POZNÁMKY

MATERIÁLY

XI MEZINÁRODNÍ VĚDECKO - PRAKTICKÁ KONFERENCE

«VĚDECKÝ POKROK NA PŘELOMU TYSYACHALETY - 2015»

27 května – 05 června 2015 roku

Díl 18
Moderní informační technologie
Matematika
Fyzika

Praha
Publishing House «Education and Science» s.r.o
2015

Vydáno Publishing House «Education and Science»,
Frýdlanská 15/1314, Praha 8
Spolu s DSP SHID, Berdianskaja 61 Б, Dnepropetrovsk

Materiály XI mezinárodní vědecko - praktická konference «Vědecký pokrok na přelomu tysyachalety – 2015». - Díl 18. Moderní informační technologie.Matematika.Fyzika.: Praha. Publishing House «Education and Science» s.r.o - 112 stran

Šéfredaktor: Prof. JUDr Zdeněk Černák

Náměstek hlavního redaktor: Mgr. Alena Pelicánová

Zodpovědný za vydání: Mgr. Jana Štefko

Manažer: Mgr. Helena Žákovská

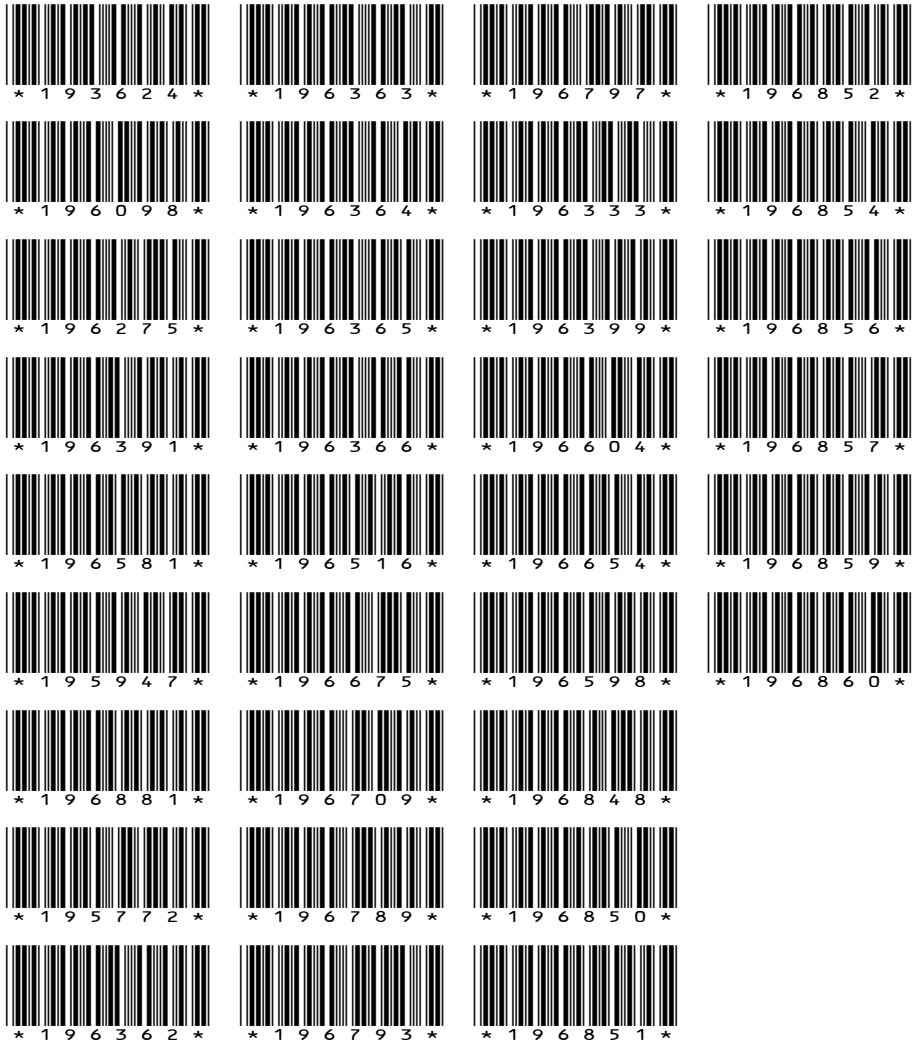
Technický pracovník: Bc. Kateřina Zahradníčková

XI sběrné nádobě obsahují materiály mezinárodní vědecko - praktická konference «Vědecký pokrok na přelomu tysyachalety»
(27 května – 05 června 2015 roku)
po sekcích Moderní informační technologie.Matematika.Fyzika.

Pro studentů, aspirantů a vědeckých pracovníků

Cena 270 Kč

ISBN 978-966-8736-05-6



INFLAČNÍ BEZPEČNOST

MATEMATIKA

UŽITÁ MATEMATIKA

FYZIKA

FYZIKA TUHÝCH LÁTEK

MODERNÍ INFORMAČNÍ TECHNOLOGIE

POČÍTAČOVÝ ENGINEERING

Скачков Д.А.
Кременчугский национальный университет имени Михаила Остроградского, Украина

МЕТОДИКА ПРОВЕДЕНИЯ ЭКСПЕРИМЕНТА ПО АНАЛИЗУ РАБОТЫ ВЕБ-ПРИЛОЖЕНИЙ

В ядре веб-приложений на базе Drupal реализован набор функций (API) для работы со всеми необходимыми компонентами: СУБД, формами, кэшем, учетными записями пользователей и их правами. Для взаимодействия с СУБД используется абстрактный интерфейс DB API, ядро Drupal оперирует ANSI-совместимым SQL для работы с БД, а структуры (таблицы) для БД определяются программистом в массивах специального вида. При этом преобразование определений таблиц и запросов под особенности конкретной СУБД выполняется специальной библиотекой [1-2].

Измеряемые параметры работы веб-приложения: LA_{CPU} – нагрузка по процессору, LA_{RAM} – объемы используемой оперативной памяти, LA_{IO} - нагрузка по диску, LA_{WBandw} – нагрузка на канал связи (трафик), QA_E – ошибки интерпретатора, QA_S – уровень ошибок в коде, полученный с помощью статического анализа, M_{bandw} – трафик базы данных, M_{QA} – показатель качества SQL запросов, M_C – количество подключений к базе данных.

Это исследование направлено на решение задачи диагностирования аномалий в работе веб-приложений при изменении вышеперечисленных параметров, с дальнейшей локализацией аномалии. Учитывая ограничения на изменение исходного кода клиентских веб-приложений, для анализа были использованы статистические данные использования ресурсов, которые предоставлены хостинг-провайдером IT-Patrol Inc. Для веб-приложений задействованных в эксперименте было задействовано логирование ошибок интерпретатора, логирование доступа к домену веб-сервера, показатели использования аппаратных ресурсов и включена трассировка функций. Основной задачей при исследовании является установка взаимосвязей влияния работы функциональных элементов на изменение диагностических показателей, как качественных, так и количественных.

Раздел 1.01 **Экспериментальная модель анализа работы веб-приложений.** Для формирования интегральной оценки работы функциональных элементов клиентских веб-приложений используется таблица 1, состоящая из критериев, значения которых представлены в двоичном виде. Результатом оценки

функции станет число в двоичном виде учитывающее приоритет критериев (в зависимости от их расположения в таблице). Такой подход позволяет сделать оценку более гибкой и адаптировать оценивание согласно тарифным планам хостинг-провайдера. Данный подход следует использовать в случае, если на тарифном плане для клиента есть ограничения на использование ресурсов (лимиты), оценка будет формироваться с их учетом. Итоговой оценкой станет среднее арифметическое от показателей работы функции за исследуемый период.

Таблица 1.

Формирование интегральной оценки работы функциональных элементов относительно потребляемых ресурсов

Function name		function1	function2	function3	function4	functionN
CPU Usage	Mysql CPU	1	0	1	0	1
	PHP CPU	0	1	0	1	0
RAM		1	1	1	1	1
Website bandwidth	Out bandwidth	1	1	1	1	1
	In bandwidth	1	0	1	0	1
MySql bandwidth	Out bandwidth	0	1	0	1	0
	In bandwidth	1	0	1	0	1
MySQL Queries	Select	1	1	1	1	1
	Update	1	1	1	1	1
	Other	1	1	1	1	1
Diskspace	Filesystem diskspace	1	1	1	1	1
	MySQL Diskspace	1	1	1	1	1
IO	Read	1	1	1	1	1
	Write	0	1	0	1	0
Hits	PHP Hits	1	1	1	1	1
	File hits	1	1	1	1	1
	MySql Connections	0	1	0	1	0
Error logs	Fatal/ Syntax	1	1	1	1	1
	Notices	1	1	1	1	1

Для структурного анализа веб-приложения и оценки работы функциональных элементов производится трассировка функций. Учитывая иерархию (уровень вложенности), показатели использования ресурсов функций агрегируются и классифицируются как нагрузка от функционального элемента (модуля).

OBSAH

MODERNÍ INFORMAČNÍ TECHNOLOGIE

POČÍTAČOVÝ ENGINEERING

VÝPOČETNÍ TECHNIKA A PROGRAMOVÁNÍ

PROGRAMOVÉ VYBAVENÍ

Неоднородность в распределении пор по поверхности образца InP обусловлена наличием дефектов на поверхности исходного монокристалла и наличием термоупругих напряжений.

Литература

[1] Сычикова Я.А. Влияние дислокаций на процесс порообразования в монокристаллах n-InP (111) / Я.А. Сычикова, В.В.Кидалов, Г.А. Сукач // Физика и техника полупроводников. – 2011. – т. 45, № 1. – С. 123 – 126.

[2] Сичікова Я.О. Дефекти структури та процеси пороутворення у фосфіді індію: монографія / Я.О. Сичікова, В.В. Кідалов, Г.О. Сукач – Донецьк: Юго-Восток, 2011. – 218 с.

[3]. Пат. 93456 Україна, МПК(2006): G01N 27/00. Спосіб дослідження смуг сегрегації домішки фосфіду індію шляхом селективного електрохімічного травлення / Сичікова Я.О., Кідалов В.В., Сукач Г.О.; заявник та патентовласник Сичікова Я.О. – № a200911327; заявл. 06.11.2009; опубл. 10.02.2011, Бюл. № 3/2011.

Исследуя показатели надежности работы веб-приложения, в рамках эксперимента можно определить основные состояния веб-приложения:

- Рабочее состояние. Ошибок нет.
- Рабочее состояние. Есть предупреждения от интерпретатора
- Частично рабочее состояние. Критические ошибки.
- Не рабочее состояние. Критическая ошибка.

В основе оценки надежности кода лежат разработанные автором сигнатуры для статического анализа (учитывающие архитектурные особенности веб-приложения). Весовые коэффициенты ошибок, в используемых сигнатурах, модифицированы с учетом классификации ошибок интерпретатора:

Таблица 2

Цены на ресурсы сервера и весовые коэффициенты параметров при формировании цены для клиентов облачных тарифных планов IT-Patrol Inc.

Параметр:	CPU 100% usage for 1 hour	Веб трафик for 1Gb	MySQL Bandwidth for 1Gb	Disk space for 10Gb/hour	MySQL Disk space for 10Gb/hour	PHP requests for 10000 requests	File requests for 100000 requests
Цена	$ 0.13	$0.02	$ 0.01	$ 0.01	$ 0.05	$ 0.01	$ 0.04
Весовой коэф-фициент	0,481481	0,074074	0,037037	0,037037	0,185185	0,037037	0,148148

С учетом введенных обозначений экспериментальную модель детектирования аномалий в работе веб-приложений можно представить следующим способом (1–6) – экспериментальные коды состояний функциональных элементов веб-приложения:

1. $QA_S \downarrow\uparrow \rightarrow [\![((LA]\!]_{CPU} \uparrow) \vee [\![(LA]\!]_{RAM} \uparrow) \vee [\![(QA]\!]_E \uparrow) \vee (LA_{IO} \uparrow)[\![\vee (M]\!]_{bandw} \uparrow)\big)$;
2. $M_{\downarrow}QAS \downarrow\uparrow \rightarrow [\![[\![(M]\!]_{\downarrow bandw} \uparrow) \vee (M]\!]_{\downarrow C} \uparrow) \vee [\![(LA]\!]_{\downarrow CPU} \uparrow) \vee [\![(LA]\!]_{\downarrow RAM} \uparrow))$;
3. $M_C \uparrow \rightarrow [\![(QA]\!]_E \uparrow) \vee [\![(QA]\!]_S \uparrow)$;
4. $LA_{Wbandw} \uparrow \rightarrow [\![(LA]\!]_{RAM} \uparrow) \wedge [\![(LA]\!]_{CPU} \downarrow)$;
5. $LA_{IO} \uparrow \rightarrow [\![(LA]\!]_{CPU} \uparrow) \wedge [\![(LA]\!]_{RAM} \uparrow)$;
6. $LA_{RAM} \uparrow \rightarrow [\![[\![(QA]\!]_E \uparrow) \vee (M]\!]_C \uparrow) \vee [\![(LA]\!]_{CPU} \uparrow)$;

Изменение значений характеристик следующими символами:

$\downarrow$ – уменьшение значения характеристики;

$\uparrow$ – увеличение значения характеристики;

$\downarrow\uparrow$ – отклонение значения характеристики от эталонного в худшую сторону.

Описанная логическая модель детектирования аномалий в работе веб-приложений не применима ко всем веб-приложениям и требует дальнейшего усовершенствования и адаптации для разных типов приложений. В данной работе она используется лишь для иллюстрации предложенного подхода в анализе.

Литература:

1. Скачков Д.А. Исследование механизмов оптимизации времени отклика веб-приложений. – Наука, техника и образование. – Москва, 2014. – №6. – С.23-25.

2. Hein D. Simloid: Evolution of Biped Walking Using Physical Simulation / D. Hein – Berlin, Institute of Informatic, 2007. – 415 p.

Мясищев А.А.
Хмельницкий национальный университет, Украина

УПРАВЛЕНИЯ ГОЛОСОМ С ПОМОЩЬЮ ANDROID И ARDUINO

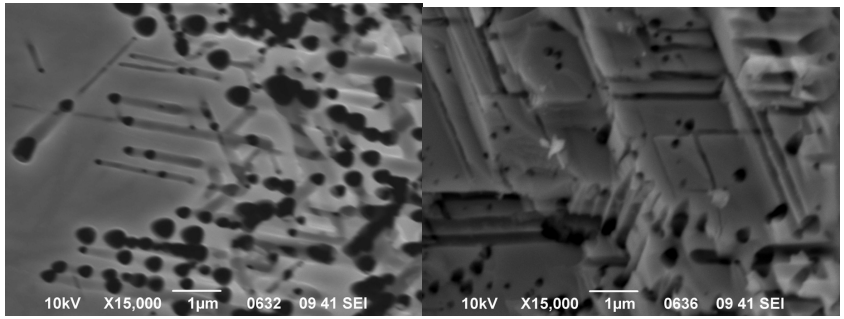
В настоящее время наблюдается значительный рост интереса к технологиям, связанным с распознаванием речи. Например, задачи управления устройствами с помощью голосовых команд. В последнее время появилась возможность управления домашней, офисной техникой с помощью Андроид – устройств голосовыми командами, что широко рекламируется как технология «умный дом».

В работе представлена программа голосового управления Ардуино с помощью Андроид – устройства через Bluetooth HC-05. К Ардуино подключены три исполнительных механизма и датчик температуры. После выполнения соответствующих команд программа синтезирует голосовое сообщения о результате работы. Этот пример является типичной подзадачей общей задачи «Умный дом». Программа также реализует простейший диалог между устройством и пользователем, отвечая на простые вопросы. Для распознавания и синтеза речи используется инструментарий Google. Если смартфон поддерживает голосовой поиск в режиме оффлайн, доступ к Интернет не обязателен. Программа для Андроид написана в среде Android Studio(язык Java), а для Ардуино – в среде разработки Ардуино на C++(проект Wiring). Тестировалась на телефоне LG G3 Stylus и планшете Acer A500.

В рамках этой работы на устройстве Андроид должны выполняться следующие задачи:

1. При нажатии на кнопку приложения «Нажми для начала диалога»(рис.1) с помощью механизма Intent(намерение) вызывается Активити, выполняющее прослушивание произнесенной фразы с последующей передачей ее сервису распознавания речи. Он может находиться на серверах Google или установлен на

даря нарушению регулярности кристаллической решетки в ядре дислокации. Такая ситуация приводит к уменьшению внутренней энергии кристалла, а поэтому, и к ослаблению химической стойкости вещества в ядре дислокации и вблизи него. При травлении монокристаллов *n*-InP вдоль кристаллографической оси [111] наблюдалась тенденция к группированию пор в симметричные скопления вокруг зародышевых пор, которые возникли раньше и связаны с выходом на (111) поверхность дислокаций и микро-, нанотрещин.



а) б)

Места выхода дислокации на поверхность кристалла служат центрами реакции. Автокаталитическое развитие процесса растворения усиливает подавляющий характер травления в области выхода дислокаций. Все это приводит к образованию на поверхности кристалла вокруг выхода дислокации так называемой «ямки травления». Симметрия и периодичность ансамбля пор повторяет симметрию и периодичность дефектной структуры полупроводника, который возникает в его приповерхностном слое [2].

Расчет плотности дислокаций исследуемого кристалла InP в местах скопления дислокаций дал значение $2x10^6$ см$^{-2}$. В областях, менее заполненных порами, плотность дислокаций составляла ~ 10^4 см$^{-2}$. Этот результат хорошо согласовывается с паспортными данными образцов InP, полученными от производителя (компания «Molecular Technology GMBH») – плотность дислокаций составляет 10^6 и 10^4 см$^{-2}$ в местах скопления дислокаций и в областях, где концентрация дислокаций значительно меньше соответственно.

Таким образом, установлено, что плотность входных отверстий пор, также как и степень пористости макроскопически однородных пористых слоев варьируются в широком диапазоне величин в зависимости от материала полупроводника, ориентации поверхности, уровня легирования, типа присутствующих в растворе анионов и условий анодирования. Площади, занятые отверстиями пор, могут составлять до нескольких десятков процентов от площади начальной поверхности [3].

FYZIKA

FYZIKA TUHÝCH LÁTEK

Сичікова Я.О.
Бердянський державний педагогічний університет

ДИСЛОКАЦИОННЫЙ МЕХАНИЗМ ПОРООБРАЗОВАНИЯ В МОНОКРИСТАЛЛАХ *N*-INP

Пористые полупроводники находят все более широкое применение в нано- и оптоэлектронике в качество излучателей, фотоприемников, сенсоров и др., а также благодаря перспективам создания устройств интегральной оптики, в которых информация обрабатывается не только в электронном, но и в оптическом виде. В частности, очень перспективным в этом аспекте является пористый InP, поскольку энергетические параметры его монокристаллов очень близки к параметрам монокристалла кремния, и на основе его легко изготовлять приборы интегральной оптоэлектроники, совместимые с кремнием.

В данной работе предложен простой и эффективный метод выявления внутренних дефектов кристаллической решетки – типа дислокаций, который заключается в сопоставлении процессов порообразования и дислокаций структуры в исходных монокристаллах *n*-InP с кристаллографической ориентацией (111).

В качестве электролита использовался 48% раствор плавиковой кислоты (HF), этилового спирта (C_2H_5OH) и воды в соотношении 1:2:1.

Рисунок демонстрирует фрагмент поверхности (а) и скола (б) пористого образца *n*-InP, из которого четко видно местоположение образования ядер пор. Края пор немного растянуты в плоскости (111). Распределение плотности пор и местоположение ядер образования пор очень неравномерно; наблюдается существенная их негомогенность. Поверхность является мезопористой (диаметр пор составляет от 100 до 600 нм). Пористые слои с выраженной в глубину образца анизотропной структурой формируются порами, которые распространяются от поверхности и ветвятся в объеме преимущественно вдоль кристаллографической оси [111] по направлениям А или В (преимущественно). Затравками пор служат дислокации, которые является источниками упругих механических напряжений, порождая вокруг себя упругие деформации.

Упругие взаимодействия исходных дислокаций с точечными дефектами кристаллической структуры приводят к повышению концентрации остаточных дефектов вблизи оси дислокации и создания облака Котрелла [1]. Известно, что дислокации существенно влияют на механические свойства кристаллов благо-

мобильном устройстве, если оно поддерживает сервис «голосовой поиск offline». Если работа производится с серверами через Интернет результаты распознавания фраз будут значительно лучше. Для решения этой части задачи используется класс RecognizerIntent.

2. Результат распознавания в виде текстовой строки сопоставляется со строкой, находящейся в памяти. Если сопоставление истинно, то запускается синтезатор речи Google и произносится фраза из памяти, соответствующая сопоставленной. Например, результат распознавания «включить красный». Соответствие этой фразе в памяти «красный включила». Синтезатор сгенерирует эту фразу. Если сопоставление ложно, то синтезатор сгенерирует фразу, соответствующую распознанной строке. Для синтеза речи используется класс TextToSpeech.

3. После окончания синтеза речи основное приложение вновь запускает Активити, выполняющее прослушивание произнесенной фразы. Это повторение выполняется до тех пор, пока не будет произнесена фраза «конец связи». После этой фразы приложение должно перейти в режим ожидания пока вновь не будет нажата на кнопка « Нажми для начала диалога «.

4. После синтеза речи выполняется ее вывод через динамики компьютера. Поэтому необходимо в программе использовать специальный механизм, который бы прослушивал работу акустического вывода речи, а после окончания запускал вновь Активити по прослушиванию речи и ее распознаванию. В этом случае будет смоделирован полноценный диалог речевого общения между пользователем и компьютером. Данный механизм реализуется с помощью абстрактного класса utteranceProgressListener. Он использует методы, которым передается управление в начале, в конце высказывания синтезатором и при появлении ошибки.

5. Если произнесенная фраза соответствует команде, например «включить синий», то приложением на Андроиде выполняется передача байта на Ардуино через Bluetooth устройство и Ардуино выполняет включение синего светодиода(имитация устройства). При команде «температура» Ардуино пересылает приложению на Андроид значение температуры, считанной с температурного датчика DS18B20.

На рисунке 1 показаны скриншоты до и после активации голосового ввода.

В строке «Распознанный текст» выводится произнесенная фраза или команда, в строке температура – значение температуры, возвращенное с Ардуино после произнесения команды «темература». Строка «Нажми для начала диалога» – это кнопка, после нажатия на которую инициализируется Активити распознавателя речи с последующей обработкой произнесенных фраз.

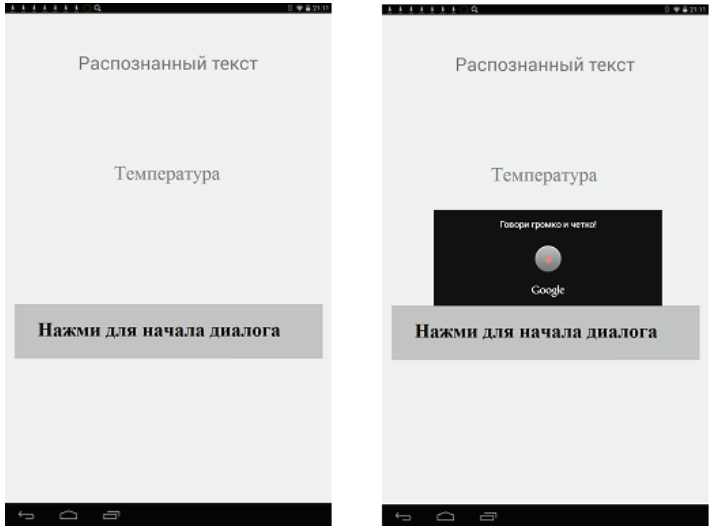


Рис.1. Скриншоты до и после активации голосового ввода.

Программа на Андроид состоит из двух больших блоков – это блок начала работы приложения (I) и блок работы приложения после нажатия на кнопку «**Нажми для начала диалога**»(II). На рисунке 2 показана блочная последовательность действий, которые выполняются каждым блоком(I, II).

Здесь приняты следующие сокращения(см. также текст программы):

1. **Блок I**:

1.1. **Запуск прил**. – выполнить запуск приложения на Андроиде;

1.2. **Подкл. Blu** – запускается метод bluet(), который подключает Андроид к Ардуино через Bluetooth;

1.3. **Blu** – выполняется проверка, подключены ли Андроид и Ардуино по Bluetooth;

1.4. **Зап. пр. Т0** – каждую секунду запускается метод run() класса bluetoothInOut, который посылает запрос к Ардуино для определения температуры и выполняет считывание с Ардуино значения температуры. Таким образом каждую секунду Андроид получает новое значение температуры;

1.5**. Ож.Кн**. – после запуска приложение переходит в ожидание нажатия на кнопку «Нажми для начала диалога».

5. Семевский Ф.Н. К вопросу оценки глобального эффекта загрязнения среды инсектицидами // В кн.: Проблемы экологического мониторинга и моделирования экосистем. – Л.: Гидрометеоиздат. Т.7. – 1985. – С.288-292.

6. Бурлибаев М.Ж. Теоретические основы устойчивости экосистем трансзональных рек Казахстана: дис... д-ра техн. наук: 25.00.27; 25.00.36 / Таразский гос. ун-т им. М.Х.Дулати. – Тараз, 2004.

7. А.А. Турсунов. Гидроэкологические проблемы Республики Казахстан. – Издательский дом CA&CC Press. Швеция. 2010.– 213 с.

8. М.Ж. Бурлибаев, Р.К. Кайдарова, А.Н. Клец, Л.В. Лященко Концепция единой системы экологического мониторинга// Гидрометеорология и экология. – 2000. – № 3-4. – С. 109-145.

9. Айдосов А.А., Айдосова Г.А., Заурбеков Н.С. Модельная оценка экологической обстановки окружающей среды при аварийных ситуациях. – Алматы, 2010 (монография). – 414 с.

10. Заурбеков Н.С. Модели экологической обстановки окружающей среды при реальных атмосферных процессах. – Алматы, 2010 (монография). – 368 с.

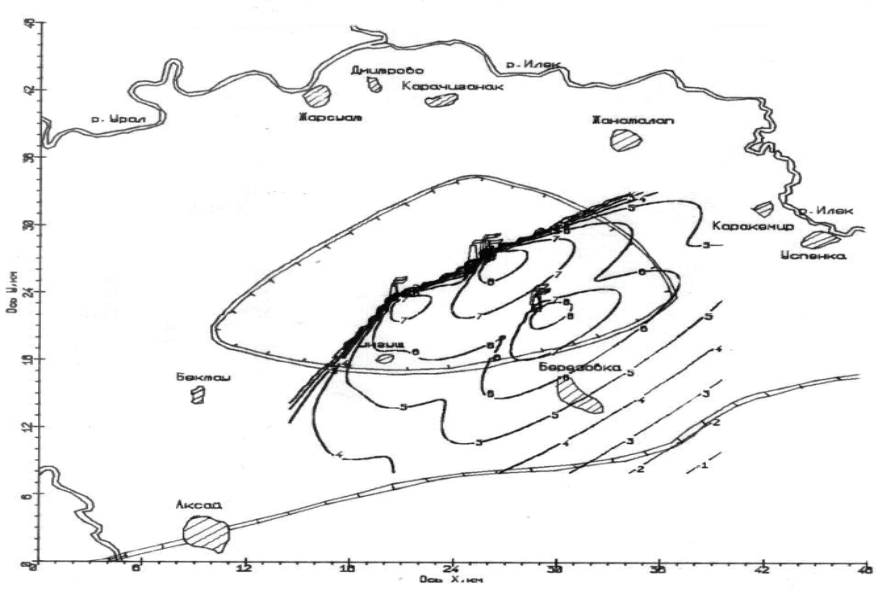


Рисунок 10 – Изолинии распределения концентрации NO_2 на высоте 10 м

Аналогичные рассуждения можно привести и к случаю неустойчивой атмосферы (рис. 6). Различие двух групп рисунков (устойчивой и неустойчивой атмосферы) обусловлено более высоким подъемом и дальним переносом примеси в случае конвекции, что приводит к более сжатым изолиниям в случае неустойчивой атмосферы на высоте z=10 м и большим различием на высоте z=100 м.

Литература

1. Берлянд М.Е. Современные проблемы атмосферной диффузии и загрязнения атмосферы. – Л.: Гидрометеоиздат, 1975. – 448 с.

2. Меллор Л., Херринг Х.Дж. Обзор моделей для замыкания уравнений осредненного турбулентного течения // Ракетная техника и космонавтика. – 1973. – (Т.11)№5. – С.17-29.

3. Садоков В.П., Важник А.И. Предварительные результаты по методу прогноза осредненных по времени полей метеоэлементов // Тез. докл. на Всесоюз. шк.-семинаре по числен. моделированию крупномасштаб. атмосфер. процессов и долгосроч. прогнозу погоды. – Дилижан, 1977.

4. Оникул Р.И., Канчан Я.С. О расчетах загрязнения атмосферы от многих источников на ЭВМ с применением унифицированных программ // Тр. ГГО. – Вып.467. – 1983. – С.41-49.

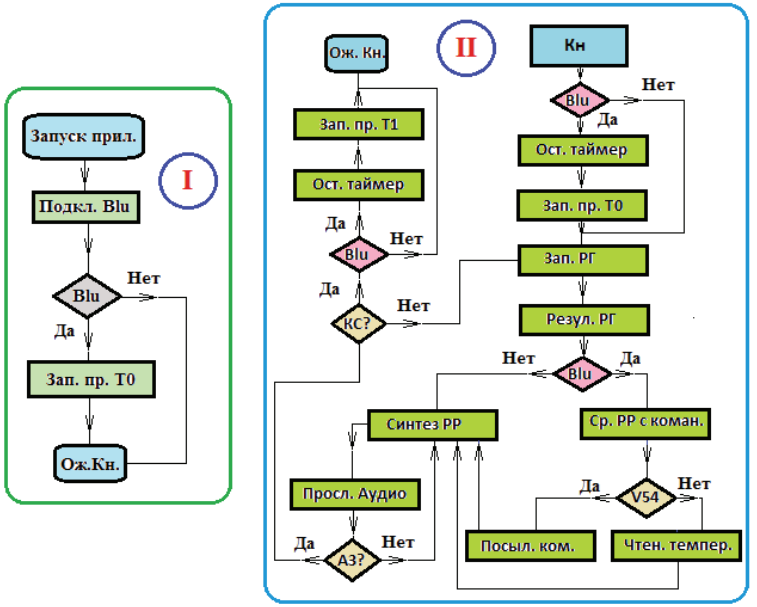


Рис.2. Блок I и блок II, схематично поясняющие работу программы приложения

2. **Блок II:**

2.1. **Кн** – нажатие на кнопку «Нажми для начала диалога»;

2.2. **Blu** – выполняется проверка, подключены ли Андроид и Ардуино по Bluetooth;

2.3. **Ост. таймер** – останавливается таймер, который запускает метод run() класса bluetoothInOut;

2.4**. Зап. пр. Т0** – каждую секунду запускается метод run() класса bluetoothInOut, который посылает запрос к Ардуино для определения температуры и выполняет считывание с Ардуино значения температуры.

