Министерство образования и науки Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего образования

«АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМ. И.И. ПОЛЗУНОВА» (АлтГТУ)

НАУКА И МОЛОДЕЖЬ

XIV Всероссийская научно - техническая конференция студентов, аспирантов и молодых ученых, посвященная 75-летию АлтГТУ

СЕКЦИЯ
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

подсекция

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Барнаул – 2017

УДК 004

XIV Всероссийская научно-техническая конференция студентов, аспирантов и молодых ученых "Наука и молодежь - 2017", посвященная 75-летию АлтГТУ. Секция «Информационные технологии». Подсекция «Информатика, вычислительная техника и информационная безопасность». / Алт. гос. техн. ун-т им. И.И.Ползунова. – Барнаул: изд-во АлтГТУ, 2017. – 64 с.

В сборнике представлены работы научно-технической конференции студентов, аспирантов и молодых ученых, проходившей 25 апреля 2017 г.

Научный руководитель подсекции:

д.т.н., профессор

Якунин А.Г.

Содержание

ПРОЕКТИРОВАНИЕ И РЕАЛИЗАЦИЯ МОБИЛЬНОГО ПРИЛОЖЕНИЯ “ПУТЕВОДИТЕЛЬ ПЕРВОКУРСНИКА”

Алексеев А.В. – студент, Сучкова Л.И. – д.т.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

В 21 веке трудно представить человека без мобильных устройств и различных гаджетов, происходит максимальное упрощение человеческих действий, бумажные носители перестают быть актуальными.

Одним из направлений применения мобильных устройств является помощь человеку при поиске объектов в зданиях, предоставление информации об однотипных объектах. Такая помощь важна для студентов, поступивших учиться в АлтГТУ, так как первокурсники, как правило, теряют очень много времени на поиски нужных аудиторий, точек питания, поиски специализированных отделов и служб вуза. В связи с этим разработка мобильного приложения, помогающего в ориентировании на незнакомых распределенных объектах и в получении необходимой информации о функционировании таких объектов, является актуальной задачей [1-3].

Если проводить анализ проблем в адаптации к условиям учебы в вузе у студентов 1 курса, то можно выделить следующие:

1) Сложность ориентации студентов 1 курса в корпусах АлтГТУ;

2) Отсутствие знаний о разделении функциональных обязанностей между различными подразделениями ВУЗа;

3) Потеря времени на поиски пищевых точек, мест для оказания услуг по печати работ с электронного носителя и т.п.;

4) Отсутствие компетенции в решении бытовых студенческих проблем;

5) Отсутствие своевременной информации о предстоящих мероприятиях в ВУЗе.

Для решения данных проблем целесообразна разработка мобильного приложения. В результате работы спроектировано многофункциональное приложение на платформе Android с интуитивно понятным и простым интерфейсом, позволяющее отображать карты корпусов, этажей АлтГТУ, а также предоставлять информационные услуги студенту-первокурснику. Для этой цели разработана и подключена база данных для хранения информации.

При работе с приложением пользователь должен указать своё местоположение, например,корпус. Корпус можно опередить 2 способами – как вручную, так и посредством поиску по GPS. Далее пользователь указывает, какой тип конечной точки его интересует. Это может быть, например, аудитория, точка питания, точка оказания услуг (сканирования, печати, продажи канцелярии), административное помещение (гардероб, актовый зал, деканат, библиотека). В зависимости от выбранного типа конечной точки выводится activity, где пользователь указывает дополнительную информацию – например, аудиторию или этаж. Приложение либо сразу показывает нужную точку пользователю и выделяет ее цветом, либо выделяются ключевые элементы для достижения целевой точки (переходы, лестницы). Существует кнопки для переключения между этажами, а так же для изменения масштаба карты.

Пользователь также может вывести всю информацию по определенным услугам, например, о точках питания, точках оказания канцелярских услуг, административным подразделениям вуза.

Операционная система Android предполагает несколько вариантов решений для того, чтобы хранить постоянные данные приложения [1]:

1) SharedPreferences для примитивов ключ-значение.

2) InternalStorage для сохранения в памяти телефона.

3) ExternalStorage для сохранения на внешней карте.

4) SQLiteDatabases

5) NetworkConnection, чтобы сохранить на веб-севере. [1]

В нашем случае для хранения информации использованSQLiteDatabases, а в activity, для

вывода информации из таблиц использованы транзакции языка SQL.

В ходе работы проанализирована предметная область, на основе исследований была поставлена цель и сформулированы задачи для её достижения. Была выбрана наиболее простая и эффективная для разработки платформа. Спроектирована база данных и мобильное приложение.

Разработанное приложение имеет следующие достоинства:

1) Способность быстро подсказать маршрут до нужных аудиторий, точек в корпусах АлтГТУ;

2) Размещение всей информации о структуре ВУЗа в одном лишь приложении;

3) Возможность обновлять предоставляемую информацию без особых денежных затрат;

4) Удобство доступа к информации;

5) Возможность составления FAQ в данном приложении, уже ранее решенных вопросов в каких-либо проблемах студента, для упрощения и понимания путей решения.

Список использованных источников

1. DeveloperAndroidStudio [электронный ресурс]: Официальный сайт. - Электрон.текст. дан. – Режим доступа: https://developer.android.com/guide/topics/data/data-storage.html

2. Gs.statcounter.com: DesktopvsMobilevsTabletMarketShareWorldwide [электронный ресурс]: Официальный сайт. - Электрон.текст. дан. – Режим доступа: http://gs.statcounter.com/platform-market-share/desktop-mobile-tablet

3. Gs.statcounter.com: Mobile Operating System Market Share in Russian Federation [электронныйресурс]: Официальныйсайт. - Электрон.текст. дан. – Режим доступа: http://gs.statcounter.com/os-market-share/mobile/russian-federation/#monthly-201404-201704

РАЗРАБОТКА МОБИЛЬНОЙ ВЕРСИИ САЙТА ДЛЯ ЭЛЕКТРОННОЙ ОЧЕРЕДИ ЗАРЯДКИ ЭЛЕКТРОМОБИЛЕЙ

Барыбин В.А. - студент, Якунин А.Г. – д.т.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

В настоящее время хоть и не часто, но мы все еще сталкиваемся с таким явлением, как очередь. В нынешнем мире у людей остро ощущается нехватка времени, а пребывание в длинных очередях: за талоном к врачу, в ожидании посылки на почте или заправки автомобиля еще более усугубляет эту проблему.

Для ее решения уже давно применяются предварительные записи, но они не всегда удобны как для посетителей, так и для самих сотрудников учреждений. Многие организации пытались предотвратить шум, ссоры между людьми, пытающимися быть первыми на приеме. Для этого нанимали на работу как охранников, так и людей, специально занимающихся организацией очередей, что приводит к дополнительным накладным расходам.

Современным и эффективным решением на сегодняшний день является применение электронной очереди, система которой автоматизирует процесс записи на прием посетителей [1-6]. При этом жалобы на хаотичную очередь и неразбериху в обслуживании сводятся к минимуму, сокращается время обслуживания посетителей, увеличивается производительность труда сотрудников, значительно минимизируются финансовые затраты, что позволяет использовать денежный ресурс и на другие направления.

Электронная очередь – это информационная система организации приема клиентов и учета рабочего времени сотрудников, реализуемая преимущественно в форме веб-сайта, функционал которого обеспечивает возможность онлайн записи клиентов на прием или обслуживание. Интерфейс веб-сайта разрабатывается таким образом, чтобы каждый человек без специальной подготовки мог разобраться в меню, не прилагая особых усилий.

В данной работе описывается веб-сайт для организации электронной очереди на заправку электромобилей. В последние годы электромобили стали набирать популярность и их число постоянно растет в силу их высокой экономической эффективности и экологической безопасности. Однако, процесс их заправки (точнее – зарядки аккумуляторов) и зарядки требуются специальные заправочные (зарядные) станции. Сам процесс зарядки автомобиля достаточно продолжителен (от 20 минут до нескольких часов), а зарядные станции – сложные дорогостоящие и высокотехнологичные сооружения, поэтому для повышения эффективности их работы и сокращения потерь времени на стояние в очередях пользователей электромобилей разработка веб-сайта для обслуживания электронных очередей крайне актуальна.

Веб-ресурс должен предоставлять следующие возможности:

- Возможность регистрации новых клиентов;
- Возможность входа/выхода под своим логином и паролем;
- Хранение данных о клиентах ресурса;
- Возможность просмотра информации о предоставляемых услугах и ценах на них;
- Возможность узнать последние новости из мира электрокаров и зарядочных станций;
- Предоставление конфиденциальной информации только для сотрудников транспортной компании;
- Предоставление данных о расположении зарядочных станций;
- Предоставление данных о графике работы зарядочных станций;
- Предоставление данных о способах связи с зарядочными станциями;
- Адаптация интерфейса сайта для работы с ним с мобильных устройств;
- Возможность пользователям самостоятельно записаться на зарядку электромобиля.

Особенности разработки:

- Удобное представление информации;
- Не требуется установка сторонних скриптов, все действия выполняются на сервере;
- Новый пользователь может сам зарегистрироваться на сайте без вмешательств администратора;
- Возможность редактировать данные в исходной базе данных предоставлено только администратору.

В ходе разработки сайта было использовано следующее ПО:

- MySQL 5.5
- phpMyAdmin 4.5.2
- Apache 2.4
- PHP 5.6
- JavaScript
- Sublime Text 2

Структура меню сайта показана на рисунке 1, а пример его отображения на мобильном устройстве – на рисунке 2.

При разработке сайта были использованы не очень тусклые, но в то же время и не сильно яркие цвета, чтобы текст сливался с фоном. Для использования на мобильных устройствах размер шрифта текста был выбран не сильно мелким. Пользователь, зайдя на главную страницу сайта, может быстро перейти в необходимый для него раздел для получения более подробной информации.

Для разрабатываемого веб-сайта была создана база данных, в которую включены четыре таблицы:

- «Пользователь» -для хранения данных о зарегистрированных пользователях;
- «Очередь» - для фиксации информации о выбранных пользователем услугах для зарядки электромобиля;
- «Тип зарядки» - для хранения данных о существующих на сегодня стандартах видов зарядки (режимы, интерфейсы, конструкции разъемов и протоколов обмена с контроллером автокара);

- «Станция» - для хранения данных о зарядочной станции.

