

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ



**Сборник
научных работ
аспирантов
и студентов
СПбГУ ИТМО**

САНКТ-ПЕТЕРБУРГ
2009

РАБОТЫ АСПИРАНТОВ

УДК 681.327.22

В. Ф. БЕЗЗУБОВ — кафедра Вычислительной техники

ВОЗМОЖНОСТЬ ПОВЫШЕНИЯ СКОРОСТИ ИНФОРМАЦИОННОГО ОБМЕНА В ОТКАЗОУСТОЙЧИВЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМАХ

Научный руководитель — д.т.н., профессор В. А. Богатырев

При построении распределенных управляющих вычислительных систем реального времени отказоустойчивость достигается введением структурной и временной избыточности.

Временная избыточность достигается путем использования в системе вычислительных устройств повышенной производительности, а также увеличения скорости межмашинного обмена, резервного копирования данных и реконфигурации системы после отказа.

Широко применяется объединение вычислительных модулей системы посредством общей магистрали, что требует для сокращения затрат времени оптимального варианта организации передачи информации при достижении компромисса между производительностью и стоимостью системы [1].

Повысить эффективность распределенных управляющих компьютерных систем предлагается, повысив скорость обмена информацией за счет применения устройства переключения (перекоммутации) [2] блоков памяти и устройства ускоренного обмена (УУО) [3], реализующего способ двойного прямого доступа к памяти [4]. Такое решение позволяет сократить время информационного обмена в два раза по сравнению с применяемыми устройствами, использующими такие контроллеры, как Intel 8257, Intel 8237, M16C/61/62 (фирма Mitsubishi Electric), DMA08 (Motorola).

В работе [4] рассматривались различные варианты организации межпроцессорного обмена и получены следующие параметры: обмен через общую память: $T_{оп} = 4tN$; обмен через общую межмашинную магистраль: $T_{ммк} = 2t(N+4)$;

— обмен посредством устройства ускоренного обмена: $T_{ууо} = t(N+16)$; обмен перекоммутацией блоков памяти: $T_{п} = \tau + 15t$, T — время, затрачиваемое на обмен информационным массивом; t — время одного процессорного цикла ввода, вывода; τ — время, затрачиваемое процессором на завершение текущей команды с момента прерывания; N — количество слов в информационном массиве.

Сравнив приведенные формулы, можно сделать вывод, что применение в управляющих вычислительных системах реального времени устройства перекоммутации блоков памяти, а также УУО позволит уменьшить время, затрачиваемое на обмен информацией и получить дополнительные временные ресурсы для реализации методов программной, информационной и временной избыточности.

Предлагается структурное решение [5], в котором резервирование осуществляется методом замещения таким образом, что при выходе из строя любого вычислительного модуля (ВМ) системы ВМ, взявший на себя функции отказавшего, имеет полный доступ к внутренним ресурсам отказавшего ВМ, что позволяет сократить время восстановления системы и соответственно повышается коэффициент готовности системы.

Литература

1. *Богатырев В.А., Иванов Л.С., Апинян В.В.* Математическая модель мультипроцессорных систем с общей магистралью // Техника средств связи. Сер. Техника проводной связи. 1985. Вып. 4.
2. Патент СССР. № 1679493 G 06 F 13/00. Устройство для сопряжения ведущей и ведомой ЭВМ / *В.Ф. Беззубов* и др.
3. А.с. СССР. № 1462341 G 06 F 15/16. Устройство для сопряжения ЭВМ. / *В.Ф. Беззубов*.
4. *Беззубов В.Ф.* Сравнительный анализ методов обмена в многопроцессорных системах // Вестн. компьютерных и информационных технологий. 2006. № 4.
5. А.с. СССР № 1798946 Н 05 К 10/00, G 06 F11/20. Резервированная вычислительная система / *В.Ф. Беззубов* и др.

УДК 681.3

С. В. БОГАТЫРЕВ — кафедра Вычислительной техники

СТРУКТУРА ЦЕНТРОВ ОБРАБОТКИ И ХРАНЕНИЯ ДАННЫХ

Научный руководитель — д.т.н., профессор А.А. Ожиганов

В корпоративных центрах обработки данных (ЦОД), построенных в соответствии с архитектурой SONA (Service-Oriented Network Architecture) выделяются уровни [1]: агрегирования (коммуникационное оборудование, средства доступа); внешний (серверы представления информации); приложений (кластеры приложений); внутренний (кластер серверов); хранилищ данных (коммутаторы сети хранения данных, дисковые системы хранения). Межуровневое взаимодействие осуществляется через коммуникационные узлы.

При разработке ЦОД необходимо найти число узлов (кратность резервирования) на каждом уровне $m=(m_1, m_2, \dots, m_n)$ и тип организации системы хранения, при котором достигается максимум надежности ЦОД $P(m) \rightarrow \max$ и минимум среднего времени пребывания запросов в нем $T(m) \rightarrow \min$, при ограничении стоимости реализации системы

$\sum_{i=1}^n m_i c_i \leq C_0$, где n число рассматриваемых при оптимизации уровней ЦОД, c_i — стоимость узла i -го уровня.

Оценивая эффективность каждого работоспособного состояния ЦОД (выраженной величиной обратной времени пребывания запросов в ЦОД) относительно эффективности исходного состояния системы T_0 (когда все узлы исправны) коэффициент сохранения эффективности K системы определим как [2]:

$$K = \sum_{k_1=1}^{m_1} \sum_{k_2=1}^{m_2} \sum_{k_3=1}^{m_3} \dots \sum_{k_n=1}^{m_n} \left[\frac{T_0}{\sum_{i=1}^M \frac{v_i}{1 - v_i \lambda / k_i}} \right] C_{m_1}^{k_1} C_{m_2}^{k_2} C_{m_3}^{k_3} \dots C_{m_n}^{k_n} p_1^{k_1} p_2^{k_2} p_3^{k_3} \dots p_n^{k_n} \times \\ \times (1 - p_1)^{m_1 - k_1} (1 - p_1)^{m_1 - k_1} (1 - p_2)^{m_2 - k_2} (1 - p_3)^{m_3 - k_3} \dots (1 - p_n)^{m_n - k_n}.$$

Здесь

$$T_0 = \sum_{i=1}^n \frac{v_i}{1 - v_i \lambda / m_i},$$

v_i — среднее время выполнения запросов узлом i -го уровня, p_i — вероятность работоспособности узла i -го уровня.

При выборе структуры ЦОД необходим учет альтернатив построения системы (сети) хранения данных, в том числе вариантов объединения дисков в RAID массивы, характеризующиеся различными показателями избыточности, скорости, стоимости и надежности, влияющими на эффективность ЦОД в целом. При оценке надежности узлов хранения данных, представляющих собой объединение дисков в RAID-массив, необходимо учитывать его организацию. Так, если массив состоит из s основных дисков, вероятность работоспособности каждого из которых r , то для RAID 0 вероятность работоспособности системы хранения равна r^s , так как любой отказ приводит к потере данных. Для RAID 1 вероятность работоспособности системы хранения равна $(1 - (1 - r)^2)^s$, так как данные дублируются в разных дисках.

При построении высоконадежной системы хранения кластерной архитектуры предполагается использовать архитектуру RADOS (Reliable, Autonomic Distributed Object Store) [3, 4]. Архитектура RADOS подразумевает разделение кластера на узлы хранения и управляющие узлы, при этом клиенты получают данные непосредственно с узлов хранения. Особенностью такого подхода является то, что управляющие узлы не содержат индекса данных, а занимаются постоянным мониторингом состояния кластера и поддержанием актуальности карты кластера. Функция размещения опирается на карту сети и, используя заданные параметры хранения данных, возвращает узлы хранения, на которых может быть размещена информация. При отказе узла это событие учитывается в актуальной карте сети, что позволяет заменить вышедший из строя узел, сохраняя работоспособность системы.

Литература

1. Архитектура и технологии ЦОД. [электронный ресурс]: <http://www.nvisiongroup.ru/tech_cod.html>.
2. Богатырев В.А. К оптимальному резервированию системы разнородных серверов // Приборы и системы. Управление, контроль, диагностика. 2007. № 12. С. 30—35.
3. Weil S. A., Leung A. W., Brandt S. A., Maltzahn C. RADOS: A Fast, Scalable, and Reliable Storage Service for Petabyte-scale Storage Clusters. Petascale Data Storage Workshop SC07. 2007.
4. Xin Q., Miller E. L. Impact of Failure on Interconnection Networks for Large Storage Systems // Proc. 22nd IEEE. 13th NASA Goddard Conf. on Mass Storage Systems and Technologies (MSST 2005). Monterey, CA, 2005.

Д. А. БОГОЛЮБОВ — кафедра Проектирования компьютерных систем

**ПРОГРАММНАЯ РЕАЛИЗАЦИЯ МЕТОДА КОНЕЧНО-ЭЛЕМЕНТНОГО АНАЛИЗА
РАДИОЭЛЕКТРОННЫХ КОНСТРУКТИВОВ**

Научный руководитель — к.т.н., доцент Н.С. Кармановский

В работе представлена методика расчетов приемно-измерительного модуля системы спутниковой навигации ГЛОНАСС. Особенностью работы данного модуля является наличие тепловыделяющих элементов, необходимых для стабилизации теплового режима. Поддержание температуры производится пятью нагревательными элементами мощностью по 0,75 Вт, равномерно распределенными по поверхности печатной платы приемно-измерительного модуля [1].

Используемые в настоящее время программные продукты не обеспечивают требуемой точности расчетов и имеют закрытые исходные коды и алгоритмы, требуют значительных вычислительных мощностей. В работе предложено использовать алгоритм фронтального исключения, реализующий метод конечно-элементного анализа [2]. Точность расчета с использованием данного алгоритма определяется размерностью матрицы жесткости фронта и может устанавливаться пользователем [3]. При программной реализации данного алгоритма рационально используется оперативная память. Алгоритм позволяет сократить время расчета тепловых режимов на 10—15 %.

Программная реализация алгоритма позволяет осуществлять «сквозное» проектирование, к примеру, совмещая тепловые расчеты с расчетами механических напряжений. При этом экономия времени расчетов может достигать до 20 %.

Литература

1. *Боголюбов Д.А., Кармановский Н.С.* Исследование тепловых режимов различных радиоэлектронных конструктивов с помощью системы COSMOSWorks // Науч.-технич. вестн. СПбГУ ИТМО. 2007. Вып. 44. С. 234—238.
2. *Копысов С.П., Пономарев А.Б., Рынков В.Н.* Открытое визуальное окружение для взаимодействия с геометрическими ядрами, генерации / перестроения / разделения сеток и построения расчетных моделей // Тр. Всеросс. конф. «Прикладная геометрия, построение расчетных сеток и высокопроизводительные вычисления». М.: ВЦ РАН, 2004. Т. 2. С. 154—164.
3. *Баранов Л.Б.* Актуальные вопросы технологии современных САПР. // Там же. С. 131—142.

М. Г. ГЕНИН — кафедра Проектирования компьютерных систем

ОРГАНИЗАЦИЯ ВЗАИМОДЕЙСТВИЯ ИНТЕГРИРОВАННОЙ БАНКОВСКОЙ СИСТЕМЫ С ВНЕШНИМИ ПОДСИСТЕМАМИ

Научный руководитель — д.т.н., профессор С.А. Арустамов

Одной из основных задач, возникающих при внедрении банковской системы, является обеспечение возможности обмена информацией с внешними подсистемами, которые не являются частью самой банковской системы. В настоящей работе рассмотрены вопросы, связанные с организацией такого взаимодействия. Основное внимание уделено так называемому on-line-взаимодействию, которое, по нашему мнению, представляет сегодня наибольший интерес.

Всю совокупность данных, обмен которыми происходит между интегрированной банковской системой (далее — ИБС) и внешними подсистемами, можно условно разделить на несколько типов:

- платежные документы,
- нормативно-справочная информация,
- отчетная информация.

На рис. 1 представлена схема обмена данными банковской системы с внешними программами.

Существует два способа обмена данными — односторонний и двусторонний.

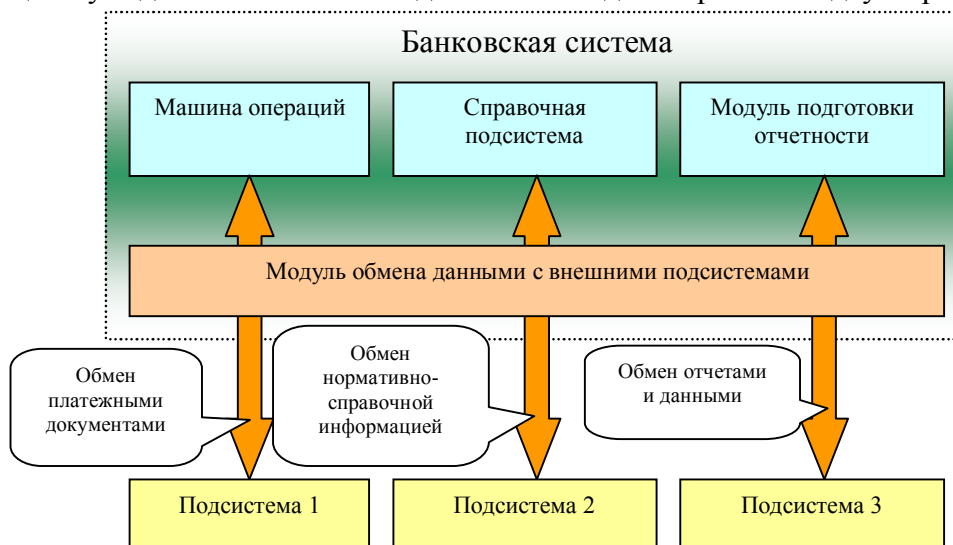


Рис. 1

Односторонний обмен происходит, когда единичным актом обмена данными между подсистемами является сброс данных из передающей подсистемы в принимающую. В случае двустороннего обмена данными единичный акт обмена включает в себя передачу данных в обоих направлениях. Типичный пример двустороннего обмена данными — это передача данных из одной системы в другую с получением передающей системой подтверждения приема данных от принимающей системы.

В каждом из перечисленных выше способов обмена можно выделить так называемые «on-line-обмен» и «off-line-обмен». On-line-обмен предполагает, что между двумя обменивающимися подсистемами установлено постоянное соединение. В этом случае обмен данными достаточно просто организовать так, чтобы не требовалось участия пользователя в процессе обмена.

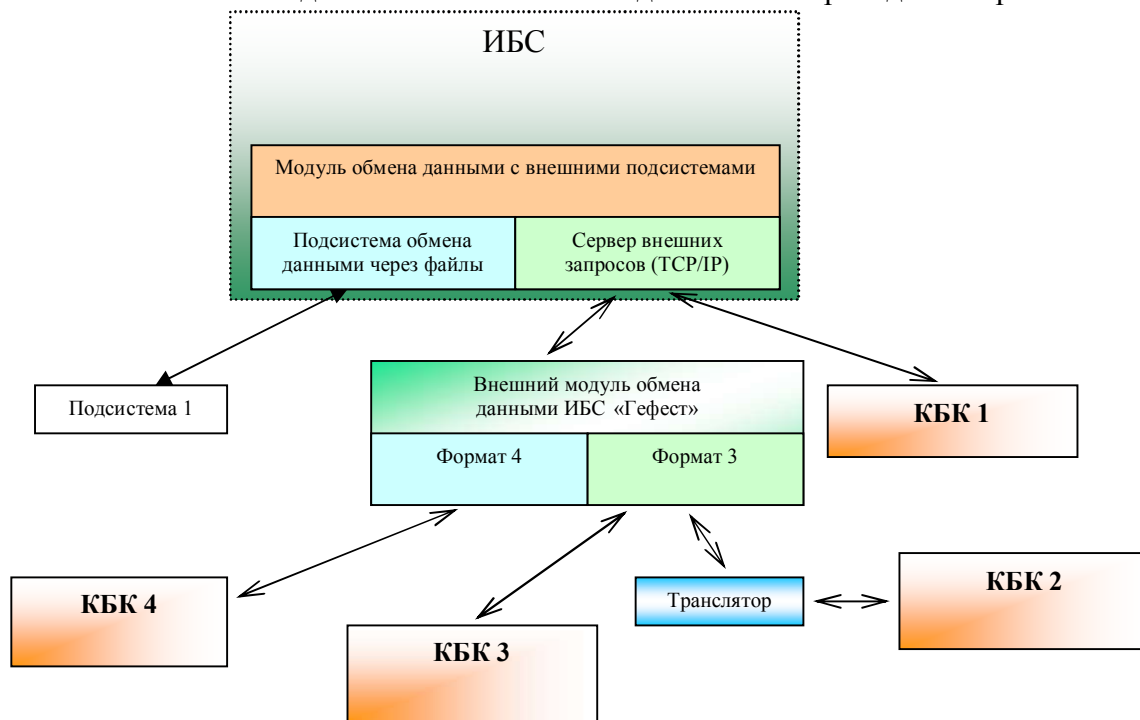
Off-line-обмен предполагает, что между двумя обменивающимися подсистемами постоянное соединение отсутствует. В такой ситуации полностью автоматизировать процесс обмена сложнее, поскольку для передачи данных необходимо выполнять дополнительные действия, зависящие от конкретной организации обмена в том или ином случае. Как правило, в процессе off-line-обмена требуется участие пользователя.

Как показывает опыт, все подсистемы можно условно разделить на две категории. В первую входят подсистемы, которые предоставляют возможность обмена способом «односторонний off-line» или «односторонний on-line», т.е. либо только сбрасывают данные в ИБС за один акт обмена, либо только принимают их. Во вторую категорию входят подсистемы типа «банк—клиент», работающие в режиме «двусторонний on-line».

Однако у файлового обмена есть принципиальные недостатки. Один из них —это зависимость от платформы, на которой работают обменивающиеся данными подсистемы. Другой существенный недостаток проявляется при организации такого обмена между удаленными подсистемами. В этом случае значительно снижается скорость обмена данными.

Представляется целесообразным использовать еще и такой способ обмена данными, который бы не зависел от конкретной платформы, а также позволил бы легко осуществлять on-line-взаимодействие не только в рамках локальной сети, но и между удаленными подсистемами [1]. Для этого может быть использован обмен по сетевому протоколу TCP/IP.

Полная схема обмена данными с внешними подсистемами приведена на рис. 2.



Комплекс «банк—клиент» (КБК) 1 работает с ИБС непосредственно по протоколу TCP/IP в формате обмена данными, определенном ИБС. Если в системе КБК для обмена данными используются файлы, то для таких КБК в системе предусмотрен внешний модуль обмена данными ИБС. КБК 3 работает непосредственно в формате 3, КБК 2 использует транслятор для перевода данных из файлов собственного формата в файлы формата 3. В этой схеме важным является то, при взаимодействии с подсистемами типа «банк—клиент» обмен данными непосредственно со стороны ИБС осуществляется только по протоколу TCP/IP. Обмен данными через файлы ведется не с самой ИБС, а с внешним модулем обмена ИБС, который является внешним по отношению к самой ИБС.

Таким образом, в работе показано, что в процессе взаимодействия банковской системы с внешними подсистемами могут применяться различные схемы такого взаимодействия. Задача организации обмена данными между банковской системой и внешними подсистемами состоит в обеспечении банку возможности использования различных схем взаимодействия. Основная роль в организации такого обмена должна приходиться на банковскую систему. Реализация в банковской системе встроенного интерфейса для организации различных схем обмена данными позволяет организовать такой обмен наиболее оптимальным способом.

Литература

1. Компания «Програмбанк». Продукты и решения — Возможности ИБС «Гефест» — [Электронный ресурс]: <http://www.programbank.ru/pbsite.nsf/0/03782095C6895C88C3256C6800406884?OpenDocument>.
2. *Калемберг Д., Комарова Н.* Сценарии обеспечения безопасной работы клиентов в системе ДБО // Банковские технологии Экспертиза. 2009. № 6. С. 8—11.

УДК 004.654

В. Н. ЗИМИН — кафедра Проектирования компьютерных систем

ПРОБЛЕМЫ СОВМЕСТИМОСТИ СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

Научный руководитель — к.т.н., доцент Б.А. Крылов

Приводятся краткие сведения о форматах хранения данных систем автоматизированного проектирования (САПР). Рассматриваются проблемы, связанные с использованием закрытых форматов данных и их совместимостью с различными САПР, также описываются универсальные открытые форматы файлов и возможность их применения в современных САПР.

В современном мире почти каждый проект, — от постройки дома до разработки нового микропроцессора — требует больших затрат времени, что отчасти компенсируется использованием различных САПР. Однако одной из проблем является корректный обмен данными в различных форматах между системами. Это подчас является не тривиальной задачей вследствие поддержки рядом производителей САПР только собственных закрытых форматов хранения данных.

Вопросы переносимости электронных документов из одной системы проектирования в другую возникли практически одновременно с появлением самих систем. Сейчас благодаря массовому появлению на рынке свободно распространяемого программного обеспечения все больше производителей включают в интерфейс своих продуктов функции импорта и экспорта в открытые форматы или же раскрывают спецификации своих проприетарных форматов.

Спецификация формата DXF для решения задач, связанных с системами автоматизированного проектирования, и при этом достаточная универсальность вместе с открытостью и относительной простотой сделали его на данный момент основным форматом межсистемного обмена. На данный момент практически все современные САПР поддерживают экспорт и импорт в данный формат. Однако, к сожалению, в области

совместимости различных САПР по-прежнему существуют проблемы. Связаны они, в первую очередь с самим форматом DXF. Формат DXF является разработкой фирмы Autodesk и нацелен на основной продукт этой фирмы — AutoCAD. Эта САПР постоянно эволюционирует, что заставляет фирму Autodesk изменять спецификацию DXF практически с каждой новой версией AutoCAD, что приводит к несовместимости версий формата. Сторонний программный продукт, работающий с одной версией DXF, может иметь проблемы обработке данных в более новом формате.

С одной стороны, стремление Autodesk совершенствовать свою программную продукцию вполне логично, и вытекающая отсюда несовместимость версий форматов закономерна. Но с другой стороны — возникает достаточно парадоксальная ситуация: формат, предназначенный для решения вопросов совместимости, сам имеет проблемы с совместимостью! Помимо того, по мере усложнения AutoCAD фирма-разработчик не полностью отражает внесенные изменения в спецификации DXF, что постепенно снижает эффективность использования DXF. Это заставило другие фирмы-разработчики САПР искать альтернативу формату DXF.

Этой альтернативой стал формат DWG — двоичный файловый формат AutoCAD. Таким образом, на данный момент подавляющее большинство различных САПР поддерживают форматы межсистемного обмена DXF или DWG. Это несмотря на существующие ограничения позволяет использовать разнонаправленные САПР в рамках одного проекта, а также относительно «безболезненно» переходить с САПР одной фирмы на другую. Сейчас все еще возникают сложности с закрытыми форматами, однако поддержка экспорта в открытые форматы типа XML, уже сейчас во многом нивелирует этот недостаток.

Литература

1. Автоматизация инженерно-графических работ / Г. Красильникова, В. Самсонов, С. Тарелкин СПб: Питер, 2001. 256 с.
2. Латышев П. Н. Каталог САПР. Программы и производители. 2008—2009. М.: Солон-Пресс, 2008. 704 с.
3. DXF [Электронный ресурс]: <<http://ru.wikipedia.org/wiki/DXF>>.
4. Создание AutoCAD [Электронный ресурс]: <http://www.compkursy.ru/grafica/autocad_history.htm>.

УДК 004.91; 004.383.4; 004.891.2; 004.896

П. А. КОСЕНКОВ — кафедра Проектирования компьютерных систем

СИСТЕМА ИНТЕЛЛЕКТУАЛЬНОГО АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ ЭЛЕКТРОННЫХ УСТРОЙСТВ

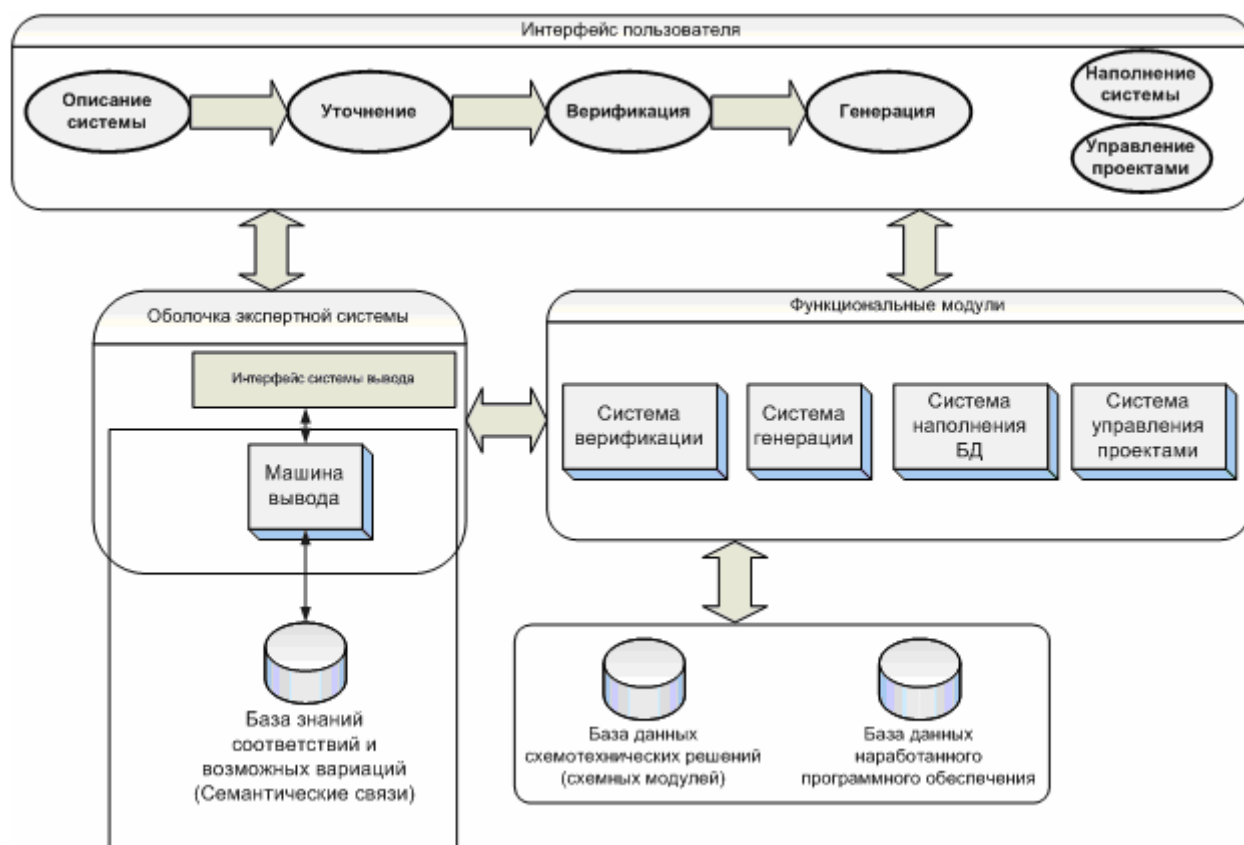
Научный руководитель — д.т.н., профессор Ю.А. Гатчин

Электроника представляет собой быстро развивающуюся отрасль науки и техники, в современном мире она заняла прочное место во всех сферах жизни и деятельности людей. Научные приборы, станки с ЧПУ, бытовая техника — везде применяется электроника [1]. Такому внедрению поспособствовало появление большого разнообразия электронных

компонентов, микропроцессоров; появление новых методов проектирования, систем автоматизированного проектирования (САПР). На сегодняшний день идет постоянное наращивание темпов вывода новых устройств на рынок и цена промедления и тем более ошибки производителя становится все значительнее [2].

