должна строиться с учетом следующих факторов:

− наличия средств централизованного управления функционированием средств антивирусной защиты с рабочего места администратора безопасности информации в ИСПДн;

− возможности оперативного оповещения администратора безопасности информационной системы обо всех событиях и фактах проявления программно-математических воздействий.

Для реализации подсистемы антивирусной защиты персональных данных при их обработке в информационной системе возможно использование антивирусных средств компаний, выпускающих антивирусное программное обеспечение.

4) Для осуществления разграничения доступа к ресурсам информационной системы при межсетевом взаимодействии (подсистема обеспечения безопасности межсетевого взаимодействия ИСПДн) применяется межсетевое экранирование, которое реализуется программными и программно-аппаратными межсетевыми экранами (МЭ). Межсетевой экран устанавливается между защищаемой внутренней и внешней сетями. МЭ входит в состав защищаемой сети. За счет соответствующих настроек задаются правила, которые позволяют ограничивать доступ пользователей из внутренней сети во внешнюю и наоборот.

5) Подсистема анализа защищенности предназначена для осуществления контроля настроек защиты операционных систем на рабочих станциях и серверах и позволяет оценить возможность проведения нарушителями атак на сетевое оборудование, контролирует безопасность программного обеспечения. С помощью таких средств (средства обнаружения уязвимостей) производится сканирование сети с целью исследования ее топологии, осуществления поиска незащищенных или несанкционированных сетевых подключений, проверки настроек межсетевых экранов и т.п. Данный анализ производится на основании детальных описаний уязвимостей настроек средств защиты (например, коммутаторов, маршрутизаторов, межсетевых экранов) или уязвимостей операционных систем или прикладного программного обеспечения. Результатом работы средств анализа защищенности является отчет, в котором обобщаются сведения об обнаруженных уязвимостях.

6) Выявление угроз НСД при межсетевом взаимодействии производится с помощью систем обнаружения вторжений (подсистема обнаружения вторжений). Такие системы строятся с учетом особенностей реализации атак и этапов их развития. Они основаны на следующих методах обнаружения атак: сигнатурные методы, методы выявления аномалий, комбинированные методы с использованием обоих названных методов. [2]

Утечка информации – это несанкционированный доступ к охраняемым сведениям за пределами организации или круга доверенных лиц.

В основе утечки лежит неконтролируемый перенос конфиденциальной информации.

Причины связаны, как правило, с несовершенством норм по сохранению информации, а также нарушением этих норм (в том числе и несовершенных), отступлением от правил обращения с соответствующими документами, техническими средствами, образцами продукции и другими материалами, содержащими конфиденциальную информацию.

Основными причинами утечки информации являются:

- несоблюдение персоналом норм, требований в работе с носителями конфиденциальной информацией, организационных требований и правил эксплуатации систем защиты (как умышленные, так и непреднамеренные);
- ошибки в проектировании систем защиты;
- ведение противостоящей стороной технической и агентурной разведок.

Причины утечки информации достаточно тесно связаны с видами утечки информации. Существуют три вида утечки информации:

- разглашение. Под разглашением информации понимается несанкционированное доведение защищаемой информации до потребителей, не имеющих право доступа к защищаемой информации.
- несанкционированный доступ к информации. Под несанкционированным доступом понимается получение защищаемой информации заинтересованными субъектами с нарушением установленных правовыми документами или владельцем информации прав или правил доступа к защищаемой информации. При этом заинтересованным субъектом, осуществляющим несанкционированный доступ к информации, может быть государство, юридические и физические лица. Отличие несанкционированного доступа от разглашения состоит в том, что НСД к информации происходит в результате преднамеренных действий заинтересованного субъекта, а разглашение может носить, как преднамеренный, так и случайный характер.
- получение конфиденциальной информацией разведками. Этот вид утечки может осуществляться с помощью технических средств (техническая разведка) или агентурными методами (агентурная разведка). [3]

Основные принципы организационной защиты информации:

- принцип комплексного подхода — эффективное использование сил, средств, способов и методов защиты информации для решения поставленных

задач в зависимости от конкретной складывающейся ситуации и наличия факторов, ослабляющих или усиливающих угрозу защищаемой информации;

- принцип оперативности принятия управленческих решений (существенно влияет на эффективность функционирования и гибкость системы защиты информации и отражает нацеленность руководства и персонала предприятия на решение задач защиты информации);

- принцип персональной ответственности — наиболее эффективное распределение задач по защите информации между руководством и персоналом предприятия и определение ответственности за полноту, и качество их выполнения. [4]

Анализируя всё выше сказанное, можно сделать вывод, что каждая организация стремиться усовершенствовать свою систему безопасности. Потому что вся информация и все базы данных предприятия это информация, которая не должна подвергаться утечке и повреждению. Иначе это приведет к большим финансовым потерям предприятия и затруднениям в работе.

Литература

1. Свободная энциклопедия Википедия: [Электронный ресурс] / (дата обращения: 10.11.2017).

2. Защита персональных данных: [Электронный ресурс] / Олег Слепов, руководитель направления защиты персональных данных, Центр информационной безопасности, компания «Инфосистемы Джет» URL: http://www.iso27000.ru/chitalnyi-zai/zaschita-personalnyh-dannyh/zaschita-personalnyh-dannyh (дата обращения: 10.11.2017).

3. Причины, виды и каналы утечки информации: [Электронный ресурс] / Студопедия.Орг - 2014-2017 год. URL: https://studopedia.org/2-150813.html (дата обращения: 10.11.2017).

4. Организационные основы защиты информации на предприятии: [Электронный ресурс] / Безопасник © 2010-2017 URL: http://bezopasnik.org/article/19.htm (дата обращения: 10.11.2017).

АКТУАЛЬНЫЕ ВОПРОСЫ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ НА ПРЕДПРИЯТИИ

ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ БЛОКЧЕЙН ДЛЯ АВТОМАТИЗАЦИИ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЙ И ОРГАНИЗАЦИЙ

Михайличенко Жанна Вальтеревна,
Орский гуманитарно-технологический институт (филиал) ОГУ, г. Орск,
Аразашвили Антон Тариэлович,
Орский гуманитарно-технологический институт (филиал) ОГУ, г. Орск

Аннотация

В статье исследуются вопросы организации хранения и обработки информации с применением децентрализованной базы данных, а также анализируются возможности и перспективность использования технологии блокчейн.

Ключевые слова: *блокчейн, децентрализованная база данных, распределённая база данных, распределённый реестр, криптовалюта*

Keywords: *blockchain, decentralized database, distributed database, distributed registry, crypto currency*

В эпоху развития и повсеместного использования цифровых технологий остро стоит проблема надёжного хранения и обработки информации. Применение современных компьютерных сетей даёт возможность размещать огромные объёмы данных на сервере и при необходимости передавать их удалённым пользователям.

При традиционной работе с электронными документами централизованной базы данных невозможна модификация одной и той же записи несколькими пользователями. Кроме того такая база данных имеет много уязвимостей: к ней можно подобрать пароль, взломать и испортить структуру, совершить DOS-атаку. Всё это ведёт к информационным потерям.

Совершенно иной подход к хранению данных предлагает технология блокчейн, представляющая собой децентрализованный криптографический сервис обмена данными.

Блокчейн – это непрерывная последовательность блоков, каждый из которых может быть запрограммирован для записи практически любой электронной информации, имеющей ценность. Содержимое блоков однозначно достоверно и может быть проверено, так как каждый блок включает метку времени и информацию о предыдущем блоке. Все блоки выстроены в одну

цепочку и хранят информацию обо всех операциях, когда-либо произведённых в базе.

Блокчейн не имеет единого сервера, управляющего его структурой и модификацией. Любой пользователь, входящий в систему, может внести запись в блокчейн и подтвердить её персональной электронной подписью. Новая информация запишется в блокчейне только тогда, когда другие пользователи системы подтвердят достоверность записи.

Система создана таким образом, что после любой операции все копии реестра синхронизируются в соответствии с обновлениями. Все пользователи блокчейна могут в любой момент свободно получить доступ к хранящимся данным. Шифрование данных в блоках осуществляется взломоустойчивыми криптографическими алгоритмами, и если на отдельном компьютере происходит попытка изменить информацию в каком-либо блоке, то остальные участники системы могут достаточно быстро информацию восстановить.

Можно выделить следующие виды блокчейна:

- Публичный, который открыт абсолютно всем участникам (майнерам) системы. База данных в этом случае хранится на любом компьютере и все знают обо всех активах. Пользователем системы может стать любой человек, причём участники конкурируют друг с другом за закрытие блока. Происходит абсолютная децентрализация и никто не может управлять всей системой.
- Сервисный, в котором база хранится распределённо на любом компьютере. Количество пользователей обычно ограничено, но обо всех операциях осведомлены все пользователи. Существует возможность создания собственного блокчейна для конкретных целей. Поэтому между майнерами нет конкуренции, они договариваются об условиях функционирования системы и контролируют её. Участники, хранящие систему, становятся клиентами майнеров.
- Приватный, где доступ к реестру имеет ограниченное количество пользователей. База данных хранится распределённо, но только на компьютерах, входящими в общую систему.

Основными преимуществами использования блокчейна являются прозрачность проводимых транзакций и множественное их дублирование таким образом, что у каждого пользователя системы всегда есть информация о каждом шаге всех партнёров.