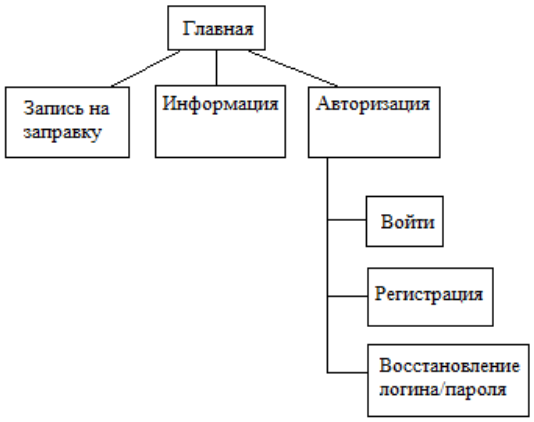


Рисунок 1 – Структура меню веб-сайта

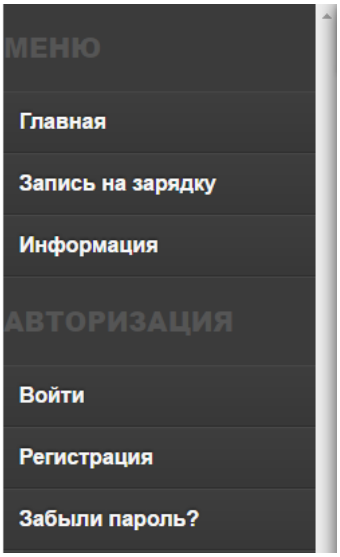


Рисунок 2 –Навигационное меню

В заключении хочется сказать, что электронная очередь находит широкое применение во многих сферах человеческой деятельности, так как она предоставляет возможность ожидать приема специалиста, не создавая «живую» очередь, обеспечивает комфортное и конфиденциальное обслуживание каждого клиента.

Список использованных источников

1. Электронные системы управления очередью в России [Электронный ресурс] - Режим доступа: http://elektroochered.3dn.ru/ – Загл. с экрана.

2. Электронная очередь. Система управления очередью [Электронный ресурс] -Режим доступа: http://dreamapp.ru/resheniya – Загл. с экрана.

3. Электронная очередь – ВКонтакте [Электронный ресурс] – Режим доступа: https://vk.com/visitsturn – Загл. с экрана.

4. Электронная очередь [Электронный ресурс] - Режим доступа: http://www.nbsystems.ru/next.html - Загл. с экрана.

5. Инфраструктура зарядки электромобилей – machinepedia [Электронный ресурс] - Режим доступа: http://machinepedia.org/index.php – Загл. с экрана.

6. Электронная очередь [Электронный ресурс] - Режим доступа: http://www.smartek.az/?a=pages&id=365&lang=ru – Загл. с экрана.

РАСЧЁТ ЦИФРОВОГО БИХ-ФИЛЬТРА МЕТОДОМ АНТИГРАДИЕНТНОЙ НАСТРОЙКИ ПАРАМЕТРОВ

Белозёров М.С. – студент, Тушев А.А. – к.т.н., доцент
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

С развитием вычислительной техники приобрели большую популярность различные методы цифровой обработки сигналов, в том числе и рекурсивные (БИХ) фильтры, которые позволяют выполнять фильтрацию сигнала с использованием сравнительно небольшого количества вычислений.

Вычисление очередного значения выходного сигнала производится по формуле (1).

$$y(n) = \sum_{i=0}^{P} b_i x(n-i) - \sum_{k=1}^{Q} a_i y(n-k) (1),$$

где x(n) – входной сигнал, y(n) – выходной сигнал, P,Q – порядок входного сигнала и обратной связи соответственно, b_i, a_i – коэффициенты фильтра, определяющие его характеристики.

Коэффициенты фильтра определяются исходя из дискретной передаточной функции фильтра:

$$H(z) = \frac{b_0 + b_1 z^{-1} + .. + b_P z^{-P}}{1 + a_1 z^{-1} + .. + a_Q z^{-Q}} (2).$$

Типичным способом получения дискретной передаточной функции фильтра является расчёт аналогового фильтра с непрерывной передаточной функцией путём аппроксимации желаемой АЧХ фильтра и её последующей дискретизации с использованием билинейного преобразования. Такой метод является достаточно громоздким.

Для расчёта БИХ-фильтра напрямую, без аналогового прототипа, можно использовать метод антиградиентной настройки параметров. Для этого необходимо задать график желаемой АЧХ фильтра таблицей значений $K_0(\omega)$, где ω – круговая частота. В качестве начального приближения коэффициентов b_i и a_i необходимо взять случайные значения в интервале [-0,5;0,5],тогда каждому значению ω можно найти значение текущего приближения АЧХ по формуле (3).

$$K(\omega) = \left|H(e^{2j\omega})\right| (3),$$

где j – обозначение мнимой единицы комплексного числа.

Принимая ω в качестве константы, а коэффициенты b_i и a_i в качестве переменных, можно определить функцию ошибки:

$$E\left(b_0, b_1, \dots, b_p, a_0, a_1, \dots, a_Q\right) = (K_0(\omega) - K(\omega))^2 (4).$$

Для получения БИХ-фильтра с АЧХ наиболее близкой к желаемой, необходимо выполнить минимизацию функции ошибки антиградиентным методом последовательно для каждого значения ω. Согласно этому методу очередное приближение коэффициентов b_i и a_i находится по формулам (5) и (6) соответственно.

$$b_i^{n+1} = b_i^n - \Delta \frac{\partial E}{\partial b_i} = b_i^n - \Delta \left[\frac{2(K_0(\omega) - K(\omega))}{S_1 S_2} \left(S_{1R} Re\left(e^{-2ij\omega}\right) + S_{1I} Im\left(e^{-2ij\omega}\right) \right) \right] (5),$$

$$a_i^{n+1} = a_i^n - \Delta \frac{\partial E}{\partial a_i} = a_i^n - \Delta \left[\frac{2S_1(K_0(\omega) - K(\omega))}{{S_1}^3} \left(S_{2R} Re\left(e^{-2ij\omega}\right) + S_{2I} Im\left(e^{-2ij\omega}\right) \right) \right] (6),$$

где Re(x) и Im(x) – функции получения коэффициентов действительной и мнимой части числа x, aS_{1R}, S_{1I}, S_{2R}, S_{2I}, S_1, S_2, K(ω) задаются следующим образом:

$$K(\omega) = \frac{S_1}{S_2}, S_1 = \sqrt{{S_{1R}}^2 + {S_{1I}}^2}, S_2 = \sqrt{{S_{2R}}^2 + {S_{2I}}^2},$$

$$S_{1R} = \sum_{i=0}^{P} b_i Re\left(e^{-2ij\omega}\right), S_{1I} = \sum_{i=0}^{P} b_i Im\left(e^{-2ij\omega}\right),$$

$$S_{2R} = \sum_{i=0}^{Q} a_i Re\left(e^{-2ij\omega}\right), S_{2I} = \sum_{i=0}^{Q} b_i Im\left(e^{-2ij\omega}\right).$$

Для получения коэффициентов b_i и a_i, удовлетворяющих формуле (2), достаточно все коэффициенты разделить на a_0.

Таким образом мы получаем метод расчёта БИХ-фильтра, позволяющий достаточно точно и быстро определить коэффициенты фильтра, имеющего АЧХ произвольной желаемой формы, без использования аналогового прототипа фильтра. Данный метод напоминает проектирование нейронной сети с обратным распространением ошибки и для ускорения работы может иметь похожую программную реализацию, которая позволит избежать многократного расчёта одних и тех же значений. На рисунке 1 изображены АЧХ идеального

полосового фильтра (синий) и АЧХ фильтра 20–го порядка (красный), полученного в ходе 5000 повторений приближения коэффициентов для каждой точки идеальной АЧХ.

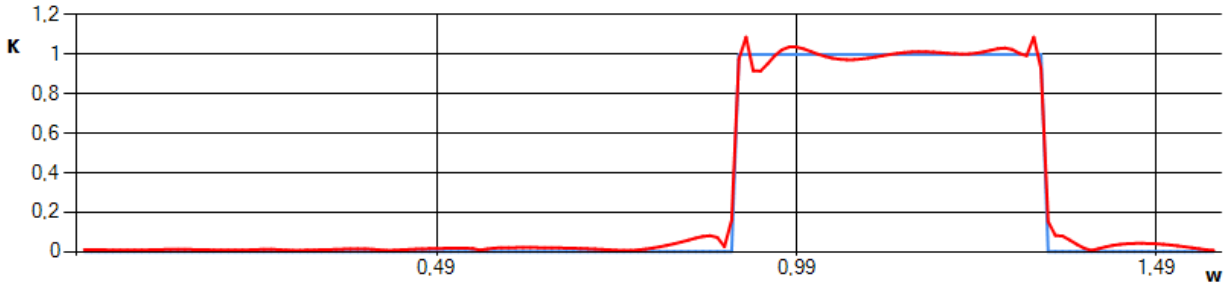


Рисунок 1 – Результат расчёта БИХ-фильтра

Библиографический список.

1. Сергеенко А.Б. Цифровая обработка сигналов. – СПб.: Питер, 2002. – 608 с.
2. Теория и практика цифровой обработки сигналов: Структуры цифровых фильтров и их характеристики [Электронный ресурс], - Режим доступа: http://www.dsplib.ru/content/filters/ch10/ch10.html
3. Амосов А.А., Дубинский Ю.А., Копченова Н.В. Вычислительные методы для инженеров: Учеб.пособие. — М.: Высш. шк., 1994. — 544 с.
4. Смит С.В. Научно-техническое руководство по цифровой обработке сигналов [пер. с англ.]. – СПб.: Автекс, 2001. – 149 с.

РАЗРАБОТКА МЕТОДА КОЛИЧЕСТВЕННОЙ ОЦЕНКИ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Будовских И.А. – магистрант
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Стремительное развитие информационных технологий (ИТ) позволяет не только повысить коммуникабельность современного общества, экономить время, получить образование, но и расширить спектр угроз информационной безопасности (ИБ) человека. Ведь зачастую такие ИТ решения как интернет – магазины, порталы государственных услуг, интернет – банкинг, требуют чтобы пользователи вводили свои персональные данные (ПДн), которые в дальнейшем обрабатываются и хранятся в базах данных (БД), часто распределенных по различным странам мира. Эти данные привлекают злоумышленников, которые в свою очередь, получив их, могут нанести их владельцу не только финансовый ущерб, но и подвести под уголовную ответственность [1].

По данным аналитического центра InfoWatch, за 2016 год 93% утечек связано с компрометацией ПДн. За исследуемый период скомпрометировано более 3,1 млрд. записей (в три раза больше, чем было зафиксировано в 2015 году) [2].

С учётом того, что интенсивно растёт количество нарушений, связанных с ПДн, а также расширяется количество видов возможных нарушений, задача совершенствования защиты этого вида информации ограниченного доступа является актуальной.

Для того чтобы обеспечить адекватную защиту ПДн, необходимо осуществить количественную оценку защищенности защищаемой информационной системы персональных данных (ИСПДн), так как она позволяет точно оценить состояние защиты ИСПДн, и тем самым избежать излишних финансовых и трудовых затрат. Анализ существующих методик оценки защищенности [3, 4] показал, что они не применимы для количественной оценки защищенности ПДн в ИСПДн, так как носят либо качественный характер [4], либо являются специализированными и направлены не на оценку защищенности ПДн [3]. В связи с этим, разработка метода количественной оценки защищенности ПДн в информационных системах (ИС) является актуальной задачей.