В рамках настоящей работы исследуются методы, позволяющие накапливать инженерный опыт не только в виде чертежей и разрозненного программного кода, как это делается сейчас, а как набор схемных решений связанного с ними программного кода. Такой подход позволит не только создавать базу уже готовых инженерных решений, но и многократно применять этот опыт в новых устройствах, при этом снижая себестоимость, повышая надежность и сокращая сроки разработки.

Разработана модель интеллектуальной САПР устройств, на выходе которой будет реализован полный набор аппаратных и программных составляющих разрабатываемой системы. В работе рассмотрены особенность системы, которые выводят ее за рамки классических САПР, — в частности, наличие экспертной системы выбора решения и агрегация наработанных инженерных решений в уже существующих проектах с открытой производственной документацией (см. рисунок).



В результате работы системы возможно формировать такие документы, как функциональные и принципиальные электрические схемы, спецификации и перечни компонентов, а также программное обеспечение, обеспечивающее базовую функциональность аппаратной части. Предполагается, что базы данных будут пополняться опробованными и подтвержденными схмотехническими и программными решениями.

Для проверки концепции и последующего тестирования системы было решено выбрать проекты с открытой производственной документацией, они наиболее адекватно удовлетворяют всем требованиям, а также не вызывают сомнений в легитимности применения [3]. Данная система позволит создавать комплексные устройства в минимальные сроки с минимальными затратами времени, и количеством итераций в разработке.

Представленный подход к созданию электронных устройств на данный момент является одним из перспективных. Несомненно, метод разработки устройств с открытой производственной документацией требует доработки. В частности, проект одноплатного компьютера на базе ARM-архитектуры является пилотным с открытой производственной документацией, на котором будут отработаны механизмы группового проектирования и создания документации, отладки предсерийных образцов и способы управления инженерным сообществом, которое формирует базу инженерных знаний.

Литература

1. *Преснухин Л.Н., Шахнов В.А.* Конструирование электронных вычислительных машин и систем: Учебник. М.: Высш. школа, 1986.
2. *Косенков П.А., Терентьев А.О.* Особенности проектирования современных встраиваемых электронно-вычислительных систем и разработка плат для прототипирования // Науч.-техн. вестн. СПбГУ ИТМО. Вып. 29. «Информационная безопасность, проектирование, технология элементов и узлов компьютерных систем». 2007.
3. *Косенков П.А.* Особенности проектов с открытой производственной документацией на примере одноплатного компьютера // Науч.-техн. вестн. СПбГУ ИТМО. Вып. 57. «Информационные технологии и телекоммуникационные системы» Реферируемое издание. 2008. С. 97.

УДК 004.056(043)

Д. В. МАЛЬШАКОВ — кафедра Проектирования компьютерных систем

ОЦЕНКА ЭФФЕКТИВНОСТИ ПРИНЯТЫХ МЕР ПО ЗАЩИТЕ ИНФОРМАЦИИ

Научный руководитель — к.т.н., доцент И.Б. Бондаренко

Развитие и распространение сложных систем защиты информации (ЗИ), компонентами которых являются технические средства, программное обеспечение, а также человек, обуславливают необходимость использования новых подходов при оценке их эффективности. Сложность оценки эффективности разработанных систем возникает из-за их динамичности, масштабируемости, открытости и децентрализации. В связи с этим оценка эффективности комплекса принятых мер по ЗИ относится к многокритериальной задаче [1], т.е. для оценки эффективности необходимо использовать множество показателей:

$$N = N_1, N_2, \dots, N_n, \quad (1)$$

В качестве показателей N_i ($i = \overline{1, n}$) можно использовать вероятность взлома рубежа защиты, время преодоления рубежа защиты, вероятность того, что информация будет передана, время доставки информации и т.д.

Для многокритериальной оценки эффективности могут быть использованы два подхода [2]. Первый из них основан на свертке частных показателей N_i к единому G , называемому комплексным показателем эффективности. Такая свертка может производиться по аддитивному

$$G_a = \sum_{i=1}^n N_i \quad (2)$$

или мультипликативному соотношению

$$G_M = \prod_{i=1}^n N_i . \quad (3)$$

Второй подход основан на использовании аппарата методов теории многокритериального выбора и принятия решений, к ним относятся: методы нелинейного программирования; генетические алгоритмы; нейронные сети.

Свойства системы ЗИ могут изменяться во времени, поэтому точное количественное определение параметров оценки эффективности является сложной задачей. Еще более трудоемкой задачей является определение сложности и стоимости средств защиты S , которая должна быть уравновешена достигнутым уровнем защиты информации.

Для решения поставленной задачи предлагается:

— затраты на компоненты защиты S_i и количественные показатели N_i в (1)—(3) считать нечеткими переменными, для которых определены минимально и максимально допустимые пределы;

— выбирать структуру системы ЗИ с учетом заданного уровня защищенности.

При этом, используя теорию нечетких множеств и методы многокритериальной оптимизации, можно определить:

— минимум вероятности взлома механизмов ЗИ;

— максимум вероятности передачи данных;

— оптимальный вид свертки локальных критериев в комплексный показатель по соотношениям (2) и (3).

Таким образом, с помощью использования теории нечетких множеств и методов многокритериальной оптимизации можно оценить эффективность принятых мер по ЗИ с учетом заданного уровня защищенности. Необходимо отметить, что при изменении любого параметра, описанного в работе, оптимизацию системы ЗИ необходимо проводить заново.

Литература

1. Нечеткие множества в моделях управления и искусственного интеллекта / Под ред. Д.А. Поспелова. М.: Наука, 1986.
2. Ярочкин В.И. Информационная безопасность: Учебник. М.: Академический проект, 2004. 544 с.

УДК 004.896

А. Н. ПЛОТНИКОВ — кафедра Проектирования компьютерных систем

ПРОЦЕСС АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Научный руководитель — д.т.н., профессор Ю.А. Гатчин

За сравнительно короткий исторический период, насчитывающий немногим более ста лет, самолет из экспериментального летательного аппарата (ЛА), демонстрировавшего

перед изумленной публикой свои довольно скромные по современному представлению возможности, превратился в надежное и незаменимое транспортное средство [1]. За это время сменилось много поколений самолетов, неизмеримо вырос их технико-экономический уровень. Этот уровень отражает не только возросшие технические возможности, но и богатый опыт исследований, накопленный в процессе создания самолетов. Однако задача создания нового самолета не стала тривиальной, поскольку для ее решения всегда требуется сделать шаг вперед за пределы прошлого опыта.

Необходимость в разработке новых ЛА возникает по двум причинам. Во-первых, происходит постепенное моральное устаревание существующих типов самолетов, а также появляются новые технические возможности, реализация которых обещает повышение технико-экономических показателей самолета и транспортной системы в целом. Во-вторых, государство и транспортные компании ставят перед авиацией задачи, решение которых с помощью существующих типов ЛА невозможно или экономически нецелесообразно.

Ключевым элементом процесса создания самолета является проектирование. Целью создания систем автоматизированного проектирования (САПР) является повышение качества и технико-экономического уровня проектируемых ЛА, повышение производительности труда проектировщиков, сокращение сроков работ, уменьшение стоимости и трудоемкости проектирования. Проследим, каковы основные направления применения САПР по этапам проектирования и конструирования ЛА [2].

— *Этап подготовки технических предложений.* Основные задачи: выбор концепций применения проектируемого ЛА и определение облика (конфигурации, состава и типовых режимов движения), обеспечивающего выполнение целевых задач.

Направления применения средств автоматизации: определение технико-экономической эффективности, поиск оптимального облика; выбор альтернативных вариантов с учетом факторов неопределенности и критериев технического риска и в завершение — имитационное моделирование для оценки выполнения целевых задач.

— *Этап эскизного проектирования.* Производится определение параметров конструкции, увязка бортовых систем и подготовка к их разработке.

Основные направления применения средств автоматизации: математическое моделирование обводов; расчеты и моделирование основных характеристик; изготовление моделей и проведение экспериментов; расчеты нагрузок, прочностные и весовые расчеты; распределение лимитов массы и контроль массово-центровочных характеристик; синтез конструктивно-силовых схем агрегатов с оптимальным распределением массы и жесткости по силовым элементам равнопрочной конструкции; имитационное моделирование режимов функционирования на фоне наихудших ситуаций и внешних условий; определение оптимального резервирования бортовых систем; выявление путей унификации элементов планера, корпуса, силовых установок и оборудования.

— *Этап технического или рабочего проектирования.* Задача — выпуск документации для создания, испытания и эксплуатации ЛА.

Вычислительные средства используются для автоматизированного конструирования узлов и деталей; выпуска и тиражирования технической и эксплуатационной документации; полунатурного моделирования и автоматизированной обработки результатов испытаний; подготовки управляющих программ для производственного оборудования; выбора унифицированных и стандартизованных деталей.

Как видно, важнейшим требованием, предъявляемым к САПР, является возможность ее использования на всех стадиях разработки проекта, начиная с анализа технического задания и разработки технического предложения и закончив выпуском комплекса технической документации, необходимой для изготовления самолета. При проектировании основное внимание следует уделить раскрытию и формализации факторов неопределенности, необходимо предоставить разработчикам ЛА инструмент для

обоснованного выбора проектных решений, опираясь на возможность оценки достоверности проектных расчетов, сравнения вариантов в условиях технического риска и уверенного поиска наилучших вариантов структуры и состава ЛА.

Литература

1. *Мишин В.П.* Основы проектирования летательных аппаратов. М.: Машиностроение, 2005. 375 с.
2. *Панкевич А.А.* Автоматизация проектирования конструкций летательных аппаратов на начальных этапах их разработки // Прикладная геометрия. 2006. № 13. С. 45—55.

УДК 681.4

Н. Н. ПРОХОЖЕВ — кафедра Проектирования компьютерных систем

ПОВЫШЕНИЕ СКРЫТНОСТИ ВНЕДРЕНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ ЗА СЧЕТ ИСПОЛЬЗОВАНИЯ ИХ КОРРЕЛЯЦИИ С ХАРАКТЕРИСТИКАМИ ИЗОБРАЖЕНИЯ

Научный руководитель — д.т.н., профессор А.Г. Коробейников

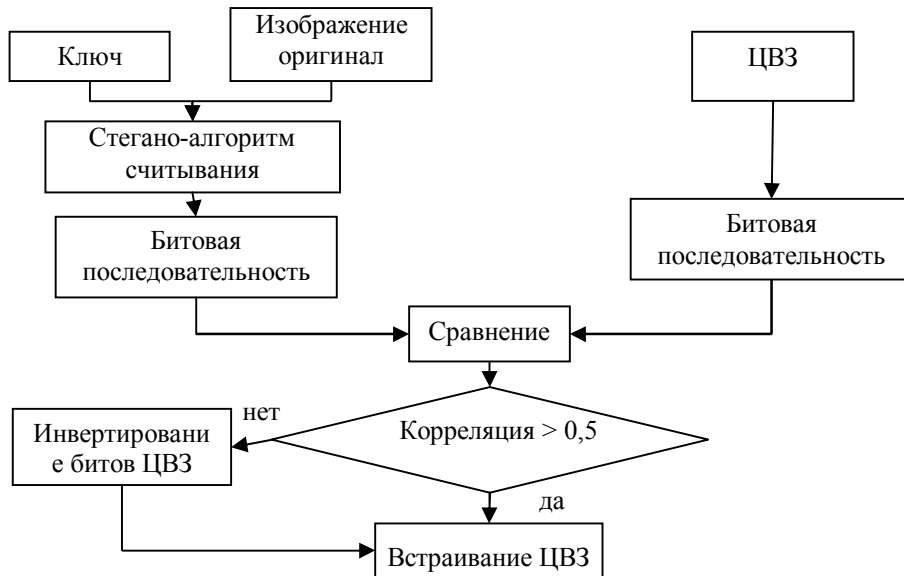
Одним из важнейших параметров стеганосистемы является скрытность внедрения цифровых водяных знаков (ЦВЗ). Данный параметр связан с устойчивостью внедренных ЦВЗ к внешним воздействиям на изображение-контейнер. Как правило, в стеганосистемах достигается некий компромисс между стремлением сделать ЦВЗ максимально устойчивыми и необходимостью сохранить высокое качество изображения-контейнера. Подавляющее большинство существующих методик повышения скрытности внедрения (при сохранении уровня устойчивости) основаны на качественном выборе областей встраивания, т.е. они учитывают специфику конкретного контейнера [см. лит.].

В данной работе предлагается методика улучшения скрытности внедрения, учитывающая особенности не только конкретного контейнера, но и конкретного ЦВЗ, внедряемого в контейнер. Описываемая методика может быть использована в подавляющем большинстве стеганосистем, вне зависимости от алгоритма, на основе которого они создаются. Методику можно отнести к категории операций так называемой предварительной подготовки ЦВЗ, она может выполняться после таких этапов подготовки ЦВЗ, как шифрование или сжатие, т.е. непосредственно перед встраиванием.

Методика основана на корреляции битовой последовательности, считываемой из областей встраивания изображения-оригинала и встраиваемой битовой последовательности ЦВЗ. На рисунке представлена блок-схема предлагаемого алгоритма.

В основе алгоритма лежит идея использования особенностей изображения-контейнера для минимизации вносимых в него изменений, для чего из изображения-оригинала выполняется чтение битовой последовательности по ключу, который будет использоваться при встраивании и/или считывании ЦВЗ. В результате будет получена битовая последовательность, отражающая некоторые характеристики изображения, в плоскости которых будут встраиваться ЦВЗ. Полученная битовая последовательность сравнивается с последовательностью ЦВЗ. Если уровень совпадения битов этих двух последовательностей больше 50 % (корреляция больше 0,5), то ЦВЗ встраивается без изменений, если уровень меньше 50 %, то биты в битовой последовательности ЦВЗ инвертируются, и в ключ добавляется соответствующий признак, который будет учитываться при дальнейшем считывании ЦВЗ.

Применение описанной методики позволяет снизить уровень изменений изображения-контейнера, выполняемых при встраивании ЦВЗ. Практические результаты использования данного метода в стеганосистемах с алгоритмом встраивания на основе дискретно-косинусного преобразования позволили уменьшить уровень вносимых искажений в среднем на 10—12 %, но в отдельных случаях снижение уровня искажений достигало 20 %.



При построении стеганосистем следует учитывать, что применение данной методики требует дополнительной вычислительной мощности, аналогичной затратам при считывании ЦВЗ.

Литература

Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография: Теория и практика. М.: МК-Пресс, 2006. 283 с.

УДК 004.032.26

Д. В. СОЛОВЬЕВ — кафедра Проектирования компьютерных систем

ИСПОЛЬЗОВАНИЕ НЕЙРОСЕТЕВОГО АЛГОРИТМА В ЗАДАЧАХ ОПТИМИЗАЦИИ СЛОЖНЫХ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

Научный руководитель — д.т.н., профессор Ю.А. Гатчин

На сегодняшний день нейронные сети используются для широкого круга задач, таких как автоматизация процессов распознавания образов, адаптивное управление, аппроксимация функционалов, прогнозирование, создание экспертных систем, организация ассоциативной памяти и многие другие. С помощью нейронных сетей можно, например, предсказывать показатели биржевого рынка, выполнять распознавание оптических или звуковых сигналов, создавать самообучающиеся системы, способные управлять автомашиной при парковке или синтезировать речь по тексту. Также нейросетевой подход в решении физико-математических задач имеет преимущества в следующих случаях:

— задача в силу конкретных особенностей не поддается адекватной формализации, поскольку содержит элементы неопределенности, не формализуемые традиционными математическими методами;

— задача формализуема, но на настоящее время отсутствует аппарат для ее решения;

— для рассматриваемой, хорошо формализуемой задачи существует соответствующий математический аппарат, но реализация вычислений с его помощью на базе имеющихся вычислительных систем не удовлетворяет требованиям получения решений по времени, размеру, весу, энергопотреблению и др.

Совместное использование трехслойного персептрона и алгоритма обратного распространения ошибки является эффективным инструментом для решения задач, не поддающихся формализации, содержащих элементы неопределенности и не формализуемые традиционными математическими методами. В настоящей работе в качестве такой задачи выступает сложный технологический процесс (ТП) вытяжки оптического волокна. Как и многие ТП оптического производства, он обладает следующими характеристиками:

— малая информативность ТП из-за сложности или невозможности контроля выходных параметров — вектора Y ;

— сложность физико-химических явлений, протекающих в ходе ТП, исключающая возможность построения аналитических математических моделей ТП;

— нестационарность ТП, являющаяся следствием физических особенностей ТП и изменений параметров, характеризующих непостоянство свойств технологического оборудования во времени;

— распределенность параметров, которая возникает из-за наличия движущихся потоков оптических материалов, при этом контроль параметров проводится в локальных областях или косвенными путями;

— длительность и многостадийность процесса изготовления оптических материалов;

— наличие множества перекрестных связей между отдельными каналами управления, приводящих к взаимосвязи управляющих воздействий от устройства управления (УУ).

Таким образом, сложные ТП, в частности, вытяжки оптического волокна, являются нестационарными, нелинейными с большой степенью многосвязности и распределенностью параметров процессом, вследствие чего использование алгоритмов искусственного интеллекта, например технологии нейронных сетей, является актуальным.

В ходе работы была изучена технология нейронных сетей, алгоритм их функционирования и обучения. Была разработана топология нейронной сети конкретно под задачу оптимизации сложного ТП вытяжки оптического волокна, разработан алгоритм обучения на базе алгоритма обратного распространения ошибки и выполнена программная реализация предлагаемого метода. Разработанная программа была включена в автоматизированный технологический комплекс оптического производства. Результаты работы алгоритма были оценены с помощью математических критериев, в частности, по критерию Стьюдента и среднему квадратическому отклонению — расхождение менее 1 %. Следовательно, предложенный алгоритм может применяться в задачах оптимизации сложных технологических процессов, в частности, сложного ТП вытяжки оптического волокна.

Литература

1. *Заенцев И.В.* Нейронные сети: основные модели. Воронеж, 1999. 76 с.
2. *Дианов Р.С.* Оптимизация технологического процесса разработки газоносного пласта с применением генетических алгоритмов и нейронных сетей. Дис. ... канд. техн. наук. Астрахань, 2004. 167 с.

3. Уоссермен Ф. Нейрокомпьютерная техника: Теория и практика. 1992. 118 с.

РАБОТЫ СТУДЕНТОВ ШЕСТОГО КУРСА

УДК 621.316.7

Т. Н. АБЛЯЗИМОВ — кафедра Проектирования компьютерных систем

РАЗРАБОТКА КОНСТРУКЦИИ БЛОКА ПИТАНИЯ ТЕРМОРЕГУЛЯТОРА СТАНДАРТА ЧАСТОТЫ СИСТЕМЫ ГЛОБАЛЬНОЙ СПУТНИКОВОЙ НАВИГАЦИИ ГЛОНАСС

Научный руководитель — ассистент Д.А. Боголюбов

В настоящее время в Российском институте радионавигации и времени (Санкт-Петербург) активно разрабатывается система глобальной спутниковой навигации ГЛОНАСС. В рамках проекта одной из ключевых стала разработка системы терморегуляции всей системы. Данная система нуждается в обеспечении электрическим питанием с помощью блока питания повышенной надежности. В связи с конструктивными особенностями блока повышенные требования предъявлялись к габаритам устройства, его надежности и потребляемой мощности.

Цель настоящей работы заключалась в создании стабильного по тепловым режимам блока питания терморегуляторов стандарта частоты.

Для достижения поставленной цели были решены следующие основные задачи:

- проанализирована конструкция терморегулирующего модуля;
- разработана принципиальная схема блока питания модуля;
- разработана конструкция блока питания терморегулятора в соответствии с государственными стандартами Российской Федерации.

В результате создана документация по монтажу устройства, проведены расчеты тепловых режимов и вибропрочности блока питания.

Данная разработка позволит повысить надежность терморегулятора стандарта частоты и, как следствие — всей системы в целом.

УДК 004.6

Н. В. БЛАГОДАРНЫЙ — кафедра Проектирования компьютерных систем

РАЗРАБОТКА СТАТИСТИЧЕСКОЙ СИСТЕМЫ КОНСОЛИДАЦИИ ДАННЫХ ИЗ РАЗЛИЧНЫХ БАНКОВСКИХ ПОДСИСТЕМ

Научный руководитель — главный инженер Управления информатики и автоматизации банковских работ Северо-Западного банка Сбербанка России С.В. Ефремов

Разрабатываемая статистическая система представляет собой программный комплекс, функциями которого являются:

- сбор данных из различных хранилищ баз данных (БД);
- предварительная обработка собранных данных;
- загрузка данных в центральную БД;

- формирование статистических отчетов по показателям эффективности производства;
- обеспечение целостности хранимых данных;
- хранение ранее сформированных отчетов на сервере;
- разграничение доступа пользователей к отчетам.

Задачей системы является объединение и унификация разнородных данных, хранящихся в БД различных банковских подсистем, а также выпуск статистических отчетов, отражающих эффективность работы различных подразделений предприятия.

Для создания системы используется платформа Microsoft SQL Server 2008. Наибольший интерес представляют средства бизнес-аналитики вышеуказанной платформы: SSIS (SQL Server Integration Services), SSAS (SQL Server Analysis Services), SSRS (SQL Server Reporting Services).

Сбор данных из различных БД, предварительная обработка и загрузка в центральную БД осуществляется с помощью служб интеграции SSIS. Предварительно разработанные пакеты, выполняющие вышеуказанные функции, запускаются по расписанию при помощи Microsoft SQL Server Agent.

Центральная база данных функционирует под управлением SQL Server 2008 Database Engine. Данный программный продукт обеспечивает целостность и безопасность хранимых данных благодаря механизмам постраничного хранения, индексирования и отказоустойчивости. Безопасность достигается путем прозрачного шифрования данных (данные на диске хранятся в зашифрованном виде, что практически сводит к нулю вероятность несанкционированного доступа).

Функции формирования статистических отчетов по показателям эффективности производства, хранения ранее сформированных отчетов на сервере и разграничения доступа пользователей к отчетам обеспечиваются с помощью SSRS. Макеты отчетов разрабатываются в среде SQL Server Business Intelligence Development Studio, после чего публикуются на сервере отчетов. Пользователи имеют доступ к серверу отчетов через web-интерфейс.

Разграничение доступа обеспечивается встроенными средствами безопасности SSRS на основе механизмов Active Directory.

Литература

Microsoft Business Intelligence [Электронный ресурс]:
<<http://www.microsoft.com/rus/bi/>>.

УДК 004.056(043)

М. С. БОНДАРЕНКО — кафедра Проектирования компьютерных систем

РАЗРАБОТКА КОМПЛЕКСА ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ МЕР ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

Научный руководитель — к.т.н., доцент, И.Б. Бондаренко

Любое современное предприятие независимо от вида деятельности и формы собственности не в состоянии успешно развиваться и вести хозяйственную деятельность без создания на нем условий для надежного функционирования системы защиты собственной информации [1].

Реализация проекта по созданию комплексной системы защиты информации должна проводиться поэтапно. Разработке и внедрению комплекса обязательно предшествует тщательное исследование информационных ресурсов предприятия, предварительно подсчитываются и распределяются ресурсы и трудозатраты на его создание и функционирование, выбираются приоритетные пути и направления развития. Затем устанавливаются возможные причины, варианты проявления и последствия нарушений информационной безопасности, сбоев программ, технических средств и систем обработки и передачи информации, несанкционированного получения, модификации (уничтожения) и распространения [2].

В работе предполагается определить комплекс организационно-технических мер по защите конфиденциальной информации на предприятии «ТГК-1 филиал Невский». Разработку необходимо осуществлять с учетом особенностей функционирования информационной системы предприятия.

При разработке необходимо:

— создать на предприятии отдел защиты информации. (Эффективность защиты информации на предприятии во многом определяется тем, насколько правильно выбрана структура органа защиты информации и квалифицированы его сотрудники);

— проанализировать информационные потоки предприятия, как внешние, так и внутренние, и при необходимости предложить меры по совершенствованию алгоритмов прохождения документов, автоматизации передачи информации;

— проанализировать оснащенность и уязвимость помещений, предназначенных для обработки конфиденциальной информации;

— оценить применяемые на предприятии меры защиты информации и предложить способы их совершенствования;

— выбрать, обосновать правильность выбора и разместить на территории технические средства защиты информации;

— выполнить все необходимые экономические расчеты.

В заключение необходимо отметить, что невозможно организовать абсолютно надежную систему защиты, такой просто не существует. Эффективность защиты информации достигается не количеством средств, потраченных на ее организацию, а ее способностью адекватно реагировать на все попытки несанкционированного доступа к информации.

Литература

1. *Грибунин В.Г.* Комплексная система защиты информации на предприятии. М.: Академия, 2007. 416 с.
2. *Мельников В.П., Клейменов С.А.* Информационная безопасность и защита информации. М.: Академия, 2007. 370 с.

А. В. БОРОВАЯ — кафедра Проектирования компьютерных систем

СИСТЕМА УПРАВЛЕНИЯ САЙТОМ «ВИЗИТНАЯ КАРТОЧКА»

Научный руководитель — к.т.н. доцент А. А. Малинин

В настоящее время актуальна тема web-программирования. Сайт может иметь удачный дизайн, интересное и хорошо организованное содержание, но для того чтобы внести в него интерактивность, сделать способным реагировать на действия пользователя, уметь собирать от посетителей сайта информацию и обрабатывать ее, необходимо использовать web-программирование.

При всем разнообразии языков программирования, которые могут быть использованы в web-строительстве, все скрипты (и соответственно средства для их написания) можно разделить на две группы: те, которые работают на стороне сервера (т.е. на компьютере, на котором расположен сам сайт) и на стороне клиента (т.е. на компьютере пользователя сайта). Без использования серверных скриптов нельзя обойтись, если необходимо собирать и хранить какую-нибудь информацию на сервере (например, для интернет-форума нужно организовать прием и сохранение отправляемых пользователями сообщений). Скрипты, работающие на стороне клиента, позволяют реагировать на действия пользователя, когда он просматривает уже загруженную в память своего компьютера страницу, изменять ее вид и содержимое без того, чтобы загружать ее с сервера снова. Очень часто для обеспечения выполнения некой задачи используются оба вида скриптов.

Существуют разнообразные языки и средства web-программирования:

— Javascript — простой и удобный язык, позволяющий легко управлять содержимым web-страницы, отслеживая различные действия пользователя и реагируя на них;

— Java — язык, специально созданный для написания программ, ориентированных на работу в компьютерных сетях;

— Flash — технология, разработанная фирмой Macromedia для создания анимированных изображений.

В рамках работы по созданию системы управления сайтом «визитная карточка» проанализированы web-технологии, и в результате выбран серверный язык программирования PHP как наиболее простой и гибкий. Код PHP можно писать совместно с html-кодом, он универсален и позволяет создавать программы, работающие с различными базами данных и графикой. Созданная система обращается к структурированной базе данных MySQL, позволяющей хранить большие объемы данных. Использован сервер Apache, система работает под управлением операционной системы Microsoft Windows 2000/2003/XP/Vista. Корректная работа сайта возможна в таких браузерах, как Explorer, Opera, Mozilla Firefox, при этом обновлять содержимое возможно в браузере без применения дополнительных программ.

Все используемые средства программирования собраны в пакете Denwer, который при сравнительно малом размере обеспечивает поддержку не только серверных функций, но и поддержку популярных языков web-программирования.