Блокчейн-сеть имеет встроенную устойчивость к ошибкам и автоматически проверяет сама себя с интервалом в десять минут, согласовывая каждую происходящую транзакцию. Таким образом, можно выделить два важных свойства данной системы: прозрачность (данные являются публичными) и надёжность (невозможность одностороннего изменения информации).

Высокая надёжность блокчейн обусловлена несколькими факторами:

1) Достаточно сложными математическими алгоритмами.

2) Специальным программным продуктом с криптографической основой.

3) Несколькими тысячами взаимодействующих между собой компьютеров во всемирной сети Интернет, включённых в систему специального назначения.

Технология блокчейн успешно применяется при операциях с криптовалютой. Однако перспективы использования децентрализованной базы данных не ограничиваются только финансовой сферой.

На основе анализа современных информационных источников были выявлены следующие возможности применения распределённых баз данных:

1) Технология блокчейн даёт возможность творческим людям (художникам, композиторам, писателям, поэтам и прочим) сохранять и подтверждать авторское право на свои работы. При этом создаются электронные копии произведений с помощью уникальных идентификаторов и цифровых сертификатов для подтверждения подлинности и авторства произведений искусства. Кроме того, достаточно надёжно можно обеспечить передачу права владения от автора к коллекционеру или покупателю с соблюдением всех юридических правил.

2) Блокчейн-компании имеют возможность использовать распределённые реестры для автоматизированного управления данными. Так для реализации системы управления базами данных и анализа информации в различных предметных областях применяются идентификационные блокчейны. Некоммерческие организации бизнес-предприятия и даже правительства используют подобные системы для фиксирования информации о бизнес-процессах, упрощения процедур ведения записей, позволяют вести свою деятельность в соответствии требованиями нормативно-правового регулирования рынка и безопасности. Все записи в системе обладают метками времени и хранятся в блокчейнах, что позволяет уменьшить сложность проверки и манипулирования данными, снизить их стоимость и привести в соответствии требованиям законодательства.

3) Технология блокчейн с успехом применяется для идентификации при входе в различного рода системы и подтверждения прав доступа. Распределённые реестры могут быть использованы для хранения любых типов данных и совершения различных транзакций безопасным и открытым способом. Комбинация принципа децентрализованности блокчейн и надёжных инструментов подтверждения личности пользователя позволяет создать цифровое удостоверение, являющееся своеобразным водяным знаком, который может быть поставлен на любую транзакцию с любым активом [1].

4) В энергетической отрасли децентрализованные распределённые реестры уже применяются для ускорения и упрощения анализа данных и тестирования, а также для управления интеллектуальными энергосистемами, работы с механизмами поддержки развития энергетики на основе возобновляемых источников. Инструменты бизнес-логики, которые обычно встроены в подобные системы, позволяют в реальном времени измерять

уровень выработки и потребления электроэнергии, а также некоторые другие показатели [1].

5) Технология блокчейн может служить надёжным средством удалённого онлайн голосования, предоставляя безопасную и прозрачную платформу для анонимных электронных выборов, использующую эллиптическую криптографию для гарантии достоверности и точности результатов. Кроме того электронная система распознавания позволит всем владельцам соответствующих цифровых ключей и идентификационных карт получать доступ к широкому спектру правительственных, банковских и других услуг [2].

6) Блокчейн может быть применён не только для повышения целостности, надёжности и прозрачности политических систем. Новая технология, в частности, позволит улучшить взаимодействие граждан с органами государственной власти, помочь как обычным гражданам общества, так и людям, претендующим на управляющие позиции в местных государственных органах. К примеру, реализована платформа гражданского управления, представляющая себя как система доступных всему миру юридических и экономических услуг, таких, например, как: услуги нотариуса, регистрация юридических лиц, регистрация и расторжение браков, выполнение финансовых операций, расчёт базового дохода на основе умных контрактов и блокчейна.

7) В социальной сфере платформы на основе децентрализованной базы данных предлагают собственную систему контроля ухода за престарелыми и нуждающимися в опеке людьми. При этом предлагаются электронные устройства в виде браслетов или медальонов со встроенными программами для удалённого сбора и анализа основных показателей жизнедеятельности людей и определения ситуаций, когда носящий их человек нуждается в помощи.

8) На рынке информационных услуг уже предлагаются программные и аппаратные решения для крупномасштабного умного управления промышленными системами и оборудованием. В основе разработок лежат принципы децентрализации, криптографической защиты и автономности.

9) Отслеживать движение товара скоро станет также более удобным и подробным, всегда можно увидеть, где он находится, за счёт внедрения технологии в цепочку поставок. Благодаря блокчейн-системе большинство сделок будут происходить в режиме реального времени и, следовательно, мгновенно.

10) Технология распределенного реестра позволит средним образовательным учреждениям на протяжении всех лет обучения записывать в блокчейн информацию об оценках всех школьников, их достижениях и участиях в предметных олимпиадах. Таким образом к моменту выпуска для каждого обучающего будет сформировано электронное портфолио, демонстрирующее компетенции подростков. Подобная система позволит избежать подделок документов об образовании и наградах учащихся, а в перспективе отказаться от проведения Единого государственного экзамена.

11) Благодаря своей надёжности и прозрачности блокчейн-технология может найти практическое применение в системе образования путём развития и легитимизации онлайн обучения. Массовые открытые интернет курсы дают возможность получить новые знания из любой точки мира за приемлемую стоимость обучения, поэтому их популярность постоянно растёт. Исходя из возможности комбинировать отдельные курсы в блоки курсов, можно предлагать различные стратегии обучения для узконаправленных специальностей. Также, блокчейн позволяет стандартизировать сертификаты и дипломы университетов и образовательных онлайн порталов, что в перспективе позволит легализовать их для всех стран мира.

Эффективность блокчейн вполне оправдана в системах, где важна надёжная синхронизировать данные, поступающие из различных источников, а также надёжное подтверждение авторства любого действия. Это страховые компании, сертификационные центры, банки, нотариальные конторы, традиционные биржи, рейтинговые агентства, логистика, конкурсы и лотереи. Новая технология распределённой базы данных позволяет существенно упростить оформление и проверку подлинности документов, идентификацию пользователей, отслеживание цепочек поставок, заключение и исполнение контрактов, удешевление финансовых операций, защиту интеллектуальной собственности, ведение различных реестров, управление предприятиями.

Технология блокчейн, появившаяся сравнительно недавно, уже применяется во многих областях. Поэтому важно понимать, что блокчейн открыл дорогу для новых, более масштабных проектов, новых профессий, идей и возможностей для развития.

Литература

1. 20 областей применения Блокчейн вне финансовых сервисов, ч.1 // [Электронный ресурс]. - Режим доступа: coinz.life/blokchejn-primenenie/

2. Обзор применения технологии блокчейн в государственном управлении // [Электронный ресурс]. - Режим доступа: fastsalttimes.com/sections/obzor/1503.html

СИНТЕЗ ЦИФРОВЫХ СХЕМ ПО АЛГОРИТМАМ ИХ ФУНКЦИОНИРОВАНИЯ В ВИДЕ ПРЕДМЕТНО-ОРИЕНТИРОВАННЫХ ГРАФИЧЕСКИХ МОДЕЛЕЙ

Парамонов Андрей Владимирович,
ООО «Орский проектно-конструкторский технологический институт машиностроения», г. Орск

Аннотация

В статье рассматривается проблема построения полных и непротиворечивых алгоритмов функционирования дискретных устройств, в частности цифровых схем. Для решения данной проблемы предлагаются к использованию предметно-ориентированные графические модели. Такие модели позволяют привлекать к разработке специалистов предметных областей применения схем и поддерживать корректность алгоритмов.

Ключевые слова: *синтез цифровых схем, предметно-ориентированные графические модели, автоматизация программирования*

Keywords: *digital circuit synthesis, domain specific graphical models, automatic programming*

Процесс проектирования цифровых схем, как правило, состоит из нескольких этапов. Начальным этапом является так называемое алгоритмическое проектирование – построение исходного описания правил функционирования будущей схемы. Очевидно, что для предотвращения появления ошибок на последующих этапах такое описание должно быть по возможности формальным.

В качестве формальных средств описания алгоритмов используются таблицы истинности, таблицы решений, графы переходов конечных автоматов, языки высокого уровня и так далее [1]. Например, алгоритм может быть записан на синтезируемом подмножестве языка VHDL [2;3] в потоковом или процедурном стиле. Такой подход, несмотря на многие достоинства для проектировщика, затрудняет восприятие алгоритма специалистами тех областей, в которых будет применяться схема.

Далее рассматриваются предметно-ориентированные графические модели (далее ПОГМ или просто модели) [4] как инструмент алгоритмического проектирования цифровых схем, который позволяет описывать формальные алгоритмы в контексте областей применения схем, поддерживать корректность алгоритмов [5;6] и при необходимости синтезировать алгоритм в виде процедурной VHDL-модели.

Предметно-ориентированные графические модели и цифровые схемы

В работах [4;5] ПОГМ рассматриваются как средство алгоритмизации задач логического управления промышленными установками. Покажем, как ПОГМ могут использоваться для синтеза цифровых схем.

Рассмотрим реляционную модель M из шести отношений:

$$M = \left(R_E, R_{CE}, R_G, R_{CG}, R_I, R_{EI}\right)$$

На рисунке 1 представлена схема данных модели M.