2.5. **Зап. РГ** – запускается распознаватель голоса, метод spi();

2.6. **Резул. РГ** – метод onActivityResult получает результаты распознавания голоса и выполняет их сравнение со строкой вопросов и команд;

2.7. **Blu** – выполняется проверка, подключены ли Андроид и Ардуино по Bluetooth;

2.8. **Ср. РР с коман**. – сравнивается результат распознавания голоса с прописанной командой. При совпадении задается значение переменной value кодом символа. Например, символ «1», соответствующий включению RED(см. программу для Ардуино), представлен кодом 49 и т.д.;

2.9. **V54** – выполняется условие value != 54. Код 54 (символ «6») – это код запроса температуры от Ардуино;

2.10. **Чтен. темпер.** – распечатывается значение температуры в строке вывода текста temtext и строковой переменной spout присваивается ее значение, которое Андроид получает каждую секунду от Ардуино;

2.11. **Посыл. ком**. – через Bluetooth на Ардуино посылается байт данных (символ) для включения или выключения соответствующего устройства(RED, GREEN, BLUE);

2.12. **Синтез РР** – вызывается метод tts.speak, выполняющий аудио синтез ответа на произнесенный вопрос, результат выполнения команды, значение температуры или произнесенную фразу, если нет соответствия между вопросом и ответом(т.е. система работает как попугай);

2.13. **Просл. Аудио** – здесь работает метод onDone класса utteranceProgressListener который следит за окончанием генерации динамиком звука синтеза речи;

2.14. **АЗ** – проверка завершения аудио вывода синтезатором речи;

2.15**. КС** – проверка произнесения фразы «конец связи»;

2.16. **Blu** – выполняется проверка, подключены ли Андроид и Ардуино по Bluetooth;

2.17. **Ост. таймер** – останавливается таймер, который запускает метод run() класса bluetoothInOut;

2.18. **Зап. пр. Т1** – каждую секунду запускается метод run() класса bluetoothInOut, который выполняет считывание с Ардуино значения температуры(запрос на температуру не посылается);

2.19. **Ож. кн.** – приложение переходит в ожидание нажатия на кнопку «Нажми для начала диалога».

В соответствии с перечисленными задачами рассмотрим основные отдельные блоки приложения.

1. Создается класс приложения MainActivity, наследуемый от класса Activity – базового класса для всех экранов приложения. Здесь используется интерфейс TextToSpeech.OnInitListener для инициализации синтезатора речи.

```
public class MainActivity extends Activity implements TextToSpeech.OnInitListener {
   // Объявление переменных
   public String sp10 = " выключить зеленый ";
   public String sp20 = " включить зеленый "; ...
// Socket, с помощью которого будут отправляться данные
// на bluetooth Arduino
   private BluetoothSocket clientSocket;
   // UUID для случая подключения к последовательному bluetooth  устройству
   private UUID uuid = UUID.fromString("00001101-0000-1000-8000-00805F9B34FB"); ...
```

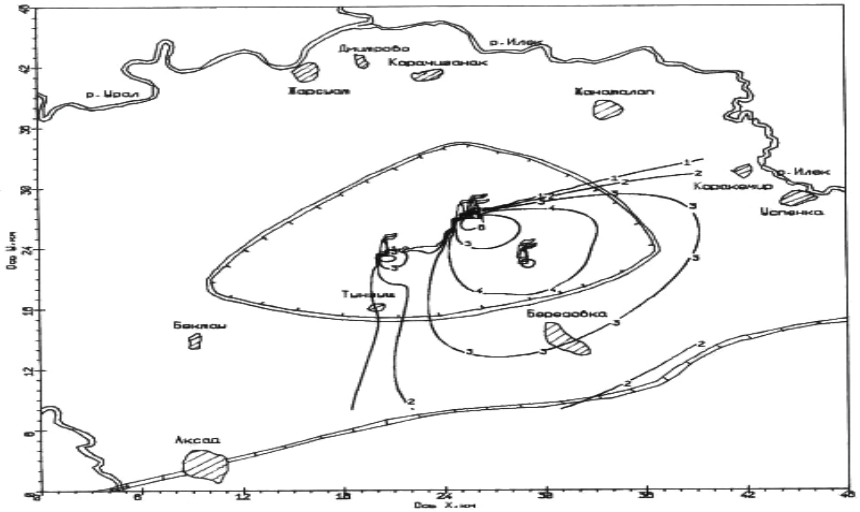



Рисунок 4 – Изолинии распределения концентрации CO_2 на высоте 10 м

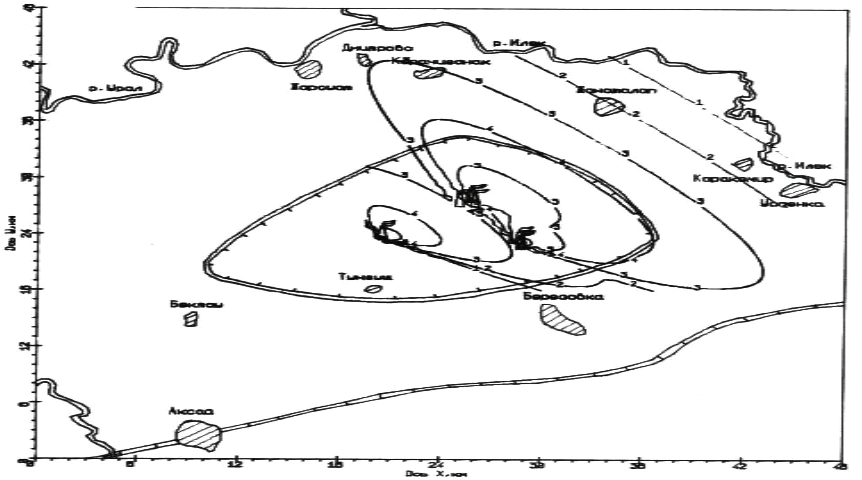


Рисунок 9 – Изолинии распределения концентрации CO_2 на высоте 100 м

В верхних слоях атмосферы с увеличением высоты увеличивается скорость ветра (см. рис. 5) и увеличивается размер вихрей, обслуживающий турбулентный обмен, что приводит к большому распространению загрязняющих примесей. Как уже указывалось, в силу поставленных условий расчета, выделить изолинии уровня единиц ПДК нет возможности (уровень 7). Может вызвать удивление сравнение рисунков 2 и 4 для аналогичных условий (меняется только скорость ветра, для рисунка 4 скорость ветра в 2 раза меньше) – размывание на рисунке 4 больше, чем на рисунке 2, хотя ветер меньше. Но изучение истинного состояния проясняет ситуацию – группа важных по вкладу в загрязнения источников 4-6 в четыре раза увеличила свою эффективную высоту, что и послужило более далекому распространению примесей.

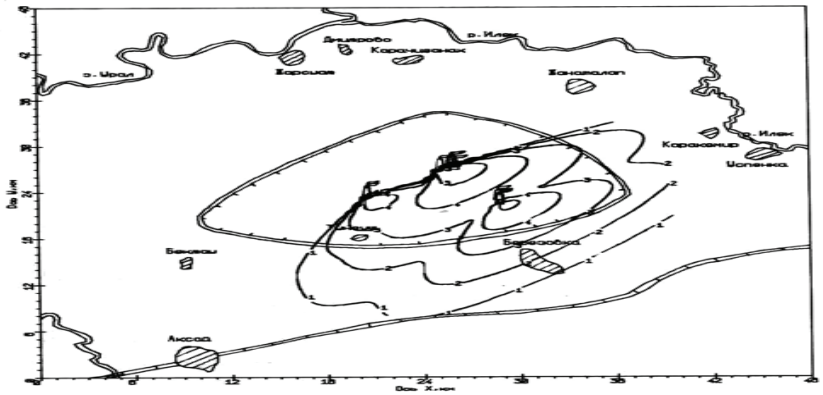


Рисунок 2 – Изолинии распределения концентрации CO_2 на высоте 10 м.

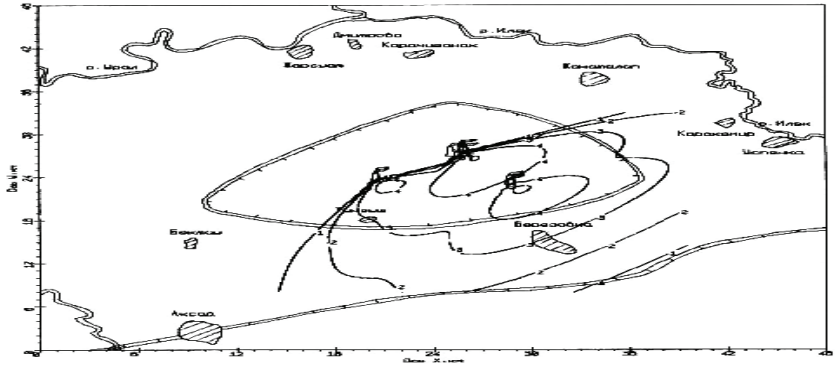


Рисунок 3 – Изолинии распределения концентрации CO_2 на высоте 100 м


```
   // Описание хеш карты для хранения
   // ключа (TextToSpeech.Engine.KEY_PARAM_UTTERANCE_ID)
   // и любого значения - строки (например - "5678")
   private HashMap<String, String> params = new HashMap<>();
   @Override
   public void onCreate(Bundle savedInstanceState) {
      super.onCreate(savedInstanceState);
      setContentView(R.layout.activity_main);
      txtText = (TextView) findViewById(R.id.input_text);
      temtext = (TextView) findViewById(R.id.textView2);
      tts = new TextToSpeech(this, this);
      tts.setOnUtteranceProgressListener(new utteranceProgressListener());
//Установка слушателя синтеза речи
      bluet(); }  // Подключение bluetooth
// Вызов активности распознавателя голоса при нажатии на кнопку
   public void click(View view) {
if(upbluetooth==0) { // Если Bluetooth подключен
// При нажатии на кнопку останавливаю таймер работы
// программы по передаче и чтению  температуры
      time.cancel(); time.purge();
// Запускаю таймер работы программы с новыми начальными
// данными(посылка запроса температуры и прием температуры)
      bluecancel = 0;  time = new Timer();
      bluetoothInOut bInOut = new bluetoothInOut();
      time.schedule(bInOut,500,1000); }
      spi(); } // Запускаю распознаватель речи
  @Override
// Следующий метод выполняет инициализацию синтезатора речи.
// Он требует назначения интерфейса TextToSeech.OnInitListener для
// базового класса приложения MainActivity
 public void onInit(int status) {
 if (status == TextToSpeech.SUCCESS) {// При успешной инициализации
tts.setLanguage(Locale.getDefault()); // выполняется использование языка
// синтезатора, установленного по умолчанию
// Передача параметра params для вызова слушателя синтезируемой речи.
params.put(TextToSpeech.Engine.KEY_PARAM_UTTERANCE_ID,"HELLO");
} else {txtText.setText("Инициализация не выполнена"); } }
... (далее классы и методы, которые кратко описаны ниже)   }
```

2. Метод spi() используется для запуска активности распознавания голоса Google с помощью механизма Intent. Активность формирует запрос к серверам Google и посылает его через Интернет.

```
   public void spi() {
```

```
// Intent подготавливает запуск активности распознавания голоса
 Intent intent =  new Intent(RecognizerIntent.ACTION_RECOGNIZE_SPEECH);
// Передача в активность параметров:
// 1.  Задает модель распознавания, оптимальную для коротких фраз
 intent.putExtra(RecognizerIntent.EXTRA_LANGUAGE_MODEL,    RecognizerIn-
tent.LANGUAGE_MODEL_WEB_SEARCH);
// 2.  Задает подсказку пользователю
intent.putExtra(RecognizerIntent.EXTRA_PROMPT, "Говори громко и четко!");
// Запускается активити, выполняющее распознавание произнесенных
// фраз и возвращающая результаты распознавания
  startActivityForResult(intent, CODE);   }
```

3. Метод onActivityResult используется в программе для получения результатов работы Активити распознавания речи. Фактически он принимает результат распознавания с серверов Google через Интернет и передает их основному приложению.

```
protected void onActivityResult(int requestCode, int resultCode, Intent data) {
// Возврат результатов распознавания речи
       super.onActivityResult(requestCode, resultCode, data);
// Если это результаты распознавания речи (CODE)
// и процесс распознавания прошел успешно
       switch (requestCode){  case CODE: {
             if (resultCode == RESULT_OK && null != data) {
 // то получаем список текстовых строк - результат распознавания.
// Строк может быть несколько, а правильные результаты идут в начале
                 ArrayList<String> spee = data.getStringArrayListExtra(RecognizerIn-
tent.EXTRA_RESULTS);
sp =spee.get(0); // Из массива строк - результатов выбирается самая первая
txtText.setText(sp); // и выводится на экран
                       spout = sp;
 // Сопоставления результата распознавания со строками вопросов
                       int r10 = sp.compareTo(sp10);   ...
// В зависимости от результата сопоставления выбирается тот или иной ответ
                       if (r10 == 0) spout = sp20;  ...
if (upbluetooth == 0) {  // Если подключение к bluetooth существует то
     // результат сравнения представляем символом
    // Например, если результат распознавания голоса соответствует строке
          // "включить зеленый" то на bluetooth посылаем символ 3 (код 51)
               ... if (r3 == 0) value = 51; ...
              // Если запрашиваем температуру, то посылаем данные
                if (value != 54) outData(value);
               if (value == 54) {
                       temtext.setText(readMessage);  // Распечатываем температуру
```


Итак, в таблице 1 приведены данные о высоте приземного слоя h, которая рассчитывается в модели по формуле [1]:

$$h = 0{,}05\frac{K_1}{z_1 w_z}, \qquad (1)$$

где $w_z = 10^{-4}$ – вертикальная составляющая скорости вращения Земли.

Таблица 1

Высота приземного слоя, рассчитанная по модели

№ варианта	T, °C	T, °C	м/с	T, °C	м	h
1	1	2	4	315	10	54,04
2	1	2	4	315	100	54,04
3	1	2	2	315	10	23,74
4	1	2	2	315	100	23,74
5	-1	15	6	45	10	102,98
6	-1	15	6	45	100	102,98
7	-1	15	3	45	10	54,79
8	-1	15	3	45	100	54,79

При расчете высоты приземного слоя h возникают множества проблем. Предложенная нами методика позволяет рассчитывать величину h по формуле (1), поэтому является одним из главных преимуществ данной модели.

В следующих рисунках 2-6 предложены результаты вычисленного в результате созданного нами программного продукта. Одним из важнейших элементов загрязнения атмосферы, влияющих на здоровье населения, является двуокиси серы SO_2, поэтому произведен расчет распределения по территории месторождения, отмеченного контуром. Нами специально выделены три из девяти групп источников, соответствующие своим истинным положениям. В карте местности ось OY направлена на север, а ось OX – на восток. Отмеченные номерами изолиний соответствуют следующим значениям концентрации:

$$c(x,y) = \frac{q(x,y,z)}{\text{ПДК}} * 10^{k/2-3,5}, \qquad (2)$$

где: k – номер соответствующей изолинии; ПДК – предельно допустимые концентрации загрязняющих веществ в атмосферном воздухе (ПДД_{SO} =0,05 мг/м^3 – среднесуточная).

Анализ результатов вычисления. Группа рисунков (рисунки 2-6) изолинии реализует вариант с различными уровнями наблюдения (Z_1=10 м, Z_2=100 м).

ПРИЛОЖЕНИЕ D 1

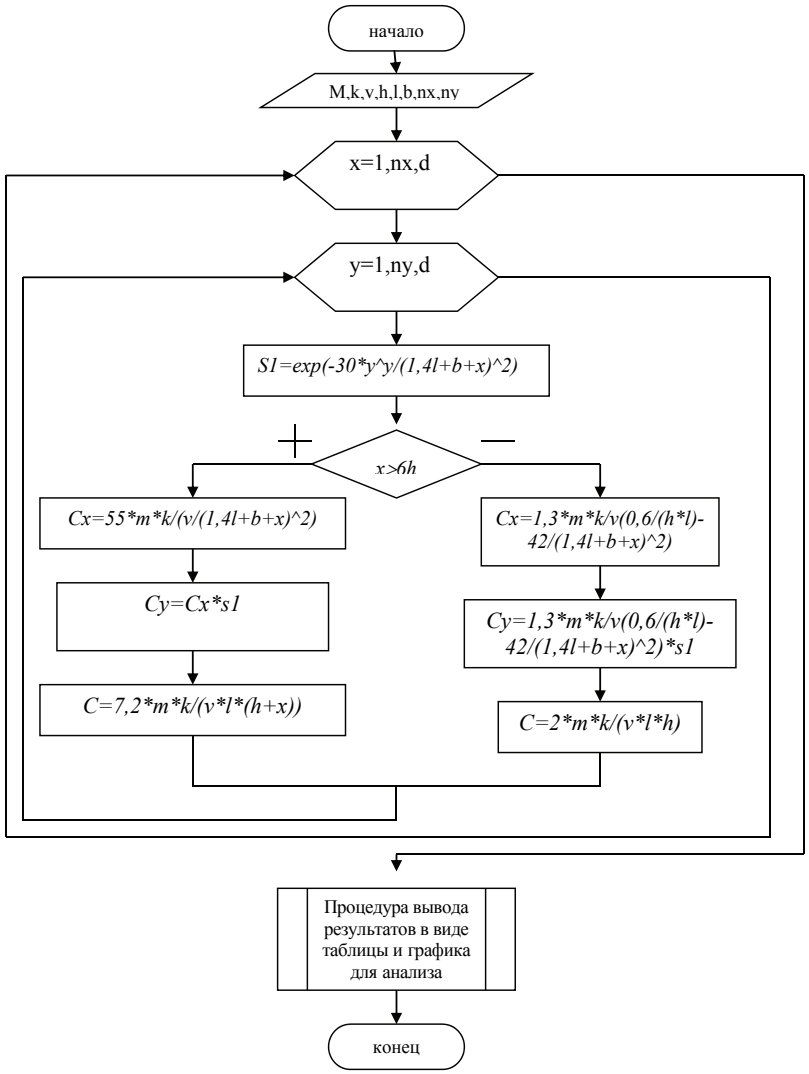


Рисунок 1- Алгоритм в виде блок-схемы для реализации на ЭВМ математической модели загрязнения выбросами нижних слоев атмосферы


```
                spout = readMessage;  }  }
// Синтез речи для выбранного ответа
                tts.speak(spout, TextToSpeech.QUEUE_ADD, params);
            }       } break; } }
```

4. Объявляем класс utteranceProgressListener, наследуемый от класса UtteranceProgressListener. Он необходим для выполнения действий после прослушивания результата синтеза речи. Выше было отмечено, что Активити распознавания речи должно запускаться автоматически после произнесенной синтезатором речи фразы до тех пор, пока не встретятся голосовая команда "конец связи". Этот класс содержит необходимый нам метод, который выполняется после завершения звука динамиком, сгенерированным синтезатором.

```
  public class utteranceProgressListener extends UtteranceProgressListener {
    @Override
    public void onDone(String utteranceId) { // Действия после окончания
  //речи синтезатором
      r19 = sp.compareTo(sp19);
      if(r19 != 0) spi(); // Если не "конец связи", то активити
//распознавания голоса запускается вновь
      else  { if(upbluetooth==0) {  // Если Bluetooth включен
        // и если произнесено "конец связи" - останавливаю таймер
        time.cancel(); time.purge();
// и запускаю таймер работы программы с новыми начальными данными
// (без посылки запроса температуры но с приемом температуры)
        bluecancel = 1;  time = new Timer();
        bluetoothInOut bInOut = new bluetoothInOut();
        time.schedule(bInOut,500,1000);  } } }
    @Override
    public void onStart(String utteranceId) { }
    @Override
    public void onError(String utteranceId) { txtText.setText("Error"); } }
```

5. Метод bluet используется для подключения bluetooth устройства Ардино с заданным адресом. Чтение температуры с Ардуино выполняется раз в одну секунду с помощью классов Timer и TimerTask.

```
  public void bluet() { // Подключение к bluetooth
Intent enableBt = new Intent(BluetoothAdapter.ACTION_REQUEST_ENABLE);
enableBt.addFlags(Intent.FLAG_ACTIVITY_NEW_TASK);startActivity(enableBt);
    // Используется bluetooth по умолчанию
    BluetoothAdapter bluetooth = BluetoothAdapter.getDefaultAdapter();
    try { // Выбираем bluetooth с конкретным адресом для простоты
BluetoothDevice device = bluetooth.getRemoteDevice("98:D3:31:B0:86:16");
// Создание RFCOMM секретного socket для входящих и исходящих сообщений
      clientSocket = device.createRfcommSocketToServiceRecord(uuid);
```

```
        // Попытка подключения к удаленному bluetooth
        clientSocket.connect();
        // Если попытка удалась, выводится сообщение внизу экрана
        Toast.makeText(getApplicationContext(), "Связь с bluetooth установлена",
        Toast.LENGTH_LONG).show();
        upbluetooth=0;     time = new Timer();
       bluetoothInOut bInOut = new bluetoothInOut();
        time.schedule(bInOut,500,1000);  //Через 500 миллисекунд после
// запуска программы начинать
        // запрашивать температуру каждую секунду
}
```

6. Класс bluetoothInOut, который наследуется от класса TimerTask необходим для запроса температуры с Ардуино один раз в секунду.

```
public class bluetoothInOut extends TimerTask {
      public void run() {
         try {
  if( bluecancel == 0 ) //Только в этом случае посылаем запрос температуры
 {OutputStream outStream = clientSocket.getOutputStream();  outStream.write(54);}
            // Получаем входной поток для приема данных
            InputStream inb = clientSocket.getInputStream();
            // Преобразование входного потока от bluetooth в строку
            DataInputStream in = new DataInputStream(inb);  bytes = in.read(buffer);
  if (bytes > 10 )  // Если через bluetooth получено (например) больше 10 байт, то
        { // преобразуем байты в строку с нулевого индекса до индекса bytes
             readMessage = new String(buffer, 0, bytes); }
        } catch (IOException e) { } }   }
```

Необходимо подчеркнуть следующие особенности работы программы.

1. Перед запуском синтезатора речи необходима его инициализация. Для этого основной класс MainActivity создается с использованием интерфейса TextToSpeech.OnInitListener. При инициализации используется метод onInit(int status).

2. Для работы метода onDone класса utteranceProgressListener, который следит за окончанием генерации динамиком звука синтеза речи, необходимо описание хеш карты для хранения ключа в params. При инициализации синтезатора необходимо выполнить передачу ключа с помощью метода params.put(TextToSpeech.Engine.KEY_PARAM_UTTERANCE_ID,» HELLO»). Необходимо также установить слушатель синтеза речи tts.setOnUtteranceProgressListener(new utteranceProgressListener());

3. Чтение температуры с Ардуино выполняется раз в одну секунду с помощью классов Timer и TimerTask, которые выполняют запуск задачи в определенное время в будущем через определенные интервалы(500 и 1000 миллисекунд соответственно по программе). Попытка организации запроса температуры с по-

мый элемент, находим элемент a_1 на этой строке. Далее по столбцу, где расположен элемент a_1, поднимаемся вверх по столбцу и элемент, стоящий по главной строке, является обратным элементом к данному элементу.

По этому алгоритму обратным элемент к элементу a_2 будет элемент a_3. Таким образом, доказано, что множество образует группу.

Литература:

1. Кострикин А.И. Введение в алгебру. Основы алгебры. М.: МЦНМО, 2012.

Заурбекова Г.Н. – магистрант

Казахский национальный университет имени аль-Фараби, Алматы, Республика Казахстан

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ЗАГРЯЗНЕНИЯ АТМОСФЕРЫ НЕФТЯНОЙ ПРОМЫШЛЕННОСТЬЮ И АНАЛИЗ РЕЗУЛЬТАТОВ

Как известно, состояние атмосферного воздуха играет огромный роль в воздействии на окружающую среду и здоровья человека. Поэтому нахождение закономерностей распространения загрязняющих примесей в атмосфере и их особенностей является важнейшей задачей в исследованиях процесса загрязнения атмосферного воздуха. Решение данной проблемы представляет определенные трудности [1-10].

Для решения данной проблемы эффективно и экономически выгодно необходимо использовать математические методы исследования распространения вредных примесей в атмосфере. Применение натурных, промышленных и полу промышленных исследовании очень дорогие, а ставить эксперименты практически невозможно. Применение удачно выбранной математической модели и численного алгоритма его решения достичь желаемого результата. Предложенные нами математические модели могут решить широкий класс задач, возникающих при математическом моделировании загрязнения атмосферы с учетом свойств поверхности земли и загрязнения воздушного бассейна.

Целью данной статьи является разработка оптимального алгоритма и численной реализации данной проблемы. Известно, что метод математического моделирования загрязнения атмосферы и переноса примесей дает возможность проверки результатов моделирования в дальнейшем путем сопоставления с фактическими данными.

Алгоритм моделирования распространения загрязняющих примесей в атмосфере нефть и газодобывающего месторождения был реализован в виде программы (рис. 1).

При этом необходимо учесть, что нами взяты следующие масштабы:

в системе $X'Y'Z'$ – 2500 м х 2500 м х 200 м.

в системе XYZ – 25 км х 25 км х 0,2 км.

Входные информации, необходимые для математической модели приведены в таблице 1.

$a_1 \cdot a_1 1 = (a(1\&2\&3@1\&2\&3)) \cdot (a(1\&2\&3@1\&2\&3)) = (a(1\&2\&3@1\&2\&3)) = a_1 1;\ a_1 1 \cdot a_1 2 = (\blacksquare(1\&2\&3@1\&2\&3)) \cdot (a(1\&2\&3@2\&3\&1)) = (a(1\&2\&3@2\&3\&1)) = a_1 2; \ldots ;\ a_1 6 \cdot a_1 1 = (a(1\&2\&3$

Теперь вычисленные значения произведения элементов множества подстановок S_3 внесем в таблицу умножения элементов множества S_3:

·	a_1	a_2	a_3	a_4	a_5	a_6
a_1	a_1	a_2	a_3	a_4	a_5	a_6
a_2	a_2	a_3	a_1	a_5	a_6	a_4
a_3	a_3	a_1	a_2	a_6	a_4	a_5
a_4	a_4	a_6	a_5	a_1	a_3	a_2
a_5	a_5	a_4	a_6	a_2	a_1	a_3
a_6	a_6	a_5	a_4	a_3	a_2	a_1

Таблицы такого вида называют таблицей Кэли. Первая строка и первый столбец таблицы называются соответственно главной строкой и главным столбцом. Все элементы, находящиеся ниже главной строки и правее от главного столбца, представляет собой квадрат. Элементы, расположенные в каждой строке и в каждом столбце квадрата, разные. Такой квадрат называют латинским. Это означает, что введенная операция умножения подстановок замкнута на множестве S_3.

В качестве примера группы покажем, что множество S_3 образует группу.

Теорема. Множество S_3 относительно умножения подстановок образует группу.

Доказательство. Проверим выполнимость условий определения группы.

1. Ассоциативность умножения подстановок из S_3, т.е. равенство

$$(a_i \cdot a_j) \cdot a_k = a_i \cdot (a_j \cdot a_k), \qquad i,j,k = 1,2,3$$

следует из таблицы. Например, если $i = 1, j = 2, k = 3$, то

$$(a_1 \cdot a_2) \cdot a_3 = a_1 \cdot (a_2 \cdot a_3). \tag{2}$$

Действительно, согласно таблице левая часть (2) имеет вид

$$(a_1 \cdot a_2) \cdot a_3 = a_2 \cdot a_3 = a_1. \tag{3}$$

Теперь рассмотрим правую часть (2). По таблице видно, что

$$a_1 \cdot (a_2 \cdot a_3) = a_1 \cdot a_1 = a_1. \tag{4}$$

Правые части равенств (3) и (4) равны между собой, тогда равны и их левые части.

2. Из первой строки и из первого столбца латинского квадрата видно, что существует элемент $a_1 \in S_3$, что для любых $a_i \in S_3$ $a_1 \cdot a_i = a_i \cdot a_1 = a_i, \qquad i = 1,2,3,4,5,6.$

3. Для того, чтобы найти обратный элемент к данному элементу, берем элемент из главного столбца, далее идем по строке, где расположен рассматривае-

следующим ее чтением в основном потоке Thread приводит к тому, что для получения текущего значения температуры необходим ее повторный запрос. Т.е. для получения правильного текущего значения температуры необходимо два раза сказать: «температура». Использование отдельного потока Thread с классом Handler работает правильно но приводит к ошибочной передаче кириллицы. Латиница передается верно, как это представлено в работе[6]. Поэтому здесь использовался способ чтения температуры с одновременным ее запросом с Андроид каждую секунду в переменную readMessage, которая доступна в любой момент синтезатору голоса. При команде «температура» ее значение берется из строки readMessage и синтезируется синтезатором.

Текст программы на языке Java с файлом разметки и манифестом для Android Studio 1.0.1. представлен в источнике [4]. Видео – ролик работы разработанной здесь системы представлен в источнике [3].

На рисунке 3. показана схема подключения к Arduino UNO устройства связи Bluetooth HC-05, датчика температуры DS18B20 и трех светодиодов красного, зеленого и синего цвета (альтернатива трем исполнительным механизмам, например свет, телевизор и кондиционер).

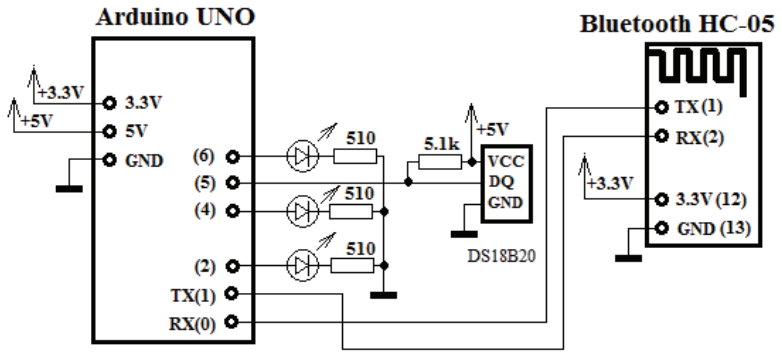


Рис.3. Схема подключения устройств к Ардуино

Программа для Ардуино написана в стандартной среде разработки Ардуино[5]:

```
#include <OneWire.h>   //Подключаем описание библиотеки шины OneWire
#include <DallasTemperature.h> //Подключаем описание библиотеки для определения температуры(DS18B20)
#define ONE_WIRE_BUS 5 //Датчик температуры подключен к 5-му выводу
char inByte;  // входящие данные
int  RED = 2;     // RED подключен к 2 выводу
int  GR = 4;      // GREEN подключен к 4 выводу
```

```
int  BL = 6;       // BLUE подключен к 6 выводу
OneWire oneWire(ONE_WIRE_BUS);   //Настройка шины 1wire для работы с 5-м
// выводом Ардуино
DallasTemperature sensors(&oneWire);  // Подключаем датчик температуры
void setup() {
  Serial.begin(9600); // инициализация порта
  sensors.begin();       //Инициализация датчика температуры DS18B20
  pinMode(RED, OUTPUT);  //Установка 2-го вывода на выход
  pinMode(GR, OUTPUT);     //Установка 4-го вывода на выход
  pinMode(BL, OUTPUT);     //Установка 6-го вывода на выход
  sensors.requestTemperatures(); // Запрос температуры
  int temp=sensors.getTempCByIndex(0); // Получение температуры с нулевого
// датчика
}
void loop() {
  if (Serial.available() > 0) {  //если пришли данные от Bluetooth на
//последовательный порт
    inByte = Serial.read(); // то считываем байт
    if(inByte == '0') {   digitalWrite(RED, LOW);  // если 0, то выключаем RED}
    if(inByte == '1') {  digitalWrite(RED, HIGH); // если 1, то включаем RED}
    if(inByte == '2') {  digitalWrite(GR, LOW);  // если 2, то выключаем GREEN}
    if(inByte == '3') {  digitalWrite(GR, HIGH); // если 3, то включаем GREEN  }
    if(inByte == '4') {  digitalWrite(BL, LOW);  // если 4, то выключаем BLUE  }
    if(inByte == '5') {  digitalWrite(BL, HIGH); // если 5, то включаем BLUE    }
    if(inByte == '6') {    // если 6, то считываем температуру
// и посылаем ее на bluetooth
    sensors.requestTemperatures(); int temp=sensors.getTempCByIndex(0);
     Serial.print("Температура, ");Serial.print(temp);  Serial.print("  ");       }}}
```

Выводы.