Так как любая автоматизированная ИС является совокупностью автоматически управляемых объектов ИТ, в которых часть функций управления выполняет человек, разрабатываемая методика основывается на количественной оценке защищенности ПДн на основе анализа актуальных угроз безопасности, и на количественной оценке защищенности ПДн на основе тестирования специалистов.

Математическая модель количественной оценки защищенности ПДн в ИС на основе анализа актуальных угроз (S1) описывается формулой (1):

$$S1 = 100 - \frac{\sum_{i=0}^{m}\left(\frac{Pст_i + \frac{\sum_{j=0}^{n} k_i * Pэкс_j}{n}}{3} + Y1\right)}{m} \quad (1)$$

где,

$Pст_i$ – вероятность реализации i-ой угрозы безопасности ПДн, которая определяется на основе статистики реализации i-ой угрозы безопасности ПДн в ИС.

$Pэкс_j$ – оценка вероятности реализации i-ой угрозы безопасности ПДнj-ым экспертом.

n – количество экспертов, реализующих оценку угроз безопасности ПДн.

m – количество угроз безопасности ПДн.

k – коэффициент квалификации специалиста, который определяется основываясь на небольшом тесте следующим образом:

1. Специалисту предлагается тест из десяти вопросов с вариантами ответов «да» и «нет».

2. Специалист отвечает на вопросы.

3. Осуществляется расчет коэффициента квалификации $k = \frac{x}{10}$, где x – количество верных ответов.

Y1 – показатель исходной защищенности ИСПДн, который зависит от перечня технических и эксплуатационных характеристик ИСПДн. Этот перечень характеристик указан в «Методике определения актуальных угроз безопасности ПДн при их обработке в ИСПДн».

Расчет показателя исходной защищенности ИС осуществляется в соответствии с (2) следующим образом:

1. Проверяется выполнение первого условия. Если условие выполняется, осуществляется расчет по соответствующей формуле, иначе проверяется выполнение следующего условия.

2. Проверяется выполнение второго условия. Если условие выполняется, осуществляется расчет по соответствующей формуле, иначе проверяется выполнение следующего условия.

3. Проверяется выполнение третьего условия. Если условие выполняется, осуществляется расчет по соответствующей формуле.

$$\begin{cases} Y1 = 100 - \frac{S_в * 100}{6}, \text{если } \frac{S_в * 100}{6} \geq 70 \\ Y1 = 100 - \frac{S_c * 100}{7}, \text{если } 35 \leq \frac{S_c * 100}{7} < 70 \\ Y1 = 100 - \frac{S_н * 100}{9}, \text{если } \frac{S_н * 100}{9} < 35 \end{cases} \quad (2)$$

где,

$S_в$ – количество технических и эксплуатационных характеристик, совпавших с уровнем защищенности «Высокий».

S_c – количество технических и эксплуатационных характеристик, совпавших с уровнем защищенности «средний».

$S_н$ – количество технических и эксплуатационных характеристик, совпавших с уровнем защищенности «низкий».

Исходя из (1), расчет вероятности реализации i-ой угрозы Py_i осуществляется по формуле (3):

$$Py_i = \frac{Pст_i + \frac{\sum_{j=0}^{n} k_i * Pэкс_j}{n} + Y1}{3} \quad (3)$$

Так же исходя из (1), расчет вероятности реализации какой-либо из угроз Ру осуществляется по формуле (4):

$$Py = \frac{\sum_{i=0}^{m} \left(\frac{Pст_i + \frac{\sum_{j=0}^{n} k_i * Pэкс_j}{n} + Y1}{3} \right)}{m} \quad (4)$$

Математическая модель количественной оценки защищенности ПДн в ИС на основе тестирования специалистов (S2) описывается формулой (5):

$$S2 = \frac{\frac{\sum_{i=0}^{t} k_i * Yит_i}{t} + \frac{\sum_{i=0}^{b} k_i * Yрс_i}{b}}{2} \quad (5)$$

где,

k – коэффициент квалификации специалиста, который определяется аналогично расчетам коэффициента квалификации при оценке на основе угроз безопасности ПДн.

t – количество анкетируемых специалистов из области ИТ и ИБ.

b – количество анкетируемых специалистов занимающихся обработкой ПДн.

$Yит_i$ – правильность выполнения теста для специалиста из области ИТ и ИБ, выраженная в процентах.

$Yрс_i$ – правильность выполнения теста для специалиста, осуществляющего обработку ПДн, выраженная в процентах.

Исходя из (5), общий уровень знаний специалистов области ИТ и ИБ ($Yит_{общ}$) определяется по формуле (6):

$$Yит_{общ} = \frac{\sum_{i=0}^{t} k_i * Yит_i}{t} \quad (6)$$

Исходя из (1), общий уровень знаний специалистов, занимающихся обработкой ПДн ($Yрс_{общ}$) определяется по формуле (7):

$$Yит_{общ} = \frac{\sum_{i=0}^{b} k_i * Yрс_i}{b} \quad (7)$$

Математическая модель количественной оценки защищенности ПДн в ИС (Yитог) описывается формулой (8):

$$Yитог = \frac{S1 + S2}{2} \quad (8)$$

Таким образом, предложенная методика позволяет произвести количественную оценку:

- уровня защищенности ПДн в ИС (в процентах);
- угроз безопасности ПДн в ИС (в процентах);
- уровня знаний специалистов области ИТ и ИБ;
- уровня знаний специалистов, осуществляющих обработку ПДн в ИС.

Список использованных источников

1. ИТ-Портал компании «ИнфосистемыДжет» [Электронный ресурс]: Защита персональных данных; JetInfo, 2009. – Режим доступа: http://www.jetinfo.ru/stati/zaschita-personalnykh. – Загл. с экрана

2. Официальный сайт InfoWatch [Электронный ресурс]: Аналитика: утечки конфиденциальной информации в 2016 году; – Режим доступа: https://www.infowatch.ru/analytics/reports. – Загл. с экрана

3. Будовских И.А., Алферова Л.Д. Формирование алгоритма расчета уровня соответствия информационной безопасности кредитных организаций стандарту Банка России // Материалы 12-ой Всероссийской научно-технической конференции «Наука и

молодежь – 2015». - г.Барнаул, Изд-во АлтГТУ, 2015г. Режим доступа: http://edu.secna.ru/media/f/information_safety_tez_2015.pdf

4. Будовских И.А., Загинайлов Ю.Н. «Оценка применимости для аудита безопасности государственных ИС методики определения угроз безопасности информации, разработанной ФСТЭК России» // Материалы XVII международной научно-технической конференции «Измерение, контроль, информатизация». – Барнаул: Изд-во АлтГТУ, 2016г. Режим доступа: http://elib2.altstu.ru/disser/conferenc/2016/19-05.pdf

РАЗРАБОТКА CAE МОДЕЛИ ДЛЯ ИССЛЕДОВАНИЯ РАСПРОСТРАНЕНИЯ ТЕПЛА В СИСТЕМАХ ДИНАМИЧЕСКОГО ТЕРМОРЕГУЛИРОВАНИЯ

Воробьев Д.С. – магистрант, Якунин А.Г. – д.т.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Системы динамического терморегулирования достаточно распространены и используются как в быту, так на производственных предприятиях. Одними из представителей таких систем являются проточные водонагреватели, которые способны производить нагрев воды в момент протекания её через нагревательные элементы, что обеспечивает бесперебойную и непрерывную поставку горячей воды.

Для таких устройств важно подобрать подходящий алгоритм управления терморегулированием, чтобы сделать его наиболее эффективным и минимизировать такие явления, как перерегулирования и пульсации [1].

Целью данной работы является разработка технологии моделирования систем динамического терморегулирования и методики вычислительного эксперимента для оптимизации конструкции алгоритмического обеспечения с помощью CAE – модели проточного водонагревателя для исследования процессов распространения тепла.

Построение исследуемой модели проточного водонагревателя было произведено с помощью программы SolidWorks, а для исследования распространения тепла использован её модуль SolidWorksflowSimulation в основе которого лежит метод конечных объемов [2].

На рисунке 1 представлено распространение тепла на поверхности модели проточного водонагревателя, а на рисунке 2 представлено общее распределение температур на срезе вдоль его модели. Данные представлены за 100 секунд работы системы с шагом в 20 секунд.

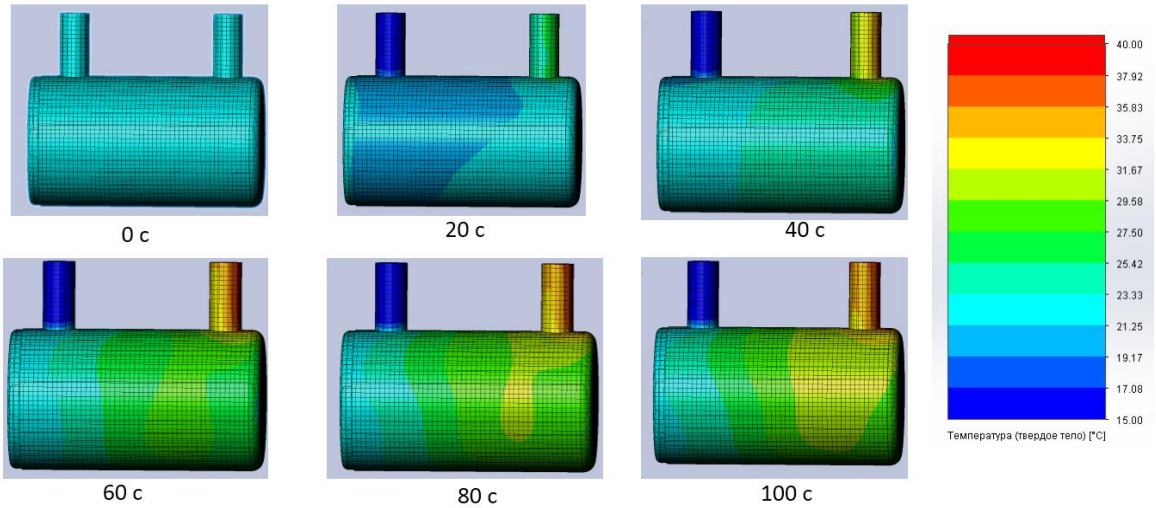


Рисунок 1 – Распределение тепла на поверхности проточного водонагревателя

Практическое применение результатов работы состоит в том, что она позволяет в ходе проведения вычислительного эксперимента проанализировать распределение тепла при

работе проточного водонагревателя ещё на этапе проектирования, что позволяет сократить число натурных испытаний до минимума.