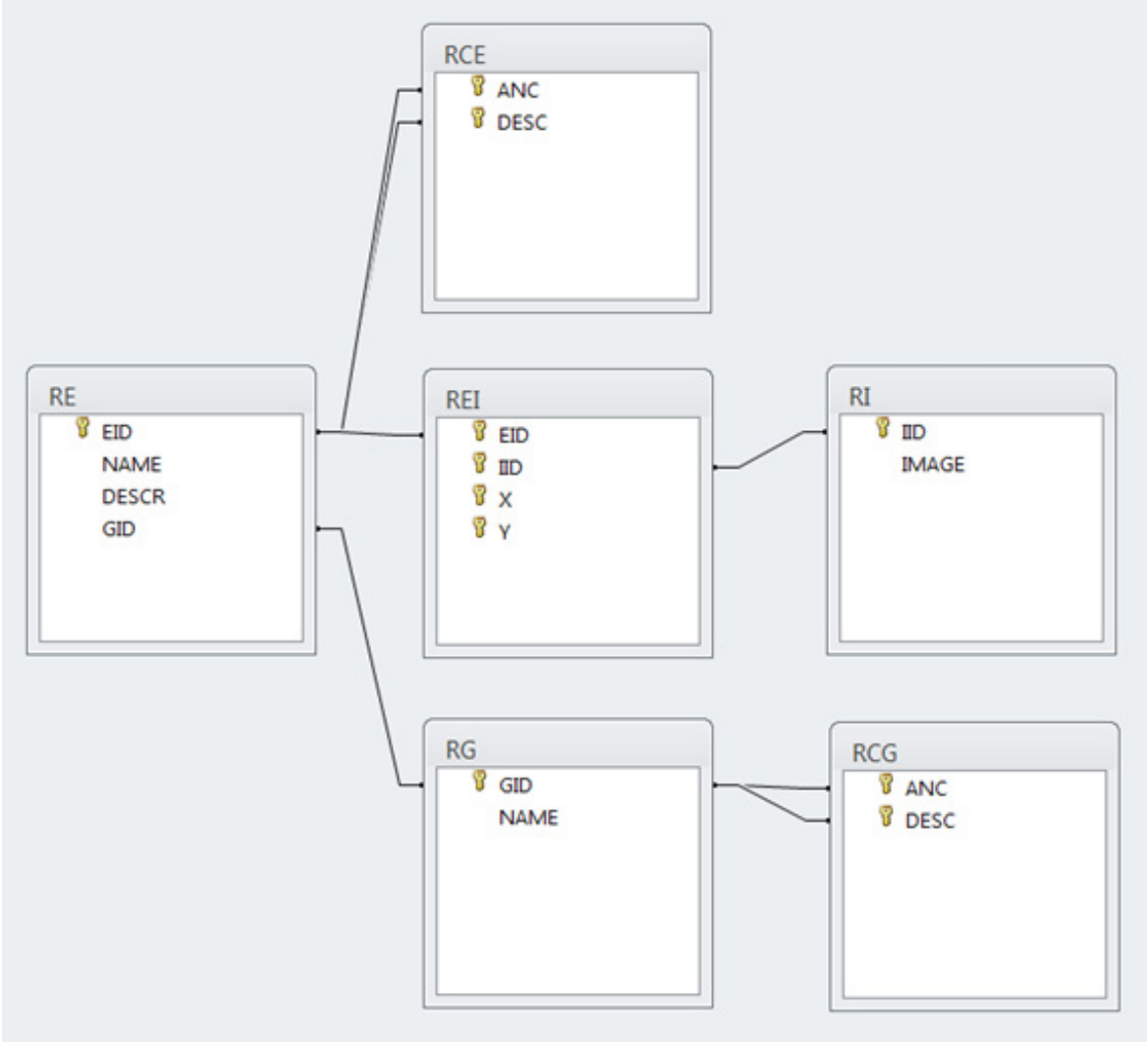


Рисунок 1 – Схема данных реляционной модели M.

Отношения R_E и R_{CE} представляют дерево так называемых элементов. К элементам относятся различные кнопки, переключатели, датчики, индикаторы, электрические двигатели и прочие устройства, подключаемые к схемам. Также к элементам относятся сами схемы (как «чёрные ящики») и вспомогательные элементы (линии связи и тому подобное). Информация об элементах содержится в вершинах такого дерева (отношение R_E), а связи между парами элементов – есть ребра дерева (отношение R_{CE}).

Отношения R_G и R_{CG} представляют дерево групп элементов аналогично дереву элементов. Каждый элемент должен быть отнесен к одной из групп этого дерева (поле *GID* отношения R_E).

Наконец отношение R_I – есть список строк, описывающих графические изображения элементов, визуально схожие с оригиналами, и R_{EI} – список соответствий элементов изображениям.

Дополнив теперь M набором некоторых правил построения дерева элементов и дерева групп L, получим так называемую ПОГМ объекта управления – $\langle L, M \rangle$.

Алгоритмическое проектирование цифровых схем

Включим в L следующие правила, необходимые и достаточные для алгоритмического проектирования:

– Отношение R_G содержит как минимум три кортежа. Первый из них описывает группу, элементы которой являются входными логическими сигналами схемы. Элементы этой группы будем называть *входами*. Второй кортеж по аналогии описывает группу *выходов*, а третий – группу, к которой относятся все остальные элементы.

– Отношение R_E описывает хотя бы один выход.

– Отношение R_I включает как минимум три изображения – по одному на каждое возможное значение логического входного или выходного сигнала схемы (ложь, истина и неопределенность).

– Каждому входу и каждому выходу из *RE* в каждый момент времени сопоставлено только одно из трех изображений, описанных в предыдущем правиле, и каждое такое сопоставление содержится в R_{EI}.

Если модель построена по данным правилам, то в любой момент времени она графически изображает объект управления и значения его входных и выходных сигналов. *Кадром* модели $\langle L, M \rangle$ будем называть модель $\langle L, M' \rangle$ отличающуюся от исходной модели только лишь номерами изображений входов и выходов в R_{EI}, либо вообще не отличающуюся от исходной модели. Например, в специализированной среде *Logic Algorithm Designer* для изменения кадра модели используется следующий механизм: пользователь выполняет клик левой кнопкой мыши по изображению значения нужного сигнала, в результате чего это изображение изменяется, показывая уже новое значение сигнала.

Любую пару кадров можно рассматривать как совокупность значений входов и выходов в текущий момент времени и соответствующую ей совокупность значений выходов в следующий момент времени. Таким образом, совокупность пар кадров тривиально определяет секвенциальный алгоритм – алгоритм, в котором значения выходов зависят от значений входов и выходов в предыдущий момент времени.

Для описания алгоритмов функционирования дискретных устройств наиболее предпочтительным средством является аппарат детерминированного конечного автомата. Покажем, как этот аппарат используется в ПОГМ.

Пусть дана функция *f: A → B*, где *A* – множество номеров входов и выходов, B – множество номеров изображений, которая ставит в соответствие каждому входу и выходу изображение значения.

Функция *g: B → {0,1,λ}*, где *B* – множество номеров изображений значений входов и выходов (*|B|=3*), ставит в соответствие каждому изображению значения само значение. Запись вида $g(f(x_i))$, где x_i – номер входа ($i=\overline{1,n}$, *n* – количество входов), будем для краткости обозначать как x_i. Аналогично запись $g(f(x_j))$, где x_j – номер выхода ($j=\overline{1,m}$, *m* – количество выходов), будем обозначать как y_j.

Ситуацией будем называть совокупность значений входов модели:

$$s=(x_1,x_2,...,x_n),$$

причем $(\forall x\in s)[x\neq\lambda]$. Любой ситуации соответствует множество кадров.

Обобщенная ситуация (ОС) $\tilde{s}$ есть ситуация, входы которой могут принимать значения $\{0,1,\lambda\}$.

Действием будем называть совокупность значений выходов модели:

$$r=(y_1,y_2,...,y_m),$$

причем $(\forall y\in r)[y\neq\lambda]$. Любому действию соответствует множество кадров.

Определим теперь автомат Мура (АМ) следующим образом:

$$A=\left\langle \hat{S},\hat{s}_0,\tilde{S},R,\Phi,\Psi\right\rangle,$$

где

$\hat{S}=\{\hat{s}_1,\hat{s}_2,...,\hat{s}_p\}$ – множество внутренних состояний АМ.

$\hat{s}_0\in\hat{S}$ – начальное состояние.

$\tilde{S}=\{\tilde{s}_1,\tilde{s}_2,...,\tilde{s}_q\}$ – множество ОС.

R – множество действий.

$\Phi:\tilde{S}\times\hat{S}\to\hat{S}$ – функция переходов.

$\Psi:\hat{S}\to R$ – функция выходов.

С учетом того, что ОС и действиям соответствуют множества кадров, АМ можно переопределить следующим образом:

$$A=\left\langle \hat{S},\hat{s}_0,\left\langle L,M_{\tilde{S}}\right\rangle,\left\langle L,M_R\right\rangle,\Phi,\Psi\right\rangle$$

$$\Phi:\left\langle L,M_{\tilde{S}}\right\rangle\times\hat{S}\to\hat{S}$$

$$\Psi:\hat{S}\to\left\langle L,M_R\right\rangle$$

Данные выражения определяют алгоритм, использующий формальный аппарат АМ и при этом имеющий представление в ПОГМ. Полученный таким образом АМ может быть преобразован в изоморфный код на языке VHDL [3,266], в том числе и автоматически.