1.Разработаны программы для смартфонов и планшетов на ОС Андроид и Ардуино , позволяющие выполнять голосовое управление устройствами, подключенными к Ардуино. Здесь используется инструментарий Google для распознавания и синтеза речи. Причем повторный запуск Активити распознавания выполняется в цикле после окончания генерации звука благодаря использования класса UtteranceProgressListener.

2. Представлена схема подключения к Ардуино устройств, которыми выполняется голосовое управление.

3.Следует отметить высокое качество распознавания произнесенных фраз при работе с серверами Google через Интернет и более низкое при работе с библиотекой речевого поиска Google в режиме offline, если мобильное устройство поддерживает этот режим.

Батыров Б.Е.
к.ф.-м.н., доцент
Северо-Казахстанский государственный университет им М. Козыбаева,
Республика Казахстан

О ГРУППЕ ПОДСТАНОВОК

Известно, что теория групп является основным разделом общей алгебры. В математической литературе эта теория достаточно глубоко разработана. В учебниках по общей алгебре для студентов математических и технических специальностей наряду с описанием теории групп приводятся примеры групп [1]. В качестве основного множества в таких примерах рассматривались числовые множества с обычными операциями сложения или умножения. Изучаются и примеры, носящие прикладной характер. Одним из таких примеров является группа подстановок S_n. Но в таких примерах редко рассматриваются их подробное доказательство.

Целью настоящей работы является изучение группы подстановок S_n на примере множества S_3.

Обозначим через M множество, состоящее n из первых натуральных чисел, т.е. $M = \{1,2,\cdots,n\}$.

Подстановкой множества состоящего из n первых натуральных чисел, называется взаимно-однозначное отображение множества M на себя. Число n в этом случае называется порядком подстановки.

Подстановки будем записывать в виде таблицы, состоящей из двух строк и n столбцов следующим образом:

$$\varphi = \begin{pmatrix} 1 & 2 \cdots & n \\ \varphi(1) & \varphi(2) \cdots & \varphi(n) \end{pmatrix},$$

где $\varphi(i)$ – одно из чисел $1,2,\cdots,n$.

Композиция определяет операцию умножения на перестановках одного порядка.

Относительно этой операции множество подстановок порядка n образует группу, которую называют симметрической и обычно обозначают через S_n. Множество подстановок S_n имеет вид:

$S_n = \{\sigma = (1\ 2\ \cdots\ \varphi\alpha_1\ \alpha_2\ \cdots)(n\ \varphi\alpha_n)\} \mid (\alpha_1, \alpha_2, \cdots, \alpha_n)$ любая перестановка чисел $1,2,\cdots,n\}$

$|S_n| = n!$, т.е. количество подстановок на множестве S_n равно $n!$

Например, если $n = 3$, то $|S_3| = 3! = 6$.

$$S_3 = \left\{ \alpha_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e;\ \alpha_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix};\ \alpha_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix};\ \alpha_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix};\ \alpha_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix};\ \alpha_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}.$$

Построим таблицу умножения для элементов множества .

To date, most of the work to clean up the sound is reduced to getting a sample from the hiss and noise – «hiss,» high-frequency noise. Hiss – even hiss. Noise – a broad term, in fact, the same.

There are two methods of cleaning. The first – the threshold – noise gate, simply filtering. It frequency filtered out. To begin with – all of top, which not clogged sound formants, namely noise.

The second method is that the program is scanned sample of noise, and then the algorithm would be deducted from the noise of the waves.

I had to use the second type of program.

Further it is necessary to amplify the signal and remove noise (filter), using the following algorithm:

```
s:=trunc(s/bit); s1:=trunk (s1/bit)-20;
if abs(s1)<11 then s1:=0;
ss [i+k]:=s1;
form1.Chart4.Series[ng].Add(s); form1.Chart3.Series[ng].Add(s1);
i:=i+bit ;
```

Then select from the signal words and working more with words.

Now we can compare the two voices, a new and already existing in the database.

Find the differences between the two signals. We calculate the percentage of matches, as far as one signal coincides with the other according to the formula:

$$P=100\%-\frac{d1-d2}{\max\{dn\}}*100 \qquad (2)$$

In the Delphi-voice analyzer developed algorithm and program in the language of Code Gear Delphi Architect 2009 can record and compare the audio material to the database. It happens that the anomalous voices defined and recognized relatively easy. In other cases, the ruggedness and the duality of sound does not allow them to identify reliably. In such cases, only the computer analysis can give more data than a regular hearing, unbiased information.

The signal can vary over a wide range of pure and easily analyzed to noisy and not treatable.

Over time, the study of the votes based on computer analysis using a variety of methods of analysis of voice put a solid foundation for accurate identification of people.

REFERENCES

1. Programming in Delphi 7 \ Author: P. Darakhvelidze, Markov
2. Programming in Delphi for Windows \ Author: AY Archangel \ Binom-Press \: 2007
3. Database Programming in Delphi 7. Training \ Author: Valeriy Faronov \ Piter \: 2006

4.При создании библиотеки голосовых команд необходимо подбирать такие команды, которые распознаются с меньшими ошибками. Особенно это относится к режиму offline.

5.Опыт показал, что при создании систем голосового управления для более надежного распознавания и автономности целесообразно использовать технологию распознавания с коротким словарем команд, которая работает всегда в режиме offline.

6.Представленный здесь голосовой интерфейс можно рекомендовать для создания систем простой справочной службы и голосового управления.

Литература.

1. А.В. Фролов Г.В. Фролов. Синтез и распознавание речи. Современные решения. / Интернет-ресурс. – Режим доступа: http://www.frolov-lib.ru/books/hi/index.html. – 2003.

2.Android. / Интернет-ресурс. – Режим доступа: http://developer.android.com/reference/android/package-summary.htm.

3. Андроид и ардуино в задачах голосового управления через Bluetooth. / Интернет-ресурс. – Режим доступа: https://youtu.be/zis9Q8AuxuU

4. Мясищев А.А. Андроид и Ардуино в задачах управления голосом и синтеза речи с использованием Bluetooth. / Интернет-ресурс. – Режим доступа: https://sites.google.com/site/webstm32/8-upravlenie-golosom-s-pomosu-android-i-arduino. – 2015.

5. Arduino. Официальный сайт. [Electronic resource]. – Mode of access: http://arduino.cc , 2014.

6. Передача данных по Bluetooth между Android и Arduino. / Интернет-ресурс. – Режим доступа: http://cxem.net/arduino/arduino64.php. – 2012.

VÝPOČETNÍ TECHNIKA A PROGRAMOVÁNÍ

Гудков К.С.
Государственный научно-исследовательский институт авиационных систем,
Московский физико-технический институт

СРАВНЕНИЕ МЕТОДОВ РЕАЛИЗАЦИИ АГРЕГАТНОЙ ФУНКЦИИ ПРОИЗВЕДЕНИЯ ЧИСЕЛ В СУБД MS SQL SERVER

В СУБД Microsoft SQL Server 2014 (и в более ранних версиях) отсутствует агрегатная функция для вычисления произведения чисел [1]. Она может оказаться полезной, например, для вычисления среднего геометрического чисел.

Существует несколько традиционных подходов для вычисления произведения чисел в СУБД Microsoft SQL Server:

- Реализация пользовательской агрегатной функции среды CLR.
- Математический метод, базирующийся на факте, что логарифм произведения равен сумме логарифмов.
- Метод, основанный на присваивании переменной внутри SELECT.
- Метод, основанный на использовании курсоров.
- Метод, основанный на использовании рекурсивных обобщённых табличных выражений (Common Table Expressions, CTE).

Для сравнения производительности была сгенерирована таблица из 100 тысяч записей, случайным образом разбитая на группы с небольшим числом перемножаемых чисел, среди которых встречаются и положительные, и отрицательные, и ноль. Задача состояла в вычислении произведения всех чисел для каждой из групп по отдельности. Сценарий по созданию таблицы выглядит следующим образом:

```
if (object_id('RandomIntNumbers') is not null)
  drop table RandomIntNumbers
create table RandomIntNumbers(ID int primary key, RandGroupID int, RandInt int)
```

Для заполнения таблицы использовались обобщённые табличные выражения:

```
;with CTERandomIntNumbers(ID, RandGroupID, RandInt) as
(
  select 1 as ID,
    abs(cast(cast(newid() as Binary(4)) as int)) % 60000 as RandGroupID,
    cast(cast(newid() as Binary(4)) as int) % 10 as RandInt

  union all

  select ID + 1 as ID,
    abs(cast(cast(newid() as binary(4)) as int) % 60000) as RandGroupID,
    cast(cast(newid() as binary(4)) as int) % 10 as RandInt
```


from a given, limited list of people. Currently, the system of identification and verification of voice are becoming increasingly popular around the world. This is primarily due to natural and habitual speech interaction between man and computer system.

To analyze voice signals necessary:

- Get a voice signal,
- Improve signal (to remove noise)
- Highlight words
- Compare the received signal to the database,
- Find the percentage of matches.

For voice signal algorithm that allows you to record sound from a microphone.

To record a sound, first set the buffer size «BufSize: = TrackBar1.Position * 500 + 100» and then the following parameters sampling: «wFormatTag: = WAVE_FORMAT_PCM, nChannels: = 1 (1 mono 2 – stereo) – the number of channels, frequency, equal to 44100 (8000 possible values, 11025. 22050 and 44100). and bit rate equal to 16 bits, leveling blocks «nBlockAlign: = nChannels * (wBitsPerSample div 8)» The number of bytes per second. For this is the result WAVE_FORMAT_PCM nSamplesPerSec * nBlockAlign.

Then open the audio device «WaveInOpen (Addr (WaveIn), WAVE_MAPPER, addr (header), Form1.Handle, 0,» set to the length of the buffer, its name, and load data into it.

Obtained from the microphone signal to be processed by a Fourier transform obtain spectrum.

The Fourier Transform – a mathematical process that allows us to take the time (seismic trace) and express it as a function of frequency (spectrum) of the formula:

$$f(p) = \int_{q=-\infty}^{+\infty} F(q) e^{2mpq}\, dq \qquad (1)$$

But it is quite complicated and therefore has been used «Fast Fourier Transform». The resulting range of 4 seconds output using TChart screen.

Figure 1. The window program (Voice Recording). Recording from a microphone and receiving range of sound.

2. Элементы исследования операций: учебное пособие / Е.Г. Давыдов. – М.: КНОРУС, 2013. – 158 с.

3. Исследование операций в экономике: Учебное пособие для вузов / Н.Ш. Кремер, Б.А. Бутко, И.М. Тришин, М.Н. Фридман; Под ред. проф. Н.Ш. Кремера. – М.: Банки и биржи, ЮНИТИ, 1997. – 407 с.

4. Математика в экономике: математические методы и модели: учебник для бакалавров / М.С. Чупрынов; под ред. М.С. Красса. – 2-ое изд., испр. и доп. – М.: Издательство Юрайт, 2013. – 541 с. – Серия: Бакалавр. Базовый курс.

Ph.D., Professor Abdimomynova M., Master IS Doumcharieva Zh., Master INF Aitbaeva Z.
Taraz State University, Kazakhstan

COMPUTER AND MATHEMATICAL MODELING OF TWO VOICE SIGNALS

In today's world, more often interested in speech technologies, in particular, identification by voice. This is due, on the one hand, the advent of high-performance computing systems based on personal computers and hardware, allowing to make the input signal to the computer, and, on the other hand, a high demand authentication systems in different fields of human activity. This method is easy to use.

Today is the time – when developing new technologies. On the streets in the stores set the camcorder. They allow you to record not only video but also audio. For example: a person walking down the street talking and the sound of the camcorder is writing gave him a computer and he analyzed his voice was checked for a match on the database. When you need to determine the identity of a specific person voice, the program will compare the spectra of a few words and give the probability of a match. Precise identification of the person is an important element in various situations, for example in law, criminology, legal paperwork, and many other areas.

Study of the problem analysis of two voice signals can be successfully applied in forensic science, case management, at security checkpoints to restrict the admission and finding people for various emergencies such as plane crashes, based on the records of talks can be restored setting and a picture of the incident, to determine who speaks a particular phrase. Moreover, the voice may be approximately appearance (appearance) portrait telephone blackmailers, terrorists and other criminals. In modern jurisprudence voice can serve as a clear piece of evidence in court. The aim is to create a program capable to analyze the human voice with a record from the database.

One of the challenges in the field of speech technology is to determine which person corresponds to a particular speech signal. System solves this problem fall into two broad classes – the system of verification and identification. Verification – a procedure to confirm the identity of the speaker, and the identification – determination of the individual


```
  from CTERandomIntNumbers
  where ID < 100000
)

insert into RandomIntNumbers(ID, RandGroupID, RandInt)
  select ID, RandGroupID, RandInt
  from CTERandomIntNumbers
       option(maxrecursion 0)
```

Для замера времени работы сценария были созданы две переменные типа datetime: @BeginTime и @EndTime. Переменная @BeginTime инициализировались в начале выполнения запроса, а переменная @EndTime инициализировалась в конце выполнения запроса. Для их инициализации использовалась функция getdate(). Суммарное время работы вычислялось при помощи: select datediff(millisecond, @BeginTime, @EndTime).

Лучшие результаты с точки зрения скорости работы были показаны при помощи CLR. Среднее время работы данного метода составило 413 миллисекунд. Данный метод универсален, то есть пользовательская агрегатная функция среды CLR работает для любой таблицы. Для реализации агрегата необходимо реализовать 4 стандартных метода Init, Accumulate, Merge и Terminate. Кроме того, необходимо создать 2 объекта SQL-сервера: сборку (assembly) и непосредственно агрегатную функцию (aggregate). Примеры реализации агрегатных функций CLR показаны, например, здесь [2].

На втором месте с точки зрения скорости работы оказался математический метод:

```
select RandGroupID, round(exp(sum(log(case when RandInt <> 0 then abs(RandInt)
else 1 end))) *
  case when sum(case when RandInt < 0 then 1 else 0 end) % 2 = 1 then -1 else 1
end *
  case when sum(case when RandInt = 0 then 1 else 0 end) > 0 then 0 else 1 end,
0) as Product
from RandomIntNumbers
group by RandGroupID
```

Среднее время работы данного метода составило 513 миллисекунд.

Конструкция «CASE WHEN THEN ELSE END» была необходима, чтобы решить проблему отрицательных чисел и нуля. Среди недостатков этого метода можно указать отсутствие гарантии корректной работы, вызванное присутствием ошибок округлений, способных привести к неправильному результату.

Третьи результаты показал метод, основанный на присваивании переменной внутри SELECT. Для его работы необходимо создать скалярную функцию SQL.

```
if (object_id('SQLProduct') is not null)
  drop function SQLProduct
go

create function SQLProduct(@RandGroupID int)
```

```
returns int
begin
  declare @ProdVar as int
  set @ProdVar = 1

  select @ProdVar = @ProdVar * RandInt
  from RandomIntNumbers RIN
  where RandGroupID = @RandGroupID

  return @ProdVar
end
```

Кроме того, как видно из устройства функции SQLProduct, для быстрой работы необходимо также создать некластерный индекс по полю RandGroupID. Среднее время работы данного метода составило 1380 миллисекунд. Перечислим недостатки метода, основанного на присваивании переменной внутри SELECT:

- Необходимость создания скалярной функции для каждой из таблиц, в которых необходимо вычислить произведение чисел.
- Необходимость создания некластерного индекса по идентификатору группы. Без него среднее время работы метода составило 8 минут.
- Отсутствие гарантии корректной работы, которое можно продемонстрировать на простейшем примере:

```
declare @TestTable as table(ID int)

insert into @TestTable(ID) values(2)
insert into @TestTable(ID) values(4)

declare @TestVar as int
set @TestVar = 1

select @TestVar = @TestVar * ID
from @TestTable
order by ID * ID

select @TestVar
```

Переменная @TestVar будет содержать 4 вместо ожидаемых 8.

Четвертые результаты показал метод, основанный на стандартном использовании курсоров. Среднее время его работы 4040 миллисекунд.

Последнее место с точки зрения скорости работы показал метод, основанный на использовании рекурсивных обобщённых табличных выражений. На описанных в рамках статьи данных метод не закончил работу в течении часа.

Таким образом, метод, основанный на присваивании переменной внутри SELECT, и математический метод не гарантируют корректность результата. Методы, основанные на обобщённых табличных выражениях и курсорах, работают слишком медленно по сравнению с методом, основанным на реализации пользовательской агрегатной функции среды CLR. Поэтому именно этот метод и является лучшим для вычисления произведения чисел в Microsoft SQL Server.

$$f_3(150) = \max \begin{cases} s_3(0) + f_2(150) = 0 + 100 = 100 \\ s_3(50) + f_2(100) = 36 + 70 = 106 \\ s_3(100) + f_2(50) = 64 + 30 = 94 \\ s_3(150) + f_2(0) = 95 + 0 = 95 \end{cases} = 106,$$

При x=200

$$f_3(200) = \max \begin{cases} s_3(0) + f_2(200) = 0 + 140 = 140 \\ s_3(50) + f_2(150) = 36 + 100 = 136 \\ s_3(100) + f_2(100) = 64 + 70 = 134 \\ s_3(150) + f_2(50) = 95 + 30 = 125 \\ s_3(200) + f_2(0) = 130 + 0 = 130 \end{cases} = 140.$$

4-й этап. Инвестиции в объеме 200 млн. тенге распределяем между 3-м этапом и четвертой компанией.

Получим

при x=200

$$f_4(200) = \max \begin{cases} s_4(0) + f_3(200) = 0 + 140 = 140 \\ s_4(50) + f_3(150) = 28 + 106 = 134 \\ s_4(100) + f_3(100) = 56 + 70 = 126 \\ s_4(150) + f_3(50) = 110 + 36 = 146 \\ s_4(200) + f_3(0) = 142 + 0 = 142 \end{cases} = 146.$$

Возвращаемся от 4-го этапа к 1-му.

Максимальный прирост выпуска продукции в 146 млн. тенге получен на 4-м этапе как

$f_4(200) = 146 = 110 + 36 = s_4(150) + f_3(50)$.

Т.е. 110 млн. тенге соответствует выделению 150 млн. тенге 4-ой компании (это означает, что из данных 150 млн. тг используется только 110 млн. тг).

Согласно 3-му этапу 36 млн. тенге получено следующим образом:

$f_3(50) = 36 = 36 + 0 = s_3(50) + f_2(0)$.

Т.е. 36 млн. тенге соответствует выделению 50 млн. тенге третьей компании.

Согласно 2-му этапу 0 млн. тенге получено при выделении 0 млн. тенге 2-ой компании. Т.е. $f_2(0) = s_2(0)$.

Таким образом, на основании данного решения руководству предприятия необходимо распределить вложения в объеме 200 млн. тг между четырьмя дочерними компаниями следующим образом:

- третьей – 36 млн. тенге;
- четвертой – 110 млн. тг (т.е. в первую и во вторую компанию лучше не вкладывать инвестиции);
- неиспользованными средствами останутся 54 млн. тг,
- прирост продукции будет максимальным и составит 146 млн. тенге.

Литература

1. Экономико-математические методы и модели: учебник для бакалавров / А.М. Попов, В.Н. Сотников; под ред. проф. А.М. Попова. – М.: Издательство Юрайт, 2011. – 479 с. – Серия; Бакалавр.

Решение:

Вначале разобьем решение задачи на 4 этапа по количеству компаний, в которые предполагается осуществить инвестиции.

1-й этап. Для первой компании уравнение Беллмана будет иметь вид $f_1(x) = s_1(x_1)$.

Т.е. нвестиции производим только первой компании. Тогда

$f_1(50) = 25$, $f_1(100) = 60$, $f_1(150) = 100$, $f_1(200) = 140$.

2-й этап. Инвестиции выделяем первой и второй компаниям. Рекуррентное соотношение для этого этапа имеет вид

$$f_2(x) = \max\{s_2(x_2) + f_1(x - x_2)\}.$$

Тогда $f_2(0) = 0$

при x=50

$$f_2(50) = \max\begin{Bmatrix} s_2(0) + f_1(50) = 0 + 25 = 25 \\ s_2(50) + f_1(0) = 30 + 0 = 30 \end{Bmatrix} = 30,$$

при x=100

$$f_2(100) = \max\begin{Bmatrix} s_2(0) + f_1(100) = 0 + 60 = 60 \\ s_2(50) + f_1(50) = 30 + 25 = 55 \\ s_2(100) + f_1(0) = 70 + 0 = 70 \end{Bmatrix} = 70,$$

при x=150

$$f_2(150) = \max\begin{Bmatrix} s_2(0) + f_1(150) = 0 + 100 = 100 \\ s_2(50) + f_1(100) = 30 + 60 = 96 \\ s_2(100) + f_1(50) = 70 + 25 = 95 \\ s_2(150) + f_1(0) = 90 + 0 = 90 \end{Bmatrix} = 100,$$

при x=200

$$f_2(200) = \max\begin{Bmatrix} s_2(0) + f_1(200) = 0 + 140 = 140 \\ s_2(50) + f_1(150) = 30 + 100 = 140 \\ s_2(100) + f_1(100) = 70 + 60 = 130 \\ s_2(150) + f_1(50) = 90 + 25 = 115 \\ s_2(200) + f_1(0) = 122 + 0 = 122 \end{Bmatrix} = 140.$$

3-й этап. Финансируем 2-й этап и третью компанию, тогда расчеты проводим по формуле

$$f_3(x) = \max\{s_3(x_3) + f_2(x - x_3)\}.$$

Получим

при x=50

$$f_3(50) = \max\begin{Bmatrix} s_3(0) + f_2(50) = 0 + 30 = 30 \\ s_3(50) + f_2(0) = 36 + 0 = 36 \end{Bmatrix} = 36,$$

при x=100

$$f_3(100) = \max\begin{Bmatrix} s_3(0) + f_2(100) = 0 + 70 = 70 \\ s_3(50) + f_2(50) = 36 + 30 = 66 \\ s_3(100) + f_2(0) = 64 + 0 = 64 \end{Bmatrix} = 70,$$

при x=150

Литература:

1. https://msdn.microsoft.com/ru-ru/library/ms173454.aspx
2. https://msdn.microsoft.com/ru-ru/library/ms131056.aspx

Трапезников Е.В.

магистр технических наук

Северо-Казахстанский Государственный университет им. М.Козыбаева

РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ ТРАНСПОРТНОЙ КОМПАНИИ

На современном этапе развития производительных сил и производственных отношений информация стала товаром со всеми присущими ей свойствами. Сегодня существуют информационная промышленность, национальные информационные ресурсы, происходит переход от индустриальной экономики к экономике, основанной на информации. Особенно это актуально для транспорта, как отрасли народного хозяйства.

Новые информационные технологии принесли новые возможности по организации транспортного процесса. Рыночные отношения ликвидировали государственный заказ. Постоянно увеличивается количество транспортных предприятий. Ужесточается конкуренция в перевозке грузов. Что делать? Как увязать новые возможности с новыми условиями игры? Как выжить без помощи государства? Особенно остро эти вопросы встают при организации грузоперевозок в междугородном сообщении. Решение этих вопросов лежит во многих плоскостях. Но есть одна плоскость, которая позволяет существенно приблизится к их решению. Это – информация и единое информационное пространство, а также задача комплексной автоматизации процесса управления транспортно-информационными потоками. До настоящего времени говорить о полноценной системе комплексной автоматизации было преждевременно, но развитие информационных технологий и приход к пониманию необходимости постановки такой задачи ведет к разработке Транспортной аналитической информационной системы, как одного из основных регуляторов системы взаимоотношений между участниками транспортного процесса. На помощь в создании информационных Интернет-сайтов может прийти универсальная технология создания профессионального Интернет-сайта транспортной компании в режиме реального времени. В чем преимущества этой технологии? Во-первых, разработка сайта осуществляется все-таки людьми, а не безадресной программой, что позволяет заказчику лично взаимодействовать с разработчиком. На первый взгляд, кажется, что нет никакого отличия от стандартной технологии разработки Интернет-сайтов, но это не так. Разработчики вступают в действие, когда это только необходимо для доведения сайта до нужного уровня.

Во-вторых, формирование дизайна и функциональность сайта формируется самим заказчиком в режиме реального времени со своего компьютера в течение нескольких минут. Достаточно только выбрать основные элементы из предоставленных каталогов. В-третьих, разработка Интернет-сайта осуществляется за несколько дней, в то время, как стандартная технология разработки сайта предполагает срок в несколько недель, к тому же часто получается таким образом, что заказчик сайта до момента получения готового сайта не видит, что он получит. В-четвертых, низкая трудоемкость разработки сайта, интерактивность в разработке позволяет существенно снизить цену сайта до 200-300 долларов США. Тем не менее, стоит сказать, что набор функций, которые необходимо подключить в функциональную часть сайта, может существенно повысить стоимость разработки сайта, но стоимость даже при этом будет существенно ниже, чем разработка профессионального сайта по стандартной технологии [1].

Проектируемое приложение представлено кнопочным интерфейсом – это интерфейс пользователя с базой данных, он разрабатывается индивидуально для каждого приложения, представляет собой пользовательскую форму, которая содержит все объекты базы. На данной форме располагаются кнопки для работы с данными приложения: бухгалтерия, заказ, «подсчитать расходы», выбор машины. Форма также предназначена для внесения изменения в приложение. В нижнем правом углу располагается кнопка выхода из данного приложения.

Отобразим диаграмму кооперации проектируемой системы, особенность которой заключается в графическом представлении не только последовательности взаимодействия, но и всех структурных отношениий между объектами, участвующими в этом взаимодействии.

На диаграмме в виде прямоугольников изображаются участвующие во взаимодействии объекты, содержащие имя объекта, его класс: выбор варианта заказа, форма деталей заказа, управляющий заказами, заказ, главный менеджер. Далее на диаграмме указываются ассоциации между объектами в виде различных соединительных линий. Между объектами изображаются динамические связи – потоки сообщений – в виде соединительных линий, над которыми располагается стрелка с указанием направления, имени сообщения, порядкового номера в общей последовательности инициализации сообщений.

Анализ решения

Максимальное значение функции цели (доход) $f_3(X) = 0{,}94$ при $x_3=2$. Это значит, в третьем филиале необходимо установить 2 банкомата.

Тогда на остальные два филиала остается 5 – 2 = 3 банкомата. Значение дохода $f_2(X) = 0{,}55$. При этом во 2-ом филиале следует установить 2 банкомата.

Следовательно, на 1-ый филиал остается 3 – 2 = 1 банкомат. При этом доход равен 0,21.

Таким образом, руководству банка необходимо принять следующее оптимальное решение:

– в 1-ом филиале разместить 1 банкомат, доход от него равен 0,21 млн. тг;

– во 2-ом филиале – 2 банкомата, доход от него равен 0,34 млн. тг;

– в 3-ем филиале – 2 банкомата, доход от него равен 0,39 млн. тг.

Суммарный доход от совместной работы 5-ти банкоматов будет равен 0,21+0,34+0,39=0,94 млн. тг за неделю.

Теперь проведем анализ задачи по оптимальному распределению инвестиций между дочерними компаниями предприятия методом динамического программирования.

Задача 2. Общее собрание акционеров промышленного предприятия выдвинуло предложение по наращиванию производственных мощностей с целью увеличения выпуска однородной продукции дочерним компаниям, принадлежащим данному предприятию.

Для реализации данной задачи собрание акционеров поручило выделить средства в объеме 200 млн. тенге с дискретностью 50 млн. тенге, причем в одну компанию можно осуществить только одно вложение. Следует отметить, что прирост выпуска продукции в дочерних компаниях зависит от выделенной суммы, и эти значения представлены компаниями предприятия и содержатся в таблице исходных условий (смотрите таблицу 3).

Таблица 3

Инвестиции, x млн. тенге	Прирост выпуска продукции, млн. тенге			
	Компания №1, $s_1(x_1)$	Компания №2, $s_2(x_2)$	Компания №3, $s_3(x_3)$	Компания №4, $s_4(x_4)$
50	25	30	36	28
100	60	70	64	56
150	100	90	95	110
200	140	122	130	142

Следует разработать план распределения денежных средств между четырьмя дочерними компаниями предприятия, чтобы данный план обеспечивал максимальный прирост выпуска продукции.

При $X=2$

$$f_3(2)=\max_{0\le x_3\le 2}\begin{bmatrix} g_3(0)+f_2(2)\\ g_3(1)+f_2(1)\\ g_3(2)+f_2(0)\end{bmatrix}=\max\begin{pmatrix}\underline{0+0{,}41}\\ 0{,}19+0{,}21\\ 0{,}39+0\end{pmatrix}=0{,}41$$ при $x_3=0$. Запишем значения $f_3(2)$ и x_3 в таблицу решения.

При $X=3$

$$f_3(3)=\max_{0\le x_3\le 3}\begin{bmatrix} g_3(0)+f_2(3)\\ g_3(1)+f_2(2)\\ g_3(2)+f_2(1)\\ g_3(3)+f_2(0)\end{bmatrix}=\max\begin{pmatrix}0+0{,}55\\ \underline{0{,}19+0{,}41}\\ \underline{0{,}39+0{,}21}\\ 0{,}41+0\end{pmatrix}=0{,}6$$ при $x_3=1;2$. Запишем значения $f_3(3)$ и x_3 в таблицу решения.

При $X=4$

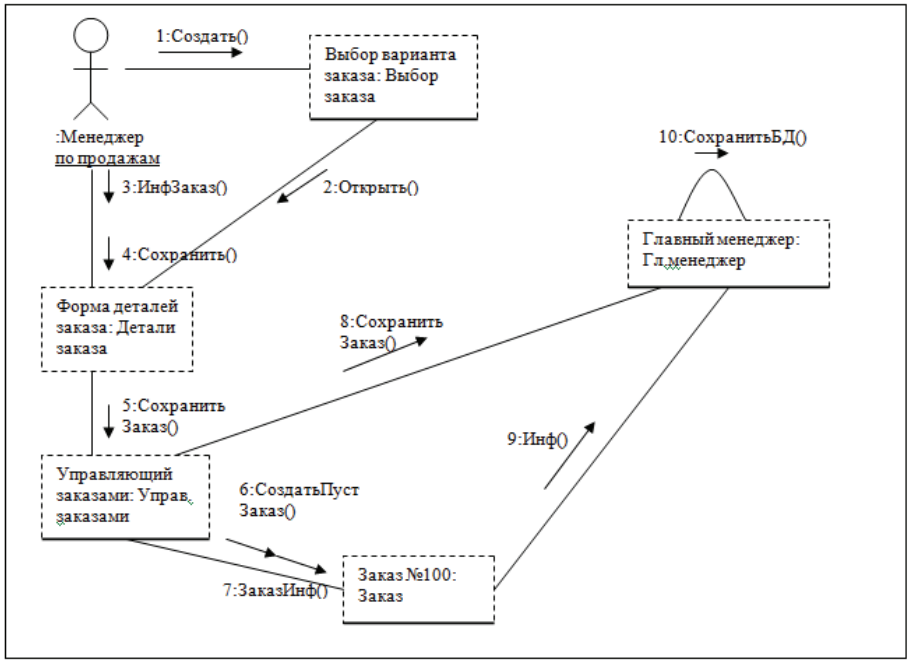
$$f_3(4)=\max_{0\le x_3\le 4}\begin{bmatrix} g_3(0)+f_2(4)\\ g_3(1)+f_2(3)\\ g_3(2)+f_2(2)\\ g_3(3)+f_2(1)\\ g_3(4)+f_2(0)\end{bmatrix}=\max\begin{pmatrix}0+0{,}67\\ 0{,}19+0{,}55\\ \underline{0{,}39+0{,}41}\\ 0{,}41+0{,}21\\ 0{,}53+0\end{pmatrix}=0{,}8$$ при $x_3=2$. Запишем значения $f_3(4)$ и x_3 в таблицу решения.