В данной работе отработана методика применения программных средств использующих метод конечных объемов, для исследования распространения тепла в проточном водонагревателе, а также выполнены исследования влияния отдельных элементов конструкции нагревателя на качество его работы.

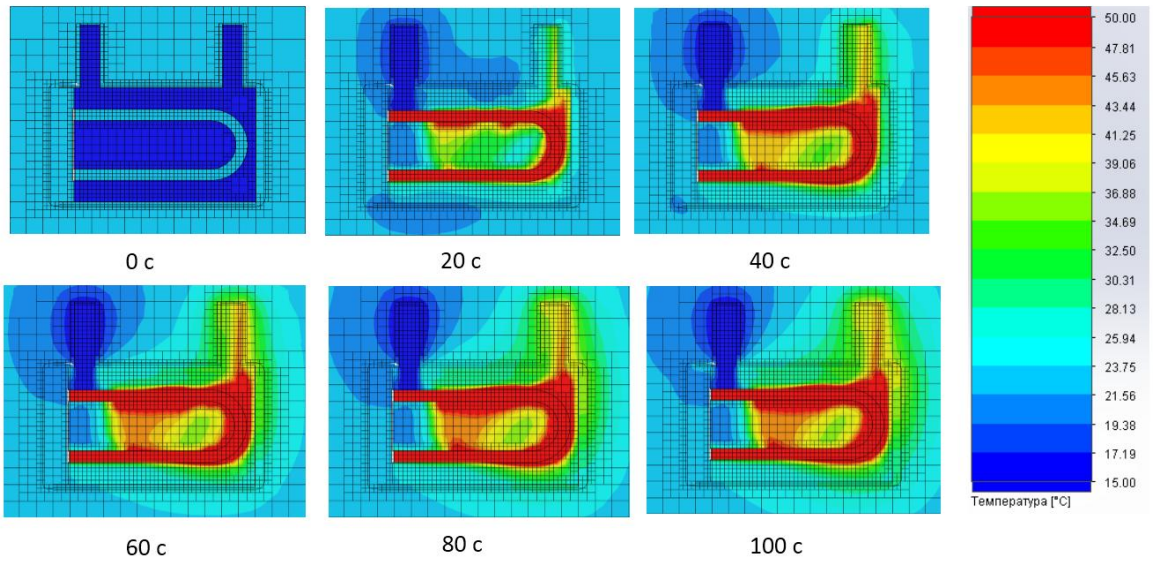


Рисунок 2 – Общее распределения тепла в проточном водонагревателе

Список использованных источников

1. Голиковская К.Ф., Краев М.В., Ибрагимов Ю.А., Никитин В.В. Исследование динамических характеристик системы терморегулирования. Отчет по НИР номер 75(э.З) Красноярск Завод-ВТУЗ, 1991г. Номер г.рег Х-63617.

2. АлямовскийА.А./ SolidWorks Simulation. Инженерный анализ для профессионалов: задачи, методы, рекомендации [Текст] / А.А. Алямовский.-М.:ДМК Пресс, 2015.-562 с.: ил.

Разработка имитационной модели на основе СМО для проектирования сети зарядных станций электромобилей

Гопаченко Ю.О. - студент, Якунин А.Г. - к.т.н., доцент

Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Ухудшение экологической обстановки городов и существенное повышения дефицита топливных ресурсов являются одними из наиболее актуальных и сложных проблем современного мира. Наиболее перспективным направлением решения данных проблем является использование транспорта на электротяге, высокое влияние на развитие которого оказывает активность развития сети зарядных станций для электромобилей [1].

Эффективное распределение зарядных ресурсов для электромобилей также является одним из важных аспектов развития. Таким образом, возникает потребность в разработке средств позволяющих проектировать и рассчитывать показатели эффективности работы сети зарядных станций. Такие показатели позволяют проанализировать и определить целесообразность размещения зарядной станции для электромобилей при заданных характеристиках. Одним из путей, позволяющих рассчитывать эти показатели, является применение имитационных моделей набаза систем массового обслуживания (СМО).

Разрабатываемая система относится к многоканальным СМО с ограниченной длиной очереди. Задавая параметры системы и анализируя процесс обслуживания входного потока

требований, можно установить зависимости между характером потока заявок, числом каналов обслуживания, производительностью отдельного канала и эффективным обслуживанием с целью нахождения наилучших путей управления этими процессами.

Таким образом достигается цель функционирования, то есть желаемое состояние системы, при котором будет обеспечен минимум суммарных затрат от ожидания обслуживания, потерь времени и ресурсов на обслуживание и от простоев каналов обслуживания [2].

В качестве входного потока требований в данной системе выступают заявки на обслуживание владельцев электромобилей, прибывающих на зарядную станцию для зарядки своих транспортных средств. Частота, с которой электромобили поступают на станцию, определяет интенсивность поступления заявок в единицу времени.

Количество электромобилей, прибывающих на станцию, определяется такими параметрами, как:

– количество электромобилей в населенном пункте, исключая владельцев авто, предпочитающих быстрой зарядке на станции медленную домашнюю быструю зарядку на станции, а также владельцев, проживающих на достаточно удаленном расстоянии от станции, в таком случае эффективность эксплуатации станции сводится к минимуму;

– запас хода электромобиля;

– средний пробег электромобиля за сутки;

– расстояние от места проживания владельца электромобиля до станции.[3, 4]

Таким образом, интенсивность поступления заявок в единицу времени, равную суткам, определяется по формуле:

$$\lambda = \sum_{i<N_{el}}^{i=1} \frac{S_{ami} + S_{di}}{S_{pri}}$$

где S_{am} – средний пробег за сутки; S_{pr} – запас хода автомобиля; S_d – расстояние от ЭЗС*; N_{el} – количество автомобилей в населенном пункте; i – идентификатор конкретного электромобиля.

Интенсивность потока обслуживания требований n-каналами в сутки определяется по формуле:

$$\mu = \frac{\Delta t}{t_{ch}} \cdot n,$$

где Δt – время активного состояния станции, t_{ch} – время заряда автомобиля.

Время активного состояния заряда станции – это количество часов в сутки, в течение которых станция функционирует, то есть обслуживает требования [5]. Данное время рассчитывается как промежуток между началом и окончанием активности:

$$\Delta t = t_2 - t_1,$$

где t_1 – время начала активного состояния; t_2 – время окончания активного стояния.

Время, затрачиваемое на заряд автомобиля – это отношение емкости аккумулятора автомобиля к мощности зарядного устройства, умноженное на 0,8, так как при быстрой зарядке постоянным током заряжается 80% объема батареи [6].

Среднее время заряда автомобиля рассчитывается как время заряда автомобиля, умноженное на его весовой коэффициент, то есть на отношение частоты заправки одного автомобиля к частоте заправки общего количества прибывающих на станцию автомобилей.

$$\overline{t_{ch}} = \sum_{i<N_{el}}^{i=1} \frac{c_{bi} \cdot 0{,}8 \cdot k_i}{P_{ch}},$$

где c_b - емкость аккумулятора, P_{ch} – мощность зарядного устройства, где k_i– весовой коэффициент, n – количество каналов обслуживания, i – идентификатор конкретного электромобиля.

Таким образом, интенсивность обслуживания автомобилей в сутки – это количество автомобилей, которое станция в состоянии обслужить за время своей активности. Определяется отношением активного времени станции к среднему времени зарядки автомобиля [7, 8].

Так как процесс работы СМО представляет собой случайный процесс с дискретными состояниями и непрерывным временем, единица интервала, равная одним суткам, является слишком протяженной для оценки протекающих в системе процессов.

Следовательно, параметры системы следует рассчитывать в течение времени активности системы через интервал равный одному часу t_j или 60 минутам. Интенсивность поступления заявок в единицу времени, равную t_j, определяется по формуле:

$$\lambda_j = \sum \lambda_i(t_j) = \frac{S_{ami} + S_{di}}{S_{pri}}(t_j)$$

Интенсивность обслуживания требований в единицу времени t_i рассчитывается как

$$\mu_j = \frac{1}{\overline{t_{ch}}} \cdot n$$

Для определения вероятностных состояний системы в определенный момент времени требуется рассчитать параметр длины очереди.

Длина очереди – это максимальное количество требований, которые может обслужить система до истечения времени активности при отсутствии свободных каналов обслуживания. Данный параметр рассчитывается исходя из момента времени активности системы – t_j.

Количество мест в очереди в момент времени t_i определяется по формуле:

$$m_{max} = \frac{t_2 - t_j}{\overline{t_{ch}}} \cdot n$$

Количество обслуженных заявок в момент времени t_j определяется отношением интенсивности входящего потока требований к интенсивности обслуживания n–каналами:

$$\rho_j = \frac{\lambda_j}{\mu_j} \cdot n$$

Заявка, поступившая в момент, когда все n каналов заняты, становиться в очередь и ожидает обслуживания. Количество мест в очереди ограничено числом m, т.е. если заявка пришла в момент, когда в очереди уже стоят m-заявок, она покидает системы необслуженной [9].

Предельные вероятности состояний системы, среднее относительно время пребывания системы в данном состоянии, рассчитываем для каждого интервала времени t_j.

На рисунке 1 представлен размеченный граф состояний, где под состояниями понимается степень загруженности каналов обслуживания.

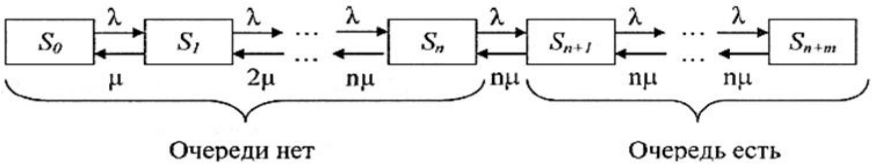


Рисунок 2 – Размеченных граф состояний

S0 – все каналы свободны S1 – занят только один канал

……

Sn – заняты все n каналов Sn+1 – заняты все n каналов и одна заявка в очереди

…….