Таким образом, в статье рассмотрены ПОГМ в качестве инструмента для алгоритмического проектирования цифровых схем. Представлен метод построения алгоритмов по ПОГМ с использованием аппарата АМ. Данный

метод позволяет выполнять алгоритмическое проектирование схем в контексте области их применения, но при этом с возможностью обеспечения формальной корректности.

Литература

1. Шалыто, А.А. SWITCH-технология. Алгоритмизация и программирование задач логического управления / А. А. Шалыто. СПб.: Наука, 1998.

2. Бибило, П.Н. Основы языка VHDL. Изд. 3-е, доп. / П.Н. Бибило. – М.: Издательство ЛКИ, 2007. – 328 с.

3. Бибило, П.Н. Синтез логических схем с использованием VHDL / П. Н. Бибило. – М.: СОЛОН-Р, 2009. – 384 с.

4. Парамонов, А.В. Графическое моделирование технологического процесса как вспомогательное средство составления алгоритма управления / А. В. Парамонов // Программные продукты и системы. – №4. -Тверь, 2016. -С. 89-93.

5. Парамонов, А.В. О корректности описания алгоритмов логического управления с помощью предметно-ориентированных графических моделей / А. В. Парамонов // Компьютерная интеграция производства и ИПИ-технологии: материалы VIII Всероссийской научно-практической конференции. – Оренбург, 2017. – С. 279-281.

6. Червенчук, В. Д. Методы и средства синтеза алгоритмического и программного обеспечения систем управления с использованием таблиц решений [Текст]: дис. … канд. технич. наук: 05.13.01 / Червенчук Владимир Дмитриевич. -Омск, 1984. -123 с.

ЗАДАЧИ АВТОМАТИЗАЦИИ ЭКОЛОГИЧЕСКОГО МОНИТОРИНГА НА УРБАНИСТИЧЕСКИХ ТЕРРИТОРИЯХ

Соловьев Николай Алексеевич, Сурина Елена Евгеньевна,
Орский гуманитарно-технологический институт (филиал) ОГУ (г.Орск)

Аннотация

В статье представлен обзор разработанных автоматизированных систем экологического мониторинга, предложены направления совершенствования их разработки на основе математического моделирования.

Ключевые слова: *экологический мониторинг, распространение загрязнителя в атмосфере , экспертные системы, зоны влияния, накопленный вред в окружающей среде.*

Keywords: *environmental monitoring, the spread of pollutants in the atmosphere, expert systems, areas of influence, accumulated harm to the environment*

Многоотраслевой промышленный потенциал Оренбургской области создает повышенную нагрузку на региональные природные экосистемы и приводит к неизбежному загрязнению атмосферного воздуха. Именно этот параметр не только оказывает крайне негативное влияние на состояние окружающей среды, но формирует социальную составляющую экологической ситуации, проявляющуюся в реакции населения. Это влияние усугубляется тем, что основные источники загрязнения атмосферного воздуха - промышленные предприятия, расположенные в крупных городах области (Оренбурге, Орске, Новотроицке, Медногорске).

Необходимо отметить, что последние 10-15 лет в области прослеживается явная тенденция к улучшению параметров состояния атмосферного воздуха в Оренбургской области. Данные Роскомстата показывают, что поступление в атмосферный воздух загрязняющих веществ, отходящих от стационарных источников выбросов, в Оренбургской области уменьшается из-года в год. При этом объёмы загрязняющих веществ от организованных и неорганизованных источников загрязнения в Оренбургской области снижаются значительно большими темпами чем в целом по Приволжскому федеральному округу и Российской Федерации (рис.1).

Однако эконометрический анализ факторного воздействия на снижение выбросов в атмосферу показывает, что эта благоприятная тенденция обусловлена в большей степени общим снижением объёмов производства в области связи с кризисными явлениями, чем влиянием реализации природоохранных мероприятий. Таким образом, учет выбросов загрязняющих атмосферу веществ, который ведется как по их агрегатному состоянию (твердые, газообразные, жидкие), так и по отдельным веществам (ингредиентам) хотя и фиксирует степень загрязнения среды, в недостаточной степени обеспечивает эффективность экологического управления.

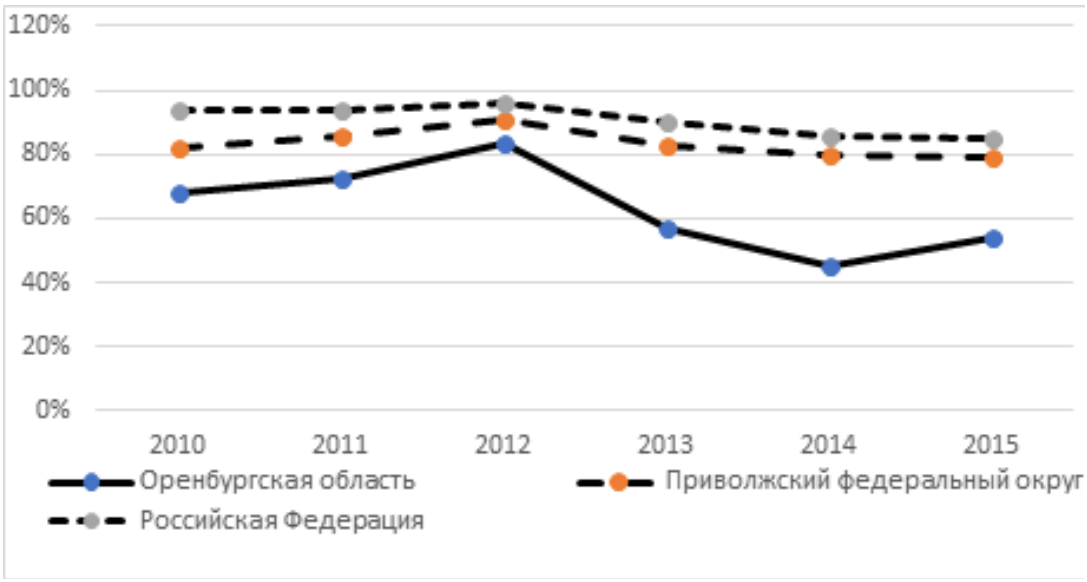


Рис.1. Динамика выбросов в атмосферу загрязняющих веществ в федеральных образованиях разных уровней (в % к 2005 г.)

В этой связи актуальным представляется исследование и расширение функций систем экологического мониторинга атмосферного воздуха как части единого мониторинга окружающей среды.

Понятие мониторинга окружающей среды, введенное в 1972 г. на Стокгольмской конференции ООН по окружающей среде, включало в себя систему повторных наблюдений одного или более элементов окружающей природной среды в пространстве и во времени с определенными целями в соответствие с заранее подготовленной программой. Это определение лишь в общем виде раскрывало цели и задачи экологического мониторинга, и в дальнейшем развивалось и закреплялось на законодательном уровне [1]. В системах государственного экологического мониторинга (государственного мониторинга окружающей среды) задачами признавались :

– регулярные наблюдения за состоянием окружающей среды, в том числе компонентов природной среды, естественных экологических систем, за происходящими в них процессами, явлениями, изменениями состояния окружающей среды;

– хранение, обработка (обобщение, систематизация) информации о состоянии окружающей среды;

– анализ полученной информации в целях своевременного выявления изменений состояния окружающей среды под воздействием природных и (или) антропогенных факторов, оценка и прогноз этих изменений;

– обеспечение органов государственной власти, органов местного самоуправления, юридических лиц, индивидуальных предпринимателей, граждан информацией о состоянии окружающей среды.

Развитие понятия экологического мониторинга проводилось и в научных работах. А.А. Горюнкова, в частности, определяет структуру и основные процедуры системы мониторинга загрязнения атмосферы (выделение объекта наблюдения, его обследование, составление информационной модели и ее идентификация, планирование измерений, оценка состояния и прогнозирование его изменения для объекта исследования) [5,253]. М.В. Волкодаева и .В. Киселев обращают внимание на совершенствование системы нормативов и стандартов качества атмосферного воздуха [4,595].

Вместе с понятием мониторинга окружающей среды разрабатывалось и понятие автоматизированной системы экологического мониторинга (АСЭМ). АСЭМ в настоящее время может рассматриваться как комплекс технических и программных средств, предназначенный для решения задач по непрерывному контролю состояния окружающей среды как территорий отдельных промышленных предприятий, так и регионов в целом. .

В настоящее время в РФ функционируют десятки, если не сотни, АСЭМ, решающие свои функциональные задачи - от отслеживания экологической обстановки до контроля основных источников загрязнения для последующего принятия управленческих решений. В последние годы в состав таких систем входят различные GIS модули, реализующие возможности картографии

загрязненности атмосферного воздуха, водного бассейна, почвенного покрова подконтрольной территории.