При $X=5$

$$f_3(5)=\max_{0\le x_3\le 5}\begin{bmatrix} g_3(0)+f_2(5)\\ g_3(1)+f_2(4)\\ g_3(2)+f_2(3)\\ g_3(3)+f_2(2)\\ g_3(4)+f_2(1)\\ g_3(5)+f_2(0)\end{bmatrix}=\max\begin{pmatrix}0+0{,}79\\ 0{,}19+0{,}67\\ \underline{0{,}39+0{,}55}\\ 0{,}41+0{,}41\\ 0{,}53+0{,}21\\ 0{,}64+0\end{pmatrix}=0{,}94$$ при $x_3=2$. Запишем значения $f_3(5)$ и x_3 в таблицу решения (см. таблицу 2).

Таблица 2

X	0	1	2	3	4	5
$f_1(X)$	0	**0,21**	0,33	0,45	0,54	0,66
X_1	0	**1**	2	3	4	5
$f_2(X)$	0	0,21	0,41	**0,55**	0,67	0,79
X_2	0	0	1	**2**	2	2
$f_3(X)$	0	0,21	0,41	0,6	0,8	**0,94**
X_3		0	0	1, 2	2	**2**
Составлено авторами на основе расчетных показателей задачи 1 с учетом данных таблицы 1						



Литература:

1. Интернет- ресурс «Информационные системы на рынке грузоперевозок»/: www.gruztraf.ru/gruzoperevozki20.php.

Трапезников Е.В.
магистр технических наук
Северо-Казахстанский государственный университет им. М. Козыбаева

РАЗРАБОТКА WEB-САЙТА ДЛЯ ТОО «KAZINSTALLCOMPANY»

ТОО «KazInstallCompany» занимается заправкой картриджей и ремонтом оргтехники. Предприятие оказывает высокий сервис обслуживания (выезжает к клиентам, картриджи после заправки проверяет на своих тестовых принтерах, на время заправки предоставляет сменные картриджи, на время ремонта оргтехники

– сменную оргтехнику) невысокой аренды и менее дорогостоящей рабочей силы, успешно конкурируем с другими аналогичными фирмами.

Контекстная диаграмма процесса обработки заказа на web-сайте, дает предпосылку к ее декомпозиции и уточнению всего процесса.

В соответствии с рисунком 1 приведена декомпозиция контекстной диаграммы первого уровня для процесса обработки заказа на web-сайте.

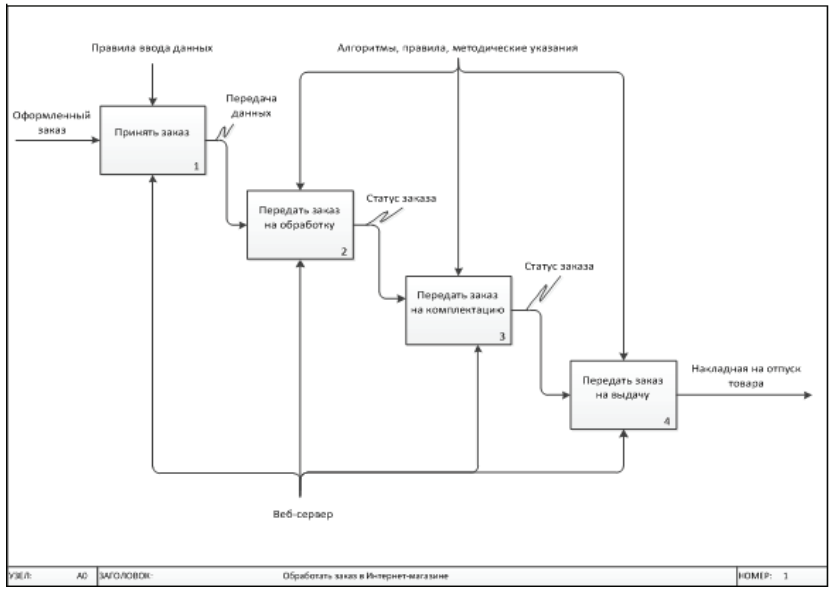


Рисунок 1 Диаграмма декомпозиции первого уровня

Согласно диаграмме, оформленный заказ передается системой на обработку, где проверяется на оплату и наличие товара на складе. В случае, если все условия обработки заказа соблюдены, заказ передается на комплектацию. После комплектации, заказ передается на выдачу. Результатом всей операции может быть накладная на выдачу запасов на сторону или уведомление об аннулировании заказа.

В соответствии с рисунком 2 представлена диаграмма декомпозиции второго уровня для операции передачи заказа на обработку. Декомпозиция второго уровня позволит более детально изучить операцию обработки заказа web-сайтом, что в последствии, поможет разработать правильно функционирующее приложение.

На диаграмме декомпозиции второго уровня для операции обработки заказа изображено четыре последовательных блока действия:

– «Проверить оплату товара» – это действие отвечает за проверку поступления денежных средств от покупателя за выбранный на web-сайте товар. На вход данного блока поступает заполненная пользователем форма заказа.

$$f_2(1)=\max_{0\le x_2\le 1}\begin{bmatrix} g_2(0)+f_1(1)\\ g_2(1)+f_1(0)\end{bmatrix}=\max\begin{pmatrix}0+0{,}21\\ 0{,}2+0\end{pmatrix}=0{,}21.$$

Нужно обратить внимание на то, что значение **0,21** было получено при сумме $g_2(0)$ и $f_1(1-0)$, т.е. при $x_2=0$. Запишем значения $f_2(1)$ и x_2 в таблицу решения.

При $X=2$

$$f_2(2)=\max_{0\le x_2\le 2}\begin{bmatrix} g_2(0)+f_1(2)\\ g_2(1)+f_1(1)\\ g_2(2)+f_1(0)\end{bmatrix}=\max\begin{pmatrix}0+0{,}33\\ 0{,}2+0{,}21\\ 0{,}34+0\end{pmatrix}=0{,}41$$ при $x_2=1$. Запишем значения $f_2(2)$ и x_2 в таблицу решения.

При $X=3$

$$f_2(3)=\max_{0\le x_2\le 3}\begin{bmatrix} g_2(0)+f_1(3)\\ g_2(1)+f_1(2)\\ g_2(2)+f_1(1)\\ g_2(3)+f_1(0)\end{bmatrix}=\max\begin{pmatrix}0+0{,}45\\ 0{,}2+0{,}33\\ 0{,}34+0{,}21\\ 0{,}39+0\end{pmatrix}=0{,}55$$ при $x_2=2$. Запишем значения $f_2(3)$ и x_2 в таблицу решения.

При $X=4$

$$f_2(4)=\max_{0\le x_2\le 4}\begin{bmatrix} g_2(0)+f_1(4)\\ g_2(1)+f_1(3)\\ g_2(2)+f_1(2)\\ g_2(3)+f_1(1)\\ g_2(4)+f_1(0)\end{bmatrix}=\max\begin{pmatrix}0+0{,}54\\ 0{,}2+0{,}45\\ 0{,}34+0{,}33\\ 0{,}39+0{,}21\\ 0{,}55+0\end{pmatrix}=0{,}67$$ при $x_2=2$. Запишем значения $f_2(4)$ и x_2 в таблицу решения.

При $X=5$

$$f_2(5)=\max_{0\le x_2\le 5}\begin{bmatrix} g_2(0)+f_1(5)\\ g_2(1)+f_1(4)\\ g_2(2)+f_1(3)\\ g_2(3)+f_1(2)\\ g_2(4)+f_1(1)\\ g_2(5)+f_1(0)\end{bmatrix}=\max\begin{pmatrix}0+0{,}66\\ 0{,}2+0{,}54\\ 0{,}34+0{,}45\\ 0{,}39+0{,}33\\ 0{,}55+0{,}21\\ 0{,}6+0\end{pmatrix}=0{,}79$$ при $x_2=2$. Запишем значения $f_2(5)$ и x_2 в таблицу решения.

3-ий этап. Решение уравнения для $f_3(X)$:

$$f_3(X)=\max_{0\le x_3\le X}[g_3(X_3)+f_2(X-x_3)].$$

В эту формулу подставим вместо X значения 1, 2, 3, 4, 5. Получим:

При $X=1$

$$f_3(1)=\max_{0\le x_3\le 1}\begin{bmatrix} g_3(0)+f_2(1)\\ g_3(1)+f_2(0)\end{bmatrix}=\max\begin{pmatrix}0+0{,}21\\ 0{,}19+0\end{pmatrix}=0{,}21$$ при $x_3=0$. Запишем значения $f_3(1)$ и x_3 в таблицу решения.

шаги. Шагом можно считать, например, какой-то период времени, если мы распределяем ресурсы производственной деятельности на несколько лет. В другом же случае шагом будет, например, номер каждого предприятия, если будет распределение между этими предприятиями определенных средств. В некоторых же других задачах может вводиться искусственно разбивка на шаги. Например, процесс управления происходит непрерывно, и в то же время мы можем его представить в виде дискретного процесса, при этом разбивая условно этот процесс на определенные отрезки (шаги). Для конкретных условий задачи при этом нужно правильно выбирать длину каждого шага таким образом, чтобы было получено более простая задача по оптимизации на каждом конкретном шаге задачи и обеспечивать при этом необходимую точность вычислений [4, стр. 364].

Рассмотрим пример эффективного распределения банкоматов между филиалами банка методом динамического программирования.

Задача 1. Руководство коммерческого банка г. Караганды считает целесообразным распределение 5 банкоматов между тремя филиалами, находящимися в городах Абай, Каркаралинск и Жезказган, и планирует получить за неделю максимальный доход (млн. тг) от их совместного использования. Функции дохода, в зависимости от применяемого количества банкоматов в каждом из трех филиалов, приведены в таблице исходных условий (см. таблицу 1).

Таблица 1

Доход по филиалам банка	Количество банкоматов, X					
	0	1	2	3	4	5
$g_1(X)$	0	0,21	0,33	0,45	0,54	0,66
$g_2(X)$	0	0,20	0,34	0,39	0,55	0,6
$g_3(X)$	0	0,19	0,39	0,41	0,53	0,64

Математическая модель задачи

Определить $f_m(X) = \max_{0 \le x_m \le X} [g_m(X_m) + f_{m-1}(X - x_m)]$

Решение:

На основе рекуррентного уравнения Р. Беллмана рассчитываем значения функций по шагам для $f_1(X)$, $f_2(X)$, $f_3(X)$, изменяя x_1, x_2 и x_3 от 0 до 5.

1-ый этап. Решение для $f_1(X)$ очевидное, т.е. $f_1(X) = g_1(X)$. Заносим эти значения в новую таблицу (см. таблицу решения).

2-ой этап. Решение уравнения для $f_2(X)$:

$f_2(X) = \max_{0 \le x_2 \le X} [g_2(X_2) + f_1(X - x_2)]$

В эту формулу подставим вместо X значения 1, 2, 3, 4, 5.

При $X=1$

Управляет проверкой оплаты ряд правил и алгоритмов платежной системы банка. Способствующими всему этому процесс ресурсами являются web-сервер и его программное обеспечение;

– «Проверить наличие товара на складе ТОО KazinstallCompany» – действие, которое выполняется сразу после проверки оплаты. Назначение этого действия – сверить количество товара указанное в заказе с количеством товара на складе. Исходной информацией для этого блока действия являются данные переданные с предыдущего шага. Управляют блоком бизнес-правила web-сайта. Ресурсом является все тот же web-сервер.

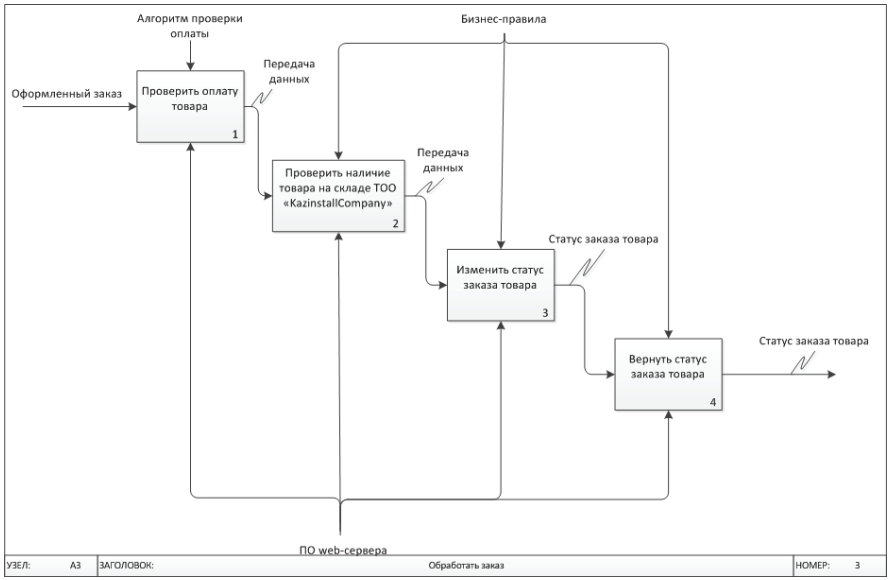


Рисунок 2 Диаграмма декомпозиции второго уровня

– «Изменить статус заказа товара» – действие, которое меняет статус заказа на основании поступивших данных с предыдущих двух блоков действий. Результатом этого блока действия станет статус заказа. Управляющим воздействием выступают бизнес-правила приложения. Ресурс – web-сервер.

– «Вернуть статус заказа товара» – действие, которое возвращает статус заказа товара после всей процедуры его обработки.

В результате построения диаграмм IDEF0 была спроектирована функциональная модель web-сайта для ТОО «KazinstallCompany».

Трапезников Е.В.
магистр технических наук
Северо-Казахстанский государственный университет им. М. Козыбаева

РАЗРАБОТКА WEB-САЙТА ДЛЯ ДЛЯ МАГАЗИНА КОМПЬЮТЕРНОЙ ТЕХНИКИ

Магазин «Chip» – ведущий национальный магазин компьютерной техники Казахстана.

Отличительная особенность этого магазина компьютерной техники – полная ориентированность на рынок Казахстана.

Сегодня магазин «Chip» включает 1 магазин общей торговой площадью около 350 кв.м. Он продолжает свое активное развитие, открыт для всего нового и прогрессивного. Магазин является стабильным в своем росте и развитии уже 8 лет, на протяжении которых успешно обеспечивает казахстанцев надежной и проверенной оргтехникой, компьютерной техникой известных мировых брендов.

Лидерство магазина «Chip» среди конкурентов обусловлено несколькими факторами:

–магазин ориентирован на клиента (госучреждения, офисы, дошкольные и школьные учреждения) и предлагает максимально возможный ассортимент компьютерной техники, оргтехники всех ценовых классов и канцелярских товаров;

–благодаря наиболее привлекательным ценам «Chip» делает компьютерную технику, оргтехнику, канцелярию доступной для всех слоев населения;

–магазин динамично развивается, применяет передовые торговые технологии и уделяет особое внимание профессиональному уровню своих сотрудников;

–сервисный центр «Chip» учитывает все потребности покупателей.

Web-сайт должен состоять из пользовательской и административной частей. Пользовательская часть сайта является общедоступной для всех пользователей сайта, на ней представлена вся информация, предназначенная для посетителей сайта. Пользовательская часть сайта должна состоять из следующих разделов:

- главная страница;
- о компании;
- новости;
- каталог товаров;
- партнеры и клиенты;
- контактная информация.

Административная часть сайта предназначена для настройки работы сайта, редактирования информации пользовательской части и осуществления функции приема заказов. Данная часть сайта должна быть доступна лишь для администратора сайта и бухгалтера-оператора, после прохождения ими процедуры авторизации. Административная часть сайта должна состоять из следующих разделов:

MATEMATIKA

UŽITÁ MATEMATIKA

Омарова М.Т.
Магистр математики, магистр менеджмента
Тынгишева А.М.
Магистр экономических наук
Карагандинский экономический университет Казпотребсоюза

ПРИМЕНЕНИЕ ПРИНЦИПА ОПТИМАЛЬНОСТИ БЕЛЛМАНА ДЛЯ РЕШЕНИЯ ЗАДАЧ ДИНАМИЧЕСКОГО ПРОГРАММИРОВАНИЯ

В последнее время особое развитие получили методы оптимального управления в задачах экономики, т.к. основной причиной такого процесса является все большее удорожание средств для решения задач управления и реализации полученных результатов. Оптимальным управлением называется выбор наилучшего среди множества всевозможных вариантов управления [1, стр. 39].

Динамическое программирование является одной из разновидностью подхода оптимизации в задачах математического программирования. Отличительной особенностью решения оптимизационных задач динамического программирования является сведение его к решению более простых «подзадач» и оптимизации целевой функции на каждом этапе. Поэтому нахождение оптимального решения (максимума или минимума функции) является задачей динамического программирования. Эта функция характеризует состояние системы, которая всегда меняется, при этом проходя этапы своего развития. Динамическое программирование позволяет выбор управления переходом от одного этапа к другому таким образом, чтобы на самом последнем этапе получить оптимум данной функции [2, стр. 57].

Таким образом, можно ввести следующее определение:

– динамическое программирование – это метод оптимизации, приспособленный к операциям, в которых процесс принятия решения может быть разбит на этапы (шаги). Такие операции называют многошаговыми [3, стр. 245].

Динамическое программирование дает возможность привести одну сложнейшую задачу с несколькими переменными ко многим задачам с маленьким количеством переменных, ускоряя процесс принятия управленческого решения и сокращая при этом время на принятие решения.

Во многих задачах и примерах, которые решаются данным методом, в процессе управления, как мы говорили ранее, происходит разбиение на некоторые

У загальній системі забезпечення безпеки банку захист інформації грає істотну роль, серед яких виділяють наступні засоби захисту:

-фізичний;

-законодавчий;

-організаційний;

-програмно-технічний.

Фізичні засоби захисту засновані на створенні фізичних перешкод для зловмисника, які перегороджують йому шлях до інформації (сувора система пропуску на територію і в приміщення з апаратурою або з носіями інформації).

До законодавчих засобів захисту відносяться законодавчі акти, які регламентують правила використання й обробки інформації обмеженого доступу і встановлюють кримінальну відповідальність за порушення цих правил.

Під організаційним розуміється захист інформації шляхом регулювання доступу до всіх ресурсів системи (технічним засобам, системам телекомунікацій та зв`язку, програмним елементам).

Програмно-технічні засоби найбільш ефективні криптографічні засоби захисту інформації. Коли фізичні засоби захисту можуть бути вирішені шляхом, наприклад, дистанційного нагляду, підключення до мережі або підкупу персоналу, а організаційні не гарантують від проникнення зловмисників, то програмно-технічні, і насамперед, криптографічні методи, якщо вони задовольняють відповідним вимогам, характеризуються найбільшою мірою «міцності».

Розглянувши загальні принципи захисту інформації в банківських автоматизованих системах, можна зробити висновок, що комплексний захист інформації в банківських автоматизованих системах має основі використання фізичних, законодавчих, організаційних та программно-технічних засобів захисту. Такі засоби повинні забезпечувати ідентифікацію та аутентифікацію користувачів, розподіл повноважень доступу до системи, реєстрацію та облік спроб несанкціонованого доступу. Організаційні заходи захисту інформації в банківських комп`ютерних системах, як правило, спрямовані на чіткий розподіл відповідальності при роботі персоналу з інформацією, створення декількох рубежів контролю, запобігання навмисному або випадковому знищенню та модифікації інформації.

ВИСНОВОК

Отже, захисту інформації в банківській АС є основні проблеми. Реалізація зазначених заходів дозволить мінімізувати ризики витоку конфіденційних даних. Не втратити довіру клієнтів і не перетворитися на черговий об’єкт статистики інцидентів у сфері інформаційної безпеки.

Література

1. Гайкович В., Прешин А. Безопасность электронных банковских систем.-М.: Единая Европа, 2014.

2. Голубєв В.О. Комп'ютерні злочини в банківській діяльності.-З.:Павел, 2007.-133 с.

3. Голубєв В.О. Програмно-технічні засоби захисту інформації від комп'ютерних злочинів.- З.: Павел, 2008.-144 с.

–управление разделами и страницами сайта;

–управление новостями;

–управление каталогом;

–управление учетными записями пользователей;

–прием заказов.

Должно быть обеспечено функционирование сайта в следующих режимах:

–штатный (непрерывная круглосуточная работа);

–сервисный (для проведения технических работ, редизайна и.т.п).

Должна быть реализована возможность масштабируемости сайта – добавления или удаления страниц и разделов сайта без ущерба действующей функциональности и дизайна.

Перспективные направления развития сайта заключаются в предоставлении заказа товаров для розничных клиентов, а также реализации возможности удобной формы заказа с мобильных приложений.

Доступ к административной части имеют пользователи с правами бухгалтера-оператора и администратора. Бухгалтер-оператор имеет возможность:

–осуществлять прием заказов и импортировать их в программу «1С:Предприятие»;

–выгружать данные о наличии и цене товаров из программы «1С:Предприятие» и прайс-листа соответственно;

–добавлять и удалять товар в каталоге;

–добавлять, редактировать новости, размещенные на сайте.

Администратор может выполнять все те же действия, что и бухгалтер-оператор, и кроме того:

–управлять учетными записями пользователей (подтверждать регистрацию пользователей, наделять пользователей различными правами доступа, добавлять, редактировать и удалять группы пользователей);

–добавлять и удалять разделы сайта;

–изменять дизайн и структуру сайта.

Авторизация на сайте должна осуществляться с использованием уникального логина и пароля. Логин выдается администратором сайта. Пароль генерируется автоматически и высылается пользователю на адрес, указанный при регистрации. В первый раз при попытке войти в административную часть система должна предлагать пользователю сменить пароль (ввести вручную новый пароль).

Трапезников Е.В.
магистр технических наук
Северо-Казахстанский государственный университет им. М. Козыбаева

ПРОЕКТИРОВАНИЕ WEB-САЙТА ДЛЯ ГИПЕРМАРКЕТА

Функциональная модель SADT отображает функциональную структуру объекта, то есть производимые им действия и связи между ними. Верхний уровень модели отражает только контекст системы. Контекстная диаграмма-вид IDEF0-диаграммы. Это диаграмма, расположенная на вершине древовидной структуры диаграмм, представляющая собой самое общее описание системы и ее взаимодействие с внешней средой. В соответствии с рисунком 1 представлена контекстная диаграмма IDEF0 [1, 2].

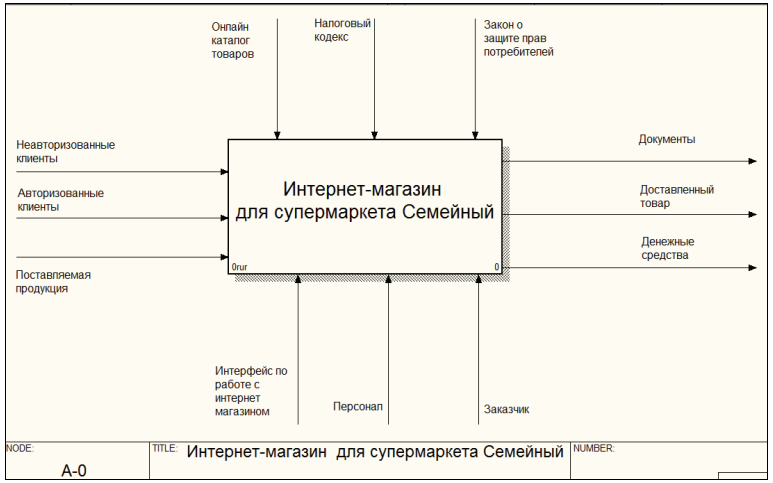


Рисунок 1 Контекстная диаграмма IDEF0. Функционирование супермаркета «Семейный»

Взаимодействие системы с окружающей средой описывается в терминах входа («Неавторизованные клиенты», «Авторизованные клиенты» и «Поставляемая продукция»), выхода (основной результат процесса – «Финансовые документы», «Доставленный товар» и «Денежные средства»), управления («Онлайн каталог товаров», «Налоговый кодекс» и «Закон о защите прав потребителей») и

Отже, основні проблеми захисту банків від загроз зумовлені їх недостатньою увагою до власної безпеки економічної інформації. Реалізація зазначених заходів дозволить мінімізувати ризики витоку конфіденційних даних. Не втратити довіру клієнтів і не перетворитися на черговий об’єкт статистики інцидентів у сфері інформаційної безпеки.

Література

1. Закон України «Про захист інформації в автоматизованих системах». № 80/94 від 05.07.94 р.
2. Зайцев А.П., Шелупанов А., Мещеряков Р. и др. Техническая защита информации: Учебник для вузов. – М.: Горячая линия-Телеком, 2009. – 615 с.

Шовкута Володимир Андрійович
Державний ВУЗ «Національний гірничий університет», Україна

ОСНОВНІ МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЇ В БАНКІВСЬКІХ АВТОМАТИЗОВАНИХ СИСТЕМАХ

ВСТУП

Вибір засобів захисту інформації в банківських автоматизованих системах – складна задача, при розв'язанні якої потрібно враховувати різні можливі дії щодо порушення роботи такої системи, вартість реалізації різних засобів захисту і наявність різних зацікавлених сторін. Кожному банку потрібна персональна система захисту інформації.

Особливо уразливими сьогодні залишаються незахищені системи зв'язку, а саме обчислювальні мережі. Інформація, циркулююча в них, може бути незаконно змінена, викрадена або знищена. З метою протидії злочинам у сфері комп`ютерної інформації необхідно грамотно вибирати заходи і засоби забезпечення захисту інформації від просочування та несанкціонованого доступу до неї. Необхідно враховувати також основні законодавчі положення в цій області, організаційні, програмно-технічні та інші заходи забезпечення безпеки інформації.

ПРИНЦИПИ ЗАХИСТУ ІНФОРМАЦІЇ В БАНКІВСЬКІЙ АС

Актуальність даної проблеми пов'язана із зростанням можливостей обчислювальної техніки. Розвиток засобів, методів і форм автоматизації процесів обробки інформації і масове застосування персональних комп'ютерів, роблять інформацію набагато більш уразливою. Основними чинниками, які сприяють цьому є:

- збільшення обсягів інформації, що накопичується, зберігається та обробляється за допомогою комп'ютерів;
- розширення кола користувачів, що мають безпосередній доступ до ресурсів обчислювальної системи та масивів даних;
- обмін інформацією в локальних та глобальних мережах, в тому числі на великих відстанях.

По–друге, інциденти такого роду можуть призвести до втрати конкурентноздатності банку, якщо, наприклад, інтелектуальна власність або база клієнтів попадуть до конкурентів.

Специфіка забезпечення інформаційної безпеки знайшла відображення в законах України «Про основи національної безпеки України» [3], «Про концепцію національної програми інформатизації», «Про національну програму інформатизації» [2], а також у Стратегії національної безпеки України, яка затверджена указом Президента.

У Законі «Про основи національної безпеки України» вперше дано офіційну оцінку значущості й системної сутності інформаційної безпеки як невід'ємної складової національної безпеки України.

У п. 2.8. Стратегії національної безпеки, присвяченому стану інформаційної безпеки в нашій державі, зазначено:

- посилюється негативний зовнішній вплив на інформаційний простір, що загрожує розмиванням суспільних цінностей і національної ідентичності;
- недостатніми залишаються обсяги вироблення конкурентоспроможного національного інформаційного продукту;
- наближається до критичного стан безпеки інформаційно-комп'ютерних систем у галузі державного управління, фінансової і банківської сфери, енергетики, транспорту, внутрішніх та міжнародних комунікацій тощо.

Ще в одному офіційному документі – «Рекомендаціях парламентських слухань з питань розвитку інформаційного суспільства в Україні» [4] ідеться, що стан розбудови інформаційного суспільства в Україні порівняно зі світовими тенденціями є недостатнім і не відповідає потенціалу та можливостям України, зокрема:

- відсутні національна стратегія розвитку інформаційного суспільства в Україні та план дій щодо її реалізації;
- немає координації зусиль державного і приватного секторів для ефективного використання наявних ресурсів;
- ефективність використання фінансових, матеріальних, кадрових ресурсів, спрямованих на виконання Національної програми інформатизації, впровадження інформаційно-комунікаційних технологій у соціально-економічну сферу, зокрема в сільське господарство, є низькою;
- є відставання у впровадженні технологій електронного бізнесу, електронних бірж та аукціонів, електронних депозитаріїв, використанні безготівкових розрахунків за товари та послуги тощо;
- рівень інформатизації галузей економіки, регіонів країни є низьким;

Одна з систем, що забезпечує захист інформації – це DLP (Data Loss Prevention) – система та інші засоби, що захищають від витоків, перекривають або контролюють ті чи інші канали, по яким інформація може покинути інформаційну систему, такі як мережеві з'єднання по різних протоколах, відчужувані носії інформації, мобільні комп'ютери, принтери і т.д.

Не завжди у банків вистачає коштів і умінь перекрити всі можливі канали. Ті носії, які залишаються без належного контролю, є провідниками відповідної частки випадкових витоків.

ВИСНОВОК

механизмов («Интерфейс по работе с интернет магазином», «Заказчик», «Персонал» – это ресурсы, необходимые для процесса функционирования супермаркета «Семейный»).

«Клиенты» – посетители сайта. Они просматривают каталог товаров. Делают заказы.

«Поставляемая продукция» – поставка готовых товаров.

«Налоговый кодекс» и «Закон о защите прав потребителей»-это правила, которыми управляется процесс функционирования web-сайта.

В оказании услуг принимает участие «Персонал». Чтобы оформить заказ и получить прибыль.

В соответствии с рисунком 2 представлена диаграмма декомпозиции IDEF0, отображающая разложение функционирования супермаркета.

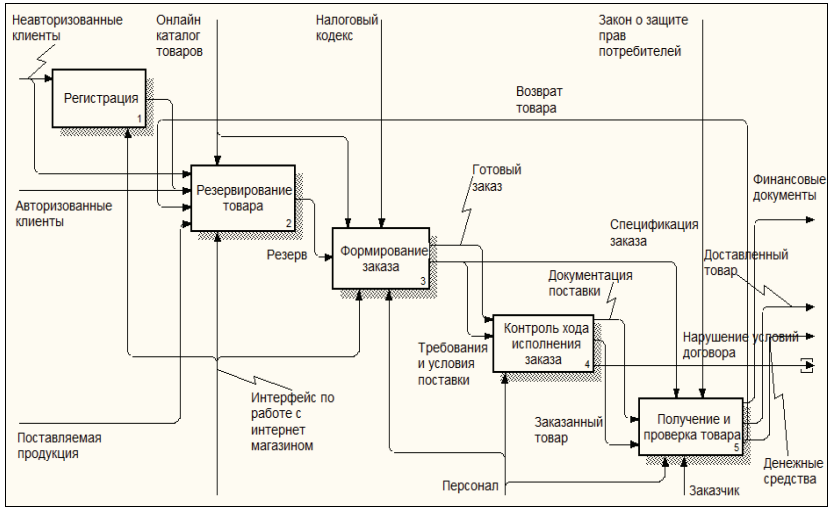


Рисунок 2 Диаграмма декомпозиции IDEF0. Функционирование супермаркет «Семейный»

Весь процесс «Функционирование супермаркет «Семейный» разбивается на:

1) «Регистрация» – создание учетной записи, для того чтобы можно было заказать товар;

2) «Резервирование товара» представляет собой выбор товара зарегистрированным пользователем, который закрепляется за данным пользователем;

3) «Формирование заказа» представляет собой уже выбранный товар, по которому формируется заказ;

4) «Контроль хода исполнения заказа» представляет собой готовый заказ, где обсуждаются требования и условия поставки товара;

5) «Получение и проверка товара» представляет собой получение заказанного товара и проверка его на целостность.

Литература:

1. Ларман К., Применение UML 2.0 и шаблонов проектирования,. 3-е издание. Пер. с англ.-М.: Вильямс, 2007. – 624 с.;

2. Фаулер М., UML. Основы.-М.: Символ-Плюс, 3-е издание, 2005. – 184 с.

Трапезников Е.В.