А. В. ГОРБАЧЕВ — кафедра Проектирования компьютерных систем

ИССЛЕДОВАНИЕ ЛОКАЛЬНО-ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ЛАБОРАТОРИИ ЗАЩИТЫ ИНФОРМАЦИИ

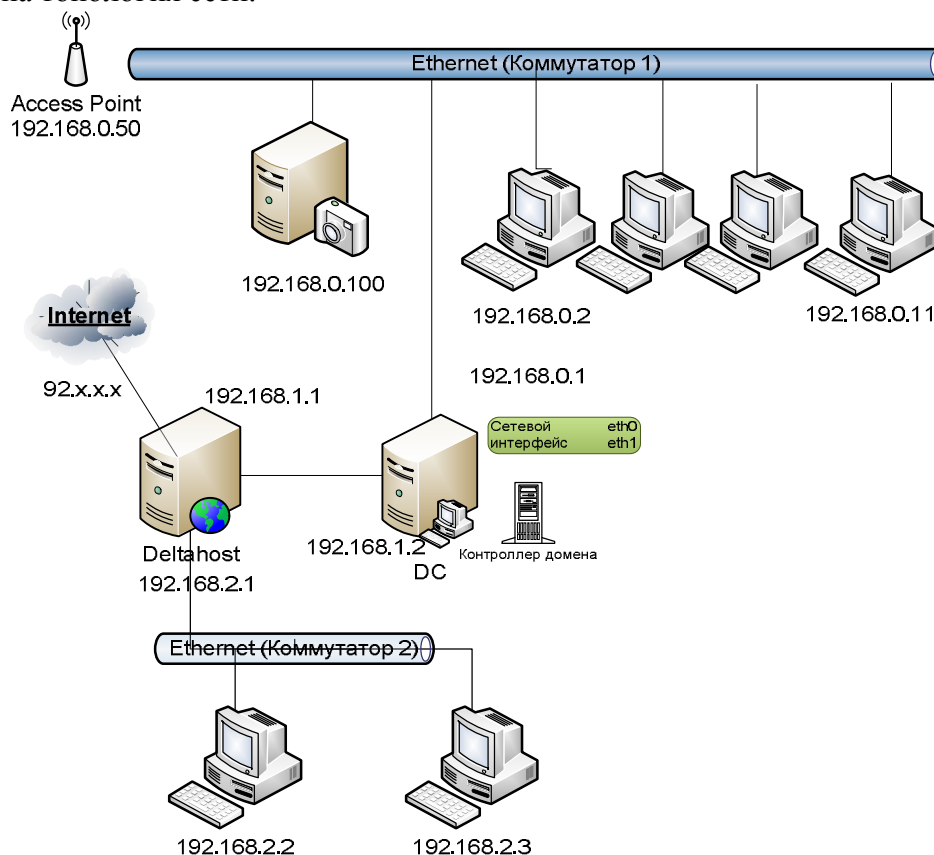
Научный руководитель — ст. преподаватель К.О. Ткачев

Возможности сети Интернет широко используются в информационных системах и бизнесе, именно по этой причине проблема надежности сетей становится все более актуальной. Ведь совсем не безразлично, получит ли человек своевременно отклик от банкомата, произведет ли клиент покупку, будут ли корректно введены данные в систему навигации ракеты и т.д.

Целью данной работы является выявление элементов сети снижающих ее производительность. Исследования проводились в лаборатории защиты информации кафедры ПКС СПбГУ ИТМО. Для выполнения поставленной задачи необходимо было измерить производительность сети и проверить ее отказоустойчивость.

Сеть делится на 3 сегмента по IP-адресации: 192.168.0.0/24 (10 Мбит/с); 192.168.1.0/24 (100 Мбит/с); 192.168.2.0/24 (10 Мбит/с).

Весь трафик внешней сети проходит по маршруту от IP-адреса 192.168.0.1 до 192.168.1.1, при этом интерфейс eth0 имеет ограниченную пропускную способность (10 Мбит/с), что снижает надежность и производительность сети. На рисунке представлена топология сети.



Для тестирования сети при предельных нагрузках с сервера Deltahost создается избыточный поток трафика на одну из машин в подсети 192.168.0.0/24 и оценивается пороговое значение, при котором начинается нестабильная работа сетевых приложений на

машинах-клиентах. Одновременно на сервере DC происходит контроль и запись графика загрузки сетевых интерфейсов.

Для оценки распределения задержек пакетов, был произведен пинг сервера Deltahost 192.168.1.1 с одной из машин в сети 192.168.0.0/24. На основе этих данных: отправлено 389 пакетов; получено 91, потеряно 298 (76 % потерь).

Время приема—передачи данных: минимальное 218; максимальное 495; среднее 394 мс.

Среднее значение задержки пакета (D) при загруженности сети на 85 %:

$$D = \sum \frac{d_i}{N} = 394 \text{ мс}, \quad (1)$$

d_i —сумма всех задержек (35854); N —количество измерений (91).

Было вычислено среднее отклонение каждой отдельной задержки от среднего значения задержки:

$$J = \sqrt{\frac{\sum (d_i - D)^2}{N - 1}} = 74 \text{ мс}, \quad (2)$$

Был определен коэффициент вариации:

$$K_V = \frac{J}{D} = 0,19, \quad (3)$$

В результате анализа схему сети и полученных данных было выяснено, что весь интернет-трафик проходит через Коммутатор 1 и сетевой интерфейс eth0 сервера DC, работающий на скорости 10 Мбит/с. При повышенной нагрузке сеть имеет неприемлемо большое значение среднего отклонения каждой отдельной задержки от среднего значения задержки и высокую вероятность потери пакета. В ходе работы было определено, что Коммутатор 1 и сетевой интерфейс eth0, сервера DC — самые слабые элементы сети и подлежат замене на более производительные.

УДК 681.4

А. В. ГОРБАЧЕВ — кафедра Проектирования компьютерных систем

РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ НА ПРЕДПРИЯТИИ «СТРОЙКОМПЛЕКС-ЭНЕРГО»

Научный руководитель — ст. преподаватель К.О. Ткачев

Развитие современных информационных технологий ведет к тому, что происходит переход к объединению автономных компьютеров и локальных сетей в единую корпоративную сеть организации. Помимо явных преимуществ такой переход несет с собой и ряд проблем, специфичных для корпоративных сетей. К причинам, приводящим к возникновению таких проблем, можно отнести сложность и разнородность используемого программного и аппаратного обеспечения, большое число узлов корпоративной сети, их территориальную распределенность и недостаточность ресурсов для контроля всех настроек, доступ внешних пользователей (клиентов, партнеров и пр.) в корпоративную сеть.

В настоящий момент очень трудно встретить сети, построенные на основе только одной сетевой операционной системы. Большое число конфигурационных параметров используемого программного и аппаратного обеспечения затрудняет его эффективную

настройку и эксплуатацию. Уже не редкость, когда узлы, объединенные в корпоративную сеть, разбросаны по разным территориям не только одного города, но и региона. Эта особенность, а также нехватка ресурсов для контроля всех настроек не позволяют администраторам лично своевременно контролировать деятельность пользователей системы на всех узлах корпоративной сети и соответствие настроек программного и аппаратного обеспечения заданным значениям. Подключение корпоративной сети к интернету приводит к тому, что зачастую очень трудно определить ее границы и всех подключенных к сети пользователей, что может привести к попыткам несанкционированного доступа к защищаемой информации [1].

Многие организации используют средства вычислительной сети для обеспечения нужд обработки и передачи данных. До использования локально вычислительных сетей основная часть обработки и обмена данными была централизована; информация и управление ею были сосредоточены в одном месте. Сейчас локально вычислительные сети логически и физически рассредоточили данные, а также вычислительную мощность и службы обмена сообщениями по всей организации.

В эпоху интенсивного обмена информацией вся совокупность элементов сети компании — ее серверы, компьютеры, базы данных — являются потенциальными целями злоумышленников и все они уязвимы [2].

Целью данной работы является создание системы защиты вычислительной сети на предприятии «Стройкомплекс-Энерго». Разрабатываемая система должна защищать конфиденциальную информацию в локально вычислительной сети предприятия. Необходимо создать и защитить локально вычислительную сеть на предприятии, состоящую из ста рабочих машин.

В ходе работы была проанализирована организационная структура предприятия и составлена схема информационных потоков. На основе результатов анализа структуры предприятия построена модель бизнес-процессов с учетом информационной безопасности и выбрана топология сети.

Чтобы сформулировать требования к информационной безопасности, была проведена оценка ресурсов организации, составлен полный список угроз безопасности. На основе оценки ресурсов организации были определены параметры потенциальных источников нежелательных событий, которые могут нанести ущерб ресурсам. Исходя из вышеперечисленного, сформулированы некоторые требования к обеспечению безопасности в информационных системах:

- управление доступом к средствам вычислительной техники, программам и данным;
- обеспечение антивирусной защиты;
- необходимость резервного копирования;
- информирование об инцидентах в области информационной безопасности.

На основе полученных данных, оценены риски для информационной системы организации, для отдельных ее подсистем, баз данных и элементов данных. После оценки рисков сделан выбор контрмер, снижающих риски до приемлемого уровня и сформирована структура системы защиты информации.

Для решения поставленной задачи, подобраны соответствующие аппаратные средства и программное обеспечение. В итоге разработана система защиты вычислительной сети, которая соответствует поставленной цели и выполняет следующие задачи:

- защита от лиц, не допущенных к работе в системе обработки информации;
- регламентация доступа законных пользователей и программ к информационным, программным и аппаратным ресурсам системы, в строгом соответствии с принятой в организации политикой безопасности;

- защита электронно-вычислительных машин сети от внедрения вредоносных программ, а также инструментальных и технологических средств проникновения;
- обеспечение целостности критических ресурсов систем защиты и среды исполнения прикладных программ;
- регистрация, сбор, хранение и выдача сведений обо всех событиях, происходящих в сети и имеющих отношение к ее безопасности;
- централизованное управление средствами системы защиты.

Литература

1. *Игнатьев В.А.* Информационная безопасность современного коммерческого предприятия. Старый Оскол: ТНТ, 2005. 448 с.
2. *Герасименко В.А., Малюк А.А.* Основы защиты информации. М.: Изд-во МИФИ, 1997. 537 с.

УДК 004.056

А. А. ГУСЕВ — кафедра Проектирования компьютерных систем

РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ «ИНТАРСИЯ»

Научный руководитель — к.т.н., доцент Н.С. Кармановский

По мере развития организации усложняется ее информационная система, основной задачей которой является обеспечение максимальной эффективности ведения бизнеса в постоянно меняющихся условиях конкуренции на рынке. Рассматривая информацию как товар, можно сказать, что утеря информации в целом приводит к материальным затратам. Например, раскрытие технологии изготовления оригинального продукта приведет к появлению аналогичного продукта, но от другого производителя, как следствие — владелец технологии, а может быть и автор, потеряют часть доходов и т.д. С другой стороны, информация является субъектом управления, и ее изменение может привести к катастрофическим последствиям в объекте управления [1].

Защита информации — это совокупность мероприятий, направленных на предотвращение ее утечки, несанкционированных и непреднамеренных воздействий. С целью всесторонней защиты информационных ресурсов на предприятиях создается комплексная система информационной безопасности.

В проекте разработана система защиты информации на предприятии «Интарсия». Проанализирована структура предприятия, структура службы безопасности предприятия. Произведена проверка возможных информационных потоков, содержащих коммерческую тайну и разработана схема охраны объекта, выбрана и разработана оптимальная структура расположения средств контроля доступа и наблюдения. Произведен экономический расчет затрат на оборудование средств защиты. На случай возникновения чрезвычайных ситуаций организована пожарная система и система оповещения.

Литература

1. Микротест. Информационная безопасность [Электронный ресурс]: <http://microtest.ru/hardware/information_security/>.

2. PERCo. Готовые решения: S-20 [Электронный ресурс]: режим доступа <[http://www.perco.ru/ security/](http://www.perco.ru/security/)>.

УДК 004.031.43

В. В. ДАВЫДКИНА — кафедра Проектирования компьютерных систем

РАЗРАБОТКА ПРОТОТИПА СИСТЕМЫ УПРАВЛЕНИЯ КРУПНЫМ ПРОИЗВОДСТВЕННЫМ ПРЕДПРИЯТИЕМ

Научный руководитель — к.т.н., доцент А.А. Малинин

Рост экономики в России, выход на ее рынок западных компаний и усиливающаяся тенденция к созданию единого финансово-информационного пространства требуют от российских компаний быстрого реагирования на изменения рыночной среды. В результате усиления интеграционных процессов в деловом мире возникают системы, объединяющие внутреннюю сферу бизнеса предприятия, деловых партнеров, клиентов, а также акционеров, потенциальных инвесторов и других заинтересованных лиц. Вследствие этого предприятиям важно сформировать оптимальные «границы» своей бизнес-среды и на основе современных технологий управления обеспечить рентабельное использование широкого арсенала внешних ресурсов, важнейшим из которых становится эффективное сотрудничество всех участников бизнеса. В серии материалов, посвященных современным технологиям управления предприятием, много компаний представляют эффективную технологию управления ресурсами компании, которая реализована в решениях «Управление ресурсами предприятия» (УРП) [1].

Система УРП представляет собой унифицированную централизованную базу данных, единое приложение и общий пользовательский интерфейс для управления финансово-экономической деятельностью: производственной, экономической и финансовой, сбытовой, закупочной, хранения продукции и материалов и др. Элементы программного обеспечения УРП-систем, предназначенные для поддержки разных функций предприятия, должны непрерывно взаимодействовать между собой. По сути, системы УРП позволяют моделировать бизнес-процессы при помощи электронной вычислительной техники и сопровождать некоторые действия того или иного сотрудника [2].

В работе создан прототип системы управления крупным производственным предприятием. Проанализированы его структура и основные бизнес-процессы, непосредственно ориентированные на поддержку стабильной работы предприятия. Проведен аналитический обзор рынка существующих систем УРП, разработаны модель интеграции бизнес-процессов предприятия с модулями системы и архитектура системы управления на основе платформы SAP NetWeaver.

Разработанный прототип системы управления крупным производственным предприятием позволит упростить и оптимизировать работу с основными бизнес-процессами предприятия, повысит уровень контроля качества информации, сделать ее доступной для всех пользователей, согласовать планирование и управление ресурсами, сократить цикл производства и выполнения заказа.

Литература

1. *Рыбников А.И.* Система управления предприятием типа ERP. Изд-во Аэроконсалт, 2004. 214 с.

2. Компания SAP Inc., Global. [Электронный ресурс]: <<http://www.sap.com/index.epx>>.

УДК 624.01.04

О. С. ЕВЛАНОВ — кафедра Проектирования компьютерных систем

РАЗРАБОТКА КОНСТРУКЦИИ МИКРОПРОЦЕССОРНОГО МОДУЛЯ КОНТРОЛЯ РАСХОДА ТОПЛИВА САМОЛЕТНЫХ ДВИГАТЕЛЕЙ

Научный руководитель — к.т.н., доцент И.Б. Бондаренко

Целью проектирования является разработка конструкции микропроцессорного модуля контроля расхода топлива самолетных двигателей. Модуль обеспечивает обработку данных, поступающих одновременно с нескольких (двух) датчиков расхода топлива.

Модуль выполнен на базе 16-разрядного микропроцессора Intel 80C186EB. Он соединяется при помощи жесткого разъема с аналоговым модулем, осуществляющим первичную обработку сигналов датчика расхода топлива. В состав модуля входит энергонезависимая память ПЗУ, обслуживаемая через локальную шину CPU.

Модуль должен обрабатывать следующие данные:

- сигналы датчиков после первичной обработки в аналоговом модуле (воспринимаемые в виде внешних прерываний);
- информацию, поступающую с бортовой цифровой ЭВМ (БЦЭВМ) по интерфейсу ARINC 429 и преобразованную в биполярный последовательный код;
- информацию от внешних устройств (других блоков, систем контроля) по интерфейсу RS—232;
- входные разовые команды;
- формировать команды контроля и управления;
- формировать данные для передачи БЦЭВМ и внешним устройствам.

Проектирование печатной платы производилось с применением САПР: P-Cad 2000. Для трассировки проводников использовалась программа SPECCTRA с доводкой вручную неразведенных проводников. Автором разработана конструкция блока сопряжения. Были проведены расчеты на вибропрочность, надежность блока, сделан тепловой расчет. Значения контролируемых параметров соответствуют техническому заданию.

Данная конструкция обладает высоким уровнем надежности и работоспособности. Экономические расчеты показали, что себестоимость разработки невелика, это способствует повышению ее конкурентоспособности на рынке.

Была разработана конструкторская документация, необходимая для изготовления данного блока.

А. А. ИВАНОВ — кафедра Проектирования компьютерных систем

РАЗРАБОТКА ИНТЕГРИРОВАННОЙ СИСТЕМЫ ОХРАНЫ НА ПРЕДПРИЯТИИ «НЕРПА»

Научный руководитель — ст. преподаватель К.О. Ткачев

Обеспечение безопасности современного промышленного предприятия является достаточно актуальной задачей, требующей для своего решения применения различных аппаратно-технических средств и проведения административно-управленческих мероприятий [1].

Традиционно основу системы безопасности многих предприятий составляет служба охраны и аппаратура охранно-пожарной сигнализации, а контроль доступа на проходной осуществляется с помощью обычных (бумажных) пропусков. При таком подходе «человеческий фактор» играет определяющую роль, что значительно снижает эффективность системы безопасности, так как невозможно полностью исключить такие факторы, как недобросовестность, нарушение служебных инструкций, а иногда и злой умысел. Поэтому при проектировании систем безопасности предприятий одной из основных тенденций на сегодняшний день является комплексный подход.

Максимальную функциональность комплекса технических средств обеспечивают современные интегрированные системы охраны (ИСО), которые представляют собой совокупность взаимосвязанных организационных мероприятий и подсистем технических средств обеспечения безопасности объекта, объединенных аппаратно, программно и структурно, они имеют общие средства сбора и обработки информации и управления [2].

ИСО на предприятии «Нерпа» должна состоять из подсистем

- охранно-пожарной сигнализации;
- контроля и управления доступом;
- видеонаблюдения

и решать следующие задачи:

- охрана главного корпуса предприятия и наблюдение за ним;
- охрана и контроль внутренних помещений;
- охрана оборудования, продукции, финансов и информации;
- осуществление контролируемого доступа в здания и помещения [3].

Также интегрированная система охраны должна включать в себя подсистемы бесперебойного (резервного) питания с большим сроком автономной работы и с возможностью хранения видеоизображений не менее 7 дней.

Для решения поставленных задач необходимо составить полный список угроз безопасности, подобрать соответствующие средства защиты и сформировать структуру защиты объекта.

В ходе работы необходимо проанализировать организационную структуру предприятия, внешние и внутренние информационные потоки, определить зоны безопасности, выбрать и расположить технические средства защиты.

Литература

1. Мир связи. Connect. 2001. № 4—5. [Электронный ресурс]: <<http://www.r-control.ru/articles/>>.
2. Барсуков, В.С. Современные технологии безопасности. 2000. 496 с.

УДК 628.16.087

Е. Е. КАРТАШОВА — кафедра Проектирования компьютерных систем

ПРИМЕНЕНИЕ ОДНОРАЗОВЫХ ЭЛЕКТРОДОВ В ЭЛЕКТРОХИМИЧЕСКИХ КОАГУЛЯТОРАХ ДЛЯ ОЧИСТКИ ПИТЬЕВОЙ ВОДЫ

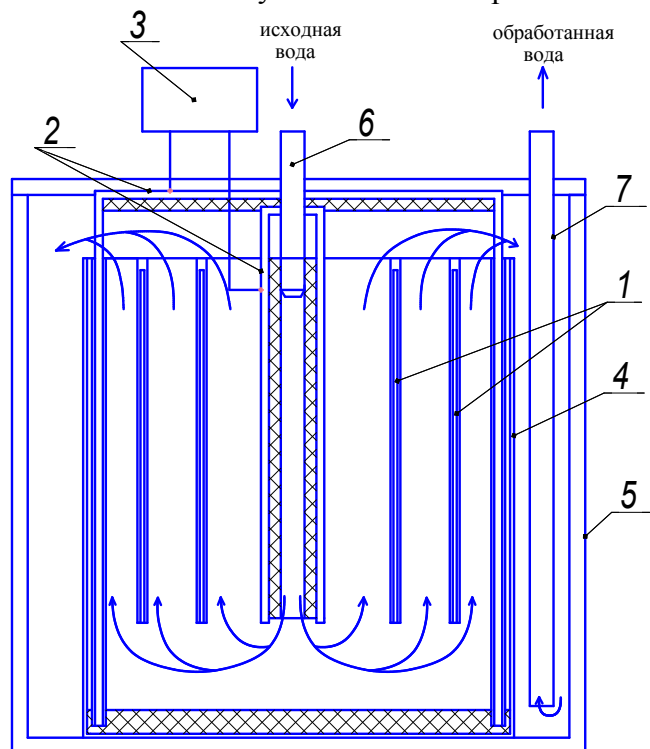
Научный руководитель — к.т.н., доцент А.В. Панков

В современном мире проблема получения качественной питьевой воды становится все более актуальной. Для очистки питьевой воды применяется широкий спектр методов: механическое фильтрование, обратный осмос, сорбция, коагуляция, мембранная сепарация, электрохимическая коагуляция и др. Электрохимический способ очистки воды сегодня признан одним из самых эффективных. При электрохимической очистке коагуляция сочетается с флотацией, удалением образовавшегося шлама через дренаж и заключительным механическим отфильтровыванием мельчайших частичек шлама. Процесс электрохимической очистки происходит под действием электрического тока с использованием растворимых электродов.

Принцип работы приборов «Водолей» и «Аквалон» основан на методе электрохимической коагуляции. В данных устройствах процесс электрообработки реализуется путем создания электрического тока с помощью системы электродов, гальванически связанных непосредственно с источником электроэнергии [1]. Недостаток технических решений, применяемых в существующих установках, заключается в необходимости периодической механической зачистки поверхности электродов от наслоений, затрудняющих выход материала электродов в воду, и в сложности обеспечения надежного гальванического контакта — это увеличивает затраты на обслуживание устройства.

Предлагается электродный блок выполнить из растворимых и нерастворимых электродов, расположенных в легкоъемной cassette. При этом нерастворимые электроды выполнить в виде плоскопараллельных пластин, соединенных с источником питания, между ними расположить растворимые электроды, не имеющие непосредственного гальванического контакта с внешними электрическими цепями [2]. Для замены одноразовых электродов достаточно снять cassette, изъять использованные электроды и вставить новые. Таким образом свободные электроды могут иметь достаточно малую толщину, что позволяет эффективно использовать материал.

Предлагаемое решение позволит снизить затраты на обслуживание устройства, увеличить экономичность за счет снижения



материалоемкости растворимых электродов, повысить надежность устройства за счет простоты в изготовлении и обслуживании устройства.

Процесс электрообработки воды в предлагаемом электродном блоке, представлен на рисунке, где 1 — растворимые электроды; 2 — нерастворимые электроды; 3 — источник питания; 4 — кассета; 5 — корпус; 6 — распределитель потока воды; 7 — выходной водовод.

Литература

1. Патент РФ № 2180322, МПКС02Р1/463, С02Р1/465. Способ электрообработки воды в установке получения доброкачественной питьевой воды методом электрохимической коагуляции и устройство для его осуществления. Опубл. 03.10.2002.
2. Яковлев С.В., Краснобородько И.Г. Технология электрохимической очистки воды. Л.: Стройиздат, 1987. 312 с.

УДК 004.056

Д. Н. КИРИЧЕНКО — кафедра Проектирования компьютерных систем

РАЗРАБОТКА КОМПЛЕКСА ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ МЕР ДЛЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ «ДАРИНА»

Научный руководитель — к.т.н., доцент И.Б. Бондаренко

В настоящее время конфиденциальная информация и персональные данные обрабатываются в автоматизированных системах практически любого предприятия. Естественно, что подобная информация нуждается в защите. Защита информации во многих бизнес-структурах пока остается слабым звеном в системе безопасности такого бизнеса в целом. Наиболее распространенные угрозы — нарушение работы корпоративной сети вследствие внедрения вредоносного кода, выход из строя технических средств или их хищение, кража или разглашение конфиденциальной информации, намеренное уничтожение или модификация ключевых данных компании. Большинство названных угроз возникают вследствие деятельности сотрудников компаний, зачастую неумышленной. В основе лежит недостаточная информированность персонала, отсутствие четких инструкций, правил, регламентов работы с информацией.

Во многих компаниях организация безопасности отдельных бизнес-процессов, кодирование информации и использование антивирусной защиты компьютеров уже стали повседневной практикой, но решение отдельных вопросов защиты информации не решает задачу обеспечения информационной безопасности бизнеса в целом.

Исходя из данных аналитического центра Perimetrix (см. рисунок) следует, что для потребителей сегодня практически в равной мере актуально решение задач защиты, как от внешних, так и от внутренних угроз, обеспечение эффективного противодействия атакам и со стороны хакеров, и со стороны инсайдеров (санкционированных пользователей, допущенных к обработке информации на защищаемом вычислительном средстве), решение задач эффективного противодействия вирусным атакам, вредоносным, шпионским и любым иным деструктивным программам, атакам, приводящим к ошибкам программирования в системном и прикладном программном обеспечении. Другими словами, задачи защиты информации должны решаться в комплексе.

Обеспечение комплексной безопасности является необходимым условием и заключается, прежде всего, в продуманности и сбалансированности способов защиты, разработке четких организационно-технических мер и обеспечении контроля над их исполнением.

К основным мероприятиям по обеспечению безопасности можно отнести организацию:

— режима и охраны предприятия (цель — исключение возможности тайного проникновения на территорию и в помещения посторонних лиц; обеспечение контроля прохода и перемещения сотрудников и посетителей; создание отдельных производственных зон по типу конфиденциальных работ с самостоятельными системами доступа; организация и поддержание надежного пропускного режима и контроля сотрудников и посетителей и др.);

— работы с сотрудниками, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;

— использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации;

— работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты;

— работы с документами, включая организацию разработки и использования документов и носителей конфиденциальной информации, их учет, хранение и уничтожение.



Организационные мероприятия играют существенную роль в создании надежного механизма защиты информации, так как возможности несанкционированного использования конфиденциальных сведений в значительной мере обуславливаются злоумышленными действиями, небрежностью и халатностью пользователей или персонала защиты. Влияния этих факторов практически невозможно избежать только с помощью технических средств. Для этого необходима совокупность организационно-правовых и организационно-технических мероприятий, которые исключали бы (или, по крайней мере, сводили бы к минимуму) возможность возникновения опасности конфиденциальной информации.

Литература

1. Аналитический центр Perimetrix [Электронный ресурс]: <<http://perimetrix.ru>>.
2. Ярочкин В.И. Информационная безопасность. М.: Академический проект, 2008. 544 с.

Е. С. КОРАБЛЕВА — кафедра Проектирования компьютерных систем

**СИСТЕМА УПРАВЛЕНИЯ ВЗАИМООТНОШЕНИЯМИ С КЛИЕНТАМИ
ТЕРРИТОРИАЛЬНО РАСПРЕДЕЛЕННОЙ ГРУППЫ ПРЕДПРИЯТИЙ**

Научный руководитель — к.т.н., доцент А.А. Малинин

Переход к рыночной экономике требует от предприятий повышения эффективности производственных процессов, конкурентоспособности продукции и услуг в результате внедрения достижений научно-технического прогресса, эффективных форм хозяйствования и управления производством, активизации предпринимательства, инициативы и т.д.

Важная роль в реализации этой задачи отводится анализу системы управления организацией. С его помощью выявляются сильные и слабые стороны, вырабатываются стратегия и тактика развития предприятия, обосновываются планы и управленческие решения, осуществляется контроль за их выполнением, выявляются резервы повышения эффективности производства, оцениваются результаты деятельности предприятия его подразделений и работников.

CRM (Customer Relationship Management — управление взаимоотношениями с клиентами) — это концепция управления взаимоотношениями с покупателем. В терминах управления бизнесом предприятия это — система организации работы правления с ориентировкой на потребности клиента, на работу с клиентом.