ФГУП «СПО «Аналитприбор», входящее в техническую рабочую группу по разработке справочника НДТ «Общие принципы производственного экологического контроля и его метрологическое обеспечение», разработало автоматизированную систему экологического контроля (АСЭК), реализующую следующие задачи:

– мониторинг за выбросами загрязняющих веществ;

– автоматическое измерения и учет объема или массы выбросов вредных (загрязняющих) веществ в непрерывном режиме;

– автоматическое измерения концентрации вредных (загрязняющих) веществ в выбросах;

– передача информации об объеме или о массе выбросов в атмосферный воздух, о концентрации вредных (загрязняющих) веществ в выбросах в государственный фонд данных государственного экологического мониторинга (государственного мониторинга окружающей среды);

– организацию деятельности по предупреждению экологических аварий и аварийных ситуаций;

– выдачу сигнализации о нештатных ситуациях, самодиагностика газоанализаторов и системы подготовки проб;

– Ведение экологической документации предприятия (выдачу экологических отчетов) предусмотренной государственной статистической отчётностью, системой государственного экологического мониторинга.

На этом функционале реализована система экологического мониторинга Оренбургского газохимического комплекса, которая позволила обеспечить непрерывный контроль состояния окружающей среды территории Оренбургской области в зоне ответственности ООО «ГАЗПРОМ ДОБЫЧА ОРЕНБУРГ»

Другим примером АСЭМ является система экологического мониторинга окружающей среды «СЭМОС», разработанная специалистами ОАО «Лига» (см. http://ligaoao.ru/eco/semos). Эта АСЭМ осуществляет функции непрерывного круглосуточного мониторинга за состоянием окружающей среды и обеспечивает своевременное информирование ответственных лиц достоверной информацией для принятия эффективных управленческих решений в области природоохранной деятельности. К достоинствам системы «СЭМОС» относятся высокая степень автоматизации получения информации от средств измерения, контроль качества и достоверности получаемых данных. Специальное уникальное программное обеспечение предоставляет возможность осуществлять автоматическое построение процедурных карт внутрилабораторного контроля. В сравнении с системой АСЭК система «СЭМОС» обладает такими преимуществами, как отображение результатов измерений и расчетов на экране монитора/вывод на печать, в том числе в картографической среде.

Анализ ряда других автоматизированных систем экологического мониторинга представлен в работах [2-5]. Основываясь на вышесказанном, нами были определены состав и функции АСЭМ (рис.2) по задачам мониторинга и управления.

Приведенные примеры, однако, показывают, что большинство АСЭМ реализуют задачи наблюдения и контроля, сводящиеся к пространственному мониторингу Значительно меньшее число ИАС нацелены на анализ и оптимизацию. Только встраивание в АСЭК математических моделей позволяет решать ряд задач анализа информации, например прогнозирование, анализ за определенные периоды времени, оперативный мониторинг в любое время. Именно на основании результатов математического моделирования процесса мониторинга стационарных источников загрязнения появляется возможность осуществить эффективное управления промышленными объектами.

Моделирование загрязнения атмосферного воздуха в стационарном режиме позволяет с достаточной точностью обнаружить очаги загрязнения, сформировать быстрое реагирование и автоматизировать сотрудничество специалистов по экологическому мониторингу разных стран. В данном аспекте успешно использование методов построения интеллектуальных и экспертных систем. Д.П. Вент, В.Ю. Волков, И. Бархум, С.Б. Аббас [3,269] рассматривают возможности создания интеллектуальных систем с удаленным доступом для оперативного принятия решений в управлении экологической ситуацией. Рассматривая АСЭМ как сложные многофункциональные системы, авторы отмечают такие их свойства как иерархичность структуры, ступенчатость развития и сильную межкомпонентную связь системы.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ЭКОЛОГИЧЕСКОГО МОНИТОРИНГА	**МОНИТОРИНГ**	**ПОДСИСТЕМА НАБЛЮДЕНИЯ И КОНТРОЛЯ**	Круглосуточный непрерывный автоматический контроль загрязнения атмосферного воздуха в границах городского округа
		ПОДСИСТЕМА ПЕРЕДАЧИ ДАННЫХ И ИНТЕГРАЦИИ С ГОСУДАРСТВЕННЫМИ АСЭМ	Обмен актуальными данными с автоматизированными источниками, (стационарные и передвижные экологические посты, автоматизированные системы экологических лабораторий инструментальных измерений и лабораторных анализов и т.д.)
		ПОДСИСТЕМА ВИЗУАЛИЗАЦИИ ДАННЫХ	Отображение результатов измерений и расчетов на экране монитора/вывод на печать, в том числе в картографической среде
	УПРАВЛЕНИЕ	**ПОДСИСТЕМА ОЦЕНКИ ПРОГНОЗНОГО СОСТОЯНИЯ И ПРИНЯТИЯ РЕШЕНИЙ**	Сигнализация о возникновении ситуаций с превышением предельно допустимых концентраций загрязняющих веществ на подконтрольной территории
			Прогнозирование изменения экологической ситуации
			Построение информационной модели объекта наблюдения
		БАЗА ДАННЫХ НАБЛЮДЕНИЙ И КОНТРОЛЯ	Контроль, обработка, накопление и хранение оперативных и справочных данных, результатов расчётов и служебной информации
			Ведение баз данных, реализация запросов на поиск и извлечение информации
			Архивирование, копирование и восстановление информационных массивов

Рис.2 Структура и функционал АСЭМ.

Приведенные примеры, однако, показывают, что большинство АСЭМ реализуют задачи наблюдения и контроля, сводящиеся к пространственному мониторингу Значительно меньшее число ИАС нацелены на анализ и регулирование качества среды наблюдения. Однако встраивание в АСЭК

математических моделей позволяет решать ряд задач анализа информации, например, прогнозирование, анализ за определенные периоды времени, оперативный мониторинг в любое время. Именно на основании результатов математического моделирования процесса мониторинга стационарных источников загрязнения появляется возможность осуществить эффективное управления промышленными объектами.

Моделирование загрязнения атмосферного воздуха в стационарном режиме позволяет с достаточной точностью обнаружить очаги загрязнения, сформировать быстрое реагирование и автоматизировать сотрудничество специалистов по экологическому мониторингу разных стран. В данном аспекте успешно использование методов построения интеллектуальных и экспертных систем. Д.П. Вент, В.Ю. Волков, И. Бархум, С.Б. Аббас [3,269] рассматривают возможности создания интеллектуальных систем с удаленным доступом для оперативного принятия решений в управлении экологической ситуацией. Рассматривая АСЭМ как сложные многофункциональные системы, авторы отмечают такие их свойства как иерархичность структуры, ступенчатость развития, сильную межкомпонентную связь внутри системы.

В свою очередь А. Мархуб в диссертации «Экспертная система поддержки принятия решений в интеллектуальной системе экологического ммониторинга атмосферного воздуха промышленного региона (на примере г. Новомосковска Тульской области)» представляет разработку научно-обоснованного метода построения интеллектуальной автоматизированной системы мониторинга (ИАСЭМ) атмосферного воздуха и экспертной системы принятия решений в реальном времени по управлению экологической ситуацией на урбанистических территориях. При этом А. Мархуб особое внимание уделяет решению проблемы неопределенности принятия управленческого решения путем применения моделей байесовских сетей доверия и формирования на их основе баз знаний АСЭМ.

Важным достоинством разработанной А. Мархубом АСЭМ является возможность отображения экологической информации в Интернете. В целом насущность применения Web-технологий для моделирования экологических ситуаций в настоящее время неоспорима. Отметим, что в этом направлении можно использовать не только инструментальные средства отображения и актуализации информации, но и возможности серверов и сервисов. Разработанная Е.А. Смирновым информационная система для моделирования распространения загрязнения атмосферного воздуха является комбинацией двух типов архитектур – сервис-ориентированной и трехуровневой [6,28]. Структурно помимо собственных приложений эта система включает в себя сервера ArcGISServer и IIS. Первый из перечисленных подключает к системе с помощью геосервисов базу пространственных данных, второй - Web- сервер компании Microsoft. На нём устанавливается ядро системы и ее расчетные и интерфейсные модули.

Подводя итог вышесказанному, мы можем заключить следующее:

– в настоящее время в достаточной степени разработан функционал АСЭМ в отношении сбора, обработки и хранения (архивации) результатов автоматических измерений, их передачи, а также выявления источников выброса в атмосферу;

– большинство реализованных АСЭМ основано на сборе точечных замеров, прогнозирование динамики атмосферы загрязнения производится в зависимости от метеорологических параметров, а также данных картографии;

– в настоящее время практически отсутствуют системы экологического мониторинга учитывающие и/или определяющие накопленный вред окружающей среде (вред окружающей среде, возникший в результате прошлой экономической и иной деятельности, обязанности по устранению которого не были выполнены либо были выполнены не в полном объеме);

– актуальным аспектом разработки АСЭМ является остается включение в их архитектуру интерактивных модулей и веб-приложений для осуществления удаленного доступа к информации.

Таким образом направлениями совершенствования АСЭМ является в первую очередь применение методов математического моделирования как в сфере математической экологии, так и в сфере разработки экспертных систем для определения зон влияния источников загрязнения на территории и акватории, на которых выявлен накопленный вред окружающей среде, объекты капитального строительства и объекты размещения отходов, являющиеся источником накопленного вреда окружающей среде.

Литература:

1. Федеральный закон "Об охране окружающей среды" (7-ФЗ) — URL https://dogovor-urist.ru/законы/закон_об_охране_среды.

2. Али Мансур Номан, Волков В.Ю., Эделынтейн Ю.Д:, Бархум Ибрахим Халил. Состояние атмосферного воздуха как объект управления- в АСЭМ. Вестник МАСИ. Информатика, экология, экономика. Том 10. -М:, 2007. С.88-95.