магистр технических наук

Северо-Казахстанский государственный университет им. М. Козыбаева

ПРОЕКТИРОВАНИЕ ИНФОРМАЦИОННО-УПРАВЛЯЮЩЕЙ СИСТЕМЫ ОТДЕЛА КАДРОВ

На сегодняшний день ТОО «Ресурсстрой» является одним из ведущих поставщиков строительных и отделочных материалов на рынке города Петропавловск.

На данное время сформировались стабильные, доверительные отношения с крупными казахстанскими, российскими, китайскими, европейскими предприятиями, заводами и организациями. ТОО «Ресурсстрой» предлагает строительные материалы в богатом ассортименте, включающем в себя более 7 000 наименований, который постоянно пополняется перечнем предлагаемой продукции, опираясь на пожелания клиентов.

Политика ТОО «Ресурсстрой» основана на индивидуальном подходе к каждому клиенту. Это означает, что все вопросы будут решены на высоком уровне, качественно и вовремя. Наша компания всегда дорожит своей репутацией, именно поэтому заказчики становятся нашими постоянными клиентами. Компания предлагает комплексные решения в области снабжения строительства любой сложности, не ограничиваясь географией города Петропавловска.

На предприятии создается автоматизированная информационная система, которая состоит из взаимосвязанных функциональных подсистем, обеспечивающих управленческий аппарат необходимой информацией. Основные функциональные подсистемы обеспечивают решение задач технической подготовки производства, перспективного планирования и прогнозирования развития производства, оперативного управления материальными, трудовыми и финансовыми ресурсами и т. д.

В данное время в ТОО «Ресурсстрой», а именно в отделе кадровой работы существует такая проблемная область как хранение и обработка информации по кадровому составу. Для получения необходимых сведений затрачивается много времени и сил на поиск, так как вся информация и какие-либо изменения о сотрудни-

Література

1. Гайкович В.Ю., Ершов Д.В. Основы безопасности информационных технологий: Учеб. пособие. – М.: МИФИ, 1995. – 252 с.

2. Галатенко В.С. Стандарты информационной безопасности. – М.: НИИСИ РАН, 2006. – 262 с.

3. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с.

Шовкута Володимир Андрійович

Державний ВУЗ «Національний гірничий університет», Україна

НЕДОЛІКИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В КОМЕРЦІЙНИХ БАНКАХ

ВСТУП

Питання поширення комп'ютерної злочинності в Україні та її масштаби здаються багатьом неактуальними. Проте, якщо суспільство адекватно не реагуватиме на такі злочинні прояви, то перед ним постануть значні загрози для його життєдіяльності. Передумовами зростання злочинності у сфері комп'ютерних мереж та високих інформаційних технологій є ускладнення технічних систем зв'язку, спрощення доступу до використання комп'ютерних технологій широкого кола фізичних осіб, підвищення знань осіб, що намагаються вчинити протиправні діяння тощо. Проблемами, які постають у сфері інформаційних та платіжних технологій є те, що злочини, пов'язані з використанням цих високих технологій, виходять за межі звичайних дій в уявлені пересічного громадянина, і представляють собою дії, які станом на сьогодні неврегульовані законодавством повністю або частково.

Особливої гостроти набуває питання захисту інформації в банківській системі, оскільки посуті, йдеться про захист власності у вигляді коштів, що залучені банками та небанківськими фінансовими установами.

ЗАХИСТУ ІНФОРМАЦІЇ В КОМЕРЦІЙНИХ БАНКАХ

Під інформаційною безпекою розуміється захищеність інформації та інфраструктури, що її підтримує, від випадкових або навмисних дій природного або штучного характеру, які можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, зокрема власникам і користувачам інформації та інфраструктури, що її підтримує [2].

Самою небезпечною загрозою є порушення конфіденційності інформації та витік інформації, оскільки банки побоюються цього за двома причинами. По-перше, кожен витік конфіденційної інформації та персональних даних банку підриває його репутацію, так як в очах його партнерів, інвесторів і клієнтів банк набуває імідж організації, яка не в змозі навести порядок в своїх власних стінах. В результаті відбувається відтік інвестицій та міграція клієнтів та конкурентів.

4 етап. Створення звіту та розробка відповідних рекомендацій, щодо підвищення захищеності ІКСМ

Обстеження обчислювальної системи інформаційної мережі проводиться з ціллю перевірки наявності документації на ІКСМ та наявності розпорядчих документів на неї.

Також проводиться збір відомостей про загальну структурну схему ІКСМ, її компоненти – склад устаткування, технічні і програмні засоби, їх зв'язки, особливості конфігурації, архітектури та топології, програмні і програмно-апаратні засоби захисту інформації, взаємне розміщення коштів. Збір відомостей інформації про види каналів зв'язку, їх характеристики. Збір відомостей про їх компонентів ІКСМ.

Обстеження інформаційного середовища проводиться з ціллю збору відомостей про технологію обробки інформації в корпоративній мережі. Також відбувається збір відомостей про інформаційні потоки; про основні вимог до захисту інформації в ІКСМ; про режим доступу до інформаційних ресурсів ІКСМ; про інформаційні носії та правила роботи з ними.

Обстеження фізичного середовища інформаційної мережі проводиться з ціллю перевірки наявності документації на компоненти фізичного середовища ІКСМ та її попередній аналіз. Збір відомостей про територіальне розміщення компонентів інформаційної мережі. Збір відомостей про наявність території, що охороняється і пропускного режиму на об'єкті. Збір відомостей про наявність на об'єкті чи категорійних приміщень. Збір відомостей про режим доступу до компонентів фізичного середовища ІКСМ. Збір відомостей про наявність в приміщеннях, де функціонує захищена ІКСМ, елементів комунікацій, систем життєзабезпечення та зв'язку, які мають вихід за межі контрольованої території. Збір відомостей про наявність системи заземлення обладнання ІКСМ та її технічних характеристик. Збір відомостей про умови зберігання магнітних, оптико-магнітних, паперових та інших носіїв інформації.

Обстеження середовища користувачів проводиться з ціллю перевірки наявності документів, що регламентують діяльність персоналу організації із забезпечення безпеки інформації в ІКСМ та їх попередній аналіз. аналіз функціонального і кількісного складу користувачів і їх обов'язків; аналіз функцій та повноважень підрозділу захисту інформації; аналіз категорій користувачів за рівнем повноважень.

Тестування на уразливості проводиться з ціллю сканування всіх компонентів ІКСМ на уразливості як зсередини, так і зовні.

ВИСНОВОК

Таким чином проведення аудиту інформаційної безпеки підприємства – це непросто «інвентаризація» ІКСМ, а ретельна та всебічна робота з дослідження корпоративної мережі, яка дає найбільш повну картину стану захищеності і дозволяє сформувати вимоги до комплексної системи захисту інформації в інформаційної мережі організації.

Проведення кваліфікованого аудиту інформаційної безпеки та виконання комплексу заходів із захисту інформаційних ресурсів за рекомендаціями, виробленим в результаті такого аудиту, дає впевненість в захищеності ІКСМ на певний період часу.

ках хранятся в архиве, личном деле и в различных документах. Создание автоматизированной системы обработки и хранения информации облегчит ручной труд, повысить эффективность работы и уменьшит время на поиск нужной информации.

Входной информации данной системы являются личные и профессиональные данные о сотруднике, результатом работы информационной системы будут отчеты. Схематически работа системы представлена в соответствии с рисунком 1.

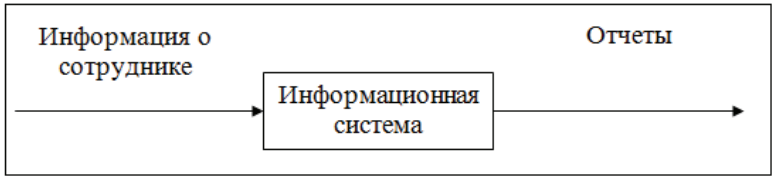


Рисунок 1 Схематическая работа системы

В соответствии с рисунком 2 контекстная диаграмма имеет очень большое значение для всего проекта в целом. Она фиксирует границы моделируемого приложения, определяя то, как моделируемого приложение взаимодействует со своим окружением.

Из рисунка 2 видно, что входной информацией будут являться методические материалы для проектирования информационной системы. Основополагающей концепцией в проектировании выступают исходные данные по сотрудникам организации, которые необходимо автоматизировать при помощи проектирования информационной системы.

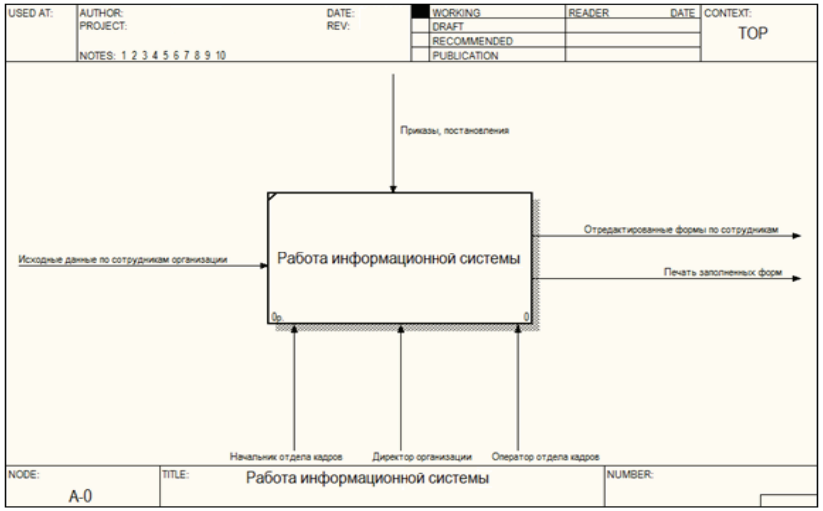


Рисунок 2 Контекстная диаграмма «Проектирование информационной системы»

После описания контекстной диаграммы проводится функциональная декомпозиция – система разбивается на подсистемы и каждая подсистема описывается отдельно (диаграммы декомпозиции). Затем каждая подсистема разбивается на более мелкие и так далее до достижения нужной степени подробности.

Весь процесс проектирования информационной системы отдела кадров разбивается на 4 блока декомпозиции:

– формирование общей концепции иллюстрирует общую идею;

– разработка страниц или шаблона представляет собой процесс разработки web-интерфейса или шаблона, макета сайта в какой-то среде разработки;

– разработка БД представляет собой процесс разработки БД в какой-то среде разработки;

– тестирование служит для тестирования всей ИС и исправления ошибок, если такие имеются.

Подобрий А.Н.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ INTRANET-ПОРТАЛА

Одними из основных задач предприятий являются задачи повышения эффективности производства и качества выпускаемой продукции, а также обеспечения нового качества управляемости за счет создания единого информационного пространства предприятия. Данная проблема решается путем создания веб-портала – единой «точки входа» для всех пользователей, предоставляющий персонифицированный и безопасный доступ ко всей совокупности информации, необходимой для выполнения повседневных обязанностей сотрудника[1].

«Система управления сайтом», или CMS – в последнее время один из самых распространенных способов администрирования Web портала. Все большее число студий web-дизайна предлагают создание сайтов на различных CMS. Многие существующие CMS не гарантируют безопасность Web сервера даже для масштабов среднего бизнеса. Каждая компания имеет проблемы с безопасностью корпоративного сайта, и прежде всего эти проблемы связаны с уязвимостью системы управления содержимым.

К современным CMS можно отнести Joomla, Drupal, 1c-bitrix, Wordpress и т.д. Все эти системы, несомненно, имеют много плюсов, но не все позволяют максимально защитить информацию, а также проинформировать пользователя о найденной ошибке или взломе системы. Это связано с отсутствием у этих систем детального разграничения прав доступа в разрезе субъектов и объектов корпоративной информационной системы, а также ведение журнала разграничения прав

система захисту корпоративних мереж. Фрагментарний підхід корисний для невеликих КС із малими інформаційними ресурсами обігу та на етапі проектування певних частин великої розподіленої системи.

література

1. Шаньгин В.Ф. Защита компьютерной информации.- М.:ДМК Пресс,2008.-544 с.

2.Э.Таненбаум. Компьютерные сети, 4-е узд. – Питер, 2003. – 992 с

3.Олифер В.Г., Олифер Н.А. – Компьютерные сети. Принципы, технологии, протоколы (4-е издание).- Питер,2010.-943 с.

Шовкута Володимир Андрійович

Державний ВУЗ «Національний гірничий університет», Україна

ПОРЯДОК ПРОВЕДЕННЯ АУДИТУ ЗАХИЩЕНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

ВСТУП

На даний час взаємодія відкритих корпоративних мереж, спільне використання інформаційних ресурсів та інформаційного простору збільшує труднощі управління доступом і безпеки інформаційно-комунікаційних систем та мереж (ІКСМ). Розгалужені інформаційні мережі, що мають велику кількість зовнішніх зв'язків, створюють достатній потенціал для несанкціонованого доступу до інформаційних ресурсів мережі. Інформація, яка циркулює в ІКСМ виступає важливим діловим активом, з точки зору матеріальної цінності. Тому, для зменшення загроз взаємодії відкритих ІКСМ необхідно приділяти все більш уваги аналізу уразливостей та приділяти більше уваги проведені аудиту корпоративних мереж.

ЕТАПИ ПРОВЕДЕННЯ АУДИТУ ІКСМ.

1 етап. Підготовка до проведення аудиту (обстеження) ІКСМ:
- формування вимог до проведення аудиту;
- створення спільної комісії з аудиту.

2 етап. Комплексне обстеження ІКСМ:
- обстеження обчислювальної системи інформаційної мережі;
- обстеження фізичного середовища інформаційної мережі;
- тестування на уразливості інформаційної мережі;
- обстеження інформаційного середовища;
- обстеження середовища користувачів.

3 етап. Аналіз захищеності ІКСМ:
- аналіз і систематизація отриманих результатів обстеження;
- ідентифікація отриманих уразливостей;
- оцінка рівня захищеності інформаційної мережі.

політиці безпеки. Політика безпеки регламентує ефективну роботу засобів захисту. Вона охоплює всі особливості процесу обробки інформації, визначаючи поводження системи в різних ситуаціях. Надійна система безпеки мережі не може бути створена без ефективної політики мережевої безпеки.

Для захисту інтересів суб'єктів інформаційних відносин необхідно поєднувати заходи наступних рівнів[1]:

- законодавчого (стандарти, закони, нормативні акти і т.п.);
- адміністративно-організаційного (дії загального характеру, підприємцями та керівництвом організації, та конкретні заходи безпеки, що мають ставлення до людей);
- програмно-технічного (конкретні технічні заходи).

Заходи законодавчого рівня дуже важливі для забезпечення інформаційної безпеки. До цього рівня можна віднести весь комплекс заходів, спрямованих на створення і підтримку в суспільстві негативного (зокрема карального) відношення до порушень і порушників інформаційної безпеки. Більшість людей не здійснюють протиправних дій тому, що це засуджується і / або карається суспільством, і тому, що так чинити не прийнято.

Інформаційна безпека – це нова сфера діяльності, тут важливо не тільки забороняти і карати, а й навчити, роз'яснити, допомогти. Суспільство має усвідомити важливість даної проблематики, зрозуміти основні шляхи вирішення відповідних проблем. Держава може зробити це оптимальним чином. Тут не треба великих матеріальних витрат, потрібні інтелектуальні вкладення[3].

Заходи адміністративно-організаційного рівня. Адміністрація організації повинна усвідомлювати необхідність підтримки режиму інформаційної безпеки і виділення на ці цілі відповідних ресурсів. Основою мірою захисту

адміністративно-організаційного рівня є політика безпеки і комплекс організаційних заходів. Під політикою безпеки розуміється сукупність документованих управлінських рішень, спрямованих на захист інформації та пов'язаних з нею ресурсів організації.

До комплексу організаційних заходів належать заходи безпеки, реалізовані людьми. Можна виділити наступні групи організаційних заходів:

- управління персоналом;
- фізичний захист;
- підтримка працездатності;
- планування відновлювальних робіт.

ВИСНОВОК

Отже, комплексний підхід до вирішення проблеми забезпечення безпеки – це раціональне поєднанні законодавчих, адміністративно-організаційних і програмно-технічних заходів та обов'язкова відповідність промисловим, національним та міжнародним стандартам, що є тим фундаментом, на якому будується вся

доступа сотрудников и, последующего анализа данных с оповещением администратора. К одними из основных недостатков и уязвимостей современных систем управления содержанием можно отнести атаки ***SQL-injection*** и ***XSS***.

Атаки SQL-injection. Внедрение SQL-кода – один из распространенных средств взлома сайтов и программ, работающих с базами данных. Средство основано на внедрении в запрос произвольного SQL-кода.

Атаки XSS. XSS – тип уязвимости интерактивных информационных систем. XSS возникает, когда в страницы, которые генерирует сервер, по какой либо причине попадают скрипты пользователей.

Проведенный анализ современных систем управления содержанием и механизмов реализации атак позволяет выработать требования, которым должна удовлетворять безопасная CMS. Прежде всего система управления должна быть полностью защищена от модификации строки запроса. Это позволит полностью избежать довольно широкого класса атак SQL-injection.[2].

Таким образом, задача разработки максимально защищённой системы управления стоит сегодня особенно остро и, на основании поставленных проблем можно выделить основные критерии информационной безопасности веб портала на современном предприятии: грамотная настройка серверного ПО; однозначная идентификация сотрудника; возможность объединять разные самостоятельные веб ресурсы и подсистемы; ведение детализированного журнала активности пользователя; ведение журнала разграничения прав доступа пользователей; проведение анализа данных на основании активности пользователя и журнала прав доступа.

Исходя из выше перечисленных критериев информационной безопасности веб портала, можно спроектировать следующую структуру (рис 1): безопасность на уровне веб – сервера, безопасность на уровне sql – сервера, ведение журнала активности веб – сервера и sql – сервера, анализ данных.

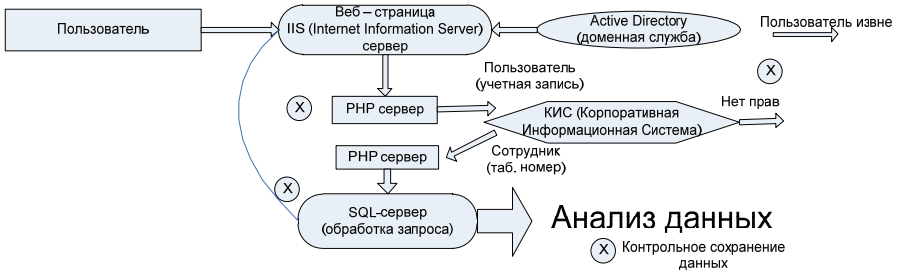


Рис. 1 Схема информационной безопасности веб портала

Безопасность на уровне веб – сервера достигается с помощью IIS сервера, доменной службы Active Directory (AD) и Корпоративной информационной системы (КИС). Данный пункт реализуется путем настройки веб-точек на IIS сервере, а также связывания IIS сервера и AD. Этот пункт осуществляет аутентификацию и идентификацию пользователей, контроль уровня доступа к веб-точке, контроль уровня доступа пользователей к каталогам, а также ведение журнала активности[4].

Безопасность на уровне sql – сервера достигается путем контроля прав доступа выбранного пользователя за счет объединения AD и КИС, а также базы прав доступа пользователей. Под механизмом стыковки AD и КИС понимается определение идентификатора сотрудника (табельный номер) на основании учетной записи пользователя.

Ведение журнала активности веб – сервера и sql – сервера необходимо для сбора информации о всех событиях, действиях пользователя. Для сохранения всей выше указанной информации каждый ресурс необходимо зарегистрировать (описать) в базе данных, с присвоением им внутреннего идентификатора и списка всех операций данного ресурса.

Журнал активности веб-сервера и sql-сервера включает в себя:

1) Фиксация подключений пользователей к веб серверу (журнал log);

2) Фиксация посещения ресурсов в соответствии с идентификаторами ресурсов, учетной записью пользователя, операции и времени посещения;

3) Фиксация выполнения sql – запросов. В моем случае, с использование Microsoft SQL Server, данная операция реализуется с помощью технологии Try/Catch и метода Execute.

Анализ данных необходим для контроля уровня доступа, поиска ошибок, поиск перспективы развития ресурсов. Хранение автоматизированного журнала системы анализа в виде xml данных позволяет создать не только иерархию данных внутри отчета, но и вести хронологический перечень всех результирующих данных со статусом их выполнения. Кроме того, на основании данной структуры, возможно проводить поиск уязвимостей и недостатков системы в целом за любой промежуток времени в разрезе любого субъекта или объекта, входящих в состав ресурсов.

На основании вышеизложенного, следует отметить, что представленная структура информационной безопасности позволяет покрыть в полной мере все поставленные задачи. Она основана на использовании современных, общедоступных языках программирования высокого уровня. Позволяет настраивать права доступа в разрезе субъектов и объектов КИС, отслеживать поведение сотрудников и проводить самостоятельный мониторинг данных.

Данная схема реализуется с помощью веб сервера IIS, либо Apach

- язык программирования php, подключенный как модуль ISAPI либо LDAP
- Корпоративная Информационная Система
- SQL сервер.

Посталака Сергій Вікторович
Державний ВУЗ «Національний гірничий університет», Україна

МЕТОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МЕРЕЖЕВИХ РЕСУРСІВЗАЩИТА У АС КЛАСУ 3

ВСТУП

Основою корпоративної інформаційної взаємодії комп’ютерних систем є забезпечення обміну інформації між клієнтською та серверною частинами мережі. Як і будь – яка інша мережа організації містить сервер чи кластер серверів та велику кількість розподілених користувацьких робочих місць, які об’єднані певною топологією та комутаційними зв’язками.

ВИКЛАДЕННЯ МАТЕРИАЛУ

Існує два підходи до проблеми забезпечення безпеки комп'ютерних систем і мереж: фрагментарний (частковий, кластерний) та комплексний.

Частковий підхід спрямований на протидію чітко визначеним загрозам в заданих умовах. Як приклади реалізації такого підходу можна вказати окремі засоби управління доступом, автономні засоби шифрування, спеціалізовані антивірусні програми і т.п.

Перевагою такого підходу є висока вибірковість до конкретної загрози. Істотним недоліком даного підходу є відсутність єдиної захищеної середовища обробки інформації. Фрагментарні заходи захисту інформації забезпечують захист конкретних об'єктів КС тільки від конкретної загрози. Навіть невелике видозміна загрози веде до втрати ефективності захисту[1].

Комплексний підхід орієнтований на створення захищеної середовища обробки інформації в КС, що об'єднує в єдиний комплекс різнорідні заходи протидії загрозам. Організація захищеної середовища обробки інформації дозволяє гарантувати певний рівень безпеки КС, що являється безсумнівним достоїнством комплексного підходу. До недоліків цього підходу відносяться: обмеження на свободу дій користувачів КС, чутливість до помилок установки і настройки засобів захисту, складність керування[1,2].

Комплексний підхід застосовують як для захисту КС великих організацій так і невеликих КС, виконують відповідальні завдання або обробних особливо важливу інформацію. Порушення безпеки інформації в КС великих організацій може завдати величезної матеріальної шкоди як самим організаціям, так і їх клієнтам. Тому такі організації змушені приділяти особливу увагу гарантіям безпеки і реалізовувати комплексну захист. Комплексного підходу дотримується більшість державних і великих комерційних підприємств та установ. Цей підхід знайшов своє відображення в різних міжнародних стандартах з інформаційного менеджменту. Даний підхід заснований на розроблених для конкретної КС

пальцев, смотреть в объектив или произносить слова. Распознавание лица – это, пожалуй, единственный биометрический способ идентификации людей, для применения которого не требуется дорогостоящая техника.

Система идентификации по чертам лиц работает с относительно простым двумерным изображением, что заметно упрощает алгоритмы и снижает интенсивность вычислений. Но даже в этом случае задача распознавания все же не тривиальна, поскольку алгоритмы очень сильно зависят от следующих факторов:

- Качество изображения;
- Заметно снижается вероятность безошибочной работы системы, если человек, которого мы пытаемся идентифицировать, смотрит не прямо в камеру;
- Изменение выражение лица человека;
- Внешность человека;
- Угол наклона головы;
- Освещение;

Технологии распознавания лица хорошо работают со стандартными видеокамерами, которые передают данные и управляются персональным компьютером. Для сравнения – приемлемое качество для видео конференции требует скорости видеопотока уже от 15 кадров в секунду. Более высокая скорость видеопотока при более высоком разрешении ведет к улучшению качества идентификации. При распознавании лиц с большого расстояния существует сильная зависимость между качеством видеокамеры и результатом идентификации.

ВИСНОВОК

Предлагаемые сегодня методы распознавания лиц интересны и близки к широкому внедрению, однако пока не возможно доверять только технологии распознавания по лицу. Она хороша как помощник для охранника или другой системы контроля доступа. Вместе с тем идентификации по лицу достаточно эффективна в случаях, когда, например, требуется сравнить фотографии – при условии, что снимки хорошего качества, а пользователь не предпринимает специальных усилий для того, чтобы намеренно изменить свою внешность.

Литераура

1. 1. А.Ф. Стеблева, Биометрические системы безопасности, Журнал «Системы безопасности» №2, 2007 // стр. 174-178

2. The Biometric Consortium Электронный ресурс. URL: http://www.biometrics.org (дата обращения 20.08.2012).

Таким образом, приведенные ранее распространенные ошибки безопасности решаются путем детального разграничения прав доступа на разных уровнях предложенной модели, а также постоянного мониторинга и анализа собранной информации касаемо активности пользователей.

Система анализа данных проводит постоянный аудит, который необходим как для сбора всей отчетности, так и для поиска и информирования об атаках и разных недочетах информационной системы. Данная система позволяет самостоятельно принимать решение о блокировке пользователя или ресурса, для предотвращения дальнейшей ошибки или атаки.

Литература

1. Официальный сайт компании «Interface Ltd.»
http://www.interface.ru
2. Официальный сайт компании « CMSList.ru»
http://cmslist.ru
3. «Модель доступа к веб-порталу на современном предприятии» Известия Самарского Научного центра Российской академии наук.- научно-технический журнал (ВАК) –Самара, 2011; 4 выпуск, 475с
4. Электронное издание «Архитектура «клиент-сервер»« Зеленков Ю.А.
http://www.mstu.edu.ru/study/materials/zelenkov/ch_7_1.html

Гуменюк Ю.М., асистент Копчикова І.В.
Вінницький торговельно-економічний інститут КНТЕУ, Україна

ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ СТАТИСТИЧНОГО МОНІТОРИНГУ РОЗВИТКУ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА В УКРАЇНІ

Проведення моніторингу соціально-економічного стану – одна з нових функцій статистичних систем у різних країнах. Якщо раніше головними завданнями статистичних служб були спостереження за перебігом процесів та деякий аналіз даних, то останніми роками в багатьох європейських країнах статистичними організаціями проводиться моніторинг у широкому його розумінні.

Вагомий внесок у обґрунтування питань, які стосуються вивчення процесу статистичного моніторингу, залежно від різних галузей дослідження, здійснили зарубіжні вчені: Д. Берроуз , Д.М. Матрос, В.А. Ковда, а також вітчизняні – В.К. Галіцин, М.В. Пугачова.

Статистичний моніторинг – це процес поточного спостереження, контролю, оцінювання, аналізу і прогнозування ключових процесів у суспільстві на базі статистичних даних [1, с. 5].

При побудові системи статистичного моніторингу (на етапі проектування) слід побудувати інформаційну модель предметної галузі та здійснити: визначення та ідентифікацію первинних джерел даних; визначити вторинні (похідні) характеристики (в тому числі моделі, методи та алгоритми, за якими вони обчислюються з первинних); класифікацію потенційних користувачів; визначити можливі труднощі отримання тих чи інших даних; визначити можливі запити користувачів; визначення форматів подання даних.

Статистичний моніторинг здійснюється та підтримується автоматизованою інформаційно-аналітичною системою на основі використання ЕОМ, мереж комунікацій, відповідного програмного забезпечення та даних системи Internet [2, с. 38].

У Держкомінформатизації (нині Державний комітет з питань науки, інновацій та інформатизації України) спільно з Держкомстатом (зараз – Державна служба статистики України) створена міжвідомча робоча група з питань моніторингу інформаційного суспільства, а в рамках Національної програми інформатизації започатковано проект «Здійснити заходи щодо запровадження Національної системи індикаторів розвитку інформаційного суспільства», серед результатів якого мають бути: 1) методичні рекомендації щодо запровадження Національної системи індикаторів (індексів) розвитку інформаційного суспільства; 2) методика оцінювання стану розвитку інформаційного суспільства в Україні на основі Національної системи індикаторів; економіко-математичне моделювання соціально-економічних систем; 3) методика оцінювання ефективності державної політики та державного управління розвитком інформаційного суспільства; 4) прогноз розвитку інформаційного суспільства в Україні на період до 2015 року; 5) пропозиції Держкомстату щодо внесення змін до системи державних статистичних спостережень з питань інформатизації та розвитку інформаційного суспільства: структури, механізмів, джерел інформації, проектів форм Державних статистичних спостережень та інструкцій до них [3, с. 243].

Статистичний моніторинг інформаційного суспільства включає: впровадження технологій електронного уряду в органи виконавчої влади всіх рівнів; розробку показників і сучасного інструментарію статистичних, соціологічних і інших обстежень, що відповідають вимогам міжнародних і національних статистичних стандартів; комплексний аналіз проблем формування інформаційного суспільства на основі статистичної, соціологічної, експертної інформації.

Виділимо основні етапи створення системи статистичного моніторингу інформаційного суспільства: 1) визначення цілей, стратегії і загальну політику щодо моніторингу інформаційного суспільства; 2) аналіз і розробка вимог; 3) визначення методики проектування; 4) проектування системи статистичного моніторингу інформаційного суспільства на основі систематичного застосування обраних на попередньому кроці методів аналізу; 5) реалізація системи та інтеграція

Биометрия. Пользователь предъявляет параметр, который является частью его самого. Биометрический класс отличается тем, что идентификации подвергается личность человека – его индивидуальные характеристики.

Биометрические системы доступа являются очень удобными для пользователей. В отличие от паролей и носителей информации, которые могут быть потеряны, украдены, скопированы. Биометрические системы доступа основаны на человеческих параметрах, которые всегда находятся вместе с ними, и проблема их сохранности не возникает. Потерять их почти невозможно. Также невозможна передача идентификатора третьим лицам.

ВИДЫ БИОМЕТРИЧЕСКИХ СИСТЕМ

Классические способы идентификации личности, в состав которых входят различные идентификационные карты, ключи или пароль не отвечают современным требования безопасности. Естественным шагом для систем безопасности стали попытки использовать биометрические технологии.

С использованием биометрических технологий будут решены следующие проблемы:

- Несанкционированное проникновение на охраняемые территории и в помещения за счет подделки, кражи документов, карт, паролей;
- Ограничение доступа к конфиденциальной информации;
- Уменьшение накладных расходов, связанных с эксплуатацией систем контроля доступа (карты, ключи);
- Минимизировать неудобства, связанные с утерей, порчей или забыванием ключей, карт, паролей;
- Осуществить ведение учета посещаемости сотрудников.

На данный момент известен ряд технологий, которые могут быть использованы в системах безопасности для идентификации личности по:

- отпечаткам пальцев;
- форме ладони;
- расположению вен на лицевой стороне ладони;
- чертам лица;
- термограмме лица;
- радужной оболочке глаз;
- сетчатке глаза;
- голосу;
- рукописному/клавиатурному подчерку.

У всех биометрических технологий присутствуют общие пути решения задачи идентификации, хотя не все отличаются удобством применения и точностью результатов.

В отличие от других биометрических технологий (идентификация по отпечаткам пальцев, радужной оболочке глаза или по голосу) системе распознавания по чертам лица не требуется непосредственный контакт с человеком, личность которого устанавливают. Человеку нет необходимости оставлять отпечатки

Балалардың ересек адамдармен бірлесіп өмір сүруге ұмтылуы бірлескен еңбек негізінде қанағаттандыра алмайды. Бұл қажеттілігін балалар ойын үстінде қанағаттандыра бастайды, ойын арқылы өздеріне ересектер ролін алып, еңбектік өмірді ғана емес, сол сияқты қарым-қатынасты да нақтылап көрсетеді.