За CRM-подходом большое будущее. Сегодня недостаточно произвести товар, его надо реализовать, приспособить для нужд конкретного индивидуума. Маркетинг начинается с идеи производства товара или замысла оказания услуги, производство настраивается на выпуск все более адаптируемых под заказчика изделий, реклама обеспечивает осведомленность о наличии товара, а CRM позволяет замкнуть весь цикл путем «правильной» работы с клиентом. Компания, освоившая технологию CRM, сможет значительно опередить своих конкурентов.

Ключевые преимущества, которые дает компании внедрение системы CRM, следующие: сокращение издержек, увеличение объема продаж и стратегическое влияние.

Ключевая возможность, необходимая в объединенной компании — это централизация системы управления, и прежде всего, общий доступ предприятий холдинга к системе ERP (Enterprise Resource Planning System — система планирования ресурсов предприятия).

Цель настоящего проекта — разработать систему управления взаимоотношениями с клиентами для территориально распределенной группы предприятий, причем разрабатываемая система должна:

- иметь функцию ввода, хранения данных;
- иметь функцию авторизации пользователей;
- анализировать цикл продаж;
- проводить синхронизацию данных (с мобильными телефонами и портативными устройствами).

Разработанная система предназначена для автоматизации CRM-стратегии компании, в частности, для повышения уровня продаж, оптимизации маркетинга и улучшения обслуживания клиентов путем сохранения информации о клиентах и истории

взаимоотношений с ними, установления и улучшения бизнес-процедур с последующим анализом результатов.

Исходя из этого были сформулированы основные принципы:

- разрабатываемая система должна обеспечивать интерактивный режим работы;
- система должна отражать иерархию всех уровней, что будет определять структуру программного обеспечения;
- система должна представлять собой совокупность информационно-согласованных модулей.

В рамках данной работы был проведен анализ требований к системе, на основе которого выбраны операционная система и среда разработки, спроектирована структура программы. Автоматизированная система реализована под управлением ОС Microsoft Windows 2000/2003/XP/Vista. Система использует СУБД Microsoft SQL Server. При разработке был использован унифицированный язык моделирования UML.

УДК 004.056(043)

И. А. КРЕМЛЕВА — кафедра Проектирования компьютерных систем

РАЗРАБОТКА КОМПЛЕКСА МЕР ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ «ТЕХПРОМ»

Научный руководитель — к.т.н., доцент И.Б. Бондаренко

Задача обеспечения безопасности любого объекта может иметь как уникальные требования, обусловленные размерами объекта, планировкой помещений, характером угроз и т.п., так и финансовые ограничения. Поэтому на этапе проектирования системы безопасности крайне важно правильно прогнозировать угрозы и подобрать компоненты и конфигурацию системы, гарантирующие максимальную степень устранения угроз при заданных ограничениях.

Наличие комплексных систем безопасности в той или иной специфической конфигурации необходимо всем предприятиям (их зданиям и территориям), оперирующим значительными объемами денег или других ценных активов, а также любым объектам, разрушение или повреждение которых влечет за собой необратимые последствия.

Любой функционирующий некоторое время производственный или административный объект обычно располагает теми или иными существующими системами безопасности, даже если последние сводятся к пожарной сигнализации и охранной вахте. При внедрении новых систем наибольшая защищенность объекта в целом и наименьшие помехи его штатному режиму работы достигаются в тех случаях, когда используются возможности интеграции новых систем с уже используемыми.

Цель настоящей работы — определение мер по защите конфиденциальной информации на предприятии «Техпром» в связи с расширением, для этого необходимо:

- проанализировать структуру предприятия, в частности такого подразделения, как служба безопасности предприятия;
- проверить на информационную безопасность схемы внутренних и внешних потоков предприятия;

- выделить зоны безопасности;
- выбрать и расположить технические средства защиты в помещениях предприятия;
- проанализировать существующие технические средства защиты;
- предоставить смету расходов;
- модернизировать структуру службы безопасности.

Проведенный анализ известных из литературы решений, позволил выявить следующие проблемы и недостатки при разработке мер по защите конфиденциальной информации на предприятии.

— Возможно подслушивание разговоров в помещении с помощью предварительно установленных радиозакладок или диктофонов.

— Отсутствует контроль телефонов и телефаксных линий связей, радиотелефонов и радиостанций.

— Возможен дистанционный съем информации с различных технических средств.

— Необходимо модернизировать устаревшую противопожарную систему и систему видеонаблюдения.

Важно отметить, что эффективность принятых мер по обеспечению безопасности на предприятии должна быть максимальной, при минимальных затратах, принятые меры должны обеспечивать защиту от утечки наиболее важной конфиденциальной информации от несанкционированного доступа.

В заключение необходимо отметить, что использование предложенных средств и методов позволит повысить информационную безопасность на предприятии «Техпром».

Литература

1. *Ярочкин В.И.* Информационная безопасность. М.: Академический проект, 2004. 544 с.
2. Закон РФ «Об информации, информатизации и защите информации». №24-ФЗ от 25.01.1995 г.
3. *Северин В.А.* Комплексная защита информации на предприятии. М.: Городец, 2008. 368 с.

УДК 004.056

В. Н. КУВШИНОВА — кафедра Проектирования компьютерных систем

РАЗРАБОТКА КОМПЛЕКСА МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В СЕТИ ИНТЕРНЕТ

Научный руководитель — к.т.н., доцент А.А. Малинин

Подключение организации к глобальной сети, такой как Интернет, существенно повышает эффективность работы организации и открывает для нее множество новых возможностей.

Хотя присоединение к Интернет предоставляет выгоду вследствие доступа к колоссальному объему информации, оно не всегда оправданно для организаций с низким уровнем безопасности. Интернет является источником потенциальных угроз, которые могут привести к плачевным последствиям для незащищенных сетей. Ошибки при проектировании, сложность конфигурирования хостов, уязвимые места, появившиеся в ходе написания программ, непродуманная политика безопасности и ряд других причин в

совокупности делают незащищенные сети открытыми для деятельности злоумышленников [1].

Система защиты организации при работе в глобальных сетях должна быть частью общего комплекса мероприятий, направленных на обеспечение безопасности информационных ресурсов.

В работе определен комплекс мер по обеспечению безопасности при работе в сети Интернет серверных и клиентских станций, который должен обеспечивать:

- разграничение доступа к информационным ресурсам сети Интернет;
- защищенность внутренней сети от несанкционированного проникновения из сети;
- защиту от вредоносных программ.

В ходе разработки комплекса мер

- проанализированы возможные угрозы информационной безопасности;
- разработана модель типового нарушителя (злоумышленника);
- проанализированы существующие средства нейтрализации угроз информационной безопасности;
- разработана политика обеспечения безопасности при взаимодействии с Интернетом.

Грамотное структурирование перечня подлежащих разработке вопросов, целей и задач, а также реализация комплекса мер по обеспечению безопасности позволяют:

- обеспечить конфиденциальность сведений;
- обеспечить непрерывность бизнес-процессов, связанных с работой внутренних корпоративных информационных служб и отдельных пользователей за счет предотвращения возможных атак извне и изнутри сети;
- обеспечить бесперебойное функционирование общедоступных сетевых ресурсов (электронная коммерция, web-портал и т.д.), представляющих компанию во внешнем мире, за счет предотвращения возможных сетевых атак;
- организовать безопасный обмен информацией между территориально разнесенными представительствами организации при использовании сети Интернет в качестве транспортной среды (при этом передаваемые данные необходимо надежно защищать от чтения или модификации в процессе передачи);
- контролировать и управлять доступом внутренних пользователей к информационным ресурсам внутренней сети или Интернета;
- контролировать и управлять доступом внешних пользователей к информационным ресурсам компании;
- обнаруживать источники производимых атак с целью выявления злоумышленника и принятия соответствующих мер [2].

Литература

1. *Леонтьев В.П.* Безопасность в сети Интернет. Изд-во «Олма Медиа Групп», 2008 256 с.
2. *Родс-Оусли М., Страссберг К.* Безопасность сетей. Изд-во «Эком», 2006. 912 с.

П. Д. КУДРЯВЦЕВ — кафедра Проектирования компьютерных систем

РАЗРАБОТКА ИНТЕГРИРОВАННОЙ СИСТЕМЫ ОХРАНЫ НА ПРЕДПРИЯТИИ «НЕВОД»

Научный руководитель — ст. преподаватель К.О. Ткачев

В современном мире перед любым предприятием возникает задача централизованного управления обеспечением безопасности. Интегрированная система охраны (далее ИСО) — это совокупность функционально и информационно связанных друг с другом подсистем безопасности, работающих по единому алгоритму и имеющих общие каналы связи, программное обеспечение, базы данных. В результате использования ИСО появляется возможность мониторинга и управления всеми подсистемами с одного рабочего места.

Спроектированной ИСО должны быть свойственны:

— возможность задавать требуемые сценарии действий любой сложности в ответ на различные события в системе (применив специальный язык сценариев, можно определить сколь угодно сложную реакцию системы на события);

— гибкость и удобство настройки (система должна иметь возможность подстраиваться под задачи конкретного объекта);

— легкость и удобство масштабирования (отсутствие ограничений на масштаб охраняемого объекта и возможность подключения любого количества рабочих мест);

— надежность (система должна иметь несколько уровней резервирования, работающих в автоматическом режиме);

— распределенность (система должна иметь возможность объединения территориально удаленных подразделений предприятия в единую систему безопасности и управления);

— модульность и открытые интерфейсы (система может быть легко расширена как за счет включения новых модулей, так и за счет интеграции системы с уже существующими системами предприятия).

Главное условие использования ИСО — все перечисленные выше требования должны реализовываться в едином информационном поле, по возможности в единой среде передачи информации, для того чтобы события и действия разных систем интегрировались между собой максимально полно [1].

ИСО, как правило, включает систему цифрового видеонаблюдения; систему контроля и управления доступом; охранно-пожарную сигнализацию; подсистемы безопасности и управления производственными процессами; системы жизнеобеспечения.

ИСО позволяют решать следующие задачи:

— снижение влияния «человеческого фактора» (система выявляет потенциально опасные ситуации, привлекает к ним внимание оператора и контролирует его действия);

— централизованное управление всеми подсистемами;

— протоколирование событий (информация о событиях в системе, срабатываниях датчиков, изменениях параметров системы и т.д. записывается в специальные архивы);

— масштабируемость;

— экономическая эффективность (снижение эксплуатационных расходов на инженерные коммуникации объекта).

Целью работы является создание интегрированной системы охраны на предприятии «Невод», включающей подсистемы: контроля и управления доступом, охранно-пожарной сигнализации и видеонаблюдения. Работа системы может поддерживаться без сетевого

напряжения не менее 5 часов, архивная видеoinформация должна храниться не менее 4 дней.

Литература

1. *Веселов* Интегрированная система безопасности на основе технологии [Электронный ресурс]: <<http://articles.security-bridge.com/articles/14/11856/>>.
2. *Игнатьев В.А.* Информационная безопасность современного коммерческого предприятия. Старый Оскол: ТНТ, 2005. 448 с.

УДК 004.056(043)

А. Ю. КУЗНЕЦОВ — кафедра Проектирования компьютерных систем

РАЗРАБОТКА КОМПЛЕКСА МЕР ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ ОАО "УСТЬ-ЛУГА"

Научный руководитель — к.т.н., доцент И.Б. Бондаренко

Ключевой становится задача создания превентивной системы безопасности предприятия, благодаря которой возникают условия для предотвращения преступных действий. Решение этой задачи возможно, если рассматривать систему безопасности предприятия как мощный управленческий инструмент, позволяющий эффективно контролировать заданный уровень безопасности и повышать его, управляя рисками. Такой подход позволяет иначе оценивать традиционные задачи по защите объекта и использовать возможности современных технологий с большей эффективностью.

Система безопасности должна способствовать реализации единой политики безопасности предприятия: система безопасности предприятия проектируется таким образом, чтобы было возможно получать точную и достоверную информацию о событиях на объекте от системы.

Управление системой безопасности должно быть централизованным: глубокая интеграция систем в единый комплекс значительно повышает управляемость и информативность системы. Интегрированное решение позволяет быстро и с высокой точностью обнаруживать и распознавать угрозы, эффективно реагировать на тревожные события и проводить комплексный анализ событий по объекту.

Ключевой задачей современной системы безопасности является создание и поддержание на предприятии единого подхода к безопасности, опирающегося на надежную масштабируемую технологию. Функциональные возможности современных систем безопасности охватывают весь блок задач, связанных с инженерно-технической защитой объектов.

В ряде случаев нет необходимости взаимоувязывания всех задач. Но в большинстве случаев решение этих задач отдельно друг от друга, путем создания автономных систем на разных платформах, создает массу проблем: отсутствие связи между системами, разные базы данных и способы работы с информацией, невозможность составить или восстановить полную картину событий, неконтролируемое присутствие человеческого фактора на критических участках объекта и т.д. Специфика угроз на многих подразделениях предприятия такова, что внедрение комплексной системы обеспечения безопасности является единственным эффективным решением, имеющим смысл как с экономической точки зрения, так и с управленческой.

В настоящей работе необходимо создать комплекс мер по защите конфиденциальной информации на предприятии «Усть-Луга», для этого необходимы:

1. анализ информационных потоков предприятия;
2. разработка зон безопасности на предприятии;
3. анализ существующих технических средств защиты;
4. организация системы контроля и управления доступом для людей и транспортных средств;
5. организация разветвленной сети видеомониторинга всех необходимых участков и секторов;
6. организация многоуровневой системы инженерно-технической защиты периметра;
7. организация единой системы сбора и обработки информации от подсистем.

Необходимо отметить, что внедрение системы безопасности предприятия должно создавать дополнительный экономический эффект: помимо снижения эксплуатационных затрат (закладывается на этапе проектирования) реальный экономический эффект от внедрения комплексной системы безопасности достигается благодаря снижению страховых взносов и использованию ресурсов системы различными службами предприятия.

Литература

1. *Ярочкин В.И.* Информационная безопасность. М.: Академический проект, 2004. 544 с.
2. Закон РФ «Об информации, информатизации и защите информации», №24-ФЗ от 25.01.1995 г.
3. *Северин В.А.* Комплексная защита информации на предприятии. М.: Городец, 2008. 368 с.

УДК 004.6

Д. Н. КУЧКО — кафедра Проектирования компьютерных систем

РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Научный руководитель — д.т.н., профессор С.А. Арустамов

С вступлением в силу Федерального закона «О персональных данных» перед всеми предприятиями (организациями) всех форм собственности, осуществляющими свою деятельность на территории РФ, органами государственной власти встал вопрос о разработке и проведении комплекса мероприятий по защите персональных данных. Персональными данными признаются любые сведения о физическом лице, в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

В целях дифференцированного подхода к обеспечению безопасности персональных данных (далее — ПД) в зависимости от объема обрабатываемых ПД и угроз безопасности жизненно важным интересам личности, общества и государства информационные системы персональных данных (далее ИСПД) подразделяются на классы:

— Класс 1 (К1) — ИСПД, для которых нарушение заданной характеристики безопасности ПД, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;

— Класс 2 (К2) — ИСПД, для которых нарушение заданной характеристики безопасности ПД, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;

— Класс 3 (К3) — ИСПД, для которых нарушение заданной характеристики безопасности ПД, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;

— Класс 4 (К4) — ИСПД, для которых нарушение заданной характеристики безопасности ПД, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

Категории ПД, обрабатываемых в информационных системах:

— обезличенные и (или) общедоступные ПД

— ПД, позволяющие идентифицировать субъект ПД

— ПД, позволяющие идентифицировать субъект ПД и получить о нем дополнительную информацию

— ПД, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни.

В общем случае компании, ИС которых отнесены к классам К1, К2, К3, должны:

— создать систему защиты ИС, в которой осуществляется обработка персональных данных, и провести оценку ее соответствия установленным требованиям;

— получить лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации;

— осуществить работы по защите речевой конфиденциальной информации (в случае воспроизведения персональных данных по акустическому каналу).

Литература

1. ФСТЭК России. Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных. 2008. 44 с.
2. ФСТЭК России. Рекомендации по обеспечению безопасности персональных данных. 2008. 40 с.

УДК 629.7.054.07

О. Ю. КУШНИР — кафедра Проектирования компьютерных систем

РАЗРАБОТКА КОНСТРУКЦИИ ПУЛЬТА УПРАВЛЕНИЯ И ИНДИКАЦИИ ДЛЯ САМОЛЕТА ЯК-130

*Научный руководитель — Н.И. Почепав,
начальник КБ ФГУПС Пб ОКБ «Электроавтоматика»*

По мере усложнения условий полета и задач, решаемых летательным аппаратом (ЛА), резко возрастает количество бортового оборудования, что приводит к избытку электромеханических индикаторов, устанавливаемых в кабине экипажа. Выход из этого положения возможен за счет отображения полетной информации, поступающей от различных датчиков на индикаторы с плоскими экранами, и расположения элементов управления на пультах, что обеспечивает сосредоточение необходимой информации на ограниченном участке приборной доски и наглядность.

Более сложной оказалась проблема отображения лавинообразно возрастающего объема информации, поступающей от разнообразных внешних и внутренних источников: приемника глобальной спутниковой системы навигации (GPS), радиомаяков ближней и дальней навигации, курсовых и глиссадных радиомаяков, азимутальных и дальномерных радиомаяков системы посадки, радиолокационных систем, систем связи и т.д. Для рационального восприятия такого количества информации ее следует предварительно обрабатывать и представлять с помощью соответствующих средств индикации.

Таким образом, расширение диапазона функциональных задач, возлагаемых на бортовые средства отображения информации, привело к массовому переходу от электромеханического оборудования к приборам с экранной индикацией.

Разработанный многофункциональный высокопроизводительный экранный пульт управления и индикации (ПУИ), позволяет решать задачи навигации, управления, а также планирования полета и обмена данными.

Разработанная конструкция ПУИ имеет следующие особенности:

- люминесцентный дисплей заменяется обладающим большей яркостью цветным жидкокристаллическим с большим размером рабочего поля по вертикали, что улучшает восприятие информации;

- ручка регулировки яркости заменена двумя клавишами;

- на управляющем поле ПУИ отсутствуют клавиши алфавитного набора, поскольку информация о параметрах плана взлета, посадки, полета по маршруту загружается из программы.

Таким образом разработана конструкция пульта управления и индикации, входящего в состав информационно-управляющего поля комплекса бортового оборудования. Детальной разработке подлежат модуль преобразования информации и модуль управления.

Литература

1. *Ефанов В.Н.* Стеклокабина экипажа: тенденции и перспективы // Мир авионики. 2001. № 1. С. 20—26.
2. *Баханов Л.Е.* Комплексная система управления вооружением и полетом как эффективное средство повышения возможностей истребителя // Мир авионики. 2001. № 3. С. 29—35.

В. О. ЛАЗАРЕВ — кафедра Проектирования компьютерных систем

РАЗРАБОТКА ПРОМЫШЛЕННОГО КОНТРОЛЛЕРА

Научный руководитель — ассистент П.А Косенков

Промышленный контроллер — управляющее устройство, применяемое для автоматизации технологических процессов, управления климатом и др. на транспорте и других отраслях в условиях, близких к промышленным.

Современный рынок средств автоматизации предлагает широкий спектр аппаратных и программных устройств для построения надежных и удобных в эксплуатации систем. К преимуществам применения контроллеров относятся снижение, вплоть до полного исключения, влияния так называемого человеческого фактора на управляемый процесс, сокращение персонала, минимизация расходов сырья, улучшение качества конечного продукта, и в результате — существенное повышение эффективности производства. Основные функции, выполняемые системами, которые включают в себя управление, обмен данными, обработку, накопление и хранение информации, формирование сигналов тревоги, построение графиков и отчетов.

Процесс проектирования современных промышленных контроллеров состоит из нескольких этапов: определение требований системы; функциональное описание; выбор процессорной системы; разработка аппаратного обеспечения; разработка программного обеспечения.

Контроллер предназначен для удаленного мониторинга промышленных объектов и управления исполнительными устройствами на объекте. Контроллер должен иметь сетевой порт совместимый с Ethernet 10BASE-T/10010BASE-TX типа RJ45, два гальванически изолированных порта RS232, два гальванически изолированных порта RS485, SD- считыватель. Контроллер должен быть оснащен GSM-GPRS модемом для удаленного доступа и соответствующими разъемами для подключения антенны.

Для предотвращения нештатных состояний системы требуется установить таймер и контроллер питания. Следует предусмотреть возможность расширения функциональности путем установки дополнительных модулей, как в корпусе контроллера, так и в виде внешних устройств.

Дополнительно контроллер может быть оснащен 6 логическими входными линиями с гальванической развязкой и 4 выходами, способными коммутировать постоянное и переменное напряжение от 12 до 250 В.

Должна быть предусмотрена возможность питания от резервного источника.

Питание контроллера осуществляется от блока постоянного питания 24 В, с возможностью работы в широком диапазоне значений напряжения от 9 до 48 В, с защитой от смены полярности и от попадания высокого напряжения в линию питания. Потребляемая мощность устройства не более 25 Вт.

Изделие предназначено для работы в закрытых неотапливаемых помещениях при: температуре окружающего воздуха от -25 до $+55^{\circ}$ С, относительной влажности от 20 до 90 %, атмосферном давлении от 84 до 110 кПа.

Масса контроллера не более 0,5 кг, габариты (не более): высота — 100; длина — 200; ширина — 120 мм.

Разработанный контроллер, может составить конкуренцию современным аналогам промышленных контроллеров удаленного доступа и мониторинга.

А. Е. МАНГУШЕВ — кафедра Проектирования компьютерных систем

УПРАВЛЕНИЕ ЖИЗНЕННЫМ ЦИКЛОМ ИНФОРМАЦИИ В СИСТЕМЕ ХРАНЕНИЯ ДАННЫХ

Научный руководитель — доцент Р.А. Халецкий

В настоящее время планарные технологии являются основой производства полупроводниковых приборов микро- и оптоэлектроники. Для отбраковки изделий проводится автоматический контроль различных характеристик, который, как правило, является наиболее трудозатратным этапом производственного цикла. Поэтому сокращение времени автоматического контроля характеристик приборов является важной задачей.

В процессе измерения параметров многократно повторяются следующие этапы:

- 1) определение момента контакта измерительных зондов с плоскостью измеряемой структуры;
- 2) измерение требуемых характеристик;
- 3) подъем измерительных зондов.

Цель настоящей работы заключается в создании методов и алгоритмов отбраковки изделий оптоэлектроники и их практической реализации с использованием универсальных цифровых мультиметров фирмы Keithley. Эти мультиметры широко используются в производстве полупроводниковых приборов, что обусловлено широким диапазоном подаваемых и измеряемых токов и напряжений, а также высокой точностью измерений и возможностью разработки собственных приложений для управления прибором через интерфейс GPIB.

Для достижения поставленной цели необходимо решить следующие_основные задачи:

- исследование особенностей протокола взаимодействия GPIB;
- создание и оптимизация алгоритмов взаимодействия цифрового мультиметра с персональным компьютером;
- создание программного интерфейса взаимодействия разработанных программных модулей с внешним программным обеспечением.

В работе предполагается:

- разработать алгоритмы определения надежности контакта измерительных зондов с плоскостью измеряемой структуры;
- разработать методы и алгоритмы измерения основных электрофизических характеристик полупроводниковых структур;
- практически реализовать алгоритмы.

В. И. МИЛУШКОВ — кафедра Проектирования компьютерных систем

РАЗРАБОТКА ВИЗУАЛИЗАЦИИ СИСТЕМЫ РЕЗУЛЬТАТОВ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ДИНАМИЧЕСКИХ СИСТЕМ

Научный руководитель — д.т.н., профессор Ю.А. Гатчин

С учетом значительной стоимости проведения испытаний автономных беспилотных подводных аппаратов, особую актуальность приобретает разработка системы моделирования поиска экологических аномалий, позволяющей решать задачи, связанные как с отработкой, комплексным анализом алгоритмов обработки информации и управления, так и с обучением операторов [1].

Рассматриваемая система позволяет формировать требования к измерительным каналам, поскольку одной из ее составных частей является блок имитаторов, моделирующий входные сигналы судового природоохранного комплекса для различных природных условий. Таким образом, в настоящее время задача создания моделирующей системы автономного подводного аппарата, позволяющей наглядно отображать изменения результатов моделирования при различных вариантах исходных данных, является важной и актуальной. Для представления результатов моделирования целесообразно использовать трехмерную визуализацию.

Целью работы является создание программного обеспечения для визуализации результатов имитационного моделирования выхода автономного необитаемого подводного аппарата на источник экологических аномалий.

Моделирующая система включает в себя модель среды, в том числе модель источника загрязнения с соответствующими параметрами и модель корабля носителя [1].

Учитывая наличие большого числа динамических моделей автономного подводного аппарата необходимо сформировать требования к процессу визуализации результатов моделирования.

Общим требованием, к функционированию системы визуализатор во всех режимах является необходимость обзора освещенной области поиска при движении по акватории. При нахождении экологической аномалии должна подсвечиваться траектория движения аппарата. Также необходимо осуществлять видеозапись результатов моделирования в файл.

Исходя из анализа существующих визуализаторов, а также с учетом сформированных требований к проектированию была выбрана система MatLab-Simulink. Преимущество этой системы заключается в возможности трехмерной визуализации результатов моделирования при использовании пакета Virtual Reality (VR) Toolbox. Этот пакет позволяет подключить созданную анимационную систему к среде MatLab-Simulink и управлять моделью динамической системы [2].

Существует возможность вывода траектории движения автономного аппарата и источника аномалии в том случае, если он подвижен. Специальный блок генерирует через равные промежутки времени маркеры выбранной формы [3]. Отладка программного обеспечения для визуализации выхода аппарата на источник экологических аномалий проводилась двумя способами: при подключении к автономной модели и при подключении к стенду математического моделирования.

В ходе работы были сформулированы требования к программному обеспечению, выбрано средство визуализации результатов имитационного моделирования, разработано и отлажено программное обеспечение для визуализации результатов моделирования поиска.

Разработанная автоматизированная система визуализации результатов моделирования поиска экологических аномалий автономным беспилотным подводным аппаратом обеспечивает наглядность результатов моделирования, облегчает процесс отладки автоматизированной обработки информации судовым природоохранным комплексом и снижает трудоемкость разработки контрольных вариантов для имитационной модели.

Литература

1. *Мальшиев П.Ю.* Судно оперативного контроля экологической и радиационной обстановки в шельфовой зоне Баренцевого и Белого морей // Тр. IX Всеросс. конф. «Прикладные технологии и гидроакустики и гидрофизики». СПб: Наука, 2008. 315 с.
2. *Долговесов Б.С.* Компьютерные системы визуализации в технологии виртуальной реальности // Программные продукты и системы. 1995. № 4. С. 52.
3. *Дьяконов В.П.* Matlab 7.* /R2006/R2007. М.: ДМК-Пресс, 2008. 768 с.

УДК 004.422.81

А. С. МОРОЗОВ — кафедра Проектирования компьютерных систем

РАЗРАБОТКА ИНТЕРАКТИВНЫХ ЭЛЕКТРОННЫХ ТЕХНИЧЕСКИХ РУКОВОДСТВ ДЛЯ СЕРВИСНЫХ ЦЕНТРОВ ПО РЕМОНТУ ЭЛЕКТРОННОЙ АППАРАТУРЫ

Научный руководитель — доцент Н.Ю. Иванова

Потребителя электронных средств интересуют преимущественно эксплуатационные характеристики приобретаемой аппаратуры, которые представлены в интерактивных электронных технических руководствах (ИЭТР).

ИЭТР представляет собой структурированный комплекс взаимосвязанных технических данных, предназначенный для предоставления в интерактивном режиме справочной и описательной информации об эксплуатационных и ремонтных процедурах, связанных с конкретным изделием. Использование ИЭТР обусловлено самой логикой научно-технического развития.

В число задач, решаемых с помощью ИЭТР, входит обеспечение:

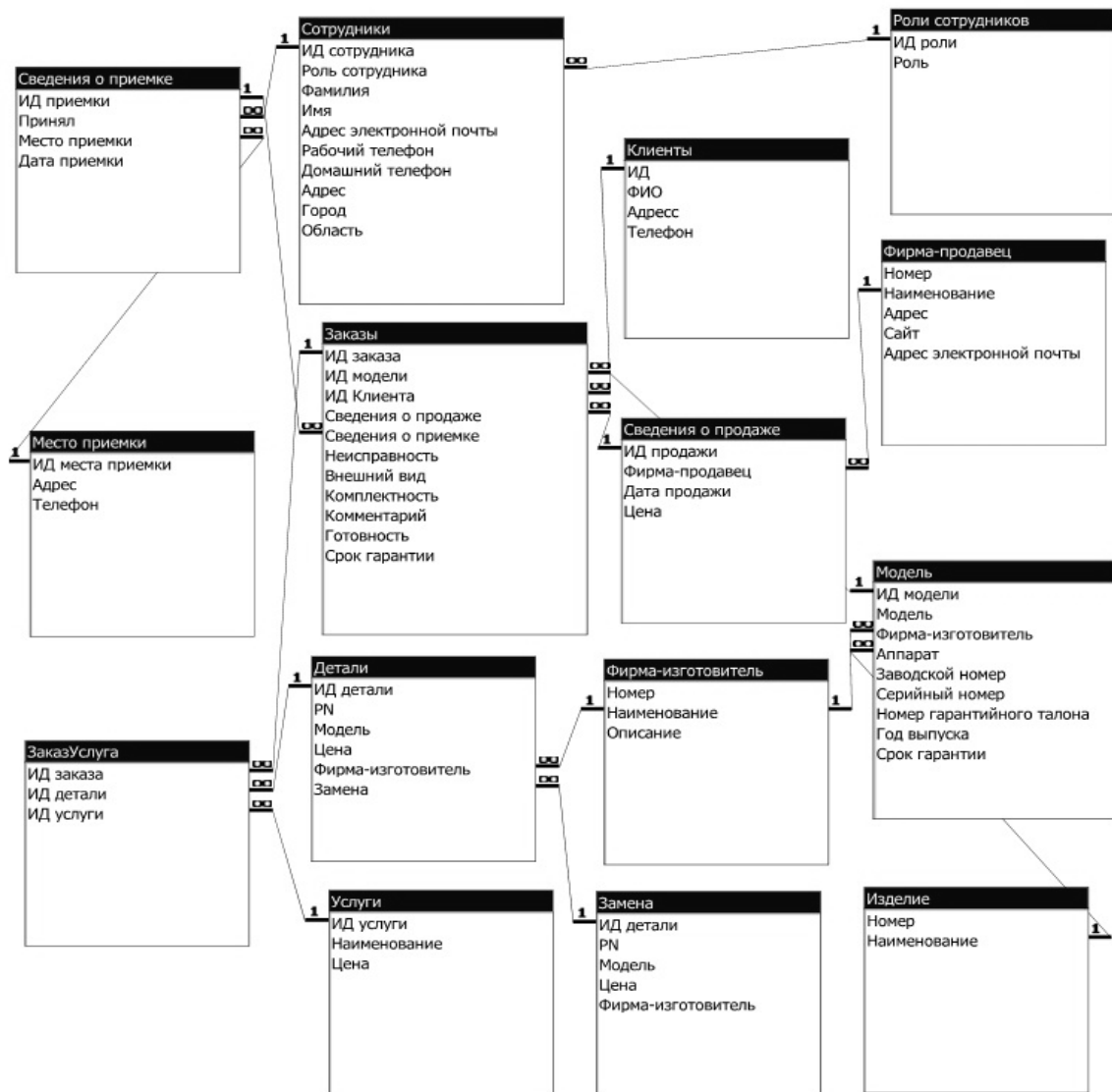
- справочными материалами для оперативного решения любых вопросов, возникающих в процессе эксплуатации и ремонта электронной аппаратуры;
- информацией об использовании изделия и возможной потребности в необходимых инструментах и материалах, о количестве и квалификации обслуживающего персонала;
- автоматического сбора и обработки данных для получения диагностической информации;
- электронными каталогами изделий и запасных частей с возможностью их автоматизированного заказа;
- обмена данными между потребителем и поставщиком;
- планирования и учета проведения ремонтных работ;

Исходя из задач, решаемых на основе использования эксплуатационно-ремонтной документации, структуру и содержание ИЭТР можно представить в виде многоуровневой системы. Разработанное ИЭТР содержит простые информационные объекты – текстовую

и графическую информацию, данные в мультимедийной форме, гипертекстовые документы.

Электронная система отображения представляет собой модульную структуру, обеспечивающую возможность отображения любых типов информации, для просмотра которой не требуется специальное программное обеспечение, достаточно стандартного Web-браузера.

На практике выделяют пять классов ИЭТР, каждый из которых характеризуется определенной функциональностью. Начиная с четвертого класса, руководства представляют собой документы, имеющие три компонента: структура, оформление и содержание, стандартизированный интерфейс пользователя и интерактивные базы данных. Руководства данного класса используют для хранения информации СУБД. Разработанное ИЭТР относится к четвертому классу и предназначено для сервисных центров и других компаний, занимающихся ремонтом электронной аппаратуры.



Информация об изделии в руководстве отображается в виде простого представления состава изделия, детального описания режимов функционирования аппаратуры, структурированных сведений о типовых неисправностях и методах их устранения.

К преимуществам ИЭТР относится сокращение сроков освоения новых изделий потребителем; быстрое получение исчерпывающей информации по вопросам эксплуатации и ремонта аппаратуры; возможность просматривать всю информацию для ремонтных операций перед их выполнением или во время ремонта непосредственно на

рабочем месте; легкость обновления информации; возможность включения специальных учебных программ, имитирующих функционирование изделия; возможность учета принятых заказов; возможность формирования различных типов отчетов.

При разработке ИЭТР были проанализированы существующие аналоги системы, разработаны структура и алгоритмы работы системы, разработана структура базы данных, создан пользовательский интерфейс.

На этапе проектирования системы был выполнен анализ бизнес-процессов системы и разработана доменная модель ИЭТР (см. рисунок).

Также были определены состав и структура данных, которые должны находиться в базе данных и обеспечивать выполнение необходимых запросов и задач пользователя.

Разработанная система состоит из следующих модулей.

— *Стартовый модуль*. Обеспечивает доступ к базе данных и осуществляет постоянный контроль параметров аутентификации пользователя и его принадлежность к группе доступа.

— *Модуль авторизации пользователей*. Выполняет проверку введенных пользователем данных, необходимых для успешного входа в систему с расширенными правами.

— *Модуль ввода, редактирования и удаления данных*. Осуществляет наполнение, редактирование и удаление информации в базе данных.

— *Модуль формирования отчетов*. Обеспечивает создание и отображение различных отчетов.

— *Модуль поиска данных*. Осуществляет поиск информации в базе данных по различным критериям.

ИЭТР было разработано в среде Microsoft Visual Studio 2008, язык программирования C#, в качестве системы управления базами данных выбрана Microsoft SQL Server 2008.

Результатом выполненной работы является программное обеспечение ИЭТР, с помощью которого сервисные центры по ремонту электронной аппаратуры смогут автоматизировать свою работу.

УДК 004.005

А. С. НИКИТЕНКО — кафедра Проектирования компьютерных систем

ВОССТАНОВЛЕНИЕ ИКТ ПРЕДПРИЯТИЯ ПОСЛЕ ДЕСТРУКТИВНЫХ СОБЫТИЙ

Научный руководитель — д.т.н., профессор С.А. Арустамов

Общеизвестно, что необходимый уровень информационной безопасности компьютерных систем достигается обеспечением приемлемого уровня рисков нарушения конфиденциальности, целостности и доступности информационных ресурсов. Нарушение доступности информационных ресурсов может произойти в результате следующих событий:

- технический сбой аппаратных либо программных средств;
- атака на ресурсы со стороны внешних или внутренних злоумышленников;
- физическое уничтожение носителей информации или средств доступа в результате воздействия деструктивных процессов или стихийных природных явлений [1,2].

Одним из главных факторов обеспечения безопасности предприятия после деструктивного события является удачный выбор расположения резервного офиса по критерию транспортной доступности, с одной стороны, и достаточной удаленности от основного офиса с целью обеспечения независимости его энергообеспечения и выведения его из зоны поражения с другой. На практике для мегаполиса идеальным расстоянием между основным и резервным офисом следует считать расстояние в 5—10 км. Меньшая удаленность не гарантирует сохранности резервного офиса при катастрофе, большая — вызывает затруднения не только при реализации плана в результате наступления катастрофического события, но и значительно повышает стоимость тестирования решения при его верификации.

Аудит информационных ресурсов и определения критического набора бизнес-процессов, необходимых для продолжения деятельности. На этом этапе принципиальным решением является определение минимального набора бизнес-процессов, которые считаются критическими для предприятия.

Оценка минимально возможной численности персонала, необходимого для поддержания бизнес-процессов в восстановительный период.

Планирование информационно-коммуникационной инфраструктуры (ИКИ) резервного офиса:

— формирование перечня оборудования, включая ПК, серверы, сетевое и оконечное оборудование, АТС с аппаратами, линии передачи данных, осуществляющие связь резервного офиса с партнерами, регуляторами бизнес-деятельности, Интернетом, головным офисом и бизнес-приложениями, размещенных вне территории России;

— разработка политики поддержания актуальности данных, необходимых для продолжения бизнеса после наступления деструктивного события.

Политика поддержания актуальности данных резервного офиса должна опираться на классификацию данных по степени важности для бизнеса и частоте их изменяемости. В зависимости от типа данных применяются различные стратегии их актуализации.

Документирование процедур DRP и осведомленность бизнес-пользователей. Важным этапом разработки DRP является его детальное документирование, включающее описание отдельных процедур, регламентирование ответственности сотрудников, реализующих процедуры восстановления, и осведомленность бизнес-пользователей в отношении существования такого плана и перспектив восстановления технической инфраструктуры бизнеса после деструктивных событий.

Особое внимание следует уделять распределению обязанностей и распараллеливанию независимых процессов восстановления данных с целью минимизации времени активации ИКИ, а также методам быстрого контроля актуальности и целостности данных, переданных в резервный офис по каналу связи, возможности корректного открытия баз данных и других проверок, подтверждающих работоспособность ИКИ.

Отработка основных положений документов для пользователей и служб ИТ проводится в ходе регулярных тестов, имитирующих различные ситуации, возникающие после деструктивных событий.

Литература

1. *Шаньгин В.Ф.* Защита компьютерной информации. Эффективные методы и средства. М.: ДМК-Пресс, 2008. 544 с.
2. *Белов Е.В., Лось В.П., Мещеряков Р.В., Шелупанов А.А.* Основы информационной безопасности. М.: Горячая линия — Телеком, 2006. 544 с.

К. Ю. ПОЛОСИХИН — кафедра Проектирования компьютерных систем

РАЗРАБОТКА КОМПЛЕКСА МЕР ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ «ПЛАНЕТА»

Научный руководитель — к.т.н., доцент И.Б. Бондаренко

С каждым годом увеличивается количество информации, растет спрос на нее, а значит и возрастает ее ценность, в связи с этим повышаются требования по ее защите. Такими же быстрыми темпами совершенствуются компьютерные технологии. Из-за ежегодного обновления компьютерных технологий возникают новые угрозы для информации. Следовательно, возрастет необходимость ее защиты. Для того чтобы защита была полной, необходимо прорабатывать ее комплексно.

Успешное развитие любой компании зависит от корректно сформулированных стратегических целей и способов их достижения. Принято считать, что в качестве таких целей могут выступать финансовые показатели, например завоевание определенной доли рынка или увеличение прибыли. Однако, как показывает практика, очень мало руководителей и собственников бизнеса уделяют достаточное внимание вопросам долгосрочного планирования в области информационной безопасности. Современные условия ведения бизнеса таковы, что при отсутствии или нечетко сформулированной стратегии информационной безопасности, желаемые финансовые показатели могут быть недостижимы.

Любое функционирующее предприятие уже располагает теми или иными системами безопасности, даже если это пожарная сигнализация и охранник вахтер. При внедрении новых систем наибольшая защищенность объекта в целом и наименьшие помехи штатному режиму его работы достигаются в тех случаях, когда используются все доступные возможности интеграции новых систем с уже используемыми.

В работе необходимо определить комплекс мер по защите конфиденциальной информации на предприятии «Планета», проанализировать структуру предприятия, в частности такого подразделения, как служба безопасности предприятия, проверить безопасность схем внутренних и внешних потоков предприятия, рассмотреть и предложить зоны безопасности, выбрать и расположить технические средства защиты в помещениях. А также необходимо организовать пожарную систему и систему оповещения на случай возникновения чрезвычайных ситуаций.

При разработке комплекса мер по защите конфиденциальной информации на предприятии «Планета» необходимы:

- 1) анализ существующей организационно-распорядительной документации и неформальных требований, отражающих политику безопасности;
- 2) разработка зон безопасности на предприятии (увеличение рабочих площадей и пересмотр концепции организации работы службы безопасности);
- 3) анализ существующих технических средств защиты (переоснащение новым современным оборудованием);
- 4) установка датчиков сигнализации на место возможных посторонних подключении к коммуникациям и размещение средств охранно-пожарного оповещения.

В заключение необходимо отметить, что статистика показывает, что во всех предприятиях убытки от злонамеренных действий непрерывно возрастают. причем основные причины убытков связаны не столько с недостаточностью средств безопасности как таковых, сколько с отсутствием взаимосвязи между ними, т.е. с нереализованностью

системного подхода. Поэтому необходимо опережающими темпами совершенствовать комплексные средства защиты информации.

Литература

1. *Ярочкин В.И.* Информационная безопасность. М.: Академический проект, 2004. 544 с.
2. Закон РФ «Об информации, информатизации и защите информации», №24-ФЗ от 25.01.1995 г.
3. *Северин В.А.* Комплексная защита информации на предприятии. М.: Городец, 2008. 368 с.

УДК 004.056

А. С. ПОНОМАРЕВ — кафедра Проектирования компьютерных систем

УПРАВЛЕНИЕ ЖИЗНЕННЫМ ЦИКЛОМ ИНФОРМАЦИИ В СИСТЕМЕ ХРАНЕНИЯ ДАННЫХ

Научный руководитель — ст. преподаватель О.В. Михайличенко

Наиболее популярными стандартами кодирования видеоданных являются MPEG-2 и MPEG-4. В настоящей работе приведены методы сокрытия информации в видеопоследовательностях, сжимаемых по стандарту MPEG-2.

Стеганографические методы, применяемые для встраивания информации в видеопоток, сжатый по стандарту MPEG-2 (далее — MPEG), должны работать в режиме реального времени, они должны обладать малой вычислительной сложностью. Таким образом, единственно приемлемыми являются методы, позволяющие встраивать данные непосредственно в видеопоток сжатых данных, чтобы избежать лишних вычислений [1].

Относительно простым в вычислениях является способ внедрения данных на этапе дискретизации видеоряда.

Разработчики этого метода утверждают, что его использование сильно ухудшает качество видеоряда, так как встраивание происходит в область, особо заметную для системы человеческого зрения. Второй проблемой при использовании данного метода является то, что встраивание происходит в кадры (кодируются без ссылок на другие кадры, содержат неподвижное изображение и применяются для построения других типов кадров), следовательно, последующие кадры имеют такие же изменения, что ведет к накоплению ошибок при воспроизведении.

Метод встраивания на уровне битовой последовательности подразумевает замену наименее значимых битов в специально выбранных кодовых словах. Этот метод наряду с его неоспоримыми достоинствами — высокой пропускной способностью и небольшой вычислительной сложностью — обладает существенным недостатком. Информация, встроенная с его помощью, может быть легко удалена. Для этого достаточно произвести встраивание любых других данных в стегаконтейнер, что приведет к незначительному ухудшению качества видеоданных, и уничтожению ранее встроенной информации.

Метод внедрения информации за счет энергетической разности между коэффициентами дискретизации обладает не высокой вычислительной сложностью. Бит встраиваемой информации внедряется в выбранную область модификацией разности

энергий между высокочастотными коэффициентами верхней части выбранной области и ее нижней части.

Проведенные исследования показали, что этот алгоритм позволяет осуществлять встраивание информации в цифровой поток 6—8 Мбит/с со скоростью 0,42 кбит/с практически без искажений видеобразия.

Центральную роль как в процессе встраивания, так и в процессе извлечения встроеной информации играют значения энергии подобластей, которые определяются четырьмя следующими факторами:

- характеристиками подобластей;
- количеством блоков n , приходящихся на одну выбранную область;
- шагом квантователя;
- размером подмножества высокочастотных коэффициентов.

Эти факторы накладывают определенные ограничения на выбор стеганоконтейнера и тем самым ограничивают его применение к случайно выбранному видеоконтенту [2].

Рассмотренные методы отвечают требованиям, предъявляемым к стеганографическим методам встраивания информации в видеопоследовательности. Выбор метода зависит от поставленной задачи: если качество конечного видеосообщения не имеет значения, по сравнению с удельным объемом встраиваемой информации, лучше использовать метод внедрения данных на уровне коэффициентов, в противном случае использование метода внедрения информации за счет энергетической разности между коэффициентами является более целесообразным.

Литература

1. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. М: Солон-Пресс, 2002. 265 с.
2. Ватолин Д., Ратушняк А., Смирнов М., Юкин В. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. М: Диалог-МИФИ, 2003. 384 с.

УДК 004.72

А. Е. ПОПОВ — кафедра Проектирования компьютерных систем

РАЗРАБОТКА И ИССЛЕДОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРИМЕТРА СЕТИ

Научный руководитель — д.т.н., профессор С.А. Арустамов

По данным ведущих аналитических агентств, число инцидентов, связанных с нарушением информационной безопасности, постоянно возрастает. Специалисты, отвечающие за защиту информации, отмечают возрастающую активность внешних злоумышленников, использующих последние разработки в области нападения. Первым рубежом защиты компании от угроз из сети Интернет является так называемый периметр сети, поэтому защита периметра компьютерной сети является основным элементом системы информационной безопасности организации [1].

Современная система защиты периметра сети должна выполнять следующие функции:

- разграничение и контроль доступа, выполнение аутентификации пользователей, трансляция IP-адресов по сети (NAT);

- интеграция с различными системами аутентификации и авторизации (RADIUS, LDAP);
- организация «демилитаризованных» зон;
- возможность контроля трафика;
- возможность обнаружения и предотвращения сетевых атак и подозрительной сетевой активности;
- легкость масштабирования сети и возможность балансировки ее нагрузки;
- управление списками контроля доступа маршрутизаторов;
- сокрытие топологии вашей вычислительной сети.

Это далеко не полный перечень функций системы защиты периметра, в зависимости от специфики организации он может изменяться. Если компания имеет несколько филиалов или отделений, то может появиться необходимость в защите VPN-сетей, в дополнительной защите какого-либо специализированного программного обеспечения, защите корпоративного сайта, и наоборот, если у компании отсутствуют внешние сервисы, рабочих станций немного и сеть основана на рабочих группах, то можно обойтись обычным межсетевым экраном.

Основной задачей системы защиты является обнаружение и блокирование атак. Исключая трафик злоумышленника из потока данных, система должна отфильтровывать потоки данных из сегментов сети, проявляющих аномальную активность, и своевременно предотвращать реализацию уязвимостей. Выбранная система должна оперативно реагировать на инциденты, оповещать о возникновении критических ситуаций и в случае необходимости давать возможность оператору информационной безопасности вмешаться в работу системы. Некоторые современные системы позволяют защищаться и от внутренних угроз. Это достигается за счет контроля исходящей корреспонденции, контроля несанкционированных подключений к внутренней сети, мониторинга подозрительных действий сотрудников [2].

Литература

1. Компьютер-пресс: защита периметра сети. [Электронный ресурс]: <<http://www.compress.ru/article.aspx?id=19159&iid=889>>.
2. Энвижн Груп: Защита периметра корпоративных систем. [Электронный ресурс]: <http://www.nvisiongroup.ru/infosec_systems.htm>.

УДК 004.72

Я. В. РЫЖОНКОВА — кафедра Проектирования компьютерных систем

ПРОЕКТИРОВАНИЕ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ И ОБЕСПЕЧЕНИЕ ЕЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ ООО «АДВЕКС»

Научный руководитель — доцент А.А. Малинин

Настоящая работа посвящена созданию корпоративной компьютерной информационно-вычислительной сети.

При проектировании локальной вычислительной сети (ЛВС) можно использовать топологии, описанные в монографии [1], из которых необходимо выбрать наилучшую с точки зрения безопасности. Физическая топология сети выбирается исходя из норм

проектирования ЛВС, изложенных в международных стандартах, и с учетом технического задания. Для упрощения процесса проектирования ЛВС выделим две ее подсистемы:

- логическая (структурная схема ЛВС, ее топология);
- физическая (кабельная система КС).

Процесс проектирования ЛВС можно условно разбить на несколько этапов:

- 1) анализ требований, предъявляемых к проектируемой ЛВС;
- 2) выбор физической топологии будущей ЛВС;
- 4) анализ план-схемы расположения активного сетевого оборудования и оборудования оконечных устройств (рабочих станций, серверов, устройств телефонии);
- 5) выбор оптимальной схемы прокладки кабельной сети КС;
- 6) подготовка проектной и сметной документации, в том числе подготовка экономического обоснования проекта.

Для рассматриваемого предприятия наиболее подходит топология типа «Звезда» [2].

В работе также необходимо провести общий расчет стоимости ЛВС, а также активного и пассивного оборудования.

Реализация предложенного проекта позволит сократить бумажный документооборот внутри фирмы, повысить производительность труда, сократить время на обработку информации. Как следствие, образуются дополнительные временные ресурсы для разработки и реализации новых экономических и инвестиционных проектов. Таким образом, решится проблема окупаемости и рентабельности внедрения корпоративной сети.

Объединение компьютеров в ЛВС требует повышенного внимания к защите информации внутри сети и разграничения доступа к внутрисетевым ресурсам для персонала. Локальная вычислительная сеть должна быть спроектирована таким образом, чтобы обеспечить надлежащую степень защищенности данных без создания неудобств при использовании ресурсами ее пользователями и администратору [3, 4].

В качестве основного средства бухгалтерского учета на предприятии предлагается использовать программный комплекс Microsoft SharePoint, который прекрасно зарекомендовал себя по всем характеристикам. Программа поддерживается новейшими операционными системами Microsoft и сервисно обслуживается специально подготовленным для этого персоналом фирмы-продавца.

В заключение отметим, что с внедрением на предприятии «Адвекс» данного проекта и подключением к глобальной сети Интернет оно получит практически неограниченные информационные возможности, оперативное получение финансовых и биржевых новостей.

Литература

1. Диева С.А., Шаваева А.Г. Организация и современные методы защиты информации. 2001.
2. Бройдо В.Л.. Вычислительные системы, сети и телекоммуникации. СПб: Питер, 2004.
3. Таненбаум Э. А. Компьютерные сети. СПб: Питер, 2006.
4. Виснадул Б. Д. Основы компьютерных сетей. М.: Мир, 2007.

А. А. САМОНОВ — кафедра Проектирования компьютерных систем

РАЗРАБОТКА ПОДСИСТЕМЫ БЕЗОПАСНОСТИ ДЛЯ СИСТЕМЫ УПРАВЛЕНИЯ ЭЛЕКТРОННЫМ ПОРТФОЛИО

Научный руководитель — к.т.н., доцент Д.И. Муромцев

Портфолио — это способ фиксирования, накопления и оценки индивидуальных достижений. В свою очередь, система управления электронным портфолио — это комплекс web-приложений, решающий задачу создания портала, с помощью которого осуществляется ведение, хранение и анализ портфолио пользователей. В качестве основы системы управления электронным портфолио целесообразно использовать готовую систему управления содержимым (контентом) от [англ. content management system, CMS](#) — [компьютерную программу](#) или систему, используемую для обеспечения и организации совместного процесса создания, редактирования и управления текстовых и мультимедиадокументов (содержимого или контента).

На сегодняшний день существует множество готовых систем управления содержимым сайта. Наиболее подходящими для создания системы управления электронным портфолио являются следующие CMS: ANGEL ePortfolio; [Elgg](#); [Mahara](#); [Pass-port](#); E-portfolio; Desire2Learn; Skillsbook.

Также очень популярны бесплатные системы CMS Drupal и Joomla, они предлагают различные расширения для создания и управления электронным портфолио. Подобные системы могут быть созданы на разных языках программирования (например, Elgg, Mahara, Joomla и Drupal — на языке php, а E-portfolio — на Java). Также они могут быть как с открытым исходным кодом (Elgg), так и коммерческими (Pass-port). Все эти системы позволяют создавать порталы, на которых в структурированной форме хранятся данные о пользователях, работы, сведения об их интересах и достижениях.

Система управления электронным портфолио предполагает обработку и хранение большого объема информации, в том числе персональной и конфиденциальной. Целью данной работы является создание сквозной подсистемы защиты такой системы. Эта система представляет собой портал, под безопасностью которого подразумевается:

- отсутствие перебоев в работе, устойчивость к перегрузкам;
- защищенность от взломов, диверсий, вредоносных программ;
- затрудненность несанкционированного доступа к служебным, закрытым разделам сайта и персональной информации;
- сохранность находящейся на сайте информации, баз данных;

Основными угрозами безопасности сайтов в настоящее время являются SQL инъекции, Cross-Site Scripting (XSS), внедрение исходного кода PHP и DoS-атаки. Внедрение SQL-кода — один из распространенных способов взлома сайтов и программ, работающих с базами данных, основанный на внедрении в запрос произвольного SQL-кода. Внедрение SQL может позволить атакующему выполнить произвольный запрос к базе данных, получить возможность чтения и/или записи локальных файлов и выполнения произвольных команд на атакуемом сервере. Межсайтовый скриптинг или XSS (аббревиатура от англ. Cross Site Scripting) — тип уязвимостей, обычно обнаруживаемых в web-приложениях, которые позволяют внедрять код злонамеренным пользователям в web-страницы, просматриваемые другими пользователями. Примерами такого кода являются HTML-код и скрипты, выполняющиеся на стороне клиента, чаще всего JavaScript. PHP-инъекция — один из способов взлома web-сайтов, работающих на языке PHP, он заключается в том, чтобы внедрить специально сформированный злонамеренный

сценарий в код web-приложения на серверной стороне сайта, что приводит к выполнению произвольных команд. DoS-атака (от англ. Denial of Service — отказ в обслуживании) и DDoS-атака (от англ. Distributed Denial of Service — распределенная атака типа «отказ в обслуживании») — атака на вычислительную систему с целью вывести ее из строя, т.е. создание таких условий, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам (серверам) либо этот доступ затруднен. Разрабатываемая подсистема должна защищать конфиденциальную информацию в системе управления электронным портфолио (СУЭП). Необходимо исследовать и оценить известные угрозы безопасности, спроектировать и создать защищенную СУЭП.

В ходе работы были изучены возможности платформ для создания СУЭП и оценены возможные угрозы и уязвимость безопасности информации. На основе результатов анализа этих данных будет разработана структура СУЭП с подсистемой защиты, в которой будут использоваться следующие меры по обеспечению безопасности:

- проверка безопасности используемых на сайте скриптов, программ;
- поддержка системы обновлений платформы, лежащей в основе СУЭП;
- обеспечение безопасности модулей расширения, которые будут дописаны для расширения функционала (семантическое хранение данных);
- использование автоматизированных систем тестирования уязвимости сайтов;
- использование при необходимости защищенных протоколов передачи данных;
- безопасность, надежность хостинга, на котором размещен сайт;
- наличие в системе управления сайтом возможности «откатить» (наличие системы учета и хранения версии), отменить внесенные изменения; восстановить случайно удаленную страницу и т.п.;
- регулярное резервное копирование;
- наличие «зеркал» сайта;
- регулярная смена паролей доступа к сайту;
- запрет на хранение паролей на компьютере, подключенном к сети Интернет;
- разделение прав доступа сотрудников, работающих с сайтом;
- установка на компьютеры всех сотрудников компании (в том числе домашние) последних версий антивирусных программ, фильтров поступающей из сети на компьютер информации и т.д.