3. Вент Д.П., Волков В.Ю., Бархум И. Интеллектуальные автоматизированные системы в экологии //"Известия ТулГУ. Технические науки". Изд-во ТулГУ. 2008. Вып.4. С. 268-273.

4. Волкодаева М.В., Киселев А.В. О развитии системы экологического мониторинга качества атмосферного воздуха // Записки Горного института. 2017. Т. 227. С. 589-596. DOI: 10.25515/PMI.2017.5.589

5. Горюнкова А.А. Современное состояние и подходы к разработке систем мониторинга загрязнения атмосферы //"Известия ТулГУ. Технические науки". Изд-во ТулГУ. 2013. Вып.11. С. 251-260.

6. Смирнов Е. А. Информационная система для моделирования распространения загрязнения атмосферного воздуха с использованием ArcGIS [Текст] // Актуальные вопросы технических наук: материалы Междунар. науч.

конф. (г. Пермь, июль 2011 г.). — Пермь: Меркурий, 2011. — С. 27-31. — URL https://moluch.ru/conf/tech/archive/4/895/.

О ПАРАЛЛЕЛЬНОМ АЛГОРИТМЕ ДЕЛЕНИЯ ЦЕЛЫХ ЧИСЕЛ БОЛЬШОЙ РАЗРЯДНОСТИ

Чурсин Вячеслав Борисович,
Орский гуманитарно-технологический институт (филиал) Оренбургского государственного университета, г. Орск

Аннотация

В статье исследуются общие принципы работы алгоритма деления целых большой разрядности, а также описывается алгоритм деления целых чисел большой разрядности в многопоточных параллельных системах.

Ключевые слова: *целые числа, параллельный алгоритм деления, многопоточное деление.*

Keywords: *integers number, parallel division algorithm, multi-thread division.*

Быстрые методы для операций над целыми числами большой разрядности (далее ЦБР-числа) очень важны для приложений, которые применяются в криптографии и компьютерной алгебре [1,91;2,64]. В данной публикации в качестве объекта исследования рассматривается модифицированный алгоритм деления, который можно рассматривать и как модификацию базового алгоритма деления и как метод параллельного деления целых чисел.

В качестве базового алгоритма деления целых чисел будем рассматривать широко известный метод деления «столбиком». Алгоритм деления целых чисел представлен **Алгоритмом 1.**

Алгоритм 1. Базовый алгоритм деления целых чисел

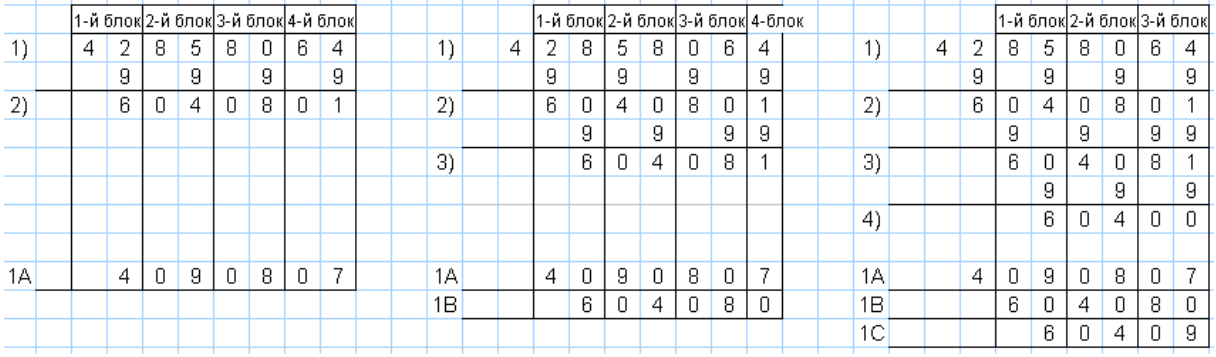
Вход: *int a, b, R, d, t,* где $a \times b > 0$, N – основание системы счисления

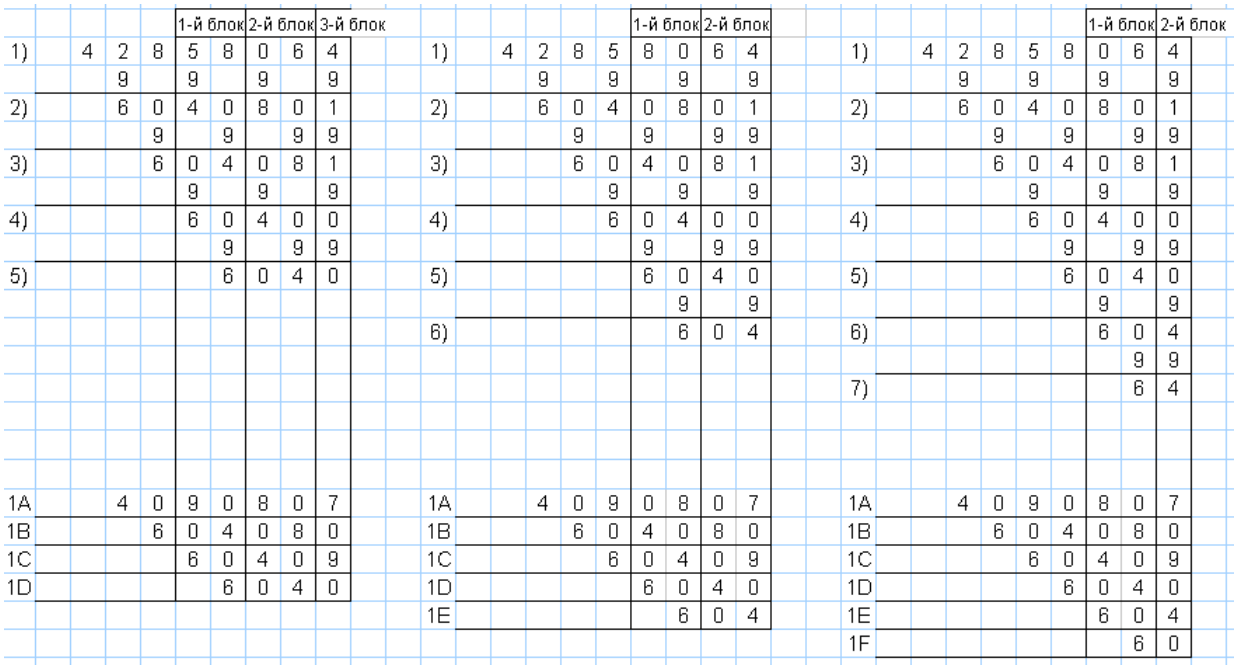
Выход: $t \equiv a \pmod{b}$, $R = \lfloor a / b \rfloor$

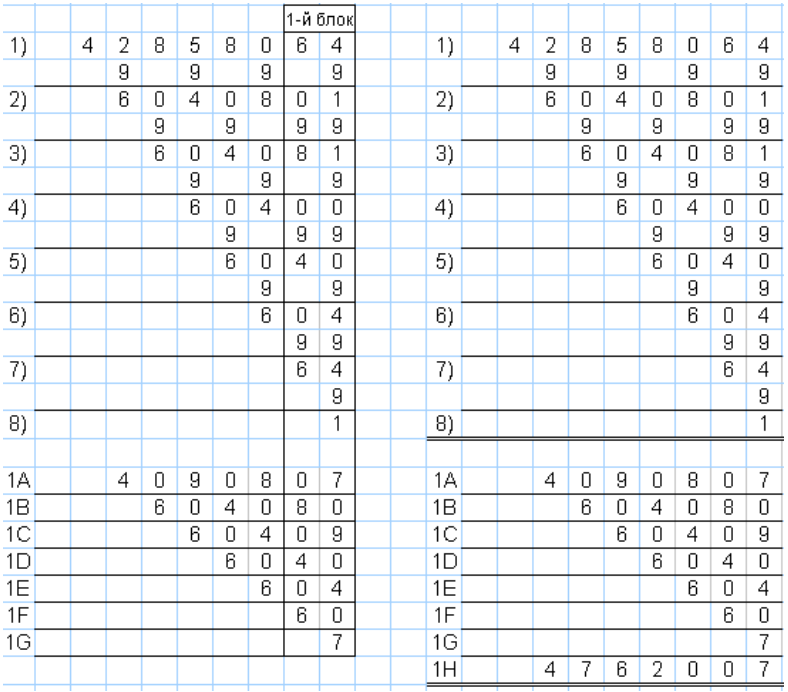
1: $R \leftarrow empty$; $d \leftarrow b$; $t \leftarrow a$;
2: while $(t \geq d)$ **do** d $\leftarrow d \times N$;
3: repeat
4: $d \leftarrow \lfloor d / N \rfloor$;
5: $q \leftarrow empty$;
6: while $(t \geq d)$ **do** $t \leftarrow t - d$; $q \leftarrow q + 1$;
7: $R \leftarrow R \times N + q$;
8: until $(d = b)$;
9: return t, R;

Выражение $\lfloor a/b \rfloor$ – операция округления до ближайшего целого в меньшую сторону (получение частного при делении целого числа a на целое b).