Талаптану әлеуметтік белсенділіктің табиғи түрі болып жеке адамның дұрыс дамуының шарты болып есептеледі. Алайда, бұл құбылыс сырттай көріне бермейді, өйткені бала маңызды орынға талаптануын көбнесе аса бір ерекше, өзі үшін қолайлы жағдайларда ғана жарыққа шығарады.

Баланың тілінің дамуына ойын өте үлкен әсер етеді. Өйткені бала өз құрбыларымен өзінің ой-пікірін жеткізе отырып, басқаларын да түсіне біледі. Ойын тіл мен іс-әркет арқылы жүзеге асады. Ойын жағдайына енген әр баладан белгілі қатынас жасау қабілетін талап етеді. Егер бала ойын барысында қатысты өз тілектерін түсінікті етіп айта алмаса, егер ойын үстіндегі жолдастарының сөздік нұсқауларын ұқпайтың болса, онда құрбылары оны жақтырмайды. Бұл жағдайдағы эмоциялық қолайсыздық тілдің дамуына себепкер болады.

Әдебиет:

1. М.Жұмабаев. Педагогика. Алматы. Рауан 1998
2. М.Мұқанов. Жас және педагогикалық психология. Алматы 1982
3. Қ.Жарықбаев. Психология. Алматы. Білім 1993
4. Қоянбаев. Педагогика. Алматы. Рауан 2000
5. Абайдың қара сөздері. Алматы. Ел 1993
6. А.Мырзабаев. Оқушылар шығармашылығын дамытуда белсенді оқытудың дидактикалық мүмкіндіктері. Қарағанды 2004
7. Б.Байжұманова. Бастауыш мектеп жасындағы балаларды творчестволық қабілетті дамытудың психологиялық ерекшеліктері.

Посталака Сергей Викторович
Державний ВУЗ «Національний гірничий університет», Україна

БИОМЕТРИЧЕСКИЕ СИСТЕМЫ АУТЕНТИФИКАЦИИ ПО ЧЕРТАМ ЛИЦА

ВСТУП

Биометрическая аутентификация – процесс доказательства и проверки подлинности заявленного пользователем имени, через предъявление пользователем своего биометрического образа и путем преобразования этого образа в соответствии с заранее определенным протоколом аутентификации.

її з іншими підсистемами. Даний крок має бути підтриманий підготовкою програм з навчання співробітників, адміністраторів і персоналу; 6) функціонування системи статистичного моніторингу інформаційного суспільства, що охоплює сукупність процедур і дій, таких як: перевірка погодженості засобів системи і їхньої відповідності сформованим вимогам, контроль за коректністю роботи, перегляд проектних і експлуатаційних рішень за результатами експлуатації, супровід (триваюча розробка) засобів системи моніторингу, відстеження позаштатних ситуацій і реакція на них [4].

Налагоджена система статистичного моніторингу відіграє важливу роль в розробці і реалізації програм розвитку інформаційного суспільства. Вона виконує функцію зворотного зв'язку і дозволяє контролювати результати виконання програми і стежити за просуванням до цільових показників; отримувати необхідну інформацію про диспропорції і перешкоди економіко-математичне моделювання соціально-економічних систем розвитку для своєчасного коректування програм і стратегій формування інформаційного суспільства.

Література:

1. Швець В., Царук О. Методологічні засади побудови системи статистичного моніторингу державного боргу // Вісник КНУ ім. Т.Шевченка, Серія ЕКОНОМІКА – 2009. – № 99-100. – С.1-7.
2. Галіцин В.К. Системи моніторингу в управлінні економікою // Моделювання та інформаційні системи в економіці. – К, 2011. – № 66.
3. Концептуальні основи статистичного моніторингу // За ред. М.В. Пугачової. – К., 2013. – 436 с.
4. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні» на 2007-2015 роки.

Ст.преподаватель, Биктимирова В.Б.
Костанайский государственный университет им. А.Байтурсынова, Казахстан

DEVELOPMENT OF A COLLECTION OF INTERACTIVE EXERCISES FOR EASY MEMORIZATION

Nowadays, throughout the world, we see that usage of the computer in the development of a fully developed personality starts in the kindergarten and becomes the common practice. In this situation the question whether or not to use information technology in the pre-school pedagogy stays very relevant. The matter is that children who come in preschool already have computer skills, because they receive them in their families. In our opinion, it's necessary to use all advantages of the computer as a mean

of developing the child's abilities, the formation of developed personality. The more a child intellectually developed, the more opportunities the educator can use in teaching.

The quality of education and development of personality increase, if computer technologies are used in preschool. By the moment when these children go to school they are usually more prepared since the world of knowledge had already been opened for them in kindergarten. We can not ignore modern technologies of information transmission, because they give us new opportunities in the field of education.

The implementation of effective methods and forms of training in preschools will lead to tremendous results. We would like to devote our study to the methods of development of children's memory with the help of a computer.

Memory – a form of mental reflection, which consists in securing, maintaining, and successive simulation of previous experience, making possible to reuse it in activities or return to the sphere of consciousness. Only memory can connect the past with the present and the future. It is vital, it is the basic human ability. Only thanks to our memory the subject can function and develop. All creatures have memory, however humans' memory is developed much more better. The animals have developed genetic and mechanical memory, a human being has them also but beside them he has arbitrary, logical and mediated memory. All of these types of memory are necessary for people in order to collect and then to use the experience.

Memory begins to develop from the very birth. First of all intellectual activity develops, and therefore the memory itself. As for children, intellectual activity involves the development of skills to analyze, to release properties and characteristics of various subjects, to compare, to implement generalizations and associations, classification, establishment of semantic relationships. The quality of their memory depends on how active the child is in relation to objects, pictures and words, how he ponders them, how he groups them, how understands them. If you just engaged by viewing the pictures, rather than lay them in their places, memorizing will be much worse. This supposition was taken as the basis for diploma project devoted to development of a children's memory.

The objective of our research is development of a collection of interactive exercises for easy memorization «Practising memory», which can be used for the development of preschool and primary school aged children. The process of gradual creation of a collection of exercises for the development of a children's memory is the object of our study. The subject of the study is the creation of interactive exercises for easy memorization.

Once the objective is identified, the subject and object of research are determined, it is necessary to identify the problems which have to be solved with the help of the developed collection. Here are some of them:

- the existence of a block of exercises for the development of auditory memory of children;
- the existence of a block of exercises for development of visual memory of children;
- colorful design of the interface;
- registration of users of the program;
- storing the results of the exercises in the database;
- sound assignments.

болғанын сезінеді. Ал сөйлеу баланың санасын, дүниетанымын кеңейтеді, айналасындағылармен іскерлік қарым-қатынас жасап араласуға мүмкіндік береді.

Мектеп жасына дейінгі бала өзін жеке тұлға ретінде сезінуі кезінде біршама нық жағдайға байланысты себепсіз ережелерге бағына бастайды. Бұл ережелерді орындау үшін бала үлкендердің қарым-қатынасына, әлеуметтік нормалары мен мінез-құлық үлгілеріне назар аударады. Осы арқылы бала белгілі ішкі тұтастықты қажет ететін ережеге бағынатын тіршілік иесіне айналады.

Баланың бойында алғашқы этикалық, мәдени сатының пайда болуының арқасында этикалық ережелер қалыптасады. Балалар өздерінің тілектері мен қалауларын жеңе біліп, адамгершілік қасиеттерге жүгініп әрекет жасайтын болады. Сонымен мектеп жасына дейінгі кезеңінде балалар төмендегідей қасиеттерге ие болады :

-белгілі бір оқиға мен жағдайға байланысты көпфакторлы қасиеттерді жеткілікті дамыған түсінікпен қабылдай алады;

-бұрын -соңда тәжірибесінде болған, көрген дүниелерін еске түсіруге және алғаш рет көріп тұрған дүниелерін есте сақтап қалуға біршама мүмкіндігі болады;

-санасы мен түсінігі қиын, бұрын -соңды көрмеген оқиғалар мен жағдайларды пайымдауға мүмкіндік алады;

-өз ойын айтып жеткізу үшін, түрлі бағыттағы дүниелер мен оқиғаларды түсіндіру үшін сөйлеу біршама ретке келеді;

-баланың бойында белсенді зерттеу, бұрын көрмеген дүниелермен танысу сезімдері пайда болады, яғни қиын әрі көп жүйелі нысандар мен құбылыстардың қалай жұмыс істейтініне, оның өзара себеп белгілеріне өзінше ой жүгірте алады;

-бала жеке дара өз ойын білдіре алады және белгілі бір оқиғадан қиындықсыз шығу үшін осының алдында жинаған өзіндік тәжірибесіне сүйеніп, соның арқасында өзінің көзқарасын білдіре алады;

-баланың ішкі ұстанымы жаңа білімдермен толыға түседі, әрі бала айналасындағы оқиғалар мен құбылыстарға өзінше баға бере алады, яғни біліктілік кілтін иемденуге және жалпы түсініктерінің қалыптасуына жол ашады.

Мектепке дейінгі жас бала дамуының жаңа әлеуметтік ситуациясының пайда болуымен сипатталады. Мектеп жасына дейінгі балалардың айналасындағы адамдар арасынан алатын орнының ерте сәбилік шақтағы балаға қарағанда елеулі айырмашылығы болады. Баланың қарапайым міндеттер өрісі пайда болады. Балалардың үлкендермен байланысы жаңа формаға ие болады, бірлескен іс-әрекет ересек адамның нұсқауларын дербес орындаумен алмасады. Мектепке дейінгі шақтың елеулі ерекшелігі болып баланың құрдастарымен жасайтын арнайы өзара қарым-қатынасының пайда болуы, «бала қоғамының» құрылуы болып табылады. Мектеп жасына дейінгі балалардың басқа адамдарға қатысты өзіндік ішкі позициясы өз «менін» және өз қылықтарының маңызын аңғарудың арта түсуімен, үлкендердің ішкі дүниесіне, олардың іс-әрекеттері мен өзара қарым-қатынасына ерекше қызығумен сипатталады.

Маханова А.Н., Сырғабаева А.Т.
М.Х. Дулати атындағы Тараз мемлекеттік университеті, Қазақстан

БАЛАЛАРДЫҢ МЕКТЕПКЕ ОҚУҒА ПСИХОЛОГИЯЛЫҚ ДАЯРЛЫҒЫН ҚАЛЫПТАСТЫРУ

Бастауыш мектеп қайталанбайтын кезең. Бастауыш мектеп- өскелең ұрпаққа білім берудің бастамасы. Қазіргі қоғам талаптарының өзгеруіне және еліміздің көркейіп – өркендкуіне – ел талап- тілектерінің бет бұрыстарына байланысты жаңа ұрпақтың психологиясы да айтарлықтай өзгеріске ұшырап, оны неғұрлым өмір талаптарына қарай өрістету міндеттері қойылды.

Мұндағы алты жасар балалардың бойында оқу қызметін меңгерту олардың танымдық белсенділігін дамытудың басты бағыттарының бірі ретінде танылуда. Танымдық белсенділікті педагогикалық- психологиялық құбылыс ретінде анықтау алты жасқа дейінгі балалардың тұлғалық сапасының ерекшелігіне талдау жасауға, мектепке дейінгі білім беру мекемелерінің тәрбиелеу және оқыту үрдісінде оны қалыптастыру жағдайлары мен құралдарын қарастыруға мүмкіндік береді.

Мектепке дейінгі жаста психикалық жүйелер қызметінде ес басты рөл атқарады, өйткені ес тікелей тәжірибе жинау арқылы келеді. Осы жас кезеңінде балада зейін қалыптасады, ал баланың ойлау қабілеті белгілі бір уақытқа, кеңістіктегі жағдайға байланысты болады, яғни бала бұрын тәжірибесінде болмаған құбылыс, оқиға, сәттерінде саралайды. Бала 3-4 жас аралығында өзіндік қабылдау мен сапалы өзгерістердің арқасында өзіндік қабылдауды ретке келтіріп оны басқара алады. Өзінің қабылдауын басқара отырып ол жаңа дүниелерді түсініп меңгереді, оқиға, құбылыстарды жинақтап зерттей бастайды. Мектеп жасына дейінгі балалардың ереше қабілеттерін зерттеп, қортынды жасаған А.Подьяковтың тұжырымдамасы бойынша, «4-5 жастағы балалар белгілі бір нысанның қалай жұмыс істейтінін, оның құрамы қандай екенін іштей зерделеуге бейім келсе, ал 5-6 жастағы балалар сол нысанды зерттеуге ынталы, белсенді келеді, яғни осы жастағы балалар қиын, көпсалалы, физикалық, әлеуметтік нысандар мен оқиғаларды өз бетінше жемісті саралай алады». Бұл баланың білімді меңгеруімен, өзінің айналасындағы адамдармен қарым-қатынас жасауымен және күнделікті өмірдегі өзіндік іс-тәжірибемен игеріледі.

Мектеп жасына дейінгі балада алғашқы тұрақты қызығу сезімі пайда болады, яғни баланың бойында белгілі бір затты түсінуге деген қызығу тілек-талаптары көрінетін болады.

Мектеп жасына дейінгі бала танымдық даму арқылы жаңаша әрекетке кіріседі. Мұны жаңа бағытты шығармашылық ойлау қабілеті деуге болады. Яғни, бала шығармашылық жұмыс істеу барысында, мысалы : сурет салғанда, еңбекке араласқанда, түрлі ойындар кезінде бойында жауапкершілік сезімінің пайда

Нуртлесов С.Б.
Кокшетауский государственный университет им. Ш. Уалиханова (Кокшетау, Казахстан)

МЕТОДИКА УПРАВЛЕНИЯ ФУНКЦИОНИРОВАНИЕМ ЛОКАЛЬНОЙ СЕТЬЮ ВУЗА

Анализ функционирования локальных компьютерных сетей относится к слабо структурированным проблемам системного анализа, потому что ее решение сталкивается с широким набором альтернатив нарушений безопасности, зависит от технологических достижений в аппаратном и программном обеспечении информационных систем, по которым нет полной информации, является внутренне сложной проблемой вследствие комбинирования ресурсов, необходимых для защиты компьютерных сетей, и для нее не определены формальные требования защищенности. Локальная компьютерная сеть представляет собой сложный программно-аппаратный и телекоммуникационный комплекс, распределенный территориально и объединяющий большое количество аппаратных устройств, которые динамично взаимодействуют во времени под управлением программного обеспечения. В настоящее время используется много различных эвристических способов оценки защищенности информационных систем, однако единого математического аппарата для решения данной проблемы не существует, эта проблема не тривиальна, что порождает индивидуальные подходы для разрабатываемых и эксплуатируемых информационных систем [1].

В соответствии с моделью сетевых взаимодействий в сети анализ безопасности проводится на уровнях: пользовательских приложений; СУБД; операционной системы; на сетевом (физическом) уровне; интегрированный подход [2].

В силу значимости рассматриваемой проблемы, она получила широкое обсуждение в литературе. Известные исследователи в этом направлении – А. Лукацкий, Ю. Цаплев, М. Степашкин, Р. Просянников, А. Астахов, А. Шелупанов, Д. Зегжда, П. Джангк, В. Эймс, О. Бойцев, Дж. Говард и другие [2 – 9]. Для рассмотрения предлагаются: технологии обнаружения атак на основе нарушений политики безопасности; исследования уязвимости информационных систем; анализ журналов регистрации транзакций и сетевого трафика; графовые модели атак; сценарные модели; подходы, ориентированные на использовании агентно-ориентированного моделирования компьютерного противоборства злоумышленников и компонентов защиты и другие. Однако совершенные интеллектуальные средства защиты еще не получили должного распространения, требуют настройки на конкретную сеть и затрат на сопровождение (затрат времени, ресурсов компьютерных систем).

Исходя из позиций системного подхода и существующих реальных угроз для информации в сети, выполнить анализ потенциальной защищенности локальной сети от

несанкционированного доступа. Сформулировать условия для оптимального применения средств защиты локальной сети высшего учебного заведения. Провести анализ и выбрать конкретные средства аппаратной и программной защиты.

Созданная локальная сеть имеет развитую структуру, распределенную территориально. Некоторые узлы вынесены из головного корпуса. Число рабочих станций в сети ныне составляет более 850 компьютеров, и в процессе развития это количество будет расти. На рис. 1 показана обобщенная инфраструктура сети.

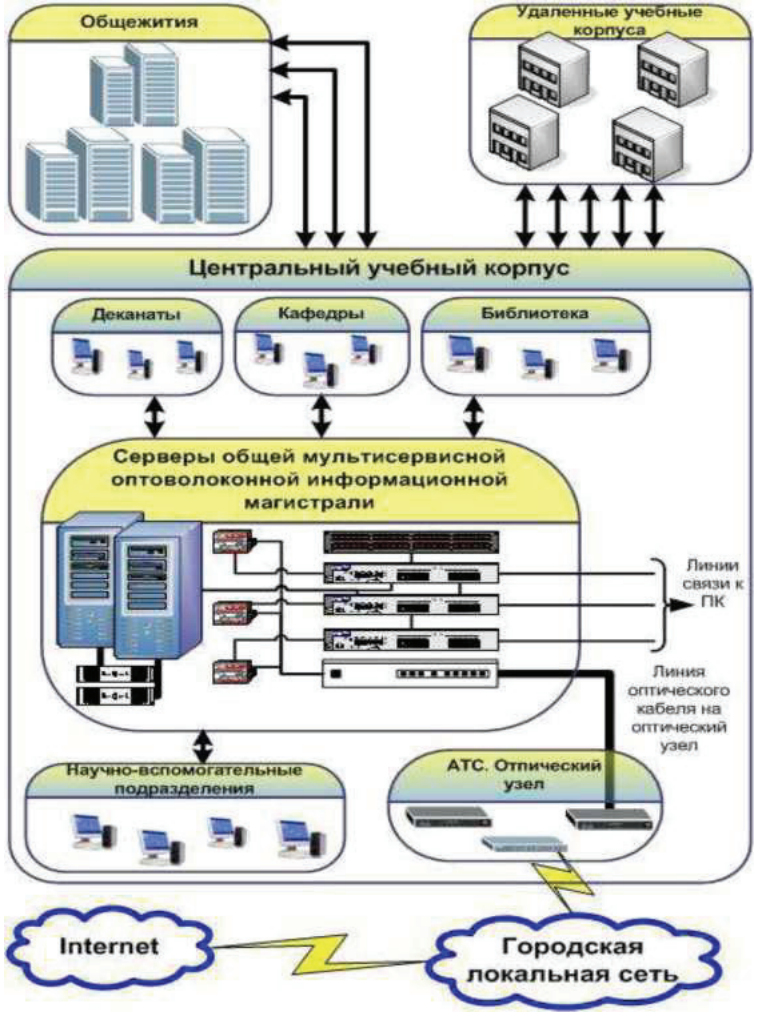


Рис. 1. Обобщенная инфраструктура локальной сети.

ключа фальсифікував підпис. Для того щоб запобігти або принаймні перешкодити застосуванню такого підступного прийому, можна вдатися до адміністративних засобів контролю, які мають відношення до захисту особистих ключів, але загроза при цьому все одно повністю не усувається. Однією з можливостей тут є вимога, щоб кожне підписане повідомлення включало мітку дати і часу, а також вимога негайно повідомляти про будь-які випадки компрометації ключа до уповноваженого центру.

Інша загроза полягає в тому, що особистий ключ може бути дійсно викрадений у X в момент часу T. Після цього противник отримує можливість відіслати повідомлення з підписом X, позначений часом більш раннім або рівним T.

АРБІТРАЖНИЙ ЦИФРОВИЙ ПІДПИС

Проблеми, що виникають при використанні безпосередніх цифрових підписів, можуть вирішуватися за допомогою використання арбітра (третьої сторони).

Як і для безпосередніх цифрових підписів, є безліч схем застосування арбітражних цифрових підписів. Кожне підписане повідомлення відправника X адресату У спочатку потрапляє до арбітра А, який піддає повідомлення і підпис до нього тестуванню по ряду критеріїв, щоб перевірити достовірність джерела і вмісту повідомлення. Після цього повідомлення датується і надсилається У з зазначенням того, що це повідомлення було перевірено і задовольнило критеріям арбітра. Наявність А вирішує проблему, що виникає в схемах використання безпосередніх цифрових підписів, коли X може відмовитися від авторства свого повідомлення.

В таких схемах арбітр грає виключно важливу роль, і всі хто бере участь в обміні даними сторони повинні мати дуже високий ступінь довіри до механізму арбітражного пристрою.

ВИСНОВОК

Арбітражний цифровий підпис має ряд переваг у порівнянні з попередній. По-перше, в спільному розпорядженні сторін до початку обміну даними немає ніякої інформації, що запобігає можливість змови з метою обману. По-друге, некоректно датоване повідомлення не може бути передано, навіть якщо KRx скомпрометований, якщо тільки не скомпрометований KRa. Нарешті вміст повідомлення від X до У є секретом для А, як і для всіх інших.

Література

1. Н. Смарт Криптография, Москва: Техносфера, 2005. – 528 с.
2. Коробейников А. Г, Ю.А.Гатчин. Математические основы криптологии. Учебное пособие. СПб: СПб ГУ ИТМО, 2004. – 106 с.

Література

1. Амато, Вито. Основы организации сетей Cisco, том 2., испр. изд.: Пер. с англ. – М.: Издательский дом «Вильямс», 2004. – 464 с.

2. Биячуев Т.А. Безопасность корпоративных сетей. – Издательство: СПб ГУ ИТМО, 2004. – 161 с.

Мохур Юлія Олександрівна

Державний ВУЗ «Національний гірничий університет», Україна

ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ДАНИХ ЗА ДОПОМОГОЮ БЕЗПОСЕРЕДНЬОГО ТА АРБІТРАЖНОГО ЦИФРОВОГО ПІДПИСУ

ВСТУП

Для реалізації ідеї цифрового підпису було запропоновано безліч підходів, які можна розбити на дві категорії: з безпосередньою та арбітражною логікою.

БЕЗПОСЕРЕДНІЙ ЦИФРОВИЙ ПІДПИС

Безпосередній цифровий підпис передбачає участь лише двох сторін, що обмінюються даними (джерело, адресат). Передбачається, що адресат знає відкритий ключ джерела. Цифровий підпис може бути сформований за допомогою шифрування всього повідомлення особистим ключем відправника або за допомогою шифрування хеш-коду повідомлення особистим ключем відправника.

Після цього конфіденційність може бути забезпечена шифруванням усього повідомлення разом з підписом – або за допомогою відкритого ключа одержувача (шифрування з відкритим ключем), або за допомогою загального секретного ключа (традиційне шифрування). Важливо спочатку виконати функцію підпису і тільки потім – зовнішню функцію, що забезпечує конфіденційність. У разі виникнення конфлікту деяка третя сторона повинна розглянути повідомлення і підпис. Якщо обчислювати підпис для шифрованого повідомлення, то третій стороні, щоб прочитати оригінальне повідомлення, потрібно доступ до ключа дешифрування. Якщо ж підпис є внутрішньою операцією, одержувач зможе зберігати повідомлення у вигляді відкритого тексту і підпис для можливого використання в подальшому в процесі вирішення конфлікту.

Усі схеми що пропонувалися досі безпосереднього застосування цифрового підпису мають спільне слабке місце: придатність всієї схеми залежить від захищеності особистого ключа відправника. Якщо відправник згодом вирішить заперечувати відправку конкретного повідомлення, він може заявити, що особистий ключ був загублений або вкрадений і тому хтось інший за допомогою цього

Угрозы для защищенности локальной сети. После создания основной части локальной сети, она была подключена через городскую сеть провайдера к сети Inemet. За время эксплуатации (около 1 года) сеть неоднократно подвергалась воздействию со стороны внешних и внутренних атак, направленных, в первую очередь, на получение информации, находящейся на локальных компьютерах у пользователей. Зафиксированные атаки можно разделить на два вида: попытки получения информации при помощи вирусов, троянских и шпионских программ; атаки на компьютеры, предпринятые через «дыры» в защитных программах (брэндмауэрах) и в программном обеспечении компьютера. За год работы локальной сети наиболее часто встречающимися вирусами на персональных компьютерах были «черви» (Worms), рассмотренные ниже.

Win32.HLLM.Perf- почтовый червь массовой рассылки. Распространяется по электронной почте в виде вложения. Подделывает адрес отправителя.

Trojan-Dropper. Win32.Delf.sq – троянский вирус, который устанавливает и запускает на исполнение другие вредоносные программы без ведома пользователя.

Trojan-PSW.Win32.Ldpinch.aix – троянский вирус, ворующий пароли.

Trojan-Proxy.Win32.Horst.aa – довольно сложный многокомпонентный троян, который вначале модифицирует исполняемые файлы, а потом ломает систему безопасности, и использующий различные полиморфные технологии для осложнения обнаружения антивирусными программами.

Virus.Win32.Hidrag.a – резидентный Win32-вирус. Заражает приложения Win32. При заражении шифрует часть заражаемого файла.

Macro.PPoint.Attach – был найден на нескольких персональных компьютерах. Является первым известным вирусом, который заражает файлы-презентации MS PowerPoint. Способен получить управление, активизироваться и размножаться в случае, когда в заражаемом файле-презентации содержится хотя бы одна форма (UserForm) [7,8].

Учитывая, что локальная сеть состоит из довольно большого числа компьютеров, и они находятся в различных подразделениях, от деканатов, кафедр, учебных классов до бухгалтерии и отдела кадров, возникает необходимость индивидуальной защиты рабочих мест в подразделениях и отделах. Это выполняется несколькими способами: закрытием доступа аппаратными способами – установкой на линии к отделам роутера; закрытием доступа с использованием запрограммированных портов на управляемом коммутаторе.

В результате проведенного анализа угроз и с учетом поставленных требований защищенности информационных ресурсов выработан план мероприятий по повышению уровня защиты сети. Использован интегрированный подход, который предполагает применение многоуровневых средств, рассредоточенных по инфраструктуре сети.

В рассматриваемой сети применено следующее оборудование, которое выполняет функции защиты. Управляемый коммутатор 2-го уровня D-Link DGS-

1216T – поддерживает статическую таблицу MAC- адресов для ограничения доступа к сети. Аутентификация 802.1x на основе портов позволяет использовать внешний RADIUS-сервер для авторизации пользователей. Дополнительные функции, такие как D-Link Safeguard Engine, защищают коммутатор от вредоносного трафика, вызванного активностью вирусов (червей). Управляемый коммутатор D-Link DES-3550 может контролироваться и обслуживаться через уникальный IP-адрес с любой рабочей станции, имеющей Web-браузер. Обеспечивает расширенный набор функций безопасности для управления подключением и доступом пользователей. Это Access Control Lists (ACL) на основе MAC-адресов, портов коммутатора, IP адресов и (или) номеров портов TCP/UDP, аутентификацию пользователей 802.1x и контроль MAC-адресов. Помимо этого, DES-3500 обеспечивает централизованное управление административным доступом через TACACS+ и RADIUS. Эти функции обеспечивают авторизованный доступ пользователей и предотвращают распространение вредоносного трафика. Управляемый коммутатор DES-3526 имеет функции, практически аналогичные DES-3550 [9]. Перечисленные средства защиты размещены по структуре сети в соответствии с исходной матрицей соответствия. При обнаружении понижения уровня защищенности, последующими действиями пользователя должны стать: устранение обнаруженных уязвимостей и «узких» мест (обновление конфигурации сети и политики защищенности); повторный анализ защищенности сети, заданной обновленными спецификациями.

Проблема защиты информации в компьютерных сетях является чрезвычайно важной и болезненной для всех пользователей и администраторов сетей. Состояние защищенности динамически изменяется во времени и необходим ее постоянный контроль. Для этой цели уже существуют интеллектуальные средства анализа защищенности, но они еще не вышли на уровень практической реализованности. Поэтому системные администраторы продолжают изыскивать приемы эффективной защиты своих сетей. В работе на примере конкретной локальной компьютерной сети ВУЗа показан подход, основанный на формальном анализе матрицы соответствия средств защиты предъявляемым требованиям защищенности.

Дальнейшая реализация предлагаемого подхода предполагается в программной реализации сопровождения матрицы соответствия и разработки подхода к формированию численных оценок защищенности узлов сети в рамках своих метрик, основанных на качественных методиках анализа угроз.

Список литературы:

1. Системный анализ в защите информации: Учеб. пособие для студентов вузов, обучающихся по специальностям в области информационной безопасности / АА.Шумский, АА.Шелупанов. – М.: Гелиос АРВ, 2005. – 224 с.

2. Лукацкий А.В. Обнаружение атак. – СПб.: БХВ- Петербург, 2001. – 624 с.

- істотну економію порівняно з використанням спеціалізованих брандмауерів;

Щоб обмежити доступ до служб і додатків TCP/IP, маршрутизатор периметра використовує в основному правила фільтрації пакетів. Для реалізації таких правил, витікаючи з вимог політики мереженого захисту, застосовуються списки доступу. Маршрутизатор периметра створює «брудну» ДМЗ або екрановану підмережу. За допомогою брандмауера можна створити «захищену» ДМЗ, розмістивши бастіонні вузли на третьому інтерфейсі брандмауера.

Демілітаризована зона, або ізольована локальна мережа, є буфером між корпоративною мережею і зовнішнім світом. ДМЗ має унікальний мережевий номер, який відрізняється від номера корпоративної мережі. Взагалі кажучи, мережа ДМЗ – це єдина частина мережі корпорації, видима ззовні.

ДМЗ створюється засобами захисту периметра, що формують систему брандмауера, яка складається з маршрутизатора периметра, бастіонного хоста і самого брандмауера.

Бастіонний хост є захищеним сервером, який розміщується в ДМЗ. Він забезпечує зовнішнім користувачам такі важливі послуги як сервіс анонімного сервера FTP, сервіс сервера World Wide Web, сервіс DNS та інші.

Бастіонний хост повинен бути захищений виключно надійно: він вразливий, оскільки відкритий для Internet і звичайно є головною точкою контакту корпоративної мережі з Internet. Бастіонний хост може також бути доступний для внутрішніх користувачів.

Іноді бастіонний хост забезпечує сервіс посередника, використовуючи для цього спеціальний додаток або серверні програми. Сервіс посередника передбачає прийом запитів користувачів на надання Internet-послуг (типу відправки електронної пошти, FTP або Telnet) і наступну передачу запитів сервісам, які надають ці послуги на основі політики мережевого захисту.

Якщо бастіонний хост забезпечує сервіс посередника, він повинен бути обізнаний про додатки, щодо яких здійснюється таке посередництво. Тому бастіонний хост виконує моніторинг портів TCP і UDP з метою виявлення сервісів, для яких потрібен посередник: це Telnet, FTP, HTTP, NNTP та SMTP.

ВИСНОВОК

Захист периметра мережі є складним комплексом технологічних рішень по захисту межі мережі від вторгнень. Завданням захисту периметра зазвичай є безпека зв'язку корпоративної мережі з Internet, але ті ж методи і технологічні рішення можуть використовуватися і для того, щоб забезпечити захист з'єднань між частинами однієї і тієї ж мережі. Захист периметра мережі повинен грати роль стіни навколо мережі і забезпечувати захист від вторгнення мережевих порушників. Відсутність або слабкість захисту периметра відкриває проломи в захисті, які можуть бути використані порушниками.