УДК 621.316.7

М. К. СЕВИКЯН — кафедра Проектирования компьютерных систем

РАЗРАБОТКА КОНСТРУКЦИИ ТЕРМОРЕГУЛЯТОРА СТАНДАРТА ЧАСТОТЫ СИСТЕМЫ ГЛОБАЛЬНОЙ СПУТНИКОВОЙ НАВИГАЦИИ ГЛОНАСС

Научный руководитель — ассистент Д.А. Боголюбов

В настоящее время системы спутниковой навигации являются одним из важнейших инструментов для обеспечения обороноспособности государства. В связи с этим представляется необходимой разработка российской системы спутниковой навигации ГЛОНАСС. Задача стабилизации и регулировки сигнала крайне важна для стабильной работы системы навигации. Эта задача реализуется с помощью стандартов частоты. Как и любая бортовая космическая аппаратура, стандарт частоты нуждается в системе терморегуляции.

Цель настоящей работы заключалась в создании основного устройства данной системы — терморегулятора стандарта частоты.

Для достижения поставленной цели были решены следующие основные задачи:

— определены необходимые для нормального функционирования терморегулятора температурные режимы;

— разработана схема термостатирования системы через квантовый дискриминатор;

— разработаны принципы функционирования, монтажа устройства в соответствии с государственными стандартами Российской Федерации.

Основные результаты работы:

— разработана конструкция терморегулятора;

— произведены расчеты вибропрочности, тепловых режимов, надежности устройства;

— разработана документация для изготовления устройства.

Описываемая разработка повысит надежность стандарта частоты и стабильность его работы в различных температурных условиях и при разных нагрузках.

УДК 628.16.087

Е. С. СЕКОРИНА — кафедра Проектирования компьютерных систем

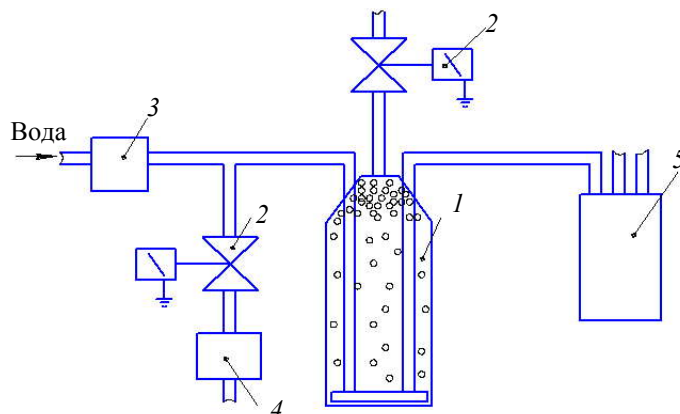
СПОСОБ УДАЛЕНИЯ ШЛАМА В УСТАНОВКАХ ДЛЯ ПОЛУЧЕНИЯ ПИТЬЕВОЙ ВОДЫ МЕТОДОМ ЭЛЕКТРОХИМИЧЕСКОЙ КОАГУЛЯЦИИ

Научный руководитель — к.т.н., доцент А.В. Панков

Одной из самых перспективных технологий очистки воды является электрохимическая коагуляция, ее основные этапы: электрообработка, коагуляция, флотация, отделение шлама [1].

На основе технологии электрохимической коагуляции разработаны приборы таких фирм, как «Водолей» и «Аквалон». Эти устройства содержат реактор, в верхней части которого закреплена емкость шламособорника. В нижней части шламособорника установлен патрубок для выхода шлама. Реактор в нижней части оснащен патрубком для выхода обработанной воды. В реакторе в процессе его заполнения основная масса шлама собирается на поверхности обрабатываемой воды и в виде постепенно утолщающегося слоя пены поступает в емкость шламособорника над горловиной реактора, но часть шлама остается в самом реакторе [2]. Оставшийся шлам отделяется с помощью механического фильтра, в который подается вода с помощью центробежного насоса. Насос разбивает частицы шлама, которые засоряют фильтр.

В настоящей работе предлагается исключить шламособорник и использовать реактор с конусообразным верхом. Образующийся шлам сбрасывается в дренаж подачей дополнительной порцией обработанной электричеством воды, что позволяет в более полной мере удалить шлам, собравшийся наверху. Отделение оставшегося шлама в воде производится с помощью



механического фильтра, куда вода будет подаваться не центробежным насосом, а под давлением воздуха от компрессора. Это исключит разбивание частиц шлама перед фильтром. На рисунке представлена схема удаления шлама в предлагаемой установке (1 — накопительная емкость; 2 — клапан; 3 — блок электродов; 4 — компрессор; 5 — фильтр).

Литература

1. ЗАО «Водолей-М» [Электронный ресурс]: <<http://vodoley-m.ru/>>.
2. Пат. РФ № 2180322, МПКС02Р1/463, С02Р1/465. Способ электрообработки воды в установке получения доброкачественной питьевой воды методом электрохимической коагуляции и устройство для его осуществления. 03.10.02.

УДК 004.056

П. Н. СЕМЁНОВ — кафедра Проектирования компьютерных систем

РАЗРАБОТКА СИСТЕМЫ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ МЕР БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ «СИГМА ПЛЮС»

Научный руководитель — к.т.н., доцент Н.С. Кармановский

В настоящее время задача защиты информации на предприятии становится все более актуальной, поскольку, завладев ею, предприятие-конкурент получает существенное преимущество, что чревато финансовыми потерями или даже банкротством компании, допустившей утечку конфиденциальной информации.

Таким образом, целями системы защиты информации предприятия являются:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз безопасности личности, предприятия, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- предотвращение других форм незаконного вмешательства в информационные ресурсы и системы, обеспечение правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющих в информационных системах;
- сохранение конфиденциальности документированной информации в соответствии с законодательством.

Алгоритм создания системы защиты конфиденциально информации таков:

- 1) определение объектов защиты;
- 2) выявление угроз и оценка их вероятности;
- 3) оценка возможного ущерба;
- 4) обзор применяемых мер защиты, определение их полноты;
- 5) определение адекватных мер защиты;
- 6) организационное, финансовое, юридическое и пр. виды обеспечения мер защиты;
- 7) внедрение мер защиты;
- 8) контроль;
- 9) мониторинг и корректировка внедренных мер.

Только комплексная система может гарантировать достижение максимальной эффективности защиты информации, поскольку системность обеспечивает наличие необходимых составляющих защиты и устанавливает между ними логическую и технологическую связь, а комплексность, требующая полноты этих составляющих, всеохватности защиты, обеспечивает ее надежность [м. лит.].

Целью работы является создание комплекса организационно-технических мер по защите информации на предприятии «Сигма Плюс». Объектом исследования является технология обеспечения информационной безопасности, а предметом — информационная безопасность предприятия.

В соответствии с поставленной целью проведено:

- 1) рассмотрение теоретической и правовой базы организации защиты информации на предприятии;
- 2) исследование системы защиты на предприятии;
- 3) исследование актуальных вопросов защиты информации для ООО «Сигма Плюс»;
- 4) разработка практических предложений.

Литература

Алексенцев А.И. Понятие и назначение комплексной системы защиты информации // Вопросы защиты информации. 1996. № 2. С. 2—3.

УДК 004.056

А. А. СЕРГЕЕВ — кафедра Проектирования компьютерных систем

РАЗРАБОТКА КОМПЛЕКСА МЕР ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ «ДЕДАЛ ИНВЕСТ»

Научный руководитель — доцент И.Б. Бондаренко

В наши дни информация имеет большую ценность. Эта ценность может определяться не только количеством труда, потраченного на ее создание, но и количеством прибыли, полученной от ее возможной реализации (поэтому промышленный шпионаж очень популярен между родственными предприятиями). Развитие вычислительных сетей в ряде случаев способствует хищению информации. Существует огромное количество фактов подтверждающих это. Человеческий фактор играет не меньшую роль в хищении и порчи информации, попытаемся определить возможные каналы утечки и сформулировать общие подходы к защите информации в организации.

Доступ в помещения, где ведется работа с конфиденциальной или секретной информацией, должен быть ограничен, там должны находиться лишь люди, работающие с закрытой информацией, обслуживающие спецаппаратуру, которые должны пройти соответствующую проверку. В случае, если в выделенное для этих целей помещение могут попасть посторонние, например, уборщицы, электрики и др., то необходимо организовать их контролируемый доступ.

Для регламентации доступа в спецпомещения, а также функционирования охраны, нами разработаны инструкции, которые повышают защищенность конфиденциальной или секретной информации.

Подготовленное для работы с закрытой информацией помещение необходимо сертифицировать в надлежащих органах на право работы с документами определенного уровня секретности.

Особое внимание следует уделить кадрам. Прежде всего, с закрытой информацией должны работать люди, прошедшие соответствующую проверку, которым доверяет руководство. Также эти сотрудники должны быть специалистами в своем деле, т.е. соответствующе обученными, так как дилетанты способны загубить хорошо поставленную работу и допустить утечку информации; работа сотрудников этого подразделения должна хорошо оплачиваться. По статистике, пособничество собственных сотрудников в утечке информации составляет до 80 % от всех видов хищения информации.

В заключение необходимо отметить, что использование предложенных средств и методов требует довольно высоких материальных затрат, в то же время затраты должны быть соизмеримы с ценностью защищаемой информации.

Литература

Краковский Ю.М. Информационная безопасность и защита информации. М.: ИКЦ МарТ, 2008. 288 с.

УДК 002.5:004

В. П. СОЛОВЬЕВ — кафедра Проектирования компьютерных систем

ИСПОЛЬЗОВАНИЕ ЛОГ-ФАЙЛОВ ДЛЯ АНАЛИЗА ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ

Научный руководитель — д.т.н., профессор Ю.А. Гатчин

Создаваемое программное обеспечение (ПО) с каждым годом совершенствуется и становится более сложным, при этом сроки, выделенные на его разработку сокращаются. Все это сказывается на качестве программного кода, требуются новые средства разработки программного обеспечения. Для контроля ошибок системы существуют разные средства прогнозирования и поиска.

Многие разработчики используют метод логгирования (от англ. logging — регистрация, запись). Метод заключается в том, что программа помещает ключевые моменты в файлы записи служебных событий (лог-файлы): информацию о работе программы, в том числе и ошибки. При сбое системы или аварийном завершении программы информация о причинах помещается в лог-файл. Последующее определение причины ошибки происходит на основании данных лог-файла, в частности, способ имеет следующее преимущество: наглядно видна вся последовательность выполнения кода программы. Недостатком способа является избыточное количество информации, содержащейся в лог-файле, что не позволяет быстро найти ошибку. Необходимо в кратчайшие сроки восстановить работоспособность системы и установить причину ошибки. Удаленное расположение лог-файла влияет на оперативность. Доступ к лог-файлу является необходимым, но недостаточным условием нахождения причины ошибки, следует разработать специальную систему, которая автоматизирует ряд функций. Требуется на протяжении всего времени работы ПО отслеживать состояние систем через лог-файлы и создавать уведомления о происходящих ошибках.

Возможна ситуация, при которой появление ошибки не фиксируется в лог-файле, такую ситуацию должен отслеживать элемент искусственного интеллекта (ИИ) системы. Элемент ИИ следит за ходом выполнения программы и сигнализирует о нестандартном поведении программы.

В случае, если система имеет распределенную структуру, возможно размещение каждой ее части физически в разных местах. Все необходимые настройки производятся в конфигурационных файлах. Система содержит сервер, агентов и получателей.

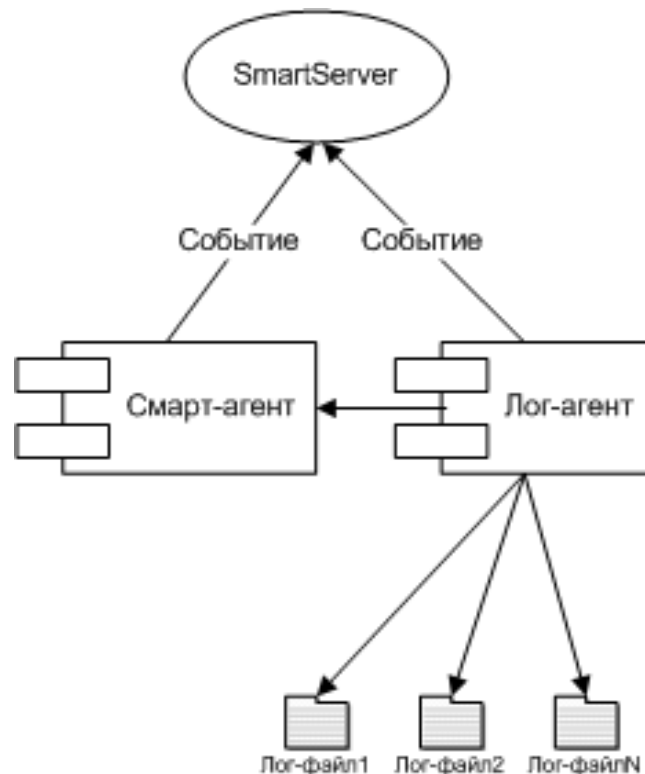
Агенты — небольшие программы, взаимодействующие с сервером. К системе можно подключить одного и более агентов.

SmartServer — главная программная часть — связующее звено между агентами, базой данных (БД) и почтой. Она принимает от агентов сообщения в XML-формате, записывает сообщения в БД, создает отчеты и отправляет уведомления на почту. Отправка уведомлений на почту происходит через SMTP-протокол. Настройка сервера происходит через конфигурационный файл. Отчеты сервер записывает в текстовом виде или xml-формате.

Получатели — база данных, почта и др.

Сервер записывает данные, полученные от агентов, в базу данных через JDBC (Java DataBase Connectivity) и отправляет уведомления по почте через протокол SMTP (Simple Mail Transfer Protocol)

Каждый агент является независимым, исключением является смарт-агент, который зависит от лог-агента, расширяя его функциональность. Взаимодействие между лог-агентом и смарт-агентом представлена на рисунке.



Несколько лог-файлов читаются лог-агентом, который передает обработанную информацию смарт-агенту. Каждый из агентов выполняют свое предназначение: первый осуществляет поиск ошибок в соответствии с шаблонами, второй проводит интеллектуальную обработку.

В работе рассмотрена проблема контроля соответствия программного обеспечения, через лог-файлы. Описан механизм функционирования системы. Тестирование системы продемонстрировало его способность к обнаружению нестандартного поведения программного обеспечения через лог-файлы.

Литература

1. *Осовский С.* Нейронные сети для обработки информации. М.: Финансы и статистика, 2004. 344 с.
2. *Рассел С., Норвинг П.* Искусственный интеллект. Современный подход. 2007. 1408 с.
3. *Джонс М. Т.* Программирование искусственного интеллекта в приложениях. 2006. 312 с.

УДК 004.056.53

А. В. СТЕПАНОВ — кафедра Проектирования компьютерных систем

РАЗРАБОТКА И АНАЛИЗ СИСТЕМЫ БЕЗОПАСНОСТИ ОБЕСПЕЧЕНИЯ ЗАЩИЩЕННОСТИ КЛИЕНТСКИХ ПЛАТЕЖНЫХ ДОКУМЕНТОВ В КОММЕРЧЕСКОМ БАНКЕ

Научный руководитель — д.т.н., профессор С.А. Арустамов

В наши дни многие банки имеют те или иные каналы для удаленного осуществления платежных операций. Отправить «платежку» можно прямо из офиса, воспользовавшись модемным соединением или выделенной линией связи. Стало реальностью выполнение банковских операций через Интернет — для этого достаточно иметь компьютер с доступом в глобальную сеть и ключ электронной цифровой подписи (ЭЦП), которая зарегистрирована в банке [1].

Удаленное обслуживание в банке позволяет повысить эффективность частного бизнеса при минимальных усилиях со стороны его владельцев, при этом обеспечиваются: экономия времени, удобство работы, высокая скорость обработки платежей, мониторинг состояния документа в процессе его обработки [2].

С тех пор как электронный обмен финансовыми активами между клиентом и банком стал реализовываться в удаленном режиме, перехват такого рода переводов является потенциальной целью злоумышленников.

Целью данной работы является создание системы обеспечения защищенности клиентских платежных документов в коммерческом банке при электронном документообороте. Разрабатываемая система предназначена для обеспечения целостности платежа и должна осуществлять контроль и предотвращение несанкционированного доступа к транзакциям между потенциальным клиентом коммерческого банка и самим банком, на всех этапах жизненного цикла.

Безопасность электронных банковских операций между клиентом и банком можно обеспечить современными методами криптографии. В ходе работы были проанализированы различные методы транспортного шифрования и электронно-цифровой подписи. На основе результатов анализа была определена совокупность мер, препятствующих нелегальным пользователям получать конфиденциальную информацию системы на основе анализа данных, передаваемых по открытому каналу связи. Данный аспект системы безопасности существен при передаче финансовой информации по сети Интернет.

Для решения данной проблемы, было предложено использовать протокол SSL (Secure Sockets Layer). Использование данного протокола позволяет решить следующие задачи:

— аутентификация web-сервера. Данная процедура гарантирует, что клиент системы связывается с конкретным сервером системы, имеющим определенный международный сертификат;

— генерация уникального сессионного ключа, наличие которого позволяет обеспечить защиту данных, даже если в одной конкретной сессии (в одном сеансе связи) она была нарушена;

— передачу данных по Интернету в защищенном виде, гарантирующем конфиденциальность и безопасность данных.

Немаловажную роль, при защите транзакций в коммерческом банке играет система набора правил разграничения доступа, так как чаще всего сами сотрудники банка являются потенциальными злоумышленниками. Разработанная система разграничения прав выполняет функции независимо от того, работает пользователь в рамках системы или пытается получить доступ к данным внесистемными средствами. В любом случае пользователь сможет получить доступ только к той информации, правами на которую он обладает. Какие бы средства ни применял пользователь, он не сможет получить доступ к платежному документу, если у него нет на это прав.

На основе собранных сведений был предложен набор мер, препятствующих злоумышленнику перехватить передачу платежного документа с целью хищения его финансовых активов как при передаче по линиям связи, так и при несанкционированном доступе к базам данных платежных документов в коммерческом банке.

Для реализации поставленной задачи было подобрано соответствующее программное обеспечение, а также специализированные программно-аппаратные комплексы, служащие для предотвращения несанкционированного доступа. В итоге разработана система безопасности обеспечения защищенности клиентских платежных документов в коммерческом банке, которая соответствует поставленной цели и выполняет следующие задачи:

- защищенность передачи документов от клиента в банк по системе «банк-клиент»;
- контроль целостности исполнения клиентских платежей;
- конфиденциальность транзакции;
- безопасность передачи данных через Интернет по протоколу SSL;
- информирование клиента об исполнении платежа.

Литература

1. *Садердинов А.А., Трайнёв В.А., Федулов А.А.* Информационная безопасность предприятия. М.: Дашков и К, 2004. 336 с.
2. *Галатенко В.А.* Основы информационной безопасности. М.: Интернет-университет информационных технологий—ИНТУИТ.ру, 2008. 208 с.

О. И. ТИТОМИР — кафедра Проектирования компьютерных систем

**РАЗРАБОТКА КОНСТРУКЦИИ БЛОКА ОБРАБОТКИ ИНФОРМАЦИИ
СИСТЕМЫ ОХРАННОЙ СИГНАЛИЗАЦИИ**

Научный руководитель — к.т.н., доцент И.Б. Бондаренко

Целью работы являлось определение конструкции платы сопряжения с ПК. Устройство предназначено для питания охранных систем измерителей, анализа появления импульсных помех в цепях питания извещателей, формирования сигналов тревоги, управления питанием устройств видеонаблюдения и охранного освещения. Разработка востребована для интегрированных охранных систем, использующихся в качестве автоматизированного рабочего места (АРМ) ПК.

Для разработки устройства контроля и обработки информации (УКОИ) была сконструирована двусторонняя печатная плата с использованием автоматизированной системы P-CAD 2004. Автоматизированное проектирование топологии позволило ускорить процесс создания конструкторской документации и повысить качество разводки печатных проводников.

Следующий этап заключался в проведении инженерных расчетов. Для разрабатываемого блока АРМ были рассчитаны надежность, вибропрочность печатной платы и параметры теплового режима. Все расчеты показали, что конструкция блока удовлетворяет требованиям технического задания.

В экономической части проекта выполнен расчет себестоимости изготовления УКОИ и нормативной цены. Расчет подтвердил конкурентоспособность изделия при производстве в промышленных условиях.

В разделе «Охрана труда» рассмотрено действие опасных и вредных факторов на разработчика устройства и определены меры для уменьшения их влияния.

В целом разработанная конструкция УКОИ удовлетворяет требованиям технического задания и обладает низкой себестоимостью.

А. А. ТИХОМИРОВ — кафедра Проектирования компьютерных систем

**РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА
ДЛЯ ОБЕСПЕЧЕНИЯ АВТОМАТИЗИРОВАННОГО РАСЧЕТА ТЕПЛОВЫХ РЕЖИМОВ
ПРИЕМНО-ИЗМЕРИТЕЛЬНОГО УСТРОЙСТВА СИСТЕМЫ
СПУТНИКОВОЙ НАВИГАЦИИ ГЛОНАСС**

Научный руководитель — ассистент Д.А. Боголюбов

Задача анализа и расчета тепловых режимов является крайне важной для стабильной работы системы навигации ГЛОНАСС. Цель настоящей работы заключалась в разработке программного комплекса для автоматизации процесса расчета тепловых режимов для данной системы. Для достижения поставленной цели были решены следующие основные задачи:

— созданы гранично-элементные модели на основе разработанных ранее чертежей и спецификаций приемно-измерительного устройства системы спутниковой навигации ГЛОНАСС;

— разработан программный комплекс, преобразующий гранично-элементную модель в массив векторов;

— разработан интуитивно понятного интерфейса.

Входными данными являются чертежи либо трехмерные модели устройства и задаваемые пользователем параметры (точность, тип используемой системы координат — евклидова или линейно-дуговая, шаг гранично-элементной сетки). Выходными данными являются массивы векторов, полученные в результате разбиения поверхностей модели на граничные элементы и преобразования полученной модели в массив).

Описываемая разработка позволит автоматизировать процесс расчета тепловых режимов приемно-измерительного устройства системы ГЛОНАСС.

УДК(004.383.4)

И. В. ТРУХАЧЕВ — кафедра Проектирования компьютерных систем

**РАЗРАБОТКА ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА
ДЛЯ ПРОЕКТИРОВАНИЯ ЭЛЕКТРОННЫХ УСТРОЙСТВ
НА БАЗЕ ЦИФРОВОГО СИГНАЛЬНОГО ПРОЦЕССОРА ОМАР-L137**

Научный руководитель — ассистент П.А. Косенков

Digital Signal Processors, цифровой сигнальный процессор (DSP), — это специализированный программируемый микропроцессор, предназначенный для цифровой обработки сигнала — математических манипуляций над оцифрованными сигналами. Эти процессоры широко применяются в беспроводных системах, системах управления при аудио- и видеообработке. Для ускорения проектирования различных электронных устройств, производятся специальные отладочные платы. С их помощью можно проводить испытания различных конфигураций этих систем.

В работе представлена разработка программно-аппаратного комплекса, предназначенного для проектирования электронных устройств на базе DSP-микропроцессора ОМАР-L137.

ОМАР-L137 — процессор приложений с низким энергопотреблением для мультимедиа, обработки графических данных, а также устройств общего назначения. Процессор поддерживает широкий ряд периферийных устройств и работает под управлением ядра операционной системы (ОС) реального времени Linux или DSP/BIOS™, что обеспечивает гибкость на уровне ОС. Энергопотребление составляет от 8 мВт в режиме ожидания; до 400 мВт — в активном режиме.

Комплекс состоит из несущей платы и сменных аппаратных модулей с микропроцессором, а также предусматривает модульную систему питания. Конструкция процессорного модуля обеспечивает возможность быстрой его замены, а также сопряжение с несущей платой и расположенными на ней портами ввода—вывода: сетевым портом совместимым с Ethernet 10BASE-T/10010BASE-TX; портом RS-232; устройствами USB1.1 и 2.0; LCD контроллером.

Объем памяти комплекса — 256 МВ. Загрузка осуществляется с внешнего запоминающего устройства типа NAND Flash. Питание всего комплекса осуществляется с

помощью отдельного сменного модуля на несущей плате. Потребляемая мощность всего комплекса не более 30 Вт.

УДК 004.056

А. С. ФЕДОТОВА — кафедра Проектирования компьютерных систем

**РАЗРАБОТКА КОМПЛЕКСА ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ МЕР
ДЛЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ
НА ПРЕДПРИЯТИИ «АПЛ СНГ»**

Научный руководитель — к.т.н., доцент И.Б. Бондаренко

В условиях формирования общего экономического пространства перед предприятиями остро встает задача сохранения коммерческой тайны. В период становления рынка недобросовестная конкуренция представляет собой серьезную угрозу этому процессу. Стало почти массовым процессом беззастенчивое заимствование интеллектуальной и промышленной собственности (методик, программ, знаний и технологий) самими сотрудниками предприятий, работающих параллельно в кооперативах, малых предприятиях и других коммерческих структурах. К этому следует добавить целенаправленные действия по сманиванию или подкупу рабочих и служащих предприятия-конкурента с целью завладеть секретами их коммерческой и производственной деятельности.

Современный промышленный шпионаж предполагает использование новейших достижений электроники, непосредственное тайное наблюдение, кражи с взломом, подкуп и шантаж. Речь идет о настоящей «тайной войне». С переходом на рыночные отношения и условия самостоятельности предприятий перед ними встали серьезные проблемы по обеспечению сохранности своих коммерческих секретов и в итоге — безопасности предприятия.

Одним из наиболее эффективных способов обеспечения информационной безопасности является использование организационно-технических мер. Что такое организационно-технические меры обеспечения информационной безопасности? Прежде всего, это создание и совершенствование системы обеспечения информационной безопасности, разработка, использование и совершенствование систем защиты информации (СЗИ) и методов контроля их эффективности.

При организации СЗИ следует использовать правовые методы защиты информации, такие как лицензирование деятельности в области защиты информации, сертификация средств защиты и применение уже сертифицированных, а также аттестация объектов информатизации по требованиям безопасности информации.

Организационно-технические методы связаны с экономическими аспектами, включающими в себя разработку программ обеспечения информационной безопасности Российской Федерации, определение порядка их финансирования, совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков. Защита информации всегда является комплексным мероприятием. В совокупности организационные и технические мероприятия позволяют предотвратить утечку информации по техническим каналам, предотвратить несанкционированный доступ к защищаемым ресурсам, что, в свою очередь, обеспечивает целостность и доступность информации при ее обработке, передаче и хранении. С использованием технических мероприятий могут быть выявлены специальные

электронные устройства перехвата информации, установленные в технические средства и защищаемое помещение

Меры по охране конфиденциальности информации, составляющей коммерческую тайну следующие:

— определение перечня информации, составляющей коммерческую тайну;
— ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

— учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

— регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

— нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа «Коммерческая тайна» с указанием обладателя этой информации (для юридических лиц — полное наименование и место нахождения, для индивидуальных предпринимателей — фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Если говорить об экономической стороне защиты информации, всегда важно соблюдать правило — стоимость системы защиты информации не должна превышать стоимость этой информации. Нецелесообразно защищать всю имеющуюся информацию и все каналы информации — необходимо определить объект защиты. Основными объектами защиты являются речевая информация и информация, обрабатываемая техническими средствами. Информация может быть представлена в виде физических полей, информативных электрических сигналов, носителей на бумажной, магнитной, магнито-оптической и др. В связи с этим защите подлежат средства и системы информатизации, участвующие в обработке защищаемой информации, технические средства и системы, не обрабатывающие непосредственно информацию, но размещенные в помещениях, где она обрабатывается и защищаемые помещения.

УДК 004.056(043)

А. А. ШАДРИН — кафедра Проектирования компьютерных систем

РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

Научный руководитель — к.т.н., доцент Н.С. Кармановский

В настоящее время необходимо защищать информационные активы, а также информацию ограниченного пользования от несанкционированного доступа, т.е. доступа, нарушающего правила разграничения с использованием штатных средств (совокупность программного, микропрограммного и технического обеспечения [1, 2]), предоставляемых средствами вычислительной техники или автоматизированными системами. Предотвращение или существенное затруднение доступа к информации на этапе разработки системы защиты конфиденциальной информации — вот основная задача данной работы.

Темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы руководящих документов, действующих на территории России [3]. Поэтому решение вопроса об оценке

уровня защищенности информации связано с проблемой выбора критериев защищенности, а также показателей эффективности применяемой системы защиты информации. При разработке системы защиты информации ограниченного доступа существует необходимость предотвращения таких угроз, как внутренние — от персонала, и внешние — от прочих организаций и отдельных лиц. Спектр средств для предотвращения несанкционированного доступа весьма широк: помимо программно-аппаратных способов защиты от внутренних угроз и несанкционированного доступа извне, а также VPN-технологий, защищающих информацию в процессе передачи по сетям, все средства защиты для аутентификации при доступе к защищенным ресурсам используют ключи — либо физические, такие как eToken, HASP, Hardlock, Smart-Card и DS-таблетки, либо логические — пароли, ключевые слова, блоки информации (PGP) [3, 4]. Использование логических ключей наименее безопасно, так как из-за отсутствия аппаратной составляющей они являются более уязвимыми для перехвата, дублирования и фальсифицирования. Помимо того, эффективность защиты напрямую зависит от используемых пользователями паролей. Использование аутентификации с помощью физических ключей решает проблему подбора и перехвата паролей, особенно при удаленной работе в сети.

Современные методики управления рисками, методики разработки и проектирования систем защиты информации ограниченного доступа должны позволять решить ряд задач для перспективного стратегического развития компании. К таким задачам относится количественная оценка текущего уровня информационной безопасности компании, что потребует выявления рисков на правовом, организационно-управленческом, технологическом, техническом уровнях обеспечения защиты информации, а также создание с последующей реализацией комплексного плана совершенствования корпоративной системы защиты информации для достижения приемлемого уровня защищенности информационных активов. Это подразумевает ряд следующих действий:

- расчет и обоснование финансовых вложений в обеспечение информационной безопасности на основе технологий анализа рисков, а также анализ расходов на обеспечение безопасности в сравнении с потенциальным ущербом или вероятностью его возникновения;

- выявление и анализ наиболее уязвимых ресурсов;

- установление имеющихся функциональных отношений и зон ответственности при взаимодействии подразделений и лиц, обеспечивающих контроль информационной безопасности, создание необходимого пакета организационно-распорядительной документации;

- разработка и согласование со службами организации, надзорными органами проекта внедрения необходимых комплексов защиты информации ограниченного пользования, учитывающего современный уровень и тенденции развития информационных технологий;

- обеспечение контроля и сервиса внедренного комплекса защиты в соответствии с изменениями условий работы организации.

Решение вышеприведенных задач существенно увеличит спектр возможностей при работе с конфиденциальной информацией. Лицам, занимающим руководящие должности, это поможет объективно оценивать текущий уровень информационной безопасности и контролировать доступ к данным ограниченного пользования, рассчитывать затраты на обеспечение защиты компании и на основе полученной оценки выработать и обосновать организаторские меры (состав и структуру службы информационной безопасности, положение о коммерческой тайне, пакет должностных инструкций и инструкции действия в нестандартных ситуациях).

Литература

1. *Ярочкин В.И.* Информационная безопасность. М.: Академический проект, 2008. 544 с.
2. Защита от несанкционированного доступа к информации. Термины и определения. [Электронный ресурс]: <www.hr-portal.ru>.
3. Информационный ресурс, представляющий и раскрывающий проблематику защиты конфиденциальной информации [Электронный ресурс]: <www.dehack.ru>.
4. Информзащита — Защита информации ограниченного доступа [Электронный ресурс]: <www.zki.infosec.ru>.

РАБОТЫ СТУДЕНТОВ ПЯТОГО КУРСА

УДК 004.891.2

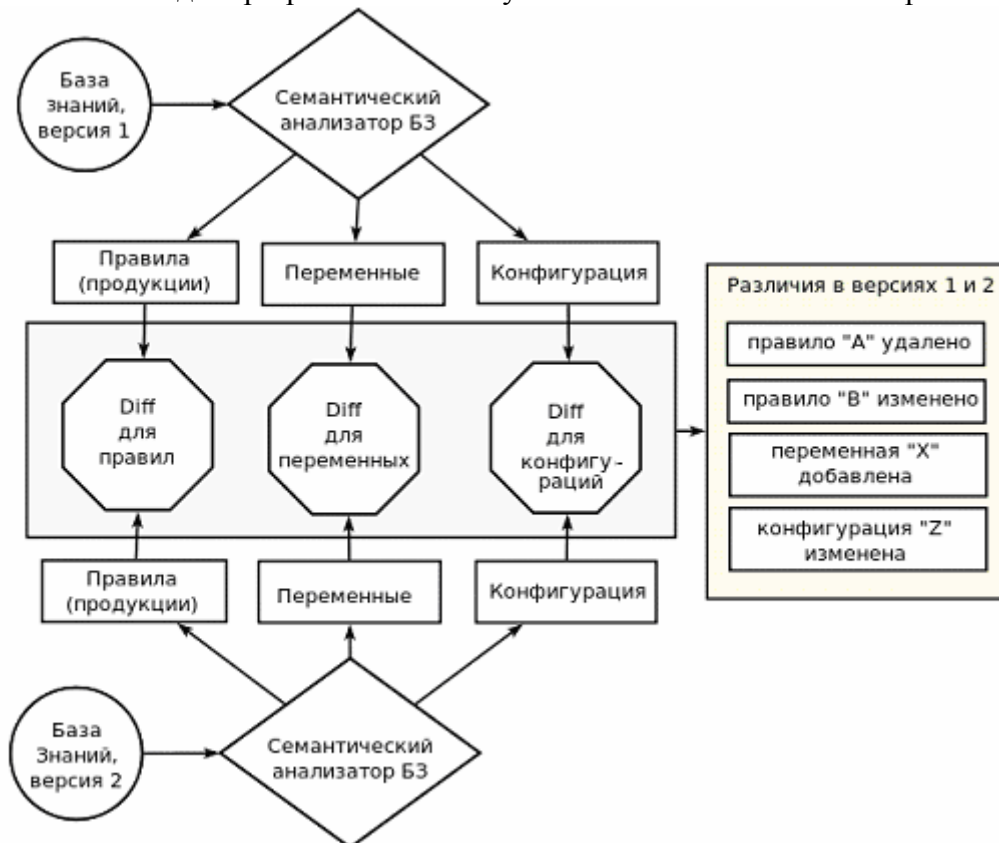
М. С. ВОРОНКОВ — кафедра Проектирования компьютерных систем

УПРАВЛЕНИЕ ЖИЗНЕННЫМ ЦИКЛОМ ИНФОРМАЦИИ В СИСТЕМЕ ХРАНЕНИЯ ДАННЫХ

Научный руководитель — к.т.н., доцент Д.И. Муромцев

Целью работы является создание программной web-оболочки для безопасной коллективной разработки и эксплуатации экспертных систем (ЭС) производственного типа. В существующих аналогах отсутствует интегрированный контроль версий баз знаний (БЗ), а также детальное разграничение полномочий разработчиков. Перечисленные недостатки частично устранимы с помощью дополнительного программного обеспечения и обучения инженеров баз знаний, что в свою очередь приводит к удорожанию разработки ЭС. Предлагаемая оболочка является интегрированным средством разработки: устраняя указанные недостатки, она облегчает работу инженеров БЗ, уменьшает время создания ЭС.

Разрабатываемая оболочка содержит модуль сравнения версий БЗ, основанный на алгоритмических принципах утилиты Diff [1], как и в других системах управления версиями (СУВ) [2]. Отличие состоит в том, что поиск изменений в версиях ЭС происходит с учетом синтаксиса команд описания, т.е. с учетом семантики БЗ (см. рисунок), что освобождает разработчика от изучения синтаксического аппарата БЗ.



Обновление БЗ до последней версии происходит в полуавтоматическом режиме: в случае обнаружения конфликтов между изменениями разработчиков предоставляется возможность их разрешения выбором из предложенных системой вариантов решения, по каждому из структурных составляющих ЭС отдельно.

Для разграничения прав разработчиков и пользователей на работу с ЭС используется принцип дискреционного управления доступом, при котором в системе безопасности для каждой пары субъект—объект задаются допустимые типы доступа [2]. В дополнение к стандартным типам доступа к ЭС, определяемым на уровне операционной системы (ОС), в разрабатываемой оболочке предусмотрены дополнительные типы доступа к различным составляющим БЗ: продукциям и переменным, конфигурациям, параметрам интерфейса. Такой подход позволяет более детально разграничивать полномочия различных специалистов по сравнению с использованием аналогичных механизмов, встроенных в ОС или системы управления версиями [3].

Разрабатываемая оболочка позволит осуществлять быструю и, что немаловажно, безопасную разработку и эксплуатацию продукционных экспертных систем за счет одновременного привлечения к разработке нескольких специалистов, инженеров БЗ, экспертов в предметной области, дизайнеров интерфейсов.

Литература

1. Free Software Foundation Documentation [Electronic resource]: <http://www.gnu.org/software/diffutils/manual/>.
2. Гостехкомиссия России. Руководящий документ: Защита от несанкционированного доступа к информации. Термины и определения. М.: ГТК, 1992.
3. Ресурсы IBM для разработчиков и IT-специалистов в России [Электронный ресурс]: http://www.ibm.com/developerworks/ru/library/1-vercon/index.html?S_TACT=105AGX99&S_CMP=GR01.

УДК 681.2-5

Е. В. ДОЛГИЙ — кафедра Проектирования компьютерных систем

ПРОЕКТИРОВАНИЕ ЭЛЕКТРОННЫХ КОМПОНЕНТОВ СИСТЕМЫ ОСВЕЩЕНИЯ

Научный руководитель — ассистент П.А. Косенков

Электроника представляет собой быстро развивающуюся отрасль науки и техники. В современном мире она заняла прочное место во всех сферах жизнедеятельности человека: научные приборы, станки с ЧПУ, бытовая техника, везде применяется электроника [1]. Такому внедрению поспособствовало появление большого разнообразия электронных компонентов, микропроцессоров; и их миниатюризация; появление новых методов проектирования, систем автоматизированного проектирования (САПР).

Была поставлена задача — применить на практике САПР и проанализировать полученный результат. В качестве объекта разработки был выбран сенсорный регулятор освещения с дистанционным управлением, предназначенный для повышения удобства управления освещением, увеличения срока службы ламп накаливания и экономии электроэнергии. Регулятор должен отвечать следующим: плавная регулировка накала

ламп; управление с помощью пульта дистанционного управления (ДУ); легкое введение в эксплуатацию; минимальные габариты и минимальная стоимость.

Выбор элементной базы осуществляется с точки зрения возможности элементов обеспечить заданные характеристики конструируемого прибора при предусмотренных условиях эксплуатации [2]. В качестве управляющего элемента используется микроконтроллер (был выбран микроконтроллер с минимально необходимым набором функций). Для возможности управления регулятором с помощью ДУ пульта применяется фотоприемник со встроенным дешифратором сигналов стандарта RC-5 Яркость ламп регулируется при помощи твердотельного реле — симистора.

Для проектирования использовалась САПР P-CAD, предназначенная для сквозного проектирования печатных плат (ПП). Она позволяет формировать принципиальные электрические схемы и топологию ПП, также имеется возможность оформления конструкторской документации [3].

Было разработано устройство, отвечающее всем требованиям. Благодаря небольшим размерам устройство может быть встроено в схему питания прибора освещения, что позволяет заменить стандартный выключатель света регулятором освещения. Миниатюризация устройства достигнута за счет применения современной элементной базы, уже готовых решений, плотной компоновки компонентов. Использование САПР P-CAD и современной элементной базы позволило за короткий срок получить устройство с минимальной стоимостью, обладающее всеми необходимыми функциями и подготовить конструкторскую документацию.

Литература

1. *Преснухин Л.Н., Шахнов В.А.* Конструирование электронных вычислительных машин и систем. М.: Высш. школа, 1986.
2. *Пирогова Е.В.* Проектирование и технология печатных плат. М.: ФОРУМ: ИНФРА-М, 2005. 76 с.
3. *Иванова Н.Ю., Петров А.С., Поляков В.И., Романова Е.Б.* Технология проектирования печатных плат в САПР P-CAD-2006. СПб: СПбГУ ИТМО, 2009. 8 с.

УДК 621.314.6

А. Н. ИВАНОВ — кафедра Проектирования компьютерных систем

РАСЧЕТ И МОДЕЛИРОВАНИЕ ИСТОЧНИКА БЕСПЕРЕБОЙНОГО ПИТАНИЯ

Научный руководитель — к.т.н., доцент И.Б. Бондаренко

Электропитание, не удовлетворяющее стандартам по частоте, амплитуде напряжения, фазе отрицательно воздействует на технику: сильные всплески напряжения способны вывести из строя блоки питания и микросхемы, что может привести к непоправимым потерям, вызванным повреждением оборудования, а систематические проблемы с электроэнергией вызывают преждевременное старение аппаратуры. Избежать таких неприятностей поможет источник бесперебойного питания (ИБП).

Перепады напряжения для сложных цифровых устройств могут быть критичными: медицинские системы жизнеобеспечения нуждаются в постоянной работе комплекса устройств, и требования к их питанию очень строги; то же относится к системам

банковской защиты и охраняемым системам; системам экстренной связи и передачи информации. Первоочередной задачей считается обеспечение нормального, корректного завершения работы или поддержания непрерывного питания в случае неожиданного отключения электроэнергии.

Источник бесперебойного питания — автоматическое устройство, которое обеспечивает питание нагрузки при полном исчезновении напряжения во внешней электросети, например, в результате аварии или вследствие недопустимо высокого отклонения параметров напряжения сети от номинальных значений. При этом ИБП использует для аварийного питания нагрузки энергию аккумуляторных батарей.

В соответствии с принципом построения можно выделить следующие ИБП:

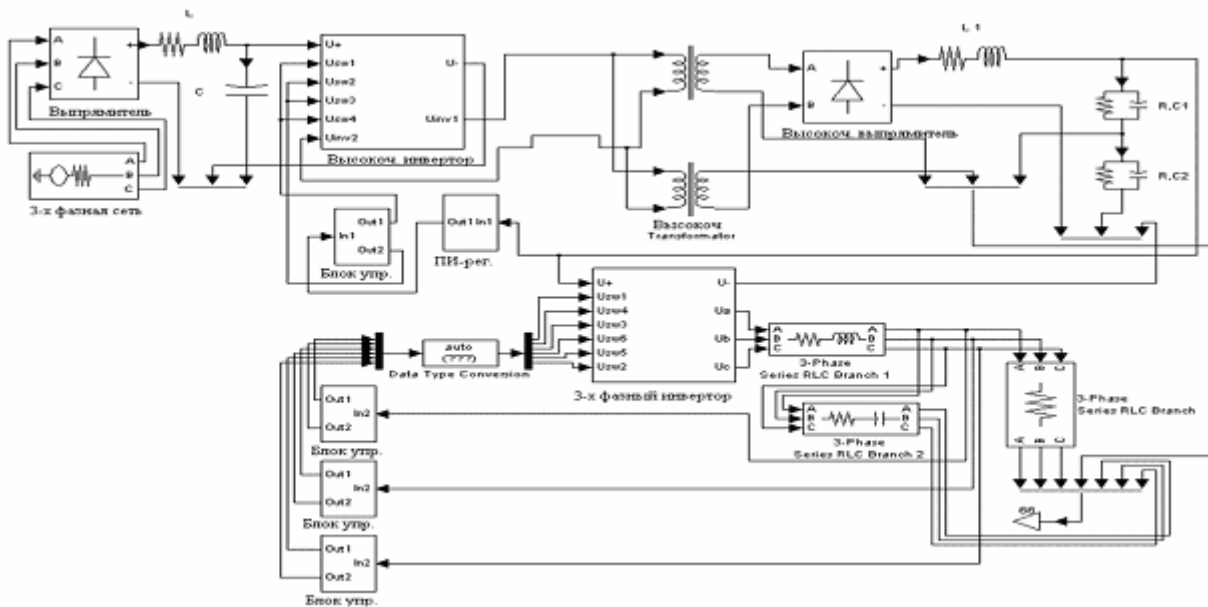
- с режимом работы «вне линии». Преимуществом ИБП такого типа является его простота и невысокая стоимость, а недостатком — ненулевое время переключения (~4—12 мс) на питание от аккумуляторов и более интенсивная их эксплуатация, потому что ИБП переводится в аварийный режим при любых неисправностях в электросети.

- ИБП с режимом «на линии». Эти устройства работают постоянно на нагрузку;

- с динамичным режимом работы. Принцип их работы в значительной степени схож с принципом работы «вне линии», за исключением наличия так называемого «бустера» — устройства ступенчатой стабилизации напряжения и использования основной схемы для заряда и подзаряда батарей.

В настоящее время для повышения эффективности ИБП применяется комбинированная схема, в частности, трехфазного ИБП с двойным преобразованием энергии.

Создание верифицированной математической модели ИБП позволяет совершенствовать его алгоритмы управления и структуру энергетической подсистемы, оптимально выбирать параметры элементов энергетической подсистемы. На рисунке приведена модель основного канала ИБП, разработанная в пакете MatLab.



Разработанная модель ИБП адекватно отражает процессы в реальном ИБП и хорошо учитывает специфику цифровой системы управления.

Благодаря математическому моделированию верифицированной математической модели ИБП возможно добиться повышения уровня КПД путем оптимальной настройки регуляторов.

Литература

3. Лопухин А.А. ИБП без секретов. М.: Высш. школа, 2004. С. 95—105.

4. *Герман-Галкин С.Г.* Силовая электроника: лабораторные работы на ПК. СПб: КОРОНА принт, 2002. 304 с.
5. Источники электропитания радиоэлектронной аппаратуры / *Г.С. Найвельт, К.Б. Мазель, Ч.И. Хусаинов* и др. М.: Радио и связь, 1985. 576 с.
6. *Борисов П.А.* Несимметричные режимы работы полупроводниковых преобразователей // Тр. Междунар. науч.-практич. конф. «Электронные средства и системы управления». Томск. 2004. С. 132—134.

УДК 004.924

А. Б. ЛИСАЧКИНА — кафедра Проектирования компьютерных систем

ПРОГРАММНЫЙ МОДУЛЬ ДЛЯ СОХРАНЕНИЯ ИЗОБРАЖЕНИЙ, ПОЛУЧЕННЫХ ПРИ ПОМОЩИ ЯДЕРНОГО МАГНИТНО-РЕЗОНАНСНОГО ТОМОГРАФА В МЕДИЦИНСКОМ ФОРМАТЕ DICOM

Научный руководитель — д.т.н., профессор Ю.А. Гатчин

В связи с производством различных диагностических центров, использующих цифровую аппаратуру крупнейшими производителями радиологического оборудования (PICKER, GE, Siemens, HP, Philips) необходима оперативная передача полученных в ходе медицинских исследований данных между этими центрами.

В связи с использованием компьютерных технологий в медицине, возникла потребность в коммуникационных возможностях, которые позволяли бы:

- объединять в сеть существующее цифровое оборудование для повышения эффективности работы и снижения затрат ручного труда;
- обеспечивать расширяемость существующей сети путем подключения к ней нового оборудования;
- интегрировать различные данные для повышения качества диагностики.

Универсальные компьютерные сетевые технологии не позволяют объединять различные виды медицинского оборудования. Поэтому его производители были вынуждены разрабатывать собственные коммуникационные интерфейсы. Однако в связи с широтой спектра используемого медицинского оборудования производства различных компаний, возникла необходимость в разработке коммуникационных стандартов.

Известно, что формат DICOM (Digital Imaging and Communications in Medicine. т.е. цифровые снимки и средства связи в медицине) является всемирным стандартом обмена данных в медицинских информационных системах. С его помощью осуществляется обмен снимками и данными, создаваемыми различными медицинскими приборами, генерирующими и обрабатывающими изображения и информацию.

Целью настоящей работы является расширение функциональности программного обеспечения кафедральной научно-исследовательской установки мини-ЯМР томографа, в результате разработки программного модуля, отвечающего за сохранения полученного изображения и данных в международном медицинском формате DICOM.

На сегодняшний день DICOM, по мнению автора, является хорошо проработанным стандартом, на который имеет смысл ориентироваться российским разработчикам.

Была исследована структура формата DICOM; изучен алгоритм для преобразования данных в формате DICOM; изучены основы визуального программирования с применением программного пакета C++ Builder. Разработан программный модуль для

сохранения изображений, полученных при помощи лабораторного ядерного магнитно-резонансного томографа в медицинском формате DICOM.

УДК 004.046

С. А. МОСЕЙЧУК — кафедра Проектирования компьютерных систем

ОСОБЕННОСТИ РЕШЕНИЯ ЗАДАЧИ НАВИГАЦИИ ПО ТОЧЕЧНЫМ ОРИЕНТИРАМ ДЛЯ НАЗЕМНЫХ ОБЪЕКТОВ

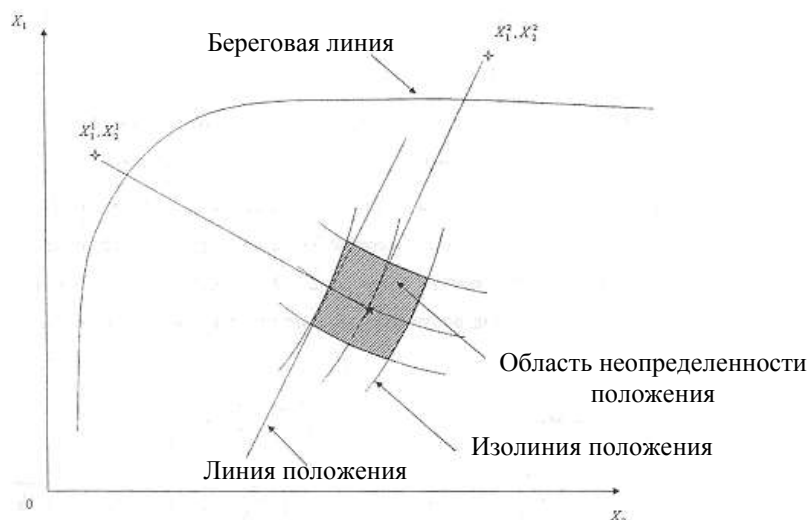
Научный руководитель — Д.Н. Кокшаров

В современном мире навигация используется в различных сферах деятельности человека — в системах позиционирования при езде на автомобиле, полете на воздушном судне, в мореплавании. При решении таких задач используются точные спутниковые навигационные системы. Здесь в качестве точечных ориентиров используются спутники. С появлением мобильных телефонов стало возможным определение координат абонента по системам GSM-позиционирования. В отличие от традиционных систем (таких, например, как GPS), системы навигации по точечным ориентирам для наземных объектов обладают более низкой точностью определения координат объекта и функционируют только в зоне покрытия сети соответствующего оператора, однако при этом они обладают рядом уникальных особенностей:

- позволяют определять положение абонента в плотной городской застройке, внутри зданий, на станциях метрополитена — везде, где работает сотовый телефон;
- позволяют определять не только собственное местоположение, но и местоположение любого абонента в сети.

В работе в качестве точечных ориентиров используются базовые станции сети. Эти особенности позволяют использовать системы GSM-позиционирования в задачах обеспечения безопасности, поиска и спасения, слежения, диспетчерского управления и т.п. Также системы навигации используются при самостоятельном передвижении мобильных роботов. Позиционирование роботов происходит как за счет использования одометрических сенсоров, оптических кодеров, так и активных маяков, которые являются точечными ориентирами.

В случае наличия безошибочного измерения дальности до одного точечного ориентира координаты объекта становятся известными с точностью до его расположения на окружности, радиус которой совпадет с измеренным значением дальности. Располагая двумя измеренными практически без ошибок значениями дальности, координаты объекта можно получить как одну из двух возможных точек позиционирования. Поскольку измерения содержат ошибки, то вместо линий будут формироваться полосы, заключенные между окружностями, равными максимально и минимально возможным значениям дальности при заданном уровне ошибок измерения. При наличии двух измерений возможные координаты объекта будут с высокой степенью вероятности располагаться внутри фигуры, формируемой в результате пересечения двух полос. При наличии большего количества измерений возникает проблема определения координат с максимальной точностью.



На рисунке приведен пример определения координат объекта на плоскости с использованием измерений дальности до двух ориентиров с известными координатами.

Задача решается методом наименьших квадратов и его модификациями (обобщенный и модифицированный МНК).

Литература

1. Степанов О.А. Основы теории оценивания с приложениями к задачам обработки навигационной информации. СПб: ГНЦ РФ ЦНИИ «Электроприбор», 2009. 496 с.
2. Степанов О.А. Применение теории нелинейной фильтрации в задачах обработки навигационной информации. СПб: ГНЦ РФ ЦНИИ «Электроприбор», 2003, 369 с.
3. Торопов А.Б., Королева Ю.В., Васильев В.В. Оптимальные и субоптимальные линейные алгоритмы для решения нелинейных навигационных задач. СПб: ГНЦ РФ ЦНИИ «Электроприбор»,
4. Смоленцев С.В. Определение координат мобильных абонентов в сетях сотовой связи стандарта GSM // Гироскопия и навигация. 2006. №4(55).

УДК 004.7

И. С. ПАНОВ — кафедра Проектирования компьютерных систем

МАСКИРОВКА БЕСПРОВОДНЫХ СЕТЕЙ WI-FI

Научный руководитель — старший преподаватель К.О. Ткачев

Для защиты Wi-Fi-сетей применяются сложные алгоритмические математические модели аутентификации, шифрования данных и другие средства обеспечения безопасности. Однако самый популярный стандарт шифрования WEP может быть относительно легко «взломан» даже при правильной конфигурации (из-за слабой стойкости алгоритма). Несмотря на то что Wi-Fi-сети, реализованные на современных компонентах, поддерживают более совершенный протокол шифрования данных WPA, сети, основанные на устаревших компонентах, не поддерживают его. Принятие стандарта

IEEE 802.11i (WPA2) в июне 2004 г. сделало более безопасной схему, которая может быть использована в новом оборудовании. В сетях требуется использовать более стойкий пароль.

Рассмотрим методику защиты беспроводных сетей, основанную на противодействии наиболее распространенным методам взлома. В настоящей работе, рассматривается стандарт шифрования WEP как более наглядный вследствие своей простоты.

Как указано в спецификации, WEP использует алгоритм шифрования RC4 с 40-битным или 104-битным ключом. При включении WEP все станции (как клиентские, так и точки доступа) получают свой ключ, который применяется для шифрования данных, прежде чем последние будут переданы на передатчик. Если станция получает пакет, не зашифрованный с помощью соответствующего ключа, он исключается из трафика. Этот метод служит для защиты от несанкционированного доступа и перехвата данных.

При использовании статистических методов вероятность угадывания определенного байта в ключе доходит до 15 %, если определен правильный вектор инициализации. По существу некоторые инициализирующие векторы «пропускают» секретный WEP-ключ для специфических ключевых байтов.

Основная задача злоумышленника — «захватить» как можно больше данных. Это может оказаться довольно не тривиальной задачей. Число векторов инициализации (четыре) меняется динамично в зависимости от длины подбираемого ключа. Обычно нужно порядка 250 000 или более уникальных векторов для взлома 64-битного ключа и около 1500 000 — для взлома 128-битного. Чем векторов инициализации больше, тем выше вероятность успешного подбора. Возможны случаи, когда и 50 000 векторов хватает для взлома ключа, но это большая редкость.

На основе вышеизложенного материала можно сделать вывод, что получить доступ к беспроводной сети защищенной только определенным стандартом шифрования, не составляет труда. Злоумышленнику необходимо всего лишь записать данные, передаваемые пользователями Wi-Fi-сети, затем произвести автоматизированный анализ полученных данных применительно к конкретной точке доступа.

Концепция данной работы заключается в том, чтобы в режиме нормальной работы точки доступа Wi-Fi с некоторой периодичностью генерировать последовательности пакетов, зашифрованных ключом шифрования, отличным от ключа, принятого пользователем, от имени (SSID) защищаемой точки доступа. Содержимое этих пакетов принципиального значения не имеет.

В процессе изучения доступных средств автоматизированного анализа было выявлено, что для успешного «взлома» записанной информации необходимо присутствие определенного количества пакетов, которые практически во всех случаях должны следовать поочередно друг за другом. В случае если цепь прерывается, автоматизированные средства анализа перестают корректно воспринимать входные данные и взлом становится невозможным.

Литература

Рошан П., Лиэри Д. Основы построения беспроводных локальных сетей стандарта 802.11. Руководство Cisco = 802.11 Wireless Local-Area Network Fundamentals. М.: Вильямс, 2004.

П. В. РОМБАЧЕВ — кафедра Проектирования компьютерных систем

**РАЗРАБОТКА АВТОМАТИЧЕСКОГО КОНТРОЛЛЕРА
СКОРОСТИ ВРАЩЕНИЯ ВЕНТИЛЯТОРОВ
СИСТЕМЫ ОХЛАЖДЕНИЯ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА**

Научный руководитель — ассистент П.А. Косенков

Работа настольного персонального компьютера сопровождается выделением тепла, что обуславливает необходимость его охлаждения. Для охлаждения компьютера используются радиаторы, активные теплоотводы (радиаторы с установленными на них вентиляторами), с жидкостным охлаждением, полупроводниковые элементы, использующие эффект Пельтье [1].

Наиболее распространенный способ охлаждения — применение активных теплоотводов. Контроль теплового режима необходимо осуществлять в трех-четырёх областях системного блока компьютера, что требует наличия трех-четырёх вентиляторов. Вентиляторы, работающие с максимальным числом оборотов, создают высокий уровень шума. При разработке технологических процессов, проектировании, изготовлении и эксплуатации машин, производственных зданий и сооружений, а также при организации рабочего места следует принимать все необходимые меры по снижению шума, воздействующего на человека на рабочем месте, до приемлемых значений [2]. Чтобы снизить уровень шума работающего компьютера, необходимо регулировать скорость вращения вентиляторов.

Управляющий элемент контроллера — микроконтроллер Attiny2313, на входы которого подается информация от однопроводных цифровых термометров DS1820, помещенных в контролируемую область. Управление скоростью вращения осуществляется с помощью сигнала, поступающего с широтно-импульсной модуляцией (ШИМ), подаваемой на управляющий чип вентилятора. ШИМ-импульс рассчитывается в микроконтроллере исходя из полученных данных о температуре в текущей контролируемой области. Так как напряжение выходного сигнала микроконтроллера не более 5 В, а управляющее напряжение вентилятора — до 12 В, сигнал, формируемый на выходе микроконтроллера, преобразуется в управляющий сигнал, передаваемый к вентилятору, посредством МОП-транзистора на затвор которого подается выходной сигнал микросхемы, на сток — напряжение 12 В. Информация о состоянии контролируемых областей выводится на двустрочный монохромный знаковосинтезирующий жидкокристаллический дисплей в формате: «№ области. температура (°C)/ частота вращения (RPM)». В первой строке дисплея постоянно отображаются сведения о состоянии первой области (обычно — область центрального процессора), во второй строке поочередно с интервалом в десять секунд — состояние остальных контролируемых областей. Коммутация контроллера с термометрами и вентиляторами осуществляется посредством разъемов WF-3, расположенных на плате, с ЖК-дисплеем с помощью разъема PLD2-10. Электропитание контроллера — от сети блока питания компьютера. Габаритные размеры контроллера позволяют поместить его в пятидюймовый отсек корпуса компьютера.

Контроллер имеет достаточно высокую конкурентоспособность, так как стоимость представленной системы охлаждения ниже стоимости систем водяного охлаждения.

Литература

1. Гук М.Ю. Аппаратные средства IBM PC: Энциклопедия. СПб: Питер, 2006. 1072 с.

УДК 004.02

В. С. СОЛОВЬЕВ — кафедра Проектирования компьютерных систем

УПРАВЛЕНИЕ ЖИЗНЕННЫМ ЦИКЛОМ ИНФОРМАЦИИ В СИСТЕМЕ ХРАНЕНИЯ ДАННЫХ

Научный руководитель — к.т.н., доцент Н. С. Кармановский

Среди всей совокупности мер обеспечения защиты информации организационно-технические стоят на особом месте, так как играют одну из наиболее важных ролей в создании и функционировании надежной системы защиты. Для обеспечения безопасности необходима регламентация деятельности по обработке и защите конфиденциальной информации и взаимоотношений обслуживающего персонала на нормативно-правовой основе таким образом, чтобы разглашение, утечка и несанкционированный доступ к информации становились невозможными за счет проведения организационных мероприятий. Мероприятия по защите конфиденциальной информации должны проводиться на всех этапах жизненного цикла объекта: проектирование и строительство здания, планировка и размещение функциональных помещений, проектирование системы, монтаж и наладка оборудования, испытания и проверка в эксплуатации оборудования, средств обработки и передачи данных.

Для выполнения решаемой задачи в необходимо:

- проанализировать деятельность и структуру типовой районной налоговой инспекции;
- провести анализ защищаемой информации;
- выявить открытые и закрытые информационные потоки;
- исследовать возможные пути утечки информации;
- регламентировать работу с конфиденциальной информацией;
- проанализировать план территории и поэтажные планы здания, выделить зоны безопасности;
- разработать структуру службы безопасности и защиты информации;
- произвести выбор и разработать схемы расположения технических средств наблюдения, контроля и управления доступом, охранно-пожарной сигнализации;
- разработать функциональную схему интегрированной системы охраны объекта — районной налоговой инспекции;
- разработать меры защиты информации в локальной вычислительной сети районной налоговой инспекции.

В проекте для здания инспекции автором реализован многорубежный принцип защиты путем оборудования помещений объекта техническими средствами охранно-пожарной сигнализации и системы контроля доступа. Для обеспечения круглосуточного визуального контроля за периметром здания инспекции, обстановкой в зонах свободного посещения и путями прохода к зонам ограниченного доступа была разработана система видеонаблюдения.

Подсистемы охранно-пожарной сигнализации, контроля и управления доступом и видеонаблюдения объединены в интегрированную систему охраны (ИСО) «Орион»,

производства компании «Болид». На центральном сервере системы установлена программная составляющая аппаратно-программного комплекса ИСО «Орион», реализующая возможность централизованного наблюдения и управления подсистемами — АРМ «Орион Про» и организовано четыре удаленных рабочих места для сотрудников отдела охраны службы безопасности и защиты информации.

Также с помощью комплекса Secret Net NT были разработаны меры по защите информации в локальной вычислительной сети инспекции.

В результате создан комплекс организационно-технических мер по обеспечению защиты конфиденциальной информации, который может применяться в качестве типового решения для любой инспекции ФНС России.

Литература

1. Постановление Правительства Российской Федерации «Об утверждении Положения о Федеральной налоговой службе» от 30 сентября 2004 г. № 506.
2. Приказ МНС РФ «О типовом положении об инспекции МНС России с предельной численностью свыше 100 единиц и типовых положениях об отделах» от 11.03.2003. № БГ-3-25/113.
3. Федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ.
4. Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера» от 06.03.1997. № 188.

УДК 004.4

Д. А. ТИМИН — кафедра Проектирования компьютерных систем

РАЗРАБОТКА АКТИВНЫХ СРЕДСТВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДЛЯ СИСТЕМЫ УПРАВЛЕНИЯ ЭЛЕКТРОННЫМ ПОРТФОЛИО

Научный руководитель — к.т.н., доцент Д.И. Муромцев

Под термином «портфолио» понимается способ фиксирования, накопления и оценки индивидуальных достижений человека. Электронное портфолио может представлять собой коллекцию работ, результатов тестирований, свидетельств об окончании курсов, сертификатов о полученных навыках и сведений о предпочитаемых областях работы. Целью создания электронного портфолио может являться демонстрация как образовательных достижений учащегося, так и направлений исследований преподавателя [1].

Электронное портфолио позволяет решить ряд задач:

- отслеживание индивидуального прогресса учащегося, достигнутого им в процессе получения образования;
- оценка образовательных достижений студента;
- публикация материалов различного формата;
- поиск научного руководителя, преподавателя;
- создание некоторого научного сообщества, на основе общих научных интересов.

Итоговый документ портфолио может рассматриваться как аналог аттестата, свидетельства о результатах тестирования (или выступать наряду с ними).

На сегодняшний день существует множество способов реализации системы управления электронным портфолио.

Альтернативой коммерческим решениям являются многочисленные системы управления контентом (CMS) которые в основном выпускаются под открытым лицензионным соглашением GNU, а следовательно, легко могут быть изменены и дополнены в соответствии с спецификой задания. Также их достоинство состоит в большом количестве свободно распространяемых расширений, увеличивающих встроенный функционал практически до бесконечности.

Очень важным аспектом в разработке систем управления электронным портфолио является защита всей критичной информации от копирования, удаления и изменения, частично такие функции предоставлены перечисленными решениями. Однако для полноценно защищенной работы системы было решено поставить задачу разработки активных средств обеспечения безопасности, которая должна решать следующие проблемы:

- защита от несанкционированной рассылки (спама);
- защита от модификации, удаления и просмотра критичных данных;
- защита от несанкционированной подмены запросов к БД (sql-внедрения);
- защита от перегрузки сервера, большим количеством запросов (DoS-так);
- выявление лиц, предпринимающих попытки взлома или подбора ключей аутентификации;
- защита от выполнения пользовательского кода;
- проверка загружаемых пользователями данных на сервер.

УДК 004.6

А. В. ФИЛАТОВ — кафедра Проектирования компьютерных систем

ЗАЩИТА ДАННЫХ, ПЕРЕДАВАЕМЫХ ПОСРЕДСТВОМ ТЕХНОЛОГИИ REST

Научный руководитель — ассистент В.В. Власов

REST (от англ. *Representational State Transfer* — передача состояния представления) — подход к архитектуре сетевых протоколов, обеспечивающих доступ к информационным ресурсам, он был описан в 2000 г. Ройем Филдингом, одним из создателей протокола HTTP. Самой известной системой, построенной в значительной степени по архитектуре REST, является современная «Всемирная паутина».

Согласно REST, сетевой ресурс должен поддерживать всего четыре операции: GET, PUT, POST и DELETE (с теми же значениями, как в протоколе HTTP). Данные должны передаваться в виде небольшого количества стандартных форматов (например, HTML, XML, JSON). Сетевой протокол (как и HTTP) должен поддерживать кэширование, не должен зависеть от сетевого слоя, не должен сохранять информацию о состоянии между парами

«запрос—ответ». Такой подход обеспечивает масштабируемость системы и позволяет ей эволюционировать с появлением новых требований.

Антиподом REST является подход, основанный на вызове удаленных процедур (Remote Procedure Call — RPC). Подход RPC позволяет использовать небольшое количество сетевых ресурсов с большим количеством методов и сложным протоколом. При подходе REST количество методов и сложность протокола строго ограничены, из-за чего количество отдельных ресурсов должно быть большим.

Основной аргумент в пользу использования технологии REST вместо RPC — это ее простота, к тому же большая часть пользователей REST остается верной протоколу SSL. Поскольку REST требует использования протокола HTTP и обычно применяется для соединений типа «точка–точка», то очень часто наличия SSL-туннеля вполне достаточно для передачи зашифрованных данных. Предприятия, желающие реализовать в REST средства безопасности уровня сообщений могут создавать свои собственные протоколы и форматы данных [1].

Также большой интерес представляет стандарт SAML. Он не зависит от платформы и состоит из утверждений, протоколов, привязок и профилей. Утверждения — это высказывания службы идентификации (identity authority) о конечном пользователе — человеке или компьютере. Утверждение — это ответ на запрос типа «Может ли Джон Смит получить доступ к серверу отдела кадров?»

В каждом утверждении содержится информация о типе сделанного запроса. Например, если запрашивается авторизация доступа к приложению отдела кадров, то утверждение SAML сообщает, разрешен или нет пользователю вход в систему, и показывает набор его прав доступа. Если запрашивается аутентификация для сетевого ресурса или приложения, утверждение SAML указывает метод аутентификации, а также ее дату и время. Таким образом, приложение может определить, приемлем ли метод аутентификации, пройденный пользователем [2].

При построении любой системы защиты информации необходимо оценить стоимость информации и только после этого применять соответствующий подход.

В целом можно утверждать, что стандарт SAML может быть успешно использован в REST архитектуре для защиты данных.

Литература

1. Дорнан Э. Рискованное дело // Сети и системы связи. 2008. № 2. С. 14—19.
2. Маквитти Л. Говоря на языке SAML // Сети и системы связи. 2004. № 4. С. 43—48.

РАБОТЫ СТУДЕНТОВ ЧЕТВЕРТОГО И ТРЕТЬЕГО КУРСОВ

УДК 004.922

*Е. В. ЛАБКОВСКАЯ — кафедра Измерительных технологий
и компьютерной томографии*

АЛГОРИТМ КОРРЕКЦИИ ГЕОМЕТРИЧЕСКИХ ИСАЖЕНИЙ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ГРУППОВЫХ ПРЕОБРАЗОВАНИЙ

Научный руководитель — ассистент Н.Д. Скалецкая

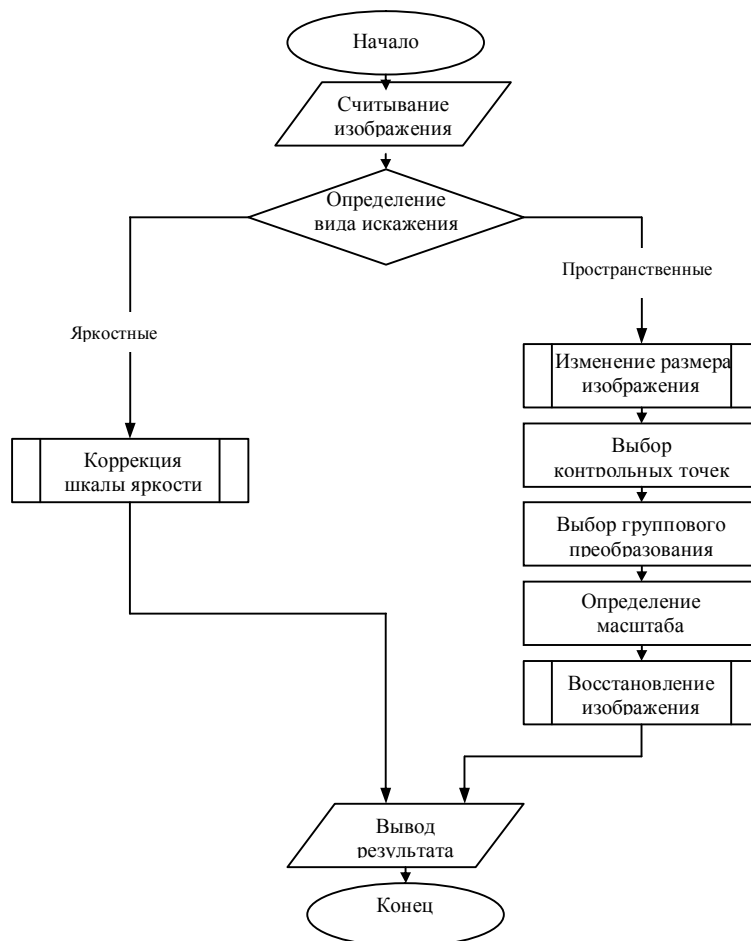
Проблемой большинства получаемых при медицинских исследованиях изображений является присутствие на них артефактов — ошибок, проявляющихся в процессе отображения и вызванных различными факторами — особенностями объекта исследования, используемым оборудованием, особенностями алгоритма реконструкции изображения и т. д. Артефакты представляют собой области с измененной интенсивностью сигнала или неправильно спозиционированные области. Пространственные искажения приводят к резкому снижению вероятности правильного распознавания изображения. В связи с этим актуальной является задача разработки методов коррекции пространственных искажений, позволяющих привести искаженное изображение исследуемого объекта к эталонному виду.

Методы коррекции яркостных искажений часто рассматриваются аналогично методам подавления шумов и выявления полезного одномерного сигнала. Применение линейных и нелинейных преобразований шкалы яркости позволяет увеличить контрастность исходного изображения, но так как артефакт, вызванный движением или присутствием металла, относится к пространственным искажениям, то вышеуказанные методы не позволят достигнуть желаемого результата. Таким образом, пространственные искажения изображений описываются групповыми преобразованиями различного вида.

Группы Ли являются очень эффективным математическим аппаратом при решении задач обработки изображений исследуемых объектов. Итак, для преобразования полученных изображений необходимо правильно подобрать методы групповых преобразований, основанные соответственно на аффинной и проективной группах Ли:

$$\begin{cases} x' = a_1x + a_2y + b_1; \\ y' = a_3x + a_4y + b_2. \end{cases} \quad \begin{cases} x' = \frac{a_1x + a_2y + b_1}{a_5x + a_6y + 1}; \\ y' = \frac{a_3x + a_4y + b_2}{a_5x + a_6y + 1}. \end{cases}$$

Для описания методики коррекции пространственных искажений были взяты магнитно-резонансные изображения головного мозга человека, полученные на томографе GE Signa Infinity 1,0 Тл. Для достижения поставленной цели, а именно, преобразования изображений с целью выявления артефактов, с применением теории групп были использованы методы коррекции пространственных искажений изображений. В ходе работы была написана программа в среде MatLab. Когда известна информация об искажениях изображения, для обработки на языке MatLab применяют функцию `cp2tform`. Эта функция служит для восстановления изображений. На основе алгоритма данной функции была построена блок-схема (см. рисунок).



В ходе работы был проведен анализ существующих методов коррекции искажений изображений, который привел к выводу, что не все методы применимы для коррекции определенных видов искажений на изображении. С использованием практических расчетов были получены результаты обработки изображений различными методами, а также приведен алгоритм обработки изображений с помощью теории групп. С помощью данного алгоритма были получены изображения, которые могут облегчить дальнейшую работу, т.е. повысить качество медицинской диагностики. Таким образом, можно устранить артефакты изображений, не прибегая к дорогостоящим технологиям.

УДК 519.85

*А. В. ОСИПОВ — кафедра Технологии приборостроения
Е. Ю. КОТЕЛЬНИКОВА — аспирант кафедры Вычислительной техники*

ЦЕЛОЧИСЛЕННАЯ ОПТИМИЗАЦИЯ В ПРОЕКТИРОВАНИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

Научный руководитель — д.т.н., профессор В.А. Богатырев

Применение современных программно-аппаратных цифровых комплексов для построения систем управления технологическими процессами позволяет повысить качество управления, снизить риск аварий, создать более экономичные режимы эксплуатации используемых систем и снизить их стоимость. Однако это не снимает одну

из основных проблем автоматизированного управления — обеспечения надежности систем. Особенно остро эта проблема стоит для автоматизированных систем управления технологическими процессами, так как их неверное функционирование зачастую приводит к тяжелым социальным, экологическим и экономическим последствиям. Надежность автоматизированной системы включает свойства безотказности, ремонтпригодности и долговечности [1].

Проектирование автоматизированных систем связано с решением задачи их структурной и параметрической оптимизации. Решение оптимизационной задачи с использованием средств MathCAD сопряжено с трудностями получения целочисленного решения [2]. Пакет расширений Solving and Optimization Extension Pack не позволяет производить оптимизацию параметров над знаком суммы целевой функции.

В работе ставится задача исследования возможностей среды MathCAD для решения задач проектирования надежности автоматизированных систем. В качестве объекта оптимизации рассматривается многоуровневая компьютерная система [3]. В результате оптимизации находится число узловых точек на различных уровнях, при котором достигается максимум надежности системы при соблюдении ограничения ее общей стоимости [4].

В работе предлагается алгоритм и программа для целочисленного решения поставленной оптимизационной задачи средствами MathCAD.

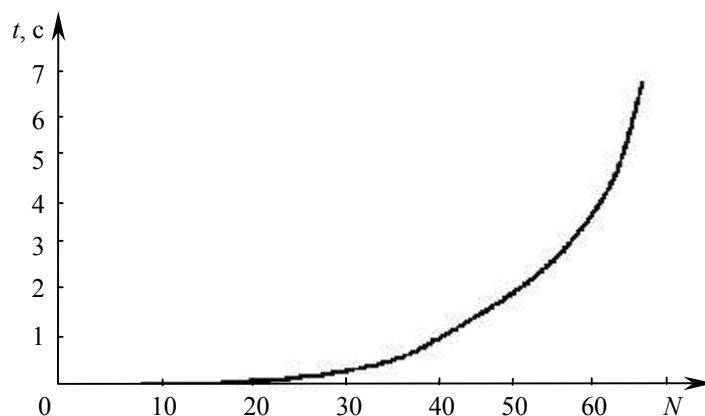
MathCAD — программа поиска максимума целевой функции:

$$P(n_1, n_2, n_3) = \left(\sum_{i=1}^{n_1} C_{n_1}^i P_1^i (1-P_1)^{n_1-i} \right)^m \left(\sum_{i=1}^{n_2} C_{n_2}^i P_2^i (1-P_2)^{n_2-i} \right) \left(\sum_{i=1}^{n_3} C_{n_3}^i P_3^i (1-P_3)^{n_3-i} \right).$$

Поиск решения:

$$y = \left| \begin{array}{l} P_0 \leftarrow 0 \\ \text{for } i_1 \in 1, 2, \dots, \left\lfloor \frac{c_0}{mc_1} \right\rfloor \\ \quad \text{for } i_2 \in 1, 2, \dots, \left\lfloor \frac{c_0 - mc_1 i_1}{c_2} \right\rfloor \text{ if } \left\lfloor \frac{c_0 - mc_1 i_1}{c_2} \right\rfloor \geq 1 \\ \quad \quad \text{for } i_3 \in 1, 2, \dots, \left\lfloor \frac{c_0 - mc_1 i_1 - c_2 i_2}{c_3} \right\rfloor \text{ if } \left\lfloor \frac{c_0 - mc_1 i_1 - c_2 i_2}{c_3} \right\rfloor \geq 1 \\ \quad \quad \quad \text{if } P_0 < P(i_1, i_2, i_3) \\ \quad \quad \quad \quad y_0 \leftarrow i_1 \\ \quad \quad \quad \quad y_1 \leftarrow i_2 \\ \quad \quad \quad \quad y_2 \leftarrow i_3 \\ \quad \quad \quad \quad P_0 \leftarrow P(i_1, i_2, i_3) \end{array} \right. y$$

Рисунок иллюстрирует, что разработанный алгоритм позволяет получать результат за приемлемое время t (ожидание не более 5 с) при небольшом количестве элементов N в системе (менее 60 элементов). Время выполнения алгоритма с ростом числа элементов системы возрастает экспоненциально.



Таким образом, предложены алгоритм и его программная реализация по решению оптимизационной целочисленной задачи проектирования вычислительных систем в среде MathCAD. В отличие от использования традиционных для оптимизации функций $\text{Minimize}(f, x_1, x_2, \dots)$ / $\text{Maximize}(f, x_1, x_2, \dots)$ предлагаемый подход позволяет найти не только целочисленное решение, но и решение, если искомые переменные находятся над знаком суммы.

Литература

6. ГОСТ 24.701-86. ЕСС АСУ. Надежность АСУ. Основные положения.
7. *Осинов А.В.* Целочисленное решение задач оптимизации компьютерных систем в среде Mathcad // Сб. тр. конф. молодых ученых. Вып. 4. Математическое моделирование и программное обеспечение. СПб: СПбГУ ИТМО, 2009. С. 253—258.
8. *Богатырев В.А., Богатырев С.В.* Векторная оптимизация структуры кластера // Сб. науч. тр. Информационные системы и технологии: теория и практика. СПб: ЛТА, 2008. С. 19—27.
9. *Богатырев В.А.* Оценка надежности и оптимальное резервирование кластерных компьютерных систем // Приборы и системы. Управление, контроль, диагностика. 2006. № 10. С. 18—21.

УДК 004.738.52

О. В. ПАРХИМОВИЧ — кафедра Проектирования компьютерных систем

ОБЗОР АЛГОРИТМА РАБОТЫ СИСТЕМ ГРАФИЧЕСКОГО ПОИСКА

Научный руководитель — ассистент В.В. Власов

Интернет до сих пор остается текстовой средой: несмотря на существование миллионов изображений, их поиск осуществляется по текстовым меткам, созданными пользователями, что не позволяет выявить нужные файлы по их содержанию. Поисковые системы не анализируют файл, поэтому обычно результат себя не оправдывает, так как у 30 % изображений метки не соответствуют содержанию.

Некоторые разработчики уже пытались создать систему интеллектуального графического поиска, способную находить изображения по схожести объектов или по цветовой гамме.

Что же должен уметь графический поисковик? Необходимо распознавать текстовый запрос и связывать его с некоторыми изображениями.

На сегодняшний день нет системы графического поиска, позволяющей корректно обрабатывать все текстовые запросы (обработку в объеме 20—40 % всех запросов нельзя назвать успешной), поэтому рассмотрим некоторые развивающиеся поисковые системы.

TinEye. Основная задача — выявление случаев использования изображения с нарушением авторских прав. Технология позволяет определить, на каких сайтах находится картинка, идентичная образцу, проанализировав ее размер и другие параметры.

Tiltomo. Ресурс позволяет искать картинки по двум параметрам тематической схожести (содержимому) или по цветовой гамме, используя базу данных фотохостинга Flickr. Существенный недостаток ресурса — ограниченность количества анализируемых изображений: пока не будет предоставлен поиск по любому изображению, нельзя говорить об анализе содержимого.

Picitup. Возможно, сделав текстовый запрос через ресурс получить список найденных изображений и выбрать среди них похожие по изображенным предметам, цветовой гамме, лицам и др. Поисковая система фиксирует запросы: к ним можно вернуться в любой момент (привязка осуществляется по IP-адресу).

Picollator. Для обнаружения объектов используются нелинейные фильтры с технологией адаптивного обучения, которые различают содержимое и анализируют его: если изображено лицо, система по предварительной обработке определяет, чье оно. Процесс распознавания связан с применением оригинальных моделей искусственных нейронных сетей. Для индексации создается каталог, в котором объекты сгруппированы по принципу схожести и связаны ссылками.

Анализ графических поисковых систем показывает, что каждой разработке свойственны достоинства и недостатки. Многие поисковые системы не обладают функциями анализа подписей к изображениям, являющихся как стандартными элементами структуры графических файлов, так и скрытых меток. Преимуществом системы была бы возможность корректировки изображения перед выдачей результата: удалять шум и выделять основной объект, а также показывать, по какой части файла происходил анализ.