Предлагаемый алгоритм многопоточного (или многопроцессорного) деления представляет собой модификацию базового алгоритма деления и подразумевает разбиение делимого числа на блоки, с каждым из которых выполняется базовый алгоритм деления столбиком с последующим суммированием промежуточных результатов для получения частного. Выполнение такого алгоритма можно продемонстрировать с помощью рисунков 1–8. Подразумевается, что выполнение поблочного деления осуществляется в отдельном потоке (или на отдельном процессоре).







Рисунки 1–8. Этапы выполнения параллельного деления

В строках 2) – 8) представлены остатки от деления для каждого из блоков, в строках 1A–1G – соответствующие частные.

Предварительный анализ трудоемкости выполнения алгоритма (представленного на рисунках 1–8) будем проводить с точки зрения количества операций вычитания, выполняемых в каждом блоке. В данном случае оказывается, что при выполнении **Алгоритма 1** требуется 26 операций вычитания, в то время как для выполнения параллельного алгоритма требуется 91 операция вычитания (1–й блок–41 операция вычитания, 2–й блок – 25, 3–й блок – 25). Таким образом, трудоемкость выполнения параллельного алгоритма в данном случае оказывается в 3,5 раза выше трудоемкости **Алгоритма 1**. Более того, негативным фактором, влияющим на общую трудоемкость предлагаемого алгоритма параллельного деления, оказывается увеличение блоков разбиения. Исходя из вышеизложенного можно сделать заключение о том, что в случае данной реализации *многопоточного* деления (один процессор–много потоков) не удастся достичь ожидаемого ускорения вычислений для операции целочисленного деления ЦБР-чисел.

В случае многопроцессорных систем, когда блоки делимого ЦБР-числа распределяются по процессорам системы, можно ожидать, что общие временные затраты могут оказаться сопоставимыми с временными затратами выполнения операции деления на первом блоке разбиения ЦБР-числа. Однако приведенный пример показывает, что и в этом случае трудоемкость вычислений параллельного алгоритма может оказаться выше, чем при последовательном выполнении операции деления. В частности, в рассматриваемом случае трудоемкость параллельного алгоритма в многопроцессорных системах может

оказаться в 1,6 (1,6≈41/26) раза выше, чем при последовательном выполнении алгоритма деления.

С целью проверки работоспособности и определения свойств *многопоточного* алгоритма был разработан модуль в инструментальной среде программирования *Free Pascal IDE for Win32 for i386* в режиме *Delphi Compatible.* Основной процедурой алгоритма является процедура *DivModThread(var a,b,R: BigInt),* которая описывается **Алгоритмом 2.**

Алгоритм 2. Параллельный алгоритм деления целых чисел

Вход: *Bigint a, b, R,* где $a>b$

Выход: $R = \lfloor a/b \rfloor$, $a=a \pmod b$

1: repeat
2: *CreateContext(a, b, ContextList);*
3: *CurrentNumTreads* ← *0*;
4: for *i* ← *0* **to** *ANT* **do** *ThreadPool[i]. Start;*
5: while *CurrentNumTreads* ≤ *ANT* **do**
6: if not *ContextList[i]. IsAdd* **then** *AddBlock(ContextList[i], R);*
7: for *i* ← *0* **to** *ANT* **do**
8: if not *ContextList[i]. IsAdd* **then** *AddBlock(ContextList[i], R);*
9: until *CompBlock(a, b)<0;*

Основными процедурами, типами и данными являются:

– *Bigint* – массив данных типа байт, *a, b, R* – делимое, делитель и частное;

– процедура *CreateContext* – процедура формирования контекста окружения для каждого из потоков. Контекст окружения (*ContextList*) потока представляет собой описание блока, включающего в себя следующую информацию: начало и конец блока делимого *(LSB, MSB)*, признак обработки суммированием частичных частных потока (если *IsAdd=false,* то суммирование частичных частных не производилось), адреса переменных *a* и *b* и другие описания.

– переменная *CurrentNumTreads* – определяет количество потоков, которые закончили деление блока;

– переменная *ANT*–определяет общее количество потоков в программе;

– *ThreadPool* – пул потоков. Пул потоков инициализируется в начале работы программы, после чего потоки переходят в режим ожидания. Поток продолжит свою работу после вызова процедуры *Start*, которая производит блочное деление и затем снова перейдет в режим ожидания. Перед окончанием работы потока значение *CurrentNumTreads* увеличивается на единицу процедурой *InterLockedIncrement*;

– процедура *AddBlock* – производит суммирование частичных частных (которые хранятся в контексте окружения потоков) с переменной *R*;

– функция *CompBlock* – возвращает значение 1, если *a>b*, значение 0, если *a=b* и значение -1 в противном случае.

В качестве платформы тестирования использовался настольный IBM-совместимый ПК процессор Intel Core с двумя ядрами с частотой 1,66 МГц и 2 ГБ ОЗУ. Используемая операционная система–MS Windows XP SP3. Полученные результаты тестирования показали совпадение с теоретическими предположениями.

Выводы:

Анализируя полученные результаты можно сделать следующие выводы:

– представленный алгоритм параллельного деления является масштабируемым;

– представленный алгоритм параллельного деления может быть реализован как в OPEN MP, так и в MPI-подобных системах. Следует при этом отметить, что в OPEN MP–подобных системах представленный алгоритм параллельного деления не является эффективной заменой последовательного алгоритма деления;

– невозможно достичь ускорения вычислений при многопоточной реализации алгоритма параллельного деления.

Литература

1. Чурсин В.Б. Об одной программной реализации многопоточного умножения целых чисел большой разрядности: Научный форум: Инновационная наука: сб. ст. по материалам IV междунар. науч.-практ. конф. – № 3(4). – М., Изд. «МЦНО», 2017. – 126 с.

2. Чурсин В.Б. Методы ускорения деления целых чисел большой разрядности: Научный форум: Инновационная наука: сб. ст. по материалам V междунар. науч.-практ. конф. – № 4(5). – М., Изд. «МЦНО», 2017. – 78 с.

ТЕХНОЛОГИЯ ИЗВЛЕЧЕНИЯ ЗНАНИЙ ИЗ СТАТИСТИЧЕСКИХ БАЗ ДАННЫХ ДЛЯ ПРИНЯТИЯ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ

Шепель Вячеслав Николаевич,
Оренбургский государственный университет, г. Оренбург,
Спешилов Евгений Алексеевич,
Оренбургский государственный университет, г. Оренбург

Аннотация

В статье говорится о роли информации, на которую опираются в процессе выработки и принятия решений. Сделан акцент на способы ее представления и обработки в рамках технологии извлечения знаний. Рассмотрена процедура определения эмпирической функции плотности $\hat{f}^{(n)}(x)$.

Процедура пригодна для использования при работе в статистических пакетах или подготовке программных продуктов.

Ключевые слова: *информация, знания, статистические данные, функция плотности, управленческие решения*

Keywords: *information, knowledge, statistics, density function, management decisions*

Роль информации в развитии общества чрезвычайно велика. От того, на сколько она актуальна, корректна, отвечает необходимым запросам зависит то, как она может использоваться, что в последствии неизбежно отражается на качестве принимаемых решений.

Постоянное увеличение количества информации процесс вполне естественный, однако, в связи с этим остро встает проблема ее обработки. Так как все накопленные данные имеют определённую ценность и значимость, то проблема нахождения информации напрямую зависит от ее актуальности, а с ростом количества данных растет и сложность их обработки [7].

Обработке подвергается любого рода информация, и в этом случае незаменимыми становятся информационные технологии, которые сегодня развиваются очень стремительно. Каждые два года происходит смена поколений аппаратных и программных средств вычислительной техники. Фактически за последние годы произошла революция в области передачи, накопления и обработки информации, затронувшая и коренным образом преобразовавшая все области человеческой жизни. Значительное увеличение возможностей компьютерной техники, развитие информационных сетей, создание новых информационных технологий приводят к радикальным изменениям во всех сферах общества: в производстве, банковском секторе, науке, образовании, медицине и т.д.

Управление в разных сферах человеческой жизни носит многоуровневый характер и требует решения многокритериальных детерминируемых задач в рамках подсистем [6]. Сама процедура при этом опирается в первую очередь на информацию, а уже от ее качества, достоверности и надежности зависит и качество принимаемых решений. Корректность обработки входных данных в совокупности с правильным выбором для этого аппарата напрямую влияют на эффективность результата решений при реализации.

На сегодняшний день наибольшую актуальность приобретает не просто процедура поиска данных, но и извлечения из них необходимых знаний.

Если раньше извлечение знаний из информации носило несколько творческий характер, то постепенно стали создаваться шаблоны. Эти шаблоны, вскоре, переросли в специальные пакеты, сначала специализированные, а затем и универсальные. Разрабатывались системы алгоритмов, статистическая обработка данных, выявление скрытых закономерностей [7]. Таким образом, можно говорить об извлечении знаний из некоторой совокупности информации, которую можно формализовать и назвать статистической базой данных.

В настоящее время, извлечение знаний достаточно сложный процесс, однако он уже имеет целый ряд решений. Кроме того, этот процесс постоянно развивается и совершенствуется, как развиваются и совершенствуются и все его методы. Так, в мировой практике, после процесса непосредственного сбора и записи данных в базу используются методы, получившие названия Data Mining. Data Mining – собирательное название, используемое для обозначения совокупности методов обнаружения в данных ранее неизвестных, нетривиальных, практически полезных и доступных интерпретации знаний, необходимых для принятия решений в различных сферах человеческой деятельности [3].