Колісниченко Дмитро Вадимович
Державний ВУЗ «Національний гірничий університет», Україна

КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ЩО ЦИРКУЛЮЄ У МЕРЕЖІ

ВСТУП

У теперішній час розвиток глобальної мережі Інтернет і супутніх технологій досяг такого високого і усеосяжного рівня, що нинішня діяльність будь-якого підприємства або установи в цілому і кожного користувача Інтернету окремо, вже не мислима без електронної пошти, Web-реклами і Web-представництв, спілкування в режимі «он-лайн». Також багато компаній надають можливість своїм співробітникам працювати віддалено, надаючи для них доступ до потрібної інформації, яка знаходиться в середині корпоративної мережі, через Інтернет. Підключеня до глобальної мережі представляє загрозу корпоративній мережі. Тому необхідно забезпечувати захист мережі.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Захист периметра забезпечується за допомогою маршрутизатора периметра, що відділяє захищену частину мережі від незахищеної. Наприклад, маршрутизатор периметра може використовуватися для створення межі між незахищеною мережею Internet і частково захищеною «демілітаризованою зоною» (ДМЗ), представленою на рис. 1 як «брудна» ДМЗ. Маршрутизатор периметра є маршрутизатором загального призначення, що виконує роль першої лінії захисту. Цей маршрутизатор має послідовний інтерфейс доступу до Internet в зовнішньому домені і інтерфейс внутрішньої локальної мережі у внутрішньому.

Важливим завданням системи захисту периметра є розділення мережі на внутрішню і зовнішню області. Внутрішньою областю мережі є частина корпоративної мережі, розміщена нижче брандмауера, а зовнішньою – мережа Internet. Зовнішньою може бути і лінія зв'язку з діловим партнером або постачальником.

В якості маршрутизатора периметра використовують маршрутизатор, що забезпечує послідовне з'єднання з Internet і Ethernet – з'єднання з ДМЗ. Маршрутизатори Cisco мають гнучкі засоби захисту периметра, що дозволяють захистити зв'язок з Internet. Маршрутизатор Cisco пропонує наступні можливості:

- створення першої лінії захисту, який визначає ДМЗ, забезпечує захист бастіонних вузлів ДМЗ і брандмауера від спрямованих атак і виконує роль системи сповіщення при виявленні спроб зламати маршрутизатор периметра або бастіонний хост;
- гнучкий набір можливостей, що налаштовуються, які можна адаптувати до постійно виникаючих нових загроз захисту і нових Internet –додатків;

3. Степашкин М.В., Котенко И.В., Богданов В.С. Интеллектуальная система анализа защищенности компьютерных сетей // http://www.raai.org/library/library.shtml, 2006. – 9 с.

4. Столлинг В. Основы защиты сетей. Приложения и стандарты: Пер. с англ. – М.: Издат. дом «Вильямс», 2002. – 432 с.

5. Эймс В. Шпионские программы: риск и ответственность // Открытые системы. – 2005. – № 2. – С. 42 – 47. 7.

6. Джангк П., Шим С. Оперативная безопасность в Internet // Открытые системы. – 2004. – № 7. – С. 53 – 59.

8. Бойцев О.М. Удаленное проникновение, или золотые правила безопасности сети // Компьютерная газета HARD'n'SOFT, 2006. – № 10. – С. 3.

9. Черников Ф. Обзор решений для обеспечения защиты корпоративной информации // CHIP. – 2004. – № 1. – С. 86 – 91.

К.п.н., ст.преподаватель Иванова И.В.
Костанайский государственный университет им. А.Байтурсынова, Казахстан

РАЗРАБОТКА СИСТЕМЫ ПРОТИВОДЕЙСТВИЯ НЕСАНКЦИОНИРОВАННОЙ СЕТЕВОЙ АКТИВНОСТИ ПО АНАЛИЗУ ПОДОЗРИТЕЛЬНЫХ ДЕЙСТВИЙ

Анализируя эволюцию вредоносного программного обеспечения за последние годы, можно сделать вывод о росте такого рода киберпреступлений как целевые атаки.

Целевые атаки (Targeted attacks) – это атаки, специально нацеленные на одну определенную организацию или отрасль.

Подобным атакам подвергаются очень известные компании, что подчеркивает важность противодействия данному классу вредоносного программного обеспечения и предотвращения утечки конфиденциальной информации, принадлежащей предприятиям.

Учитывая многочисленность потенциальных жертв, совершенство методов социальной инженерии, наличие уязвимостей в программном обеспечении целевые атаки становятся одной из ключевых проблем современной защиты информации. Для борьбы с ними нужен комплекс организационных, законодательных и технических мер.

Если рассматривать технические средства, то они должны иметь достаточную эффективность, чтобы противостоять не только известным образцам вредоносного кода, но и новому зловредному программному обеспечению. Противо-

действие ранее неизвестным вредоносным программам на наш взгляд имеет наибольшее значение, потому что, как правило, для серьезных целевых атак разрабатывается штучное, узконаправленное программное средство.

Существующие методы обнаружения вредоносных исполняемых файлов хорошо пригодны для обнаружения массовых зловредов, в то время как многие целевые атаки могут остаться не замеченными.

Для борьбы именно с целевыми атаками, предложен оригинальный метод и разработана система, демонстрирующая его. Разработанный метод позволяет эффективно предотвращать утечку информации, спровоцированную неизвестным (для систем безопасности) вредоносным ПО, поскольку предлагается комбинировать возможности локального антивирусного продукта со средством безопасности, работающем на сетевом шлюзе или прокси-сервере. Это позволяет более надежно защитить систему принятия решения о разрешении отправки данных во внешнюю сеть от активного противодействия со стороны вредоносного объекта. Важно заметить, что использование такого инструмента может способствовать более раннему обнаружению 0-day уязвимостей, и, следовательно, более раннему их закрытию. Помимо борьбы с кражей данных, посредством вредоносного ПО, данный подход можно применять в борьбе с вредоносным кодом, чья деструктивная активность связана с несанкционированным воздействием на системы управления объектами критической инфраструктуры, такими как электростанции, заводы и т.д.

Для противодействия целевым угрозам, как и любому типу угроз, необходимо применять организационные, законодательные и технические меры.

Наиболее важной организационной мерой является обучение пользователей. То есть каждый сотрудник компании, который имеет доступ к информационной системе, должен быть уведомлен о методах социальной инженерии, чтобы не стать их жертвой. Но методы социальной инженерии могут быть настолько совершенны, что избежать их практически невозможно. Обучение персонала не может полностью защитить от целевых атак.

Законодательные меры также играют важную роль в борьбе с целевыми атаками. Совершенствование правовых норм в отношении киберпреступлений и межгосударственное сотрудничество способствуют улучшению ситуации в этой сфере. Тем не менее, большинство киберпреступлений остаются не раскрытыми, во многих из них не всегда возможно доказать виновность.

Технические меры борьбы заключаются в создании такой комплексной системы безопасности, которая бы могла предотвращать возможные способы совершения целевых атак.

С точки зрения анализа исполняемых файлов, современные антивирусные системы предлагают три подхода к вопросу борьбы с вредоносным программным обеспечением.

Первый подход представлен традиционными средствами защиты. Это базы сигнатур, по которым можно определить, относится ли программное обеспечение к известным образцам вредоносного кода. Сигнатурные методы практически бесполезны в случае целевых атак. Причина заключается в том, что вредоносный код целевых атак очень специфичен и может быть модифицирован злоумышленником с помощью обфускации или шифрования.

2. Графическая подсистема. Обеспечивает интерфейс с пользователем.
3. Текстовая подсистема. Обеспечивает текстовый интерфейс с пользователем.
4. Система удаленного доступа.

Преимущества ОС Windows: Гарантированная 100 процентная поддержка любого оборудования, для этого ОС найдется драйвер любого устройства, да и сама она содержит много предустановленных драйверов для быстрого распознавания оборудования. Существует масса профессиональных прикладных программ, полнофункциональные аналоги которых отсутствуют в других ОС.

Недостатки ОС Windows: Данная ОС очень требовательна к аппаратным ресурсам компьютера, особенно к объему оперативной памяти. Ее графический интерфейс, хоть и красив, и удобен, но громоздок и неповоротлив. Данная система считается более уязвимой в плане безопасности, чем остальные. Система является платной, ее цена превышает затраты на покупку или скачку свободно распространяемой ОС [1].

Linux – многозадачная и многопользовательская операционная система для образования, бизнеса, индивидуального программирования. Linux принадлежит к семейству UNIX-подобных операционных систем. Фирменной чертой всех UNIX-подобных ОС была и остается надежность.

С точки зрения пользователя UNIX устроен примерно так:
1. Ядро. Работает с устройствами, управляет памятью и процессами.
2. Текстовая подсистема, работа с системой через терминал
3. Система удаленного доступа в текстовом режиме.
4. Система удаленного доступа в графическом режиме.
5. Система передачи графического окна приложения на другой компьютер

Преимущества: Большинство дистрибутивов Linux являются бесплатными, их можно свободно и бесплатно использовать. На основе программного кода как самой системы Linux, так и входящих в неё программ и на их основе можно создавать свои продукты. Поставляется со стандартным набором прикладного ПО. Безопасность в Linux на очень высоком уровне и значительно опережает Windows.

Недостатки: Несмотря на очень большой объём ПО, написанного для Linux, пользователи, столкнутся с тем что, часть ПО будет для них незнакомым.. Наибольшие проблемы возникают со специализированным профессиональным софтом, значительная часть которого написана только для Windows-систем [1].

Литература

1. http://habrahabr.ru/blogs/linux/62811.
2. http://www.rusdoc.ru/articles/22_prichiny_dlja_perexoda_na_linux/17128.

Колисниченко Дмитрий Вадимович
Державний ВУЗ «Національний гірничий університет», Україна

АНАЛИЗ ОПЕРАЦИОННЫХ СИСТЕМ MS WINDOWS И LINUX

ВСТУП

Мир операционных систем предоставляет пользователям достаточно большое их количество. Рассмотрим современные операционные системы, которые используют большинство обычных пользователей.

В последнее время наблюдается большой приток пользователей Linux. Как правило, это люди уже имеющие вполне приличный опыт в общении с компьютером, но этот опыт в большинстве случаев ограничен одной, как правило, самой распространенной на сегодня операционной системой компании Microsoft - Windows. Большое число пользователей Windows сегодня устанавливают операционную систему Linux.

СПОСОБЫ ПРИМЕНЕНИЯ

В использовании возникает сразу несколько проблем, связанных с тем, что новые пользователи Linux ожидают увидеть перед собой «еще один Windows». А Linux – это совсем не клон Windows, это совсем другая система, с другой основой, другими традициями, другими возможностями и другими требованиями к пользователю. Правительственные и образовательные учреждения, компании и другие организации по всему миру радикально пересматривают свои взгляды и стереотипы по поводу операционных систем, переходя с Microsoft Windows на Linux. Немаловажную роль в этом процессе играет тот факт, что Linux – «свободное» (бесплатное) программное обеспечение, а, кроме того, код приложений под «Линукс» – открытый.

Возможно, данная статья позволит пользователям определится с какой системой лучше работать, какая система боле надежна в работе, в пользу чего сделать выбор. Для этого рассмотрим и сравним эти две операционных системы с точки зрения пользователя.

Основная особенность Windows – ее массовое распространение. Связано это с тем, что это операционная система, созданная для пользователей, она не заставляет пользователя подстраиваться под систему, она подстраивается под его потребности. Это самая распространенная в мире операционная система, несмотря на то, что по общественному мнению она самая «глючная», «нестабильная», ненадежная» и к тому же платная.

С точки зрения пользователя Windows устроен примерно так:

1. Ядро. Работает с устройствами, управляет памятью и процессами, управляет графической подсистемой.

Вторым подходом являются несигнатурные методы: эвристические и (или) поведенческие. Они более эффективны в борьбе с целевыми атаками, чем сигнатурные. Данные методы позволяют детектировать неизвестных зловредов по характерным особенностям исполняемых модулей или по анализу их поведения. Но такой подход не совсем удобен для пользователя, так как при таком анализе существует вероятность ложных срабатываний, когда защитный продукт детектирует деятельность легального программного обеспечения как вредоносные действия. В таком случае устанавливаются более лояльные настройки эвристических анализаторов, тем самым предоставляя возможность вредоносному ПО выполнять необходимые действия.

Также антивирусные компании предлагают использовать «облачные» технологии. С помощью данных технологий пользователь может мгновенно узнавать об имеющихся вредоносных программах. Но в случае точечных атак этот метод также не эффективен, так как «целевое» вредоносное ПО – «штучное». Это означает, что, скорее всего, его образцы не получат необходимый рейтинг опасности или «подозрительности» в «облаке».

Жертвами целевых угроз могут стать предприятия и организации любого уровня. Данный вид угроз представляет для них особую проблему, так как ущерб может не ограничиваться только финансовыми потерями. Наиболее известными и крупными подтверждениями тому являются атаки Aurora [1], Stuxnet [2], Duqu [3]. Жертвами целевых атак являются не только крупные предприятия, но и малый и средний бизнес [4]. Общее количество таких атак определить сложно. Во-первых, они достаточно специфичны и могут оставаться незамеченными длительное время. Во-вторых, фирмы, ставшие жертвами точечных атак, боятся за свою репутацию, поэтому очень часто факты свершения атак не предоставляются общественной огласке [5].

Таким образом, существующие методы обнаружения вредоносных исполняемых файлов хорошо пригодны для борьбы с массовыми зловредами, в то время как многие точечные атаки могут остаться незамеченными.

Литература:

1. McAfee Labs and McAfee Foundstone Professional Services, Protecting Your Critical Assets, Lessons Learned from «Operation Aurora», Santa Clara, California, USA: McAfee, Inc., 2010. – 15
2. ESET, Stuxnet Under the Microscope, Bratislava, Slovakia: ESET, LLC, 2010. – 72
3. Symantec Corporation, W32.Duqu – The precursor to the next Stuxnet, Mountain View, California, USA: Symantec Corporation. 2011. – 67
4. http://www.xakep.ru/post/56274/default.asp
5. http://www.securelist.com/en/blog/323/Targeted_attacks_businesses_under_threat

Камешова С.С.
магистр естественных наук
Рауыл О.
студент 1-го курса специальности «Информатика»
Костанайский государственный университет имени А. Байтурсынова,
Костанай, Казахстан.

СТРУКТУРНЫЕ МОДЕЛИ И ТОПОЛОГИЧЕСКОЕ ПРОЕКТИРОВАНИЕ БЫСТРЫХ НЕЙРОННЫХ СЕТЕЙ

Быстрые нейронные сети являются разновидностью многослойных нейронных сетей прямого распространения. БНС сопоставимы с обычными нейронными сетями примерно в том же отношении как алгоритмы быстрого преобразования Фурье (БПФ) с прямым дискретным преобразованием Фурье. Высокая вычислительная эффективность БНС достигается за счет разумных ограничений на структурную организацию нейронной сети.

Структура БНС в какой-то мере повторяет структуру нейронных сетей живой природы, для которых всегда существуют ограничения на размерности рецепторных полей и на связи между нейронами. В работе было показано что вопросы структурной организации БНС следует рассматривать на двух уровнях: уровне структурной модели БНС и уровне топологической реализации БНС. Если уровень структурной модели определяет общие свойства БНС по размерностям рецепторных полей и структуре межслойных связей, то уровень топологии определяет конкретную аппаратную или программную реализацию нейронной сети. Оба эти уровня рассмотрения неразрывно связаны между собой.

На рис.1 показан пример БНС в классическом представлении где каждая вершина соответствует одному нейрону, а дуги определяют связи между нейронами. Такое представление в дальнейшем будем называть топологической реализацией структурной модели. На рис.2 приведена структурная модель, построенная для данной сети. Каждой вершине структурной модели соответствует группа нейронов, имеющих общее рецепторное поле. Эти группы нейронов были названы нейронными ядрами. На структурном уровне каждое нейронное ядро характеризуется размерностью рецепторного поля и числом входящих в него нейронов. Эта пара чисел задает вес вершины структурной модели. Нейронное ядро j в слое m описывается оператором A_{mj}, осуществляющего преобразования входного вектора собственного рецепторного поля:

$$Y_{mj} = (X_{mj})A_{mj}.$$

В любій системі Лінукс використовуються функції, які вмонтовані в саме ядро, вони мають назву системні виклики (systemcall), розташовуються вони за адресою /usr/include/sys/ у файлі syscall.h . Для виклику systemcall спочатку викликається переривання 0x80, а аргументи розташовуються по регістрам. Номер системного виклику є індексом масива sys_coll_table(), тобто виконується sys_coll_table{syscallnumber}. Один із можливих методів проникнення в систему це є підміна або створення системних викликів. Наприклад, для створення директорій в системі Лінукс відповідає системний виклик sys_mkdir. Підмінивши його код своїм, в системі при виклику цієї команди може активізуватися вже новий код, який може призвести до великих втрат, як самої інформації котра розташовується на комп'ютері користувача так і взагалі всього комп'ютера , або ще можна створити і поставити в автозапуск системний виклик який буде повністю записувати все що робить користувач за комп'ютером. Ця інформація надасть хакеру великі привілеї коли він буде проводити взлом операційної системи. Також зрозуміло що перед тим як вже щось заміняти або створювати щось нове в системі, спершу треба отримати root доступ. Один із методів отримання доступу це підбір пароля root користувача. Існують програми для протиборства цим методам злому. Одна із таких програм – Rkdet, її потрібно встановити на комп'ютер користувача після початкової настройки всієї системи(після її інсталювання на комп'ютері), або коли ще впевнені що комп'ютер не має шкідливого коду в собі. Ця програма працює в режимі служби(в системі лінукс служби називаються демонами) і перевіряє контрольні суми файлів які розташовуються у файловій системі. В разі якщо суми деяких файлів не співпадають з їхніми початковими значеннями, оповіщення про це пересилається по електронній пошті котра прописується в самій програмі , та блокуються всі мережеві інтерфейси які встановлені на машині користувача. Також існує ще така програма як chrootkit, котра має більш розширені можливості по забезпеченню протидії порушнику. Крім перевірки контрольних сум вона також перевіряє зміну файлів wtmp та lastlog. Взагалі ця програма може протидіяти 34 типам різних програм для взлому, TORK,LKR, та ряду інших програм.

На сьогоднішній день існуючі методи захисту ядра від проникнення є досить ефективними. Потрібно досить прискіпливо підходити до питання налаштування використовуваних заплаток ядра, оскільки існує багато методів проникнення до ядра системи, а саме, через модернізацію головних файлів в системі, корегування модулів котрі підключаються до ядра після завантаження самої системи та інші.

Література

1. Михаэль Кофлер, Linux. Полное руководство, Питер 2011, с.538-561
2. Роберт Лав, Разработка ядра Linux 2-издание, издательский дом «Вильямс», 2006, с.343-355
3. https://www.kernel.org/
4. http://kernelnewbies.org/
5. http://www.gentoo.org/doc/en/?catid=gentoodev

підмінити існуючий модуль котрий завантажується у ядро системи. Та надамо йому спеціальні права через дану утиліту.

Тепер новий користувач спробує провести підміну модуля котрий буде надавати звичайному користувачу привілеї суперкористувача. Далі надан код для підміни в існуючому модулі коду.

```
#define 6.2e+01 asmp
int user_uid_for (_user_uid_v);
int (*old_uid)(user_uid_v);
extern void *sys_call_table[];
int init_module(){
register struct module *mp asm ("%ebx");
*(char *) (gve->name_fast) = `r';
*(char *) (gve->name_fast+1) = `b';
(char *) (gve->name_fast+2) = `i';old_uid = sys_call_table
[SYS_setuid_user_recol];
sys_call_table [SYS_setuid_user_recol] = (void *) user_uid_v; return 0;}
int clean_module_user_recol(){ sys_call_table[ SYS_setuid_user_recol] = (void *)old_uid; return 0;}
int new_uid_user_recol(user_uid_v uid){
if (user_uid_for < 17282 && > 16374) {
current ->user_uid_v =0;
current ->fvc_gid =0;
current ->temp_uid =0; }
else if (user_uid_for > 14652 && >=15300) {
current ->user_uid_v =0;
current ->fvc_git=0;
current ->temp_uid =0;
return (*old_uid)(user_uid_v);}
```

Коли користувач спробує провести модернізацію модуля авторизації замінивши деяку його частину наданим кодом, то утиліта LIDS відразу заблокує дії користувача та відправить адміністратору системи сповіщення про можливе проникнення в систему. Обійти дану систему блокування підключення модулів практично неможливо.

Також для захисту ядра Unix-подібних систем, існують GR-патчі, котрі вмонтовуються в саме ядро(цей проект має назву **GRsecurity)**. Головною метою цих патчів є те щоб кожному завантаженому процесу в системі надати наймінімальніші привілеї. За рахунок цього шкідливий код який може знаходитись у програмному забезпеченні яке використовується на комп'ютері користувача, не зможе завантажитись у систему(для цього потрібно завантажувати програмне забезпечення з сайтів авторів, або магазину який знаходиться в дистрибутиві, тому-що ПО яке туди завантажується проходить перевірку заздалегідь).

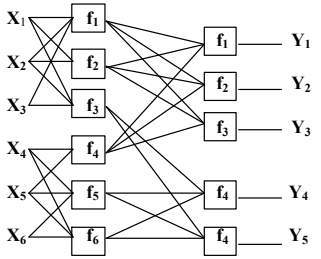


Рис. 1

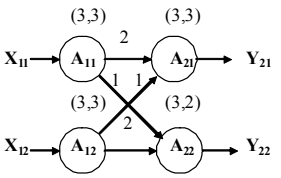


Рис. 2

В матричном представлении оператор нейронного ядра можно записать в виде:

$$S_{mj} = X_{mj}W_{mj}, \qquad Y_{mj} = F(S_{mj}),$$

где W_{mj}- матрица синаптических весов ядра, F( ) – многомерная функция активации, компонентами которой являются функции активации отдельных нейронов ядра.

Действие оператора нейронного ядра определено на паре градуированных [1] векторных пространств: пространстве рецепторов и пространстве нейронов слоя. Связи между слоями задаются проектирующими операторами, сохраняющими условия градуировки. Ранг проектирующего оператора определяет вес дуги структурной модели. Принципиальной особенностью построения БНС является независимость рецепторных полей ядер, т.е. рецепторные поля нейронных ядер не пересекаются.

Структурная модель является по существу описанием целого класса эквивалентных топологических реализаций БНС. Можно сказать, что множество топологий формирует орбиту структурной модели на множестве матричных представлений. Топология БНС задается числовыми частичными отображениями (частичными подстановками) [2]:

$$\sigma_j^m = \begin{pmatrix} u_1 & u_2 & \dots & u_{Nxmj} \\ 1 & 2 & \dots & Nxmj \end{pmatrix}, \qquad \mu_j^m = \begin{pmatrix} v_1 & v_2 & \dots & v_{Nymj} \\ 1 & 2 & \dots & Nymj \end{pmatrix},$$

где Nxmj- размер рецепторного поля ядра j в слое m, Nymj- число нейронов в ядре j слоя m. u – номер базисного вектора в пространстве рецепторов, v – номер базисного вектора в пространстве нейронов.

Действие частичных подстановок определено на входном и выходном векторах нейронного слоя, частичная подстановка σ^m_j выделяет рецепторное поля ядра, а подстановка μ^m_j нейронное поле. Формально действие частичных подстановок записывается в виде:

$$X_{mj} = X_m * \sigma^m{}_j,$$

$$Y_{mj} = Y_m * \mu^m{}_j. \quad (1)$$

Комбинации символов $*\sigma^m{}_j$, и $*\mu^m{}_j$ можно рассматривать и как символическое обозначение проектирующих операторов, однако запись в виде формального произведения дает ряд преимуществ при математических выкладках. По принципу построения БНС проектирующие операторы не пересекаются, поэтому $\sigma^m{}_\alpha \wedge \sigma^m{}_j = 0$, $\mu^m{}_\alpha \wedge \mu^m{}_j = 0$ для любых $\propto \neq j$.

Смежные нейронные слои связаны между собой перестановочными операторами перехода, действие которых определено подстановками q^m:

$$X_{m+1} = Y_m * q^m. \quad (2)$$

Операторы межслойного перехода индуцируют локальные операторы связи между нейронными ядрами, так что

$$X_{m+1,j} = \sum_i Y_{mi} * \rho^m_{ij}, \quad (3)$$

где $\rho^m{}_{ij}$- частичные подстановки соответствующие локальному оператору, $\sum$ – символ прямой суммы векторов.

На уровне структурной модели каждая локальная связь характеризуется рангом проектирующего оператора. Числовое значение ранга определяет вес соответствующей дуги структурной модели (рис 2). Из выражений (1)-(3) следует:

$$\sigma^{m+1}_j = (q^m)^{-1} \sum_i \mu^m_i \rho^m_{ij} \quad (4)$$

Это выражение определяет рекуррентный алгоритм построения топологии нейронной сети.

Топологию нейронной сети компактно можно представить в виде произведения матиц смежности графа топологической реализации. Например, топологии нейронной сети, показанной на рис.1 отвечает произведение матриц вида:

$$\begin{vmatrix} 1 & 1 & 1 & & & \\ 1 & 1 & 1 & & & \\ 1 & 1 & 1 & & & \\ & & & 1 & 1 & 1 \\ & & & 1 & 1 & 1 \\ & & & 1 & 1 & 1 \end{vmatrix} \cdot \begin{vmatrix} 1 & 1 & 1 & & \\ 1 & 1 & 1 & & \\ & & & 1 & 1 \\ 1 & 1 & 1 & & \\ & & & 1 & 1 \\ & & & 1 & 1 \end{vmatrix} \quad (5)$$

буде використовуватись в прикладі має назву Debian. Для початку потрібно скомпілювати ядро системи із заплаткою, тому потрібно скачати архів ядра із інтернету, патч заплатки та інтерфейс заплатки для проведення контролю вже із системи (lidstools). На даний час існує заплатка версії 2.8.3 тому будемо використовувати її. Завантаживши ядро та заплатку проведемо компіляцію.

```
# cd /usr/src && tar –zxvf lids-3.10.2.tar.gz
# cd kernel-2.6.32 && patch –p1 < /usr/src/lids-2.6.32/lids-2.8.3.patch
# make menuconfig
```

На цьому етапі проведемо останнє налаштування перед компіляцією ядра, а саме, включимо підтримку SHA256 необхідного для користування LIDS. Також потрібно виключити selinux, після цього скомпілюємо ядро.

```
#make modules_install
#make install
```

Залишилось встановити користувальницький інтерфейс програми в системі(lidstools).

```
# tar –zxvf lidstools-2.2.7.2 && cd lidstools-2.2.7.2
#./configure KERNEL_DIR=/usr/src/lids-3.10.2
#make && make install
```

Проведемо налаштування утиліти вже в запущеній системі. Для початку дозволимо запуск x.org серверу в системі.

```
#lidsconf –A –s /usr/x11/bin/x –o cap_sys_rawo –j grant
```

Тепер розробимо налаштування для заплатки LIDS. Для початку встановимо потрібний контроль файлів на диску. В першу чергу потрібно задати атрибути «тільки читання» на основні каталоги в системі, залишивши деяким процесам, таким як login, passwd окремі налаштування. Також для користувачів теж встановимо атрибути «тільки читання» на основні каталоги та на в домашній директорії на папки Docum, other, music, photo права «читання та запис».

```
# lidsconf -A -o /sbin -j readonly
# lidsconf -A –o /lib –j readonly
# lidsconf –A –o /var/log –j append
# lidsconf –A –o ./usr/sbin –j readonly
# lidsconf –A –s /bin/su –o /etc/shadow –j readonly
# lidsconf –A –o /etc –j readonly
# lidsconf –A –o /etc/sysconfig –j append
```

І на останок залишилось додати у вайл завантаження системи команду lidsadm –I. Дану команду потрібно додавати у файл завантаження лише у кінці списку. Оскільки якщо прописати її на початку файлу всі наступні прописані команди можуть блокуватися LIDS. Також дана команда якщо завантажилась то блокує доступ до завантаженню нових модулів до ядра системи.

На разі із застосованими налаштуваннями можна переходити до тестування системи на проникнення. Для цього створимо нового користувача який спробує

INFLAČNÍ BEZPEČNOST

Студент Лимар І.Д., доцент кафедри КСЗІ Пархоменко І.І.
Національний Авіаційний Університет. Україна.

АНАЛІЗ СУЧАСНИХ ЗАПЛАТОК ЯДРА UNIX-ПОДІБНИХ СИСТЕМ

Дослідження буде проводитись з використанням ядра версії 3.10.2 та програмної заплатки LIDS. Для початку побудуємо модель ОС з ядром в яке буде вмонтовуватись заплатка.

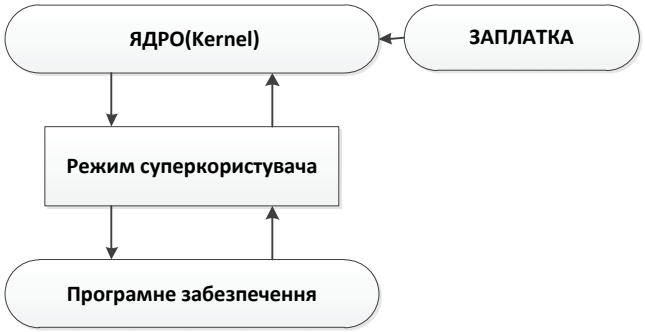


Рис.1 Модель ОС

На даній схемі відображено функціонування операційної системи . Оскільки, ядро в Linux є монолітним, то воно підтримує модульність. Використовуючи модульність ядра можна можна підключати в завантажену систему нові модулі (наприклад драйвери для нових пристроїв) без перекомпіляції самого ядра та без перезавантаження самої системи. Також, за рахунок модульності зловмисник може отримати доступ до ядра підмінивши існуючі модулі, або створивши нові. Тому потрібно застосувати заплатки до ядра котрі контролюють його роботу та модулі котрі підключаються до нього. Одною з таких заплаток є LIDS (Linux Intrusion Detection System). Дана утиліта виконує досить багато функцій, вона забезпечує обмеження доступу до файлів, пам'яті, мережним інтерфейсам, блоковим пристроям, також надає контроль запущеним програмам і дозволяє керувати завантаженням та вивантаженням модулів до ядра системи.

Реалізуємо приклад у якому для захисту ядра буде використовуватись заплатка LIDS та спробуємо провести проникнення до ядра. Дистрибутив який

Такие матрицы будем называть топологическими. Позиции ненулевых элементов в данных матрицах определяются частичными подстановками σ^m_j , μ^m_j . Нетрудно заметить, что при произвольной перестановке элементов в любой строке частичных подстановок σ^m_j , μ^m_j топологические матрицы не изменяются. Неоднозначность в выборе частичных подстановок можно устранить если ограничиться множеством подстановок в которых отсутствуют инверсии [3]. при этом элементы строк будут всегда упорядочены по возрастанию.

При отсутствии инверсий отпадает необходимость в отображении вторых строк подстановок поскольку они всегда будут упорядочены по возрастанию. Таким образом расположение нейронного ядра в топологической матрице достаточно задать парой упорядоченных множеств U^m_j,V^m_j, образующих верхние строки частичных подстановок σ^m_j ,μ^m_j. Введенные множества будем называть топологическими. Учитывая сказанное, построим удобный для программной реализации алгоритм построения топологии БНС. Приведем вначале описание алгоритма, а затем покажем, что он удовлетворяет общему соотношению (4).