Sn+m – заняты все n каналов и все m мест в очереди

Переходы из одного состояние в другое могут совершаться только из соседних состояний, под влиянием потоков событий с интенсивностями поступления заявок – λ_i. Для каждого состояния определяется предельная вероятность – это вероятность того, что в исследуемый интервал времени, система будет находиться в данном состоянии. Формулы для расчета предельных вероятностей состояний:

$$p_0 = (1 + \frac{\rho}{1!} + \frac{\rho^2}{2!} + \cdots + \frac{\rho^n}{n!} + \frac{\rho^{n+1}}{nn!} \cdot \frac{1-(\frac{\rho}{n})^m}{1-\rho/n!})^{-1},$$

$$p_1 = \rho p_0, p_2 = \frac{\rho^2}{2!} p_0, \ldots, p_n = \frac{\rho^n}{n!} p_0,$$

$$p_{n+1} = \frac{\rho^{n+1}}{nn!} p_0; p_{n+2} = \frac{\rho^{n+2}}{n^2 n!} p_0; \ldots; p_{n+m} = \frac{\rho^{n+m}}{n^m n!} p_0$$

На основе полученных данных можно рассчитать показатели эффективности работы системы [10]:

– вероятность отказа:

$$P_{отк} = p_{n+m} = \frac{\rho^{n+m}}{n^m n!} p_0$$

– вероятность образования очереди:

$$P_{оч} = \sum_{i=0}^{m-1} p_{n+i} = \frac{\rho^n}{n!} \cdot \frac{1-(\frac{\rho}{n})^m}{1-\frac{\rho}{n}} p_0$$

– относительная пропускная способность:

$$Q = 1 - P_{отк}$$

– абсолютная пропускная способность:

$$A = \lambda \cdot Q$$

– среднее число занятых каналов:

$$k_{зан} = \frac{A}{\mu} = \rho Q$$

– среднее число заявок, находящихся в очереди:

$$L_{оч} = \frac{\rho^{n+1}}{nn!} \cdot \frac{1-\left(\frac{\rho}{n}\right)^m \left(m+1-\frac{m}{n}\rho\right)}{\left(1-\frac{\rho}{n}\right)^2}$$

– среднее время ожидания в очереди:

$$T_{оч} = \frac{L_{оч}}{\lambda}$$

– среднее число заявок в системе:

$$L_{сист} = L_{оч} + k_{зан}$$

– среднее время пребывания заявки в СМО:

$$T_{сист} = \frac{L_{сист}}{\lambda}$$

Исходя из полученных результатов можно оценить загруженность и эффективность работы исследуемой системы, максимальные и минимальные значения показателей работы системы.

Рассчитав показатели, при которых достигается цель функционирования системы, можно определить диапазон отклонения максимальных и минимальных показателей от «оптимальных». Исходя из данного диапазона, определяется степень необходимого изменения исходных характеристик исследуемой системы. Таким образом, ориентируясь на оптимальные показатели эффективности, можно установить наиболее приемлемые характеристики электрических заправочных станций (ЭЗС), такие как географическое расположение относительно населенного пункта, количество каналов обслуживания ЭЗС и мощность зарядных устройств, а также целесообразность размещения ЭЗС в данном населенном пункте.

Список использованных источников

1. Парк электромобилей в России на начало 2016 года [Электронный ресурс]: Режим доступа https://www.autostat.ru/infographics/25457/

2. Кошуняева Н.В., Патронова Н.Н. Теория массового обслуживания (практикум по решению задач)/САФУ им. М.В.Ломоносова. – Архангельск; САФУ, 2013 – 107 с.

3. Щетина В. А., Морговский Ю. Я., Центер Б. И., Богомазов В. А. Электромобиль: техника и экономика – Л.: Машиностроение, 1987.- - 253с.: ил.

4. Ставров О.А. Электромобили – М.: Транспорт, 1968. – 104с.

5. Ивченко Г.И., Каштанов В.А., Ковалев И.Н. Теория массового обслуживания: Учеб.пособие – М.: Высш. школа, 1982. – 256 с., ил.9

6. Средний пробег легкового автомобиля в России - 16,7 тыс. км в год. [Электронный ресурс]: Режим доступа https://www.autostat.ru/news/6069/

7. Б. П. Бусыгин " Электромобили. Учебное пособие - МАДИ, 1979 год, 37 стр.

8. Самаров К.Л. Математика. Элементы теории массового обслуживани, учеб.пособие - М.: Учебный центр "Резольвента", 2009. - 18 с.

9. И.В. Солнышкина Теория систем массового обслуживания : учеб.пособие / И.В. Солнышкина. – Комсомольск-на-Амуре : ФГБОУ ВПО «КнАГТУ», 2015. - 76 с.

10. Галанина О.В. Экономико-математическое моделирование: модели теории массового обслуживания : учеб.пособие – С-Петербург : СПГАУ, 2013. – 20 с.

ОРГАНИЗАЦИЯ ПОДГОТОВИТЕЛЬНОГО ЭТАПА АКУСТИЧЕСКОГО И ВИБРАЦИОННОГО КОНТРОЛЯ ЗАЩИЩЕННОСТИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

Деменко А.М. - студент, Загинайлов Ю.Н. - к.в.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Актуальность

Одной из функциональных задач решаемых специалистами по ИБ в организации является организация контроля защищённости информации объекта информатизации. Формирование такой компетенции у студентов вуза связана с проблемой, которая заключается в том, что этот вопрос рассматривается и излагается в специальных нормативных документах ФСТЭК России в текстовом виде строго инженерным языком, что затрудняет восприятие содержательной части материала и увеличивает время на его освоение. В связи с этим актуальна задача формирования учебного контента, соответствующего требованиям педагогических технологий для образовательного процесса.

Контент

В современных условиях информация играет решающую роль как в процессе экономического развития, так и в ходе конкурентной борьбы на внутреннем и внешнем рынках. Успешное функционирование и развитие предприятий все больше зависит от дальнейшего совершенствования их деятельности в области обеспечения информационной безопасности.

В этих условиях промышленный шпионаж, как сфера тайной деятельности по добыванию, анализу, хранению и использованию информации приобретает большой размах и охватывает все стороны рыночной экономики. Многие технические средства, находившиеся ранее под контролем у спецслужб, стали доступны частным лицам и вопрос их приобретения связан лишь с рыночной стоимостью и умением их использовать.

Одним из источников важной информации организации являются совещания, на которых представляются материалы по имеющимся результатам и планам работ. Присутствие большого количества людей и большие размеры помещений ставят перед этими организациями проблему сохранения коммерческой тайны.

Защита информации при проведении совещаний с участием представителей сторонних организаций имеет актуальное значение и основными задачами по обеспечению информационной безопасности является выявление и своевременная локализация возможных технических каналов утечки акустической информации. Основными

мероприятиями в данной области являются аттестационный и эксплуатационный контроль выделенных помещений [1].

Контроль эффективности защиты заключается в проверке соответствия качественных и количественных показателей эффективности мер технической защиты установленным требованиям или нормам эффективности защиты информации. В настоящее время, для проведения контроля защищенности, все более широко применяются программно-аппаратные комплексы, имеющие в своем составе программные средства проведения трудоемких расчетов различных показателей, относящихся к оценке защищенности объектов информатизации.

Но, учитывая высокую стоимость и сложность технического обслуживания данных комплексов, многие организации применяют более простые средства измерений, а расчеты выполняют вручную.

В зависимости от природы сигналы распространяются в определенных физических средах. В общем случае средой распространения могут быть газовые (воздушные), жидкостные (водные) и твердые среды [2].

Технические средства разведки служат для приема и измерения параметров сигналов.

В зависимости от физической природы возникновения информационных сигналов, среды распространения акустических колебаний и способов их перехвата технические каналы утечки акустической (речевой) информации можно разделить на: воздушные, вибрационные, электроакустические, оптико-электронный и параметрические [6].

Методика инструментального контроля выполнения норм противодействия акустической речевой разведке основывается на инструментально-расчетном методе определения отношений «речевой сигнал / акустический (вибрационный) шум» (далее – «сигнал/шум») в контрольных точках в октавных полосах со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц. Полученные отношения «сигнал/шум» сравниваются с нормированными. Методика ориентирована на использование контрольно-измерительной аппаратуры общего применения.

Для проведения инструментального контроля при отсутствии автоматизированных комплексов должны быть созданы передающая и приемная измерительные системы на основе аппаратуры общего применения. Передающая измерительная система размещается в контролируемом помещении, а приемная – в контрольной точке. Далее на схемах представлен состав приемной и передающей системы:

В качестве тестового сигнала могут быть использованы гармонические (тональные) сигналы со среднегеометрическими частотами октавных полос.

Определение числовых значений отношений «сигнал/шум» в контрольных точках необходимо проводить в периоды минимальной зашумленности мест речевой деятельности (отсутствие персонала в помещении, выключение шумящего технического оборудовании и т.п.). Лучше всего проводить контроль в ночное время.

На подготовительном этапе необходимо [3]:

- провести осмотр и анализ архитектурно-планировочных решений помещения;
- составить план-схему помещения, отметить на ней выбранные для оценки звукоизоляции конструкции (рисунок 1);
- описать заданную ограждающую конструкцию, пояснить возможные пути утечки речевой информации через нее;

- на плане помещения и выбранной ограждающей конструкции выбрать контрольные точки.

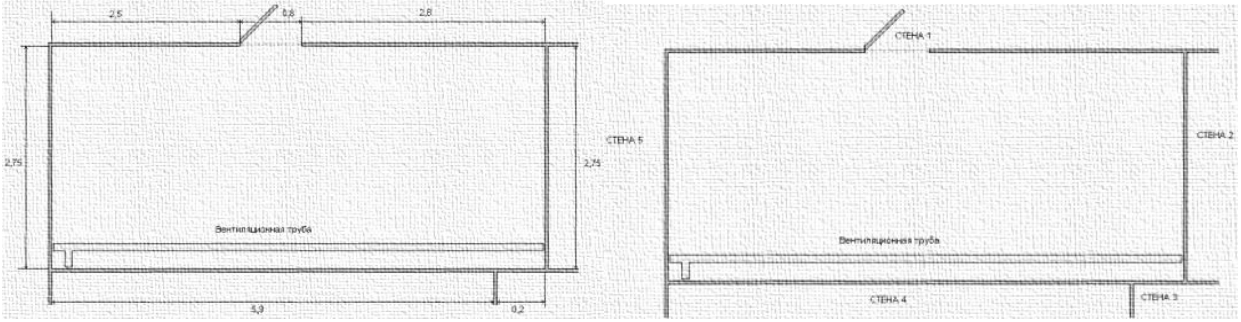


Рисунок 1 - План-схема помещения и нумерация стен

Контрольными точками являются места возможной установки акустических и вибрационных датчиков аппаратуры акустической речевой разведки, или места расположения отражающих поверхностей лазерного излучения, а также места непреднамеренного прослушивания речи, в которых при инструментальном контроле производятся измерения отношений “сигнал /шум” с целью последующей оценки выполнения норм противодействия акустической речевой разведке[4].

При контроле выполнения норм противодействия акустической речевой разведки с применением микрофонов (в том числе с применением направленных микрофонов) контрольные точки должны выбираться на расстоянии 0,5 м от внешних поверхностей обследуемой ограждающей конструкции.

Если ограждающая конструкция состоит из неоднородных участков, то акустические измерения необходимо выполнять отдельно для каждого участка.

При контроле выполнения норм противодействия речевой разведки с применением вибрационных средств наряду с ограждающими конструкциями необходимо учитывать элементы инженерно-технических систем, попадающих в акустическое поле речевых сигналов [1].

Если границей контролируемой зоны являются ограждающие конструкции, то контрольные точки для вибрационных измерений выбираются непосредственнона внешних по отношению к источнику речевого сигнала поверхностях ограждающих конструкций. Если ограждающая конструкция состоит из неоднородных участков, то вибрационные измерения необходимо выполнять отдельно для каждого участка[5].

Если граница контролируемой зоны пересекает коммуникации инженерно-технических систем, то контрольные точки для вибрационных измерений выбираются непосредственно на поверхности этих элементов, на расстоянии не превышающем 0,5 м от места их входа (выхода).

Таким образом, контрольные точки следует располагать как представлено на рисунке 2, где слева представлена стена №1 а справа стена №2.

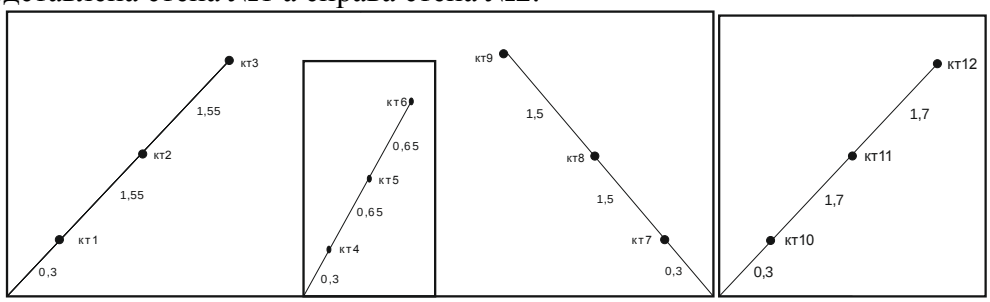


Рисунок 2 - Стена 1

Вибродатчики должны располагается непосредственно на поверхностях ограждающих конструкций и на различных конструктивных элементах инженерно-технических систем - при контроле защищенности от речевой разведки с использованием вибрационных средств и на плоскостях остекления оконных проемов - при контроле защищенности от речевой

разведки с использованием оптико-электронных средств разведки. Крепление вибродатчиков должно обеспечивать плотное (монолитное) соединение вибродатчика с обследуемой поверхностью (клеевое или резьбовое).

Контроль выполнения норм противодействия речевой разведке с применением оптико-электронных (лазерных) средств необходимо проводить с использованием вибрационных измерений на участках (полотнах) оконного остекления[3].

Контрольные точки следует выбирать из условия их размещения в двух-трех местах на каждом участке (полотне) остекления. При двойном остеклении без использования жалюзи между стеклами вибрационные измерения необходимо проводить как на внешнем, так и на внутреннем остеклении.

Далее представлено схематичное расположение контрольных точек для двух стен, для остальных делается подобным образом.

Измерительный микрофон должен быть размещен на расстоянии от 1 до 2 м от внешней поверхности испытываемой ограждающей конструкции, на уровне ее середины, и направлен в сторону от улицы или дороги с транспортным потоком.

Если ограждающая конструкция имеет балконы, лоджии или другие выступающие элементы фасада, то микрофон должен быть размещен на расстоянии 1 м от вертикальной плоскости, проходящей через наиболее выступающие точки этих элементов фасада, на уровне середины ограждающей конструкции.

Защищенность речевой информации от ее перехвата оптико-электронной аппаратурой разведки обеспечивается, если значение контролируемого параметра, рассчитанного по результатам вибрационных измерений на полотнах оконного остекления, не превышает его нормированного значения[4].

При контроле выполнения норм противодействия перехвату речевой информации по каналу непреднамеренного прослушивания контрольные точки выбираются на расстоянии 0,5 м от ограждающих конструкций и на высоте 1, 5 м от пола с внешней стороны по отношению к контролируемому рабочему помещению. Если технологические окна систем вентиляции и кондиционирования совпадают с границей контролируемой зоны, то контролируемые точки выбираются непосредственно во входных (выходных) отверстиях воздуховодов систем вентиляции и кондиционирования.

В результате данной работы была рассмотрена организация подготовительного этапа акустического и вибрационного контроля защищенности объекта информатизации. В частности, был детально представлен подготовительный этап проведения акустического и вибрационного контроля защищенности объекта информатизации, основные принципы. Также были составлены схемы помещения и нумерация стен и типового расположения контрольных точек для проведения измерений в ходе акустического и вибрационного контроля.

Список использованных источников

1 Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 253 с.: ил. - Библиогр. в кн. - [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557

3 Бузов Г. А., Калинин С. В., Кондратьев А. В. Защита от утечки информации по техническим каналам: Учебное пособие. – М.: Горячая линия – Телеком, 2005. – 416 с.

4 Хорев А.А. Технические каналы утечки акустической (речевой) информации. «Специальная техника» №3, 2004 г.

5 Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), Гостехкомиссия России, 2002.

6 Хорев А.А. Технические каналы утечки акустической (речевой) информации. «Специальная техника» №1, 1998 г. стр.

ТЕХНИЧЕСКИЕ АСПЕКТЫ ПРИ СЪЁМЕ ЭЛЕКТРОМИОГРАФИЧЕСКИХ СИГНАЛОВ

Ермаков А.В. - магистрант, Якунин А.Г. - д.т.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Качество электронной системы съема, усиления и регистрации биопотенциалов во многом определяется параметрами входной цепи, образованной электродами отведений и резистивными суммирующими схемами, а также входных каскадов усиления [1].

Свойства входной цепи определяют степень подавления синфазных помех, вызванных наводками от силовой и осветительной сети и электрических установок. Неодинаковое для разных электродов изменение во времени сопротивления кожа-электрод совместно с нестабильностями электрических параметров электродов приводит к изменению коэффициента передачи входной цепи по постоянному току и искажению амплитудно-частотной характеристики (АЧХ) системы электрод-вход усилителя биопотенциалов. При этом может происходить преобразование синфазной помехи в разностную, которая, складываясь с полезным сигналом, имеет аддитивный характер[2-3].

На входные цепи усилителей биоэлектрических сигналов наряду с воздействием синфазных и разностных помех от индустриальных источников (сети питания, электросиловые приборы) воздействуют синфазные и разностные помехи биологического происхождения (артефакты), из которых наиболее сильно проявляют себя помехи от тремора мышц пациента.

Снижение влияния синфазных биологических и индустриальных помех достигается применением усилителей с достаточно большим коэффициентом подавления этих помех. Устранение влияния противофазных помех и наводок достигается уменьшением площади замкнутого контура, образованного проводами отведений, применением методов экранирования и симметрирования входных цепей.

В качестве усилителей биоэлектрических сигналов широко используются усилители постоянного тока с непосредственными связями. Входные каскады усилителей выполняются по симметричным дифференциальным схемам, обеспечивающим высокий уровень подавления синфазных помех.

Качественные характеристики дифференциальных каскадов определяются их схемотехническими особенностями и используемыми усилительными элементами. Дифференциальный каскад (ДК) на биполярных транзисторах обладает большим усилением по напряжению, достаточно высоким значением коэффициента режекции, но сравнительно небольшим входным сопротивлением, особенно для разностного сигнала. Для улучшения характеристик используют транзисторы с большим коэффициентом усиления тока базы β_0, дифференциальные каскады с генераторами стабильного тока в цепи отрицательной обратной связи и динамическими нагрузками, "токовые зеркала" и микротоковые режимы транзисторов. Эффективным средством повышения качественных показателей дифференциальных усилителей (ДУ) служит использование составных транзисторов.

Применение составных транзисторов позволяет существенно увеличить входное сопротивление по разностному сигналу в сравнении с ДУ на простых биполярных транзисторах, более чем на порядок повысить коэффициент режекции. Коэффициент усиления разностного сигнала практически не изменяется. Наилучшие результаты дает схема общий коллектор - общий эмиттер, в которой могут быть получены входное сопротивление для разностного сигнала порядка сотен килоом, входное сопротивление для сигнала среднего уровня - сотни мегаом [4].

Особый интерес для построения усилителей биоэлектрических сигналов представляют высококачественные дифференциальные усилители на операционных усилителях (ОУ). Простейший дифференциальный каскад строится на ОУ с отрицательной обратной связью (рисунок 1а). При большом коэффициенте усиления и выполнении условия R3/R4 = R1/R2

выходное напряжение зависит только от разностного входного сигнала и не зависит от сигнала среднего уровня, то есть:

$$U_{вых} = (U'_{вх} - U''_{вх})\frac{R2}{R1}.$$

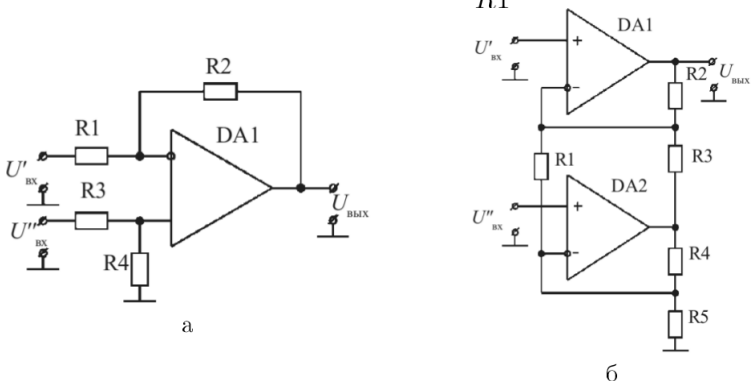


Рисунок 1 – Принципиальный схемы: а) дифференциального усилителя на ОУ; б) дифференциального усилителя с повышенным входным сопротивлением

Недостатками простого дифференциального каскада на ОУ являются низкие входные сопротивления и трудность регулировки коэффициента усиления, которая возможна только путем одновременного пропорционального изменения сопротивления двух резисторов (R2 и R4).

Повышение входного сопротивления достигается использованием неинвертирующих входов ОУ (рисунок 1б). Такая схема обеспечивает установку заданного коэффициента усиления с помощью лишь одного резистора (R1). Величины сопротивлений резисторов должны удовлетворять условию R2/R3 = R5/R4, а выходное напряжение определяется соотношением:

$$U_{вых} = (U'_{вх} - U''_{вх})\left(\frac{R2+R5}{R1} + \frac{R2}{R3} + 1\right)$$

Для этой схемы характерно значительное неравенство входных сопротивлений по прямому и инверсному входам, следствием чего является недостаточный уровень подавления синфазной помехи.

Значительно лучшие результаты дает схема на трех ОУ (рисунок 2), в которой глубина обратной связи обоих входных усилителей оказывается одинаковой[3]. Для этой схемы величины сопротивлений должны удовлетворять соотношению R2/R3 = R5/R4, кроме того, обычно выбирают R2 = R3. Тогда выходное напряжение определяется формулой:

$$U_{вых} = (U'_{вх} - U''_{вх}) \cdot \frac{R5}{R4} \cdot \left(\frac{2 \cdot R2 + R1}{R1}\right)$$

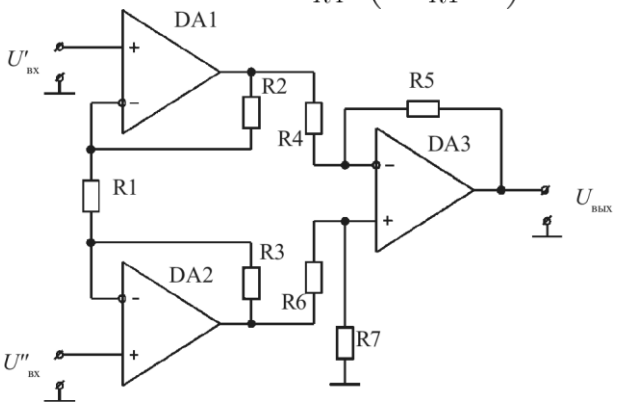


Рисунок 2 - Принципиальная схема инструментального усилителя на трёх УО

В этом случае также сохраняется возможность регулировки усиления при помощи одного резистора, а коэффициент передачи синфазного сигнала при правильном выборе величины R7 и идеальных ОУ равен нулю. Благодаря этим положительным свойствам схема на трех ОУ является базовой при построении высококачественных инструментальных

усилителей, предназначенных, в частности, для усиления и регистрации биоэлектрических сигналов. При этом ОУ и пассивные элементы формируются на одном кристалле в виде интегральной микросхемы, а высокие качественные показатели достигаются путем технологической подгонки элементов в процессе изготовления.

Появление выходного сигнала при действии на входе усилителя синфазной помехи может быть вызвано не только несовершенством внутренней структуры ОУ, но и преобразованием синфазного сигнала в разностный во входных цепях усилителя.

Для уменьшения влияния синфазных помех применяются специальные компенсационные схемы. Ввиду сравнительно малого сопротивления тканей биообъекта величина синфазной помехи на всей его поверхности практически одинакова. Напряжение синфазной помехи снимается с одного или нескольких активных электродов и подается на инвертирующий усилитель, выход которого подключается через индифферентный [5] электрод N между биообъектом и общим проводом (рисунок 3).

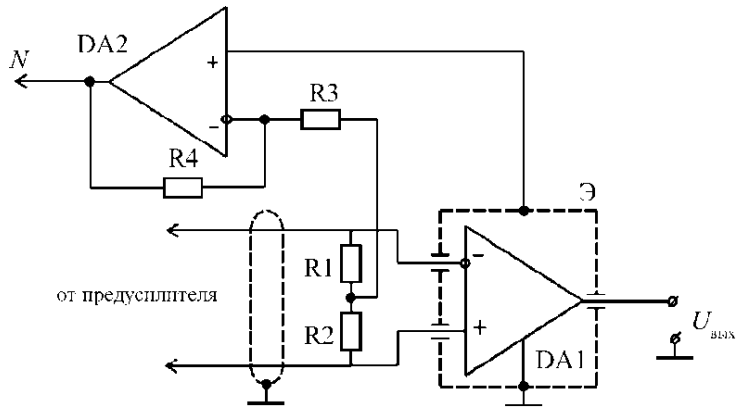


Рисунок 3 - Принципиальная схема компенсатора синфазной помехи

За счет противофазного подключения компенсирующего напряжения происходит существенное снижение уровня синфазной помехи на входе канала усиления. Качество компенсации определяется величиной коэффициента усиления усилителя DA2. При этом необходимо обеспечивать устойчивость схемы компенсации.

Список использованных источников

1) Зайченко К. В., Жаринов О.О. // Съем и обработка биоэлектрических сигналов: Учеб. пособие / Под ред. К. В. Зайченко. СПбГУАП. СПб., 2001. 140 с.: ил. ISBN 5-8088-0065-X

2) Шваб А. Электромагнитная совместимость/Пер. с нем. В.Д. Мазина и С.А. Спектора^Под ред. И.П. Кужекина.. 2-е изд., перераб. и доп. - М.: Энергоатомиздат, 1990.-480 с.

3) Хабигер Э. Электромагнитная совместимость. Основы ее обеспечения в технике: Пер. с нем./ И.П. Кужекин; Под ред. Б.К. Максимова.- М.: Энергоатомиздат, 1995.-304 с.

4) Теория и проектирование диагностической электронно-медицинской аппаратуры: Учеб.пособие / Ахутин В. М. и др. Л.: Изд-во ЛГУ, 1980. 148 с.

5) Гутников В. С. Интегральная электроника в измерительных устройствах. Л.: Энергоатомиздат, 1988. 304 с.

ВИДЫ И СВОЙСТВА ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ, ОБУСЛОВЛЕННЫЕ СЕТЕВОЙ АКТИВНОСТЬЮ

Заинковский В.Н. – магистрант, Якунин А.Г. –д.т.н., профессор
Алтайский государственный технический университет им И.И. Ползунова (г. Барнаул)

С развитием информационных технологий, основная цель которых обработка, хранение и передача информации, ко всем ранее известным инцидентам добавились новые, которые связаны с использованием более современных технологий. Значительный вклад в список добавившихся инцидентов вкладывают угрозы, которые производятся с использованием локальных и глобальных вычислительных сетей [1].

Процесс осуществления инцидентов получил название атаки или вторжения.

Атакой называется любое действие нарушителя, которое направлено на нарушение функциональности вычислительной системы либо, получение несанкционированного доступа к информационным, вычислительным или сетевым ресурсам.

Выявление атак является самой важной задачей информационной безопасности, так как обнаружение помогает блокировать атаку для уменьшения ее последствий и предотвратить утерю, порчу, искажение, несанкционированное разглашение и компрометацию защищаемой информации, а также сообщить о производящейся атаке и ее результатах.

Атака может производиться как на вычислительную, так и на информационную системы.

Информационная система — это множество средств обработки информации, которые объединены в единую систему.

Вычислительная система – в данном случае предполагается единица информационной системы [2].

Атака на информационную или вычислительную системы, как и любое действие, имеет свой жизненный цикл, который разделяет ее на этапы (рис. 1). Каждый этап можно описать следующим образом:

Рисунок 1 – Этапы атаки на информационную систему

1) подготовка – старания нарушителя заполучить как можно больше информации об объекте атаки, чтобы, основываясь на ней, спланировать последующие этапы вторжения[3].

2) вторжение – нарушитель получает несанкционированный доступ к ресурсам тех вычислительных систем, на которые происходит атака.

3) атакующее воздействие – реализуются цели, для которых и производилась атака, например, таких, как нарушение работы информационной системы, похищение информации из системы, удаление или модификация данных системы и т. д. При этом атакующий часто выполняет операции, которые направлены на стирание следов присутствия взлома в

информационной системе.

4) развитие атаки – взломщик стремится расширить объекты атаки для того, чтобы продолжить несанкционированные действия на других составляющих информационных систем [3].

Некоторые этапы в определенных атаках могут не присутствовать, например, такие, как атаки типа DDoS не содержат в себе этапа «Вторжение в систему».

Инциденты информационной безопасности могут быть продуманными или случайными (являются следствием ошибки либо природных явлений) и могут быть вызваны как техническими, так и физическими средствами. Их последствиями могут стать такие события, как несанкционированные изменения информации, уничтожение информации или другие события, которые делают информацию недоступной, а также нанесение урона активам организации либо их хищение. События, о которых не было сообщено или которые не были опознаны как инциденты, не могут быть изучены, и в их отношении не могут быть применены защитные меры для предотвращения повторного появления этих событий.

Отказ в обслуживании является широкой категорией инцидентов, которые имеют одну общую черту. Такие инциденты приводят к сбоям в системах, сервисах или сетях, которые не могут продолжать работу с прежней производительностью, чаще всего при полном отказе в доступе авторизованным пользователям.

Выделяют два основных типа инцидентов "отказ в обслуживании", создаваемых техническими средствами, это: уничтожение ресурсов и истощение ресурсов.

Некоторыми типичными примерами таких преднамеренных технических инцидентов являются следующие:

- зондирование сетевых широковещательных адресов с целью полного заполнения полос пропускания сети трафиком ответных сообщений;
- передача данных в непредвиденном формате в систему, сервис или сеть в попытке разрушить или нарушить работу;
- одновременное открытие нескольких сеансов с конкретной системой, сервисом или сетью в попытке затормозить ее работу, блокировать либо разрушить ее.

Инциденты, которые создаются нетехническими средствами или которые приводят к потере информации, сервиса и (или) устройств обработки, могут быть вызваны следующими неисправностями и нарушениями, такими, как:

- нарушение систем безопасности, которые приводят к хищениям либо нанесением ущерба;
- неправильное функционирование или перегрузка системы;
- неконтролируемые изменения в системе;
- неправильное функционирование программного либо аппаратного обеспечения.

Категория инцидентов "сбор информации" в общем случае включает действия, которые связаны с определением потенциальных целей атаки и предоставлением данных о сервисах, которые были запущены на идентифицированных целях атаки. Инциденты такого типа предполагают проведение разведки с целью определения следующего:

- существования какой-либо цели получения представления о топологии сети, вокруг нее, и с кем эта цель сообщается;
- потенциальных уязвимостей цели или уязвимости непосредственной сетевой среды, которые можно использовать.

Типичными примерами атак, которые направлены на сбор информации техническими средствами являются следующие:

- сбрасывание записей DNS (системы доменных имен) для целевого домена Интернета (передача зоны DNS);
- отправка тестовых запросов по случайным сетевым адресам с целью найти работающие системы;

- зондирование системы с целью идентификации (например, по контрольной сумме файлов) операционной системы хоста;

- сканирование доступных сетевых портов на протокол передачи файлов системе с целью идентификации соответствующих сервисов и версий программного обеспечения этих сервисов;

- сканирование одного или нескольких сервисов с известными уязвимостями по диапазону сетевых адресов.

Приведенное изучение видов и свойств инцидентов в информационной безопасности позволяет быстрее и эффективнее подбирать и использовать защитные методы борьбы против них в вычислительных сетях.

Список использованных источников

1. Белов Е.Б. Основы информационной безопасности / Е.Б. Белов, В.П. Лось. – М.: Горячая линия – Телеком, 2006. – 544 с.

2. Кевин М. Защита от вторжений. Расследование компьютерных преступлений / М. Кевин, К. Просис. – СПб.: Лори, 2005. – 476 с.

3. Расторгуев С.П. Основы информационной безопасности / С.П. Расторгуев. – М.: Академия, 2007. – 160 с.

4. Милославская Н.Г. Интрасети: обнаружение вторжений / Н.Г. Милославская, А.И. Толстой. – М.: ЮНИТИ-ДАНА, 2001. – 587 с.

5. Хорошко В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков. – Казань: Юниор, 2003. – 504 с.

ОСОБЕННОСТИ ПРИМЕНЕНИЯ ТЕМПОРАЛЬНОЙ ГРАММАТИКИ ПРИ АНАЛИЗЕ ДАННЫХ

Ивченко С.П. - студент, Сучкова Л.И. – д.т.н., профессор
ФГБОУ ВО «Алтайский государственный технический университет им.И.И. Ползунова»
г. Барнаул

На данный момент по причине развития вычислительной мощности компьютеров ежедневно генерируются огромные объемы данных во всевозможных областях науки и техники, причем данные зачастую содержат скрытые закономерности, имеют причинно-следственные связи. Для выявления таких связей ключевым является учет времени появления данных, или их темпоральный аспект [1].

Временные ряды отражают динамику изменения данных, однако поиск в них осмысленной информации сложен. Особый интерес представляет поиск временных шаблонов, но они обычно связаны с конкретной предметной областью и жестко к ней привязаны [2]. Наиболее сложно поиск и описание темпоральных закономерностей реализуется для нескольких временных рядов.

Вышеизложенное послужило основанием для проведения наших исследований, основной целью которых является:

– разработка алгоритмов и программной реализации методики выявления темпоральных закономерностей в группе рядов с помощью грамматики специального вида;

- разработка грамматики, способной в полной мере описать результаты, найденные в процессе анализа временных рядов.

В основе данной работы лежит метод поиска информации в многомерных рядах, называемый универсальной темпоральной грамматикой [3]. Особенностью данного метода анализа данных является разбиение сложной задачи поиска информации на простые подзадачи и простые для понимания уровни временной абстракции.

Символьная иерархия временных шаблонов строится снизу-вверх, из логических

описаний базовых элементов. Далее описаны отдельные уровни данной грамматики.

Уровень примитивов состоит из описания входных данных и описаний нескольких аспектов. Входные данные представляют собой численные временные ряды. К каждому массиву входных данных привязана переменная. Описание аспектов содержит временную размерность, указывающую длительность каждого базового сегмента данных и список описаний примитивных шаблонов.

Примитивные шаблоны, как и все соответствующие им конструкции на прочих уровнях, представляют собой триплеты и состоят из лейбла, аббревиатуры, и списка условий [4]. Аббревиатура должна быть уникальной, как минимум на данном уровне абстракции. Лейбл может быть любым, но желательно осмысленным. Условия содержат базовые переменные и интервалы, указывающие, когда требуется применять данный примитивный шаблон.

Следующий уровень состоит из описаний аспектов и связанных с ними наследственностей. Описания наследственностей состоят из аббревиатуры, лейбла и условий. Условия состоят из аббревиатур и интервалов. Интервалы, указывают минимальную и максимальную длительность последовательности примитивных шаблонов, чтобы они могли считаются наследственностью.

Все последующие уровни содержат только описание соответствующих уровню конструкций. Все они состоят из лейбла, аббревиатуры и условий. Описания объектов на данных уровнях различаются только условием. На каждом последующем уровне в условиях используются объекты из предыдущего уровня. Описание условия на данном уровне событий представляет из себя список наследственностей, которые произошли одновременно.

Описания условий на уровне последовательностей представляют собой список событий, которые могут следовать друг за другом. Условия на уровне временных шаблонов представляют собой список последовательностей, отображающий их возможный порядок следования.

Исходными данными на уровне примитивных шаблонов является матрица чисел, полученная из временных рядов, и описания примитивных шаблонов, сформированные экспертом в соответствующей предметной области.

Данный метод работает не с численными данными, а с семиотическими, то есть символьными, поэтому перед использованием входные данные нужно преобразовать. Для этого эксперт описывает несколько диапазонов значений, и присваивает им некое имя. Это примитивные шаблоны.

Данный метод получает на вход несколько временных рядов в виде матрицы и множество примитивных шаблонов, состоящих из численного диапазона сопоставленного с названием шаблона. Матрица примитивных шаблонов формируется из исходной матрицы заменой чисел на семиотические обозначения соответствующих шаблонов.

После того как исходная матрица с временными рядами была преобразована в матрицу примитивных шаблонов, осуществляется непосредственный анализ данных.

Первым этапом анализа является нахождение наследственностей, отражающих временной концепт длительности. Следующим шагом алгоритма является поиск событий. Событие — это совпадение, или частичное совпадение начала и конца нескольких наследственностей в разных временных рядах. События отражают временной концепт совпадения. Следующим этапом анализа является поиск последовательностей - нескольких событий, идущих друг за другом по времени. Далее производится поиск временных шаблонов. В большинстве случаев многие найденные последовательности будут похожи друг на друга, и могут иметь всего лишь небольшие различия. Подобные последовательности объединяются во временной шаблон. Степень сходства временного шаблона определяется с помощью специального алгоритма основанного на алгоритме Левенштейна [5]. Временной шаблон является объединением нескольких похожих последовательностей и отражает временной концепт вариативности. Все описанные выше шаги анализа временных рядов были реализованы программно. Для написания программы был выбран язык программирования C#. Одной из основных причин выбора данного языка является

встроенный в него язык запросов LINQ [6], который широко использовался при написании программы.

Для лингвистического описания найденных темпоральных закономерностей была разработана специализированная грамматика. Для парсинга был создан лексический анализатор [7], реализованы средства синтаксического [8] и семантического анализа [9].

Разработанное программное обеспечение предназначено для анализа данных с помощью темпоральной грамматики. Скриншот главного окна представлен на рисунке 1.

Вывод результатов анализа производится через текстовое поле занимающее большую часть главного окна. В нижней части окна расположена строка состояния, информирующая пользователя о текущем выполняемом действии, и успешности результатов анализа данных. Все результаты анализа выводятся в текстовое поле в главном окне программы, при желании их можно отредактировать, удалив не интересующие пользователя данные.

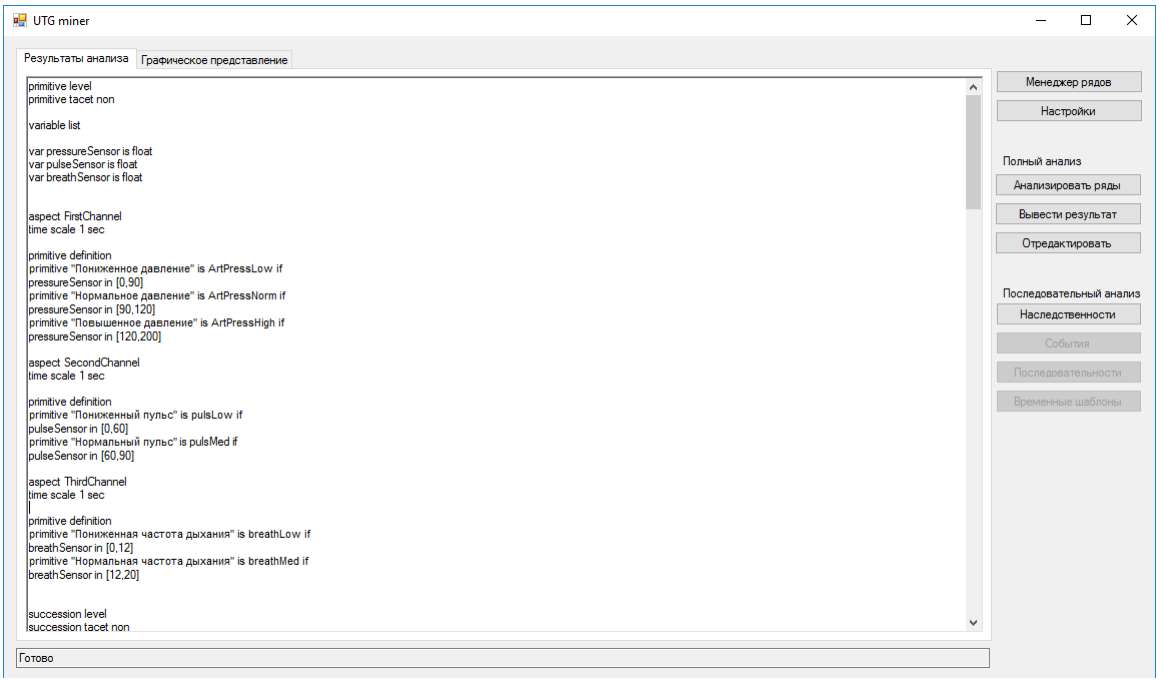


Рисунок 1 - Пользовательский интерфейс

По результатам работы можно сделать следующие выводы. Разработан ряд алгоритмов, реализующих все этапы поиска закономерностей в данных на основе темпоральной грамматики, включая предварительную обработку исходных данных. Для представления результатов работы алгоритмов была разработана специализированная грамматика, позволяющая сформировать итог поиска в виде понятного для человека текста. На основе разработанных алгоритмов создано программное обеспечение, предназначенное для анализа групп временных рядов.

Список использованных источников

1. Mörchen F. Unsupervised pattern mining from symbolic temporal data [Электронныйресурс] / F. Mörchen. Режимдоступа: http://www.mybytes.de/papers/moerchen07unsupervised.pdf

2. Дюк В. DataMining. Учебный курс [Текст] / В. Дюк, А. Самойленко. – СПб.: Питер, 2001. - 368.: ил. + 1 эл.опт. диск (CD ROM)

3. Mörchen F. Mining hierarchical temporal patterns in multivariate time series [Электронныйресурс] / F. Mörchen, A. Ultsch. Режим доступа: http://www.uni-marburg.de/fb12/datenbionik/pdf/pubs/2004/moerchen04mining

4. Mörchen F. Efficient mining of understandable patterns from multivariate interval time series [Электронныйресурс] / F. Mörchen, A. Ultsch. Режим доступа: http://www.mybytes.de/papers/moerchen07efficient.pdf

5. Карахтанов Д.С. Программная реализация алгоритма Левенштейна для устранения

опечаток в записях баз данных [Текст] / Д.С. Карахтанов // Молодой ученый. — 2010. — №8. — С. 158-162.

6. Фримен А. LINQ. Язык интегрированных запросов в C# 2010 для профессионалов [Текст] / А. Фримен, Д. Раттц. — М.: Вильямс, 2011. — 656 с.

7. Карпов Ю.Г. Теория автоматов [Текст] / Ю.Г. Карпов. - СПб.: БХВ-Петербург, 2003. - 208 с.

8. Малявко А.А. Формальные языки и компиляторы: учебник НГТУ [Текст] / А.А. Малявко. - Новосибирск: Изд-во НГТУ, 2013. - 431 с.

9. Вылиток А.А. Металингвистические формулы и синтаксические диаграммы [Текст] А.А. Вылиток. - М.: МАКСПресс, 2012. - 24 с.

РАЗРАБОТКА ВЕБ-САЙТА ДЛЯ ТРАНСПОРТНОЙ КОМПАНИИ «РОСТЕХНО»

Исаев В.В. - студент, Гребеньков А.А. – к.ф.-м.н., доцент
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

На сегодняшний день грузоперевозки – огромная инфраструктура, обладающая