Одной из главных отраслей науки в области управления массивами данных – статистика. Статистика позволяет ориентироваться в сложных явлениях окружающего мира, поскольку всякая, достаточно сложная природная, социальная или техническая система подчиняется статистическим по своей форме проявления закономерностям [2]. Статистические методы обработки разработаны, в первую очередь, для случайных величин. Исчерпывающей же характеристикой случайной величины является закон распределения [4].

В практике статистического анализа и моделирования точный вид закона распределения анализируемой генеральной совокупности, как правило, бывает неизвестен. Мы располагаем лишь выборкой из интересующей генеральной совокупности [8]. Если это одномоментные наблюдения для одного признака, то матрица выборочных данных (в.д.) имеет вид:

$$(\text{в.д.})=\begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix}. \qquad (1)$$

Строить свои выводы и принимать решения мы вынуждены на основании расчета ограниченного ряда выборочных характеристик. К основным выборочным (эмпирическим) характеристикам [1] относятся:

- эмпирическая функция распределения $\hat{F}^{(n)}(x)$;

- эмпирическая функция плотности $\hat{f}^{(n)}(x)$;

- эмпирическая относительная частота $\hat{p}_i^{(n)}$ появления i-го возможного значения x_i дискретной случайной величины;

- эмпирические начальные и центральные моменты анализируемой случайной величины $\hat{m}_k(n)$ и $\hat{m}_k^o(n)$;

- порядковые статистики $x_{(i)}(n)(i=1,2,\dots,n)$.

Наиболее информативной для непрерывных случайных величин является выборочный аналог функции плотности (эмпирическая функция плотности) $\hat{f}^{(n)}(x)$. В статье предлагается алгоритм (процедура) определения $\hat{f}^{(n)}(x)$ пригодный для использования при работе в статистических пакетах или подготовке программных продуктов.

Процедура определения эмпирической функции плотности $\hat{f}^{(n)}(x)$:

1) Отмечаются наименьшее $x_{\min}(n)$ и наибольшее $x_{\max}(n)$ значения в выборке (1).

2) Диапазон $[x_{\min}(n),\ x_{\max}(n)]$ разбивается на s равных интервалов группирования; при этом количество интервалов должно быть в пределах 7-20. В выборе s можно пользоваться приближенной формулой $s \approx 1 + 3{,}2\ \lg(n)$.

3) Отмечаются крайние точки каждого из интервалов $c_0, c_1, c_2, ..., c_s$ в порядке возрастания; для чего определяется длина интервала $\Delta_{k(x)} = (x_{\max}(n) - x_{\min}(n))/[s]$, затем $c_{k(x)} = c_{k(x)-1} + \Delta_{k(x)}$, а также их середины $x_1^0, x_2^0, ..., x_s^0$.

4) Подсчитываются числа выборочных данных, попавших в каждый из интервалов: $\nu_1, \nu_2, ..., \nu_s$ (очевидно, $\nu_1 + \nu_2 + ... + \nu_s = n$); выборочные данные, попавшие на границы интервалов, либо равномерно распределяются по двум соседним интервалам, либо относятся только к какому-либо одному из них.

5) Для каждого интервала рассчитывается эмпирическая функция плотности $\hat{f}^{(n)}(x) = \dfrac{\nu_{k(x)}}{n\Delta_{k(x)}}$, где $k(x)$ – порядковый номер группирования, который накрывает точку x; $\nu_{k(x)}$ – число наблюдений, попавших в этот интервал, $\Delta_{k(x)}$ – длина интервала.

6) Строится гистограмма, для чего на оси абсцисс откладываются крайне точки каждого из интервалов $c_0, c_1, c_2, ..., c_s$, по оси ординат эмпирическая функция плотности $\hat{f}^{(n)}(x)$. Тогда k-му интервалу будет соответствовать прямоугольник, основанием которого является замкнутый слева интервал $[c_{k-1}, c_k)$, а высота $\hat{f}^{(n)}(x) = \dfrac{\nu_{k(x)}}{n\Delta_{k(x)}}$.

7) По виду гистограммы принимается гипотеза о модели закона распределения анализируемой генеральной совокупности (например, нормальный, экспоненциальный, равномерный и т.д.).

8) Рассчитываются оценки неизвестных параметров гипотетического закона распределения $\theta_1', \theta_2', ..., \theta_k'$ (например, для нормального закона распределения выборочное среднее $\bar{x}(n)$ и выборочную дисперсию $s^2(n)$).

Эмпирическая функция плотности $\hat{f}^{(n)}(x)$ – получена. Возникает необходимость в экспериментальной проверке гипотезы, о виде закона распределения анализируемой генеральной совокупности, т.е. наша цель

– проверить, не противоречит ли высказанная гипотеза *H* имеющимся выборочным данным.

Задача может быть решена качественно или количественно [8].

В заключении отметим, за последние два десятилетия информационные технологии в производстве и бизнесе вышли за рамки обычной компьютеризации и автоматизации – они стали основой эффективного использования финансового менеджмента и маркетинга, успешного управления ресурсами предприятия и взаимоотношениями с клиентами. Более того, информационные технологии дали бизнесу доступ к серьезному потенциалу, накопленному в научных областях: статистическому анализу и численному моделированию, теориям сложных систем и нейронных сетей [5]. На сегодняшний день существует достаточно большое количество различных информационных продуктов, которые могут проводить самые разнообразные расчеты. Входящие данные достаточно легко можно обработать, используя прикладные статистически пакеты, однако на практике, в процессе проведения анализа входящей информации и ее статистической обработки, вид закона распределения (которому бы подчинялся неизвестный анализируемый массив данных) часто бывает не определен. Это ведет к некорректному применению аппарата обработки данных, а значит и к неверному выводу, что в последствие приведет к высокой погрешности выработанных решений. Поэтому правильно организованная технология извлечения знаний из статистических баз данных способствует эффективной организации процедуры принятия управленческих решений.

Литература

1. Айвазян В.С. Прикладная статистика. Основы эконометрики Т.1. Теория вероятностей прикладная статистика: Учебник для вузов / В.С. Айвазян, С.А. Мхитарян. – В 2 т. 2-е изд., испр. – М.: ЮНИТИ-ДАНА, 2001. – 656 с.

2. Афанасьев В.Н. Использование в образовании статистической методологии познания // Сборник материалов Всероссийской научно-методической конференции «Университетский комплекс как региональный центр образования, науки и культуры» [Электронный ресурс]. – Оренбург: ОГУ, 2014. – С. 1814-1820. – Режим доступа: http:// elib.osu.ru/bitstream/123456789/776/1/1814-1820.pdf

3. Дюк В.А. Применение технологий интеллектуального анализа данных в естественнонаучных, технических и гуманитарных областях / В.А. Дюк, А.В. Флегонтов, И.К. Фомина // Известия Российского государственного педагогического университета им. А.И. Герцена. – 2011. – № 138. – С. 77-84.

4. Орлов А.И. Устойчивые экономико-математические методы и модели. Разработка и развитие устойчивых экономико-математических методов и моделей для модернизации управления предприятиями. – Saarbrücken (Germany), LAP (LAMBERT Academic Publishing), 2011. – 436 с.

5. Спешилова Н.В. Информационные технологии в бухгалтерском учете // Материалы международной научно-практической конференции «Состояние, перспективы экономико-технологического развития и экологически безопасного производства в АПК». Ч.II. – Оренбург: Издательский центр ОГАУ, 2010.– С. 30 – 36.

6 Шепель В.Н. Многокритериальные детерминированные задачи принятия решений подсистем высших учебных заведений / В.Н. Шепель Н.В. Спешилова // Интеллект. Инновации. Инвестиции. – 2016. – №12. – С.124-128.

7. Шепель В.Н. Проблемы извлечения знаний. /В.Н. Шепель, С.С. Акимов // Материалы Всероссийской научно-методической конференции «Университетский комплекс как региональный центр образования, науки и культуры». – [Электронный ресурс]. – Оренбург: ОГУ, 2015. – С. 1562-1565. – Режим доступа: http://elibrary.ru/item.asp?id=23153373

8. Шепель В.Н. Процедура построения выборочного аналога функции плотности // Вестник ОГУ. – 2012. – №2 (138). – С.320-322.

СОДЕРЖАНИЕ

ФОРМИРОВАНИЕ ЕДИНОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА ПРЕДПРИЯТИЯ/ОРГАНИЗАЦИИ

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ И ОРГАНИЗАЦИИ

АКТУАЛЬНЫЕ ВОПРОСЫ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ НА ПРЕДПРИЯТИИ

Научное издание

СБОРНИК МАТЕРИАЛОВ

Всероссийской научно-практической конференции

«АКТУАЛЬНЫЕ ПРОБЛЕМЫ АВТОМАТИЗАЦИИ УПРАВЛЕНИЯ НА ПРЕДПРИЯТИИ И В ОРГАНИЗАЦИИ»

Научно-издательский центр «Логос»
Web-site: http//центр-логос.рф
E-mail: logos.centr@mail.ru

Подписано в печать 20.03.2018. Формат 60x84 1/16
Бумага офсетная. Гарнитура «Times». Печать цифровая.
Усл. печ. л. 4,88 Заказ № 771. Тираж 500 экз.
Отпечатано с готового оригинал-макета в типографии издательско-полиграфического комплекса СКФУ, г. Ставрополь, пр. Кулакова, 2