Пусть для вершин A_{mj} топология задается парами (U^m_j,V^m_j), а для вершин слоя m+1 парами (U^{m+1}_j,V^{m+1}_j). Структурные связи между двумя смежными слоями запишем в виде ранговой матрицы:

$$R^m = \begin{vmatrix} r^m_{11} & r^m_{12} & \dots & r^m_{1l} \\ r^m_{21} & r^m_{22} & \dots & r^m_{2l} \\ \vdots & \vdots & \dots & \vdots \\ r^m_{k1} & r^m_{k2} & \dots & r^m_{kl} \end{vmatrix}$$

где r_{ij} – ранги проектирующих операторов межслойных связей. Каждой вершине слоя m соответствует строка ранговой матрицы, а каждой вершине слоя m+1 столбец матрицы. Сумма элементов строки i равна порядку множества V^m_i, а столбца j – порядку множества U^{m+1}_j. Введем в рассмотрение числовое множество $T^m=\{1,2,...,N_m\}$, где $N_m=\mathrm{card}(T^m) = \sum_i \sum_j r^m_{ij}$. (Нетрудно проверить, что значение N_m равно числу нейронов в слое m и совпадает с размерностью рецепторного поля слоя m+1. Разместим элементы множества T^m в виде матрицы (рис 3.), подобной по структуре матрице R^m, причем размещение выполним так чтобы выполнялось условие $\mathrm{card}(T^m_{ij}) = r^m_{ij}$. Подмножество элементов принадлежащих i-ой строке обозначим T^A_i , а j-ому столбцу T^B_j. Введем две произвольные подстановки на множестве T^m которые обозначим q^A и q^B. Тогда алгоритм построения топологических множеств будет определяться правилом:

$$V^m_i = T^A_i q^A, \qquad U^{m+1}_j = T^B_j q^B$$

Графически алгоритм можно представить схемой, показанной на рис.3.

Покажем теперь, что данный алгоритм удовлетворяет соотношению (4). Из

$$\left|\begin{array}{cccc|cc} T_{11}^m & T_{12}^m & \dots & T_{1l}^m & T_1^A & \xrightarrow{q^A} \; V_1^m \\ T_{21}^m & T_{22}^m & . & T_{1l}^m & T_2^A & \xrightarrow{q^A} \; V_2^m \\ \dots & \dots & .. & \dots & \dots & \xrightarrow{q^A} \; \dots \\ T_{k1}^m & T_{k2}^m & \dots & T_{kl}^m & T_k^A & \xrightarrow{q^A} \; V_k^m \end{array}\right.$$

$$\begin{array}{cccc} T_1^B & T_2^B & \dots & T_l^B \\ \downarrow q^B & \downarrow q^B & \dots & \downarrow q^B \\ U_1^{m+1} & U_2^{m+1} & \dots & U_l^{m+1} \end{array}$$

Рис.3

схемы рис. 3 следует:

$$U_j^{m+1} = \sum_i V_i^m q^m, \quad \text{где } q^m = \left(q^A\right)^{-1} q^B. \tag{6}$$

Поскольку $V_i^m = \left\{1,2,\dots,N_{ymj}\right\}\left(\rho_{ij}^m\right)^{-1}\left(\mu_j^m\right)^{-1}$, а также

$U_j^{m+1} = \left\{1,2,\dots,N_{ymj}\right\}\left(\sigma_j^{m+1}\right)^{-1}$, то из (6) получим

$$\left(\sigma_j^{m+1}\right)^{-1} = \sum_i \left(\rho_{ij}^m\right)^{-1}\left(\mu_j^m\right)^{-1} q^m \quad .$$

Обращение последнего выражения, очевидно, приводит к (4). Использование двух подстановок q^A и q^B вместо одной q^m делает алгоритм симметричным и более удобным при реализации.

Если $q^A = q^B$ то $q^m = \left(q^A\right)^{-1} q^B = e$, где e – тождественная подстановка.

Будем называть топологию для которой последнее равенство выполнено компактной и расширенной в противном случае. Для расширенной топологии между топологическими матрицами смежных слоев необходимо вводить перестановочную матрицу, соответствующую подстановке q^m. В общем случае для задания топологии необходимо фиксировать подстановки q^A , q^B и размещение множества T^m. При хранении топологии можно без потери информации сократить объем данных, если предварительно произвести «нормализацию» размещения множества T^m, следуя одному из ниже приведенных правил:

$$\text{a)} \quad T_{*a}^m = T^m q^A, \quad q_{*a}^A = e, \quad q_{*a}^B = \left(q^A\right)^{-1} q^B = q^m \quad ,$$

$$\text{b)} \quad T_{*b}^m = T^m q^B, \quad q_{*b}^B = e, \quad q_{*b}^A = \left(q^B\right)^{-1} q^A = \left(q^m\right)^{-1}. \tag{7}$$

Здесь символ «*» указывает значение после нормализации, а символы «a,b» варианты нормализации. Если топология компактная тогда нормализация любого типа приводит к равенству $q_*^A = q_*^B = e$. Таким образом для компактной топологии

співвідношення доходів і витрат. Одна з цікавих можливостей програми, яка стосується планування витрат, – це складання бюджету. Складаючи його, можна вказати плановані джерела і суму доходу, а також те, скільки грошей, і на що ви будете витрачати. Далі ви зможете оцінити, наскільки ваші фактичні витрати відрізняються від запланованих, і подумати, на чому можна заощадити. Склавши бюджет, ви також зможете побачити різницю між доходами і витратами. В останній версії підвищена надійність програми за рахунок виправлення виявлених помилок. Переваги Family: можливість задовольнити вимоги середньої сім'ї для контролю бюджету; можливість побудувати свою фінансову облікову схему.

Описово переглянувши обидві програми, я пропоную до розгляду порівняльну таблицю, що детально зображує основні характеристики програмних продуктів та результати досліджень з визначення переваг та можливостей кожної з вище вказаних програм. Адже у кожної програми є свої плюси та мінуси.

Таблиця 1

Характеристика програмного продукту	**HomeBank**	**Family 10.1.6**
Можливість вести облік одним користувачем	-	+
Зручний інтерфейс	+	+
Наявність типових облікових операцій	+	+
Налаштування вигляду програми	+	-
Запис даних у певний файл	+	+
Можливість введення даних з файлу	-	-
Захист даних	-	+
Наявність подання даних у вигляді схем	+	+
Набір стандартної звітності	+	+
Можливість складання бюджету	-	+
Можливість зміни даних	+	+

Порівняльні характеристики програмних продуктів «HomeBank» та «Family 10.1.6»

Отже, завдяки фінансовому плануванню сімейного бюджету можна набагато швидше й ефективніше досягти поставлених цілей. Завдяки правильно складеному сімейному бюджету ви економите свої гроші. Крім того, завдяки сімейному бюджету ви завжди будете готові до непередбачених ситуацій. Використання подібних програмних продуктів значно полегшить життя багатьом сім'ям.

Література:

1. Панов М. М. Облік сімейного бюджету. Управління сімейним бюджетом. – М.: Инфра–М, 2014. – 304 с.

2. Неміровський Б.І., Старожукова І.А. Бюджетирование.– М.: «Диалектика», 2006. – С. 512.

Бербенюк А.С.
Буковинський державний фінансово-економічний університет

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОГРАМНИХ ПРОДУКТІВ ДЛЯ ОБЛІКУ СІМЕЙНОГО БЮДЖЕТУ

Планування сімейного бюджету дисциплінує у питанні фінансів, відкриває очі на не завжди конструктивні пріоритети розподілу коштів, а також може стати інструментом поліпшення фінансового становища сім'ї. Проте, перш ніж братися за планування сімейного бюджету, врахуйте, що це також певна робота, яка потребує часу, уваги, концентрації і рішучості.

Найголовніше при плануванні сімейного бюджету – встановити кількість витрат, які відбуваються протягом певного періоду часу. Адже дуже часто передбачувані витрати кардинально відрізняються від реальних. Навчитися планувати бюджет родини шляхом обліку всіх витрат, збирання чеків і т. д. – це досить кропітка праця. І якщо ви ніколи в житті цього не робили, навіть докладаючи максимум зусиль, через пару тижнів почнете лінуватися, забувати про це і пропускати. В результаті ви навіть і не дійдете до планування бюджету і не врахуєте, в чому ж ваші дії не вірні.

У наш час важко уявити собі сім'ю, яка б не розраховувала витрати сімейного бюджету. Тому, я вважаю, що порівняльний аналіз всіх існуючих програмних продуктів для введення обліку витрат сімейного бюджету є вкрай необхідним та актуальним. Метою роботи є дослідження програмного забезпечення для обліку витрат сімейного бюджету. Порівняльний аналіз найбільш популярних програмних продуктів для введення обліку сімейного бюджету є основним завданням цієї роботи.

Є кілька варіантів програм для ведення сімейного бюджету на домашньому комп'ютері або ноутбуці. Я обрала найбільш популярні програми для обліку сімейного бюджету, такі як «HomeBank» та «Family 10.1.6».

HomeBank – програма для ведення обліку особистих фінансів, аналізу структури витрат і планування сімейного (особистого) бюджету. Програма проста у використанні, не вимагає знань в області бухгалтерії, є підтримка російської мови, а також вбудована довідкова система по використанні HomeBank (англійською мовою). Програма дозволяє створювати власні статті витрат і доходів, вести облік даних по кожній з них, виводити звіти у вигляді діаграм, планувати доходи і витрати, експортувати дані з бази в окремий файл. Оформлення зовнішнього вигляду програми налаштовується. Для ведення бухгалтерського обліку великих підприємств, установ або організацій можливостей цієї програми, звичайно, буде не достатньо. А ось для домашнього використання з метою обліку фінансів сім'ї HomeBank підійде повністю. Сайт програми – homebank.free.fr.

Оскільки Family – це сімейна програма, то тут є можливість вести облік доходів і витрат кожного з членів родини. Кожен може сам записувати свої витрати. При бажанні, можна поставити пароль на свій обліковий запис. При цьому витрати все одно залишаться видні для інших, але ніхто не зможе зробити запис в програмі від вашого імені. Для кожного користувача можна проглядати діаграму

достаточно хранить только размещение множества T^m, а для расширенной – размещение T^m и подстановку q^m Покажем, что оба варианта нормализации эквивалентны, для этого выполним над нормализованным представлением по типу «*a» выполним нормализацию типа «*b»

$$T^m_{*a} q^B_{*a} = T^m q^A \left(q^A\right)^{-1} q^B = T^m q^B = T^m_{*b},$$

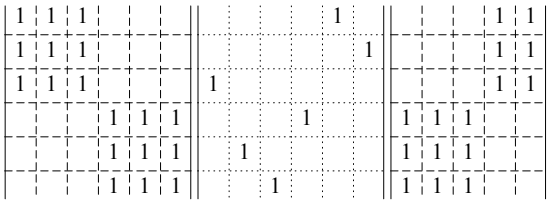
$$\left(q^B_{*a}\right)^{-1} q^A_{*a} = \left(q^B_{*a}\right)^{-1} e = \left(\left(q^A\right)^{-1} q^B\right)^{-1} = \left(q^B\right)^{-1} q^A = q^A_{*b} = \left(q^m\right)^{-1}.$$

Таким образом, мы приходим к нормализованному представлению типа «*b», определяемом правилом (7). Повторение нормализации типа «a» возвращает нас к исходному состоянию.

В качестве примера рассмотрим построение топологий для структурной модели показанной на рис.2. Ниже приведены ранговая матрица и схемы построения двух вариантов топологии:

$$R = \begin{vmatrix} 2 & 1 \\ 1 & 2 \end{vmatrix}, \quad \begin{array}{cc|c} (12) & 3 & (123) \to V_1^1 \\ 4 & (56) & (456) \to V_2^1 \\ \downarrow & \downarrow & \\ (124) & (356) & \\ U_1^2 & U_2^2 & \end{array} \cdot, \quad \begin{array}{cc|c} (12) & 3 & (123) \to V_1^1 \\ 4 & (56) & (456) \to V_2^1 \\ \downarrow q^B & \downarrow q^B & \\ (456) & (123) & \\ U_1^2 & U_2^2 & \end{array}$$

Подмножества U_i^1, V_j^2 можно выбрать произвольно. Выберем их равными $U_1^1 = (123)$, $U_2^1 = (456)$, $V_1^2 = (123)$, $V_2^2 = (45)$, в этом случае топологические матрицы первого варианта точно соответствуют представлению (5). Для второго варианта выбрано $q^A = e$, $q^B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 4 & 2 & 3 \end{pmatrix}$ и сохранены прежние значения U_i^1, V_j^2. Расширенная топология для этого случая имеет следующее матричное преставление:



От расширенной топологии всегда можно перейти к компактной, выполнив умножение левой или правой смежной топологической матрицы на перестановочную, очевидно, что при этом информация о подстановке q^m теряется и поэтому обратный переход будет неопределен.

В данной работе представлены два уровня структурного описания БНС: структурная модель и топологическая реализация. Показано, что адекватным инструментом проектирования топологий является математический аппарат числовых частичных отображений. На основе этого аппарата предложен машинно-ориентированный алгоритм построения топологий БНС. Топологическое проектирование позволяет оптимальным образом выбрать программную или аппаратную реализацию БНС из класса эквивалентных.

Литература

1. А.И. Кострикин, Ю.М. Манин. Линейная алгебра и геометрия.- М.:- «Наука» – 1986.-304с.

2. Мальцев А.И. Алгебраические системы.- М.: Наука, 1970.

3. Кострикин А.И. Введение в алгебру. Основы алгебры. – М.: Физматлит. 1994, -320с.

По данным диаграммы можно сказать следующее: наибольший удельный вес загрязненности наблюдается в г.Рудном – 77,44% от общего показателя по области и в Житикаринском районе – 16,48%. В г.Костанай – 1,93%, в остальных регионах удельный вес количества загрязняющих веществ ниже 1% от общего показателя по области.

По данным диаграммы можно сказать следующее: наибольший процент загрязненности наблюдается в г.Рудном – 77,44% от общего показателя по области и в Житикаинской районе – 16,48%. В г.Костанай – 1,93%, в остальных регионах показатель количества загрязняющих веществ ниже 1 процента.

Режим отображения данных «Гистограмма». В режиме отображения данных «Гистограмма» мы с вами можем увидеть группировку по показателю «Количество загрязняющих веществ». Группировка будет произведена в количестве 5 интервалов.

Количество загрязняющих веществ в интервале от 317,92 до 76044,8 тонн имеют 18 регионов области. Количество загрязняющих веществ в интервале от 76044,8 до 151772 тонн имеет 1 регион. Количество загрязняющих веществ в интервале от 303226 до 378953 тонн имеет 1 регион. В соответствующих режимах отображения данных можно изменять направления осей, параметры отображения данных, типы графиков, метки и значения, проценты и т.д.

Современный уровень сложности задач, решаемых с помощью информационных систем, постоянно растет. Именно поэтому с позиций даже самого сдержанного оптимизма вполне логично ожидать дальнейшую оптимизацию уже существующих информационных систем и создание новых, многоцелевых систем глобального масштаба, функционально обеспечивающих решение вопросов от банального справочного общения с компьютером до автоматизированного сбора и интерпретации информации, управления, проектирования, моделирования и прогнозирования различных процессов.

Литература:

1. http://www.basegroup.ru – Технологии анализа данных
2. http://kostanay-priroda.kz – сайт Управления природных ресурсов и регулирования природопользования акимата Костанайской области.

В режимах отображения данных: Таблица, Статистика, Диаграмма, Гистограмма непосредственно проводится статистический анализ.

Режим отображения данных Таблица. В режиме отображения данных «Таблица» активизируем кнопку «Показать онлайн статистику». В результате в нижней части рабочей области отобразится статистическая информация: среднее значение, максимальное значение, минимальное значение, отклонение, сумма всех значений, количество.

Среднее количество загрязняющих веществ по Костанайской области в 2013 году составило 24763,609 тонн. Проведем фильтрацию данных с целью подсчета количества районов, в которых количество загрязняющих веществ соответственно ниже и выше среднего показателя по области.

Для этого активизируем кнопку «Фильтрация» и настроим окно. В итоге получаем, что в 18 регионов из 20 рассматриваемых количество загрязняющих веществ ниже среднего показателя по области. Соответственно в 2 регионах из 20 данный показатель выше среднего. К ним относятся Житикаринский район и г.Рудный.

Следует также отметить что максимальное количество загрязняющих веществ зафиксировано в г.Рудном, минимальное – в Жангельдинском районе.

Режим отображения данных «Статистика». В режиме отображения данных «Статистика» дополнительно к основным статистическим характеристикам можно выполнить обзор статистики. Однако в нашем примере на каждый регион приходится по одному значению, поэтому группировка с указанием процентной доли, приходящейся на каждый регион одинаковая – по 5%. Следует также отметить, что среднее отклонение показателей каждого региона от среднего показателя по области составляет 85234,760 тонн. Данное значение в 3,4 раза превышает среднее значение, что характеризует достаточно высокую степень вариации (изменчивости) исследуемого показателя.

Режим отображения данных «Диаграмма». В данном режиме отображается удельный вес количества загрязняющих веществ каждого региона в процентах от общего по области.

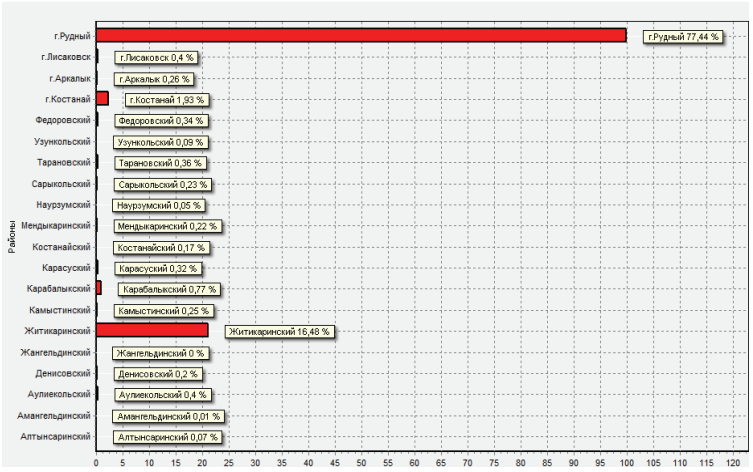


Рисунок 5 – Режим отображения данных Диаграмма

PROGRAMOVÉ VYBAVENÍ

Д.т.н. Рындин А.А., к.т.н. Сапегин С.В.
Воронежский государственный технический университет, Россия

ОСОБЕННОСТИ ЖИЗНЕННОГО ЦИКЛА КОМПОНЕНТОВ В СОСТАВЕ СОВРЕМЕННЫХ ПРОГРАММНЫХ КОМПЛЕКСОВ

Одним из популярных подходов к рационализации разработки программных компонентов различной степени сложности является построение и использование различного рода технологий, включая различные парадигмы, языки и среды программирования. Системы, построенные с учетом технологичности программирования, как правило, отличаются достаточно простой архитектурой, определенным набором инструментальных средств, единообразными стандартами разработки. Однако, поиск наиболее подходящего в каждом конкретном случае набора технологий и методологий является достаточно важной задачей.

Рассмотрим постановку задачи о разработке программного компонента в общем виде. Структуру каждого набора требований к компоненту ИС S_i можно представить в виде:

$$S_i = (1 + A(t)) \cdot S_{i,tech} + (1 + B(t) + C) \cdot S_{i,user} + S_{D(t)} \quad (1)$$

где $S_{i,tech}$ - технологии, используемые в работе компонента (включая технологии взаимодействия с другими компонентами системы); $S_{i,user}$ - пользовательские требования к компоненту; $A(t), B(t)$ – множители, характеризующие изменение требований к компоненту в течение его срока работы; C - составляющая согласования требований к компоненту между различными пользователями компонента корпоративной ИС; $S_{D(t)}$ - набор требований, определяющих процесс совмещения различной функциональности в компоненте (условие существования множителей $A(t), B(t)$). Таким образом, задачу о разработке компонента ПО в общем виде можно представить, как достижение за ограниченное время набора требований S_x, максимально близкого к некоторому идеальному набору требований S_{ideal}. В общем случае, достижение в процессе разработки самого набора требований S_{ideal} невозможно по следующим причинам:

1. Время разработки компонента ПО ограничено.

2. Набор требований к разрабатываемому компоненту ПО часто формируется не одним пользователем, а целой группой (или даже несколькими группами), причем каждый участник группы может выдвигать требования, плохо согласующиеся с требованиями остальных членов группы.

3. Требования к компоненту ПО как со стороны пользователей, так и со стороны взаимодействующего ПО, меняются с течением времени.

4. Анализ свойств процесса достижения пользовательских требований во многих случаях, как правило, не учитывает субъективного характера самого процесса, т.е. квалификации разработчиков, работающих над компонентом ПО.

Исходя из приведенной концепции, задачу достижения максимального экономического эффекта от использования отдельного программного компонента системы можно определить, как

$$\int_{T_0}^{T_0+T} f(S(t);F(t)) \to \max \quad , \tag{2}$$

где $S(t)$ – набор бизнес-требований, $F(t)$ – реализованная функциональность, T – время использования компонента, T_0 – момент начала использования, f – функция, оценивающая соответствие функциональности компонента $F(t)$ актуальным требованиям $S(t)$, $f \in [0,1]$. В качестве простейшего, самого грубого варианта функции f можно использовать выражение вида

$$f = \frac{D(S(t), F(t))}{|S(t)|} \quad , \tag{3}$$

где D – мощность симметричной разности множеств $S(t)$ и $F(t)$ в момент времени t, $|S(t)|$ – мощность множества $S(t)$. Практика показывает, что зависимость расстояния между множествами $S(t)$ и $F(t)$ (т.е. степени соответствия функциональности компонента бизнес-требованиям) в случае процесса интенсивной (целенаправленной) разработки имеет S-образный характер. Это обусловлено тем, что в начале цикла разработки ресурсы затрачиваются не столько на реализацию бизнес-функций, сколько на выстраивание архитектуры ПС. Поэтому, варианты функции f, более соответствующие статистическим данным, следует искать среди семейств S-функций различной кривизны. Схематичный график функции f, иллюстрирующий идеальный жизненный цикл такого компонента, представлен на рис. 1.

архитектуры пройти все этапы построения аналитической системы: от консолидации данных до построения моделей и визуализации полученных результатов.

Рассмотрим пример статистического анализа экологических данных в среде Deductor Academic.

Шаг 1. Создание входного файла данных. Исходные данные внесем в текстовый файл и сохраним для дальнейшего ввода данных в программу и последующего их анализа.

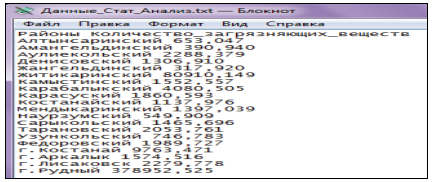


Рисунок 1 – исходный текстовый файл

Шаг 2. Импорт текстового файла данных в Deductor Academic. Запустим Deductor Academic. Используя мастер импорта данных, импортируем данные.

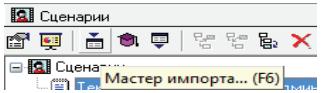
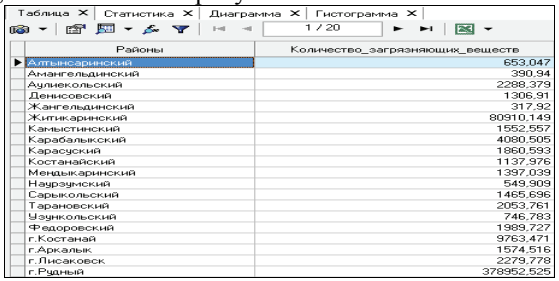


Рисунок 2 – мастер импорта данных

Для 1 столбца «Районы» тип данных определим как строковый, для 2 столбца «Количество загрязняющих веществ» тип данных определим как вещественный. Далее выберем следующие способы отображения данных: Таблица, Статистика, Графики. Нажав кнопку «Готово» получим исходные данные, представленные так, как показано на рисунке 3.



Районы	Количество_загрязняющих_веществ
Алтынсаринский	653,047
Амангельдинский	390,94
Аулиекольский	2288,379
Денисовский	1306,91
Жангельдинский	317,92
Житикаринский	80910,149
Камыстинский	1552,557
Карабалыкский	4080,505
Карасуский	1860,593
Костанайский	1137,976
Мендыкаринский	1397,039
Наурзумский	549,909
Сарыкольский	1465,696
Тарановский	2053,761
Узункольский	746,783
Федоровский	1989,727
г.Костанай	9763,471
г.Аркалык	1574,516
г.Лисаковск	2279,778
г.Рудный	378952,525

Рисунок 3 – Результаты импорта исходных данных

Найменування раунків/субрахун-ків у цифровому і літературному вигляді	+	+	
Можливість переміщення об'єктів аналітики з однієї групи в іншу	+	+	
Введення господарських операцій вручну	+	+	
Наявність типових документів	+	+	
Набір стандартної звітності	+	+	
Набір довільної звітності	-	+	
Можливість зміни документів	-	+	

Отже, застосування підприємствами програмних продуктів з комп'ютеризації бухгалтерського обліку суттєво змінює процес ведення обліку. Використання комп'ютерних технологій спрощує не тільки ведення обліку, а і позбавляє необхідності постійно контролювати вихідні показники регістрів і звітності. Кожна програма має свої переваги та недоліки, свої особливості автоматизації та ведення бухгалтерського обліку. Однак у всіх них єдина мета – спростити роботу бухгалтера шляхом її автоматизації.

Література:

1. Крук Н.Р. Методичний посібник «Автоматизація розв'язування комплексу задач обліку з використанням системи «Парус – Бухгалтерія 7.40».
2. Молчанов С.С. «Бухгалтерский учет за 14 дней. Экспресс-курс».

Нурпеисова Ж.С.
магистр экон.наук, старший преподаватель
Костанайский государственный университет имени А.Байтурсынова

АНАЛИЗ ЭКОЛОГИЧЕСКИХ ДАННЫХ В СРЕДЕ DEDUCTOR ACADEMIC

В последние десятилетия среди специалистов многих отраслей науки отмечается постоянно растущий интерес к использованию математико-статистических методов и компьютерных технологий для анализа данных.

Все существующие алгоритмы первичной обработки результатов экологического мониторинга и их применение немыслимы без программных вычислительных средств, которых на данный момент огромное количество. Часть из программ имеют специальную направленность, часть являются универсальными.

Технология, рассмотренная в примере, система Deductor Academic – это аналитическая платформа, основа для создания законченных прикладных решений в области анализа данных. Реализованные в Deductor технологии позволяют на базе единой

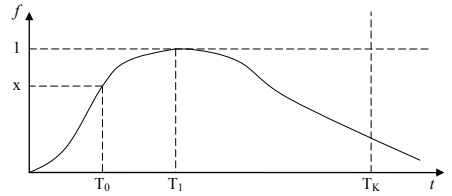


Рис. 1. Жизненный цикл компонента

Процесс работы службы в режиме промышленной эксплуатации, как показывает практика, наиболее перспективен с точки зрения получения эффекта. При этом, за счет изменения среды существования службы, а также за счет неизбежной реструктуризации бизнес-процессов полезность (степень удовлетворения бизнес-требований) программного средства снижается вплоть до момента T_k, когда принимается решение о выводе службы из эксплуатации. Основными причинами вывода программного средства из эксплуатации являются:

1. Снижение уровня используемой функциональности до некоего критического порога (служба становится фактически бесполезной в новых условиях);
2. Несоответствие службы реалиям архитектуры (при смене операционной системы, модели данных, среды взаимодействия служб, стандартов и т.д.);
3. Замена службы на новую версию, либо полное распределение функционала службы между другими, введенными в эксплуатацию, службами.

ЛИТЕРАТУРА:

1. Вендров А.М. Проектирование программного обеспечения экономических информационных систем. – М.: Финансы и статистика, 2000.
2. Мишенин А.И. Теория экономических информационных систем. – М.: Финансы и статистика, 2000. – 240 с..
3. Jorge Dias Jr. A Software Architecture Process for SOA Definition. LAP: Lambert Academic Publishing, 2009, 160 p.

Одочук О. О.
Буковинський державний фінансово-економічний університет

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОГРАМНИХ ПРОДУКТІВ ДЛЯ БУХГАЛТЕРСЬКОГО ОБЛІКУ

Застосування комп'ютерних технологій у бухгалтерському обліку значно підвищує продуктивність праці бухгалтерів, оперативність обробки даних і точність ділової інформації, сприяє прийняттю більш об'єктивних фінансових й управлінських рішень. Автоматизація процесу обліку дає можливість економити підприємству свій час і кошти. Саме це і зумовлює актуальність обраної теми, оскільки організація бухгалтерського обліку в умовах його комп'ютеризації залежить у першу чергу від реалізованого на відповідних технічних засобах програмного забезпечення, вибір якого є найважливішим моментом у створення комп'ютерних систем бухгалтерського обліку (КСБО), оскільки відповідає вибору форми обліку на підприємстві.

У наш час важко уявити собі підприємство, яке б не використовувало у своїй діяльності спеціальні програми для автоматизації обліку. За теперішнього часу, програм для автоматизації обліку існує досить багато, тому вкрай необхідними, на мій погляд, є публікації щодо порівняльного аналізу існуючих програмних продуктів.

Метою роботи є дослідження інформаційного забезпечення управління системою оплати праці в умовах комп'ютеризації. Одним із завдань даної статті є порівняльний аналіз найбільш популярних на сьогодні програмних продуктів, таких як «Парус-бухгалтерія» та «1С: Бухгалтерія» для вибору оптимальнішої автоматизації ділянки бухгалтерського обліку.

Модуль «Парус-Бухгалтерія» призначений для автоматизації ведення бухгалтерського обліку в бюджетних установах будь-якого рівня.

Характерні риси платформи «Парус -Бухгалтерія»:

- інтуїтивно зрозумілий інтерфейс;
- об»єднання облікових та управлінських можливостей у поєднанні із комунікаційними можливостями Web-технологій;
- доступність і можливість автоматизації підприємства поетапно;
- широкі функціональні можливості, які дозволяють автоматизувати усі ділянки обліку підприємства.

Він забезпечує формування повної і достовірної інформації про фінансово-господарську діяльність, для потреб внутрішніх і зовнішніх користувачів та контрагентів; реєстрацію первинних документів та підготовку річної, квартальної, місячної звітності бюджетної установи

«1С: Бухгалтерія» – це універсальна програма масового призначення для автоматизації бухгалтерського обліку.

Даний пакет дозволяє автоматизувати ведення всіх розділів бухгалтерського обліку: операції по банку і касі; основні засоби та нематеріальні активи; облік матеріалів; облік товарів та послуг; облік виробництва продукції; облік валютних операцій; розрахунки з покупцями і постачальниками; розрахунки з підзвітними особами; облік розрахунків по заробітній платі з працівниками, нарахування ПДФО; розрахунки з бюджетом інші розділи обліку

У рамках програми «1С: Бухгалтерія» запропоновано продукт 1С: «Зарплата і кадри для України», що містить основу для автоматизованого обліку кадрів (рис.1)

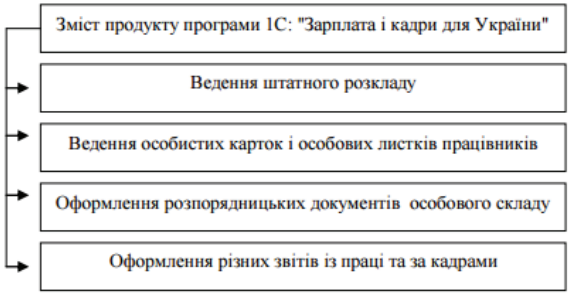


Рис. 1. Зміст програмного продукту 1С: «Зарплата і кадри для України»

Програма дозволяє вести облік одночасно на декількох фірмах, при цьому співробітники можуть працювати як на одному, так і на декількох підприємствах. Інформація про працівників підприємства зберігається у двох основних довідниках – «Фізичні особи» і «Співробітники». Кожному з них належить декілька допоміжних довідників. Така структура дозволяє вести в електронному вигляді особисту картку зі збереженням всіх необхідних даних.

Таблиця 1

Порівняльні характеристики програмних продуктів «Парус-бухгалтерія» та «1С: Бухгалтерія» версія 8.1

Характеристика програмного продукту	Парус-бухгалтерія	1С: Бухгалтерія 8.1	
Можливість ведення декількох юридичних осіб	-	+	
Розбивка записів на господарські операції	+	+	
Наявність типових господарських операцій	+	+	
Самостійна настройка типових господарських операцій	+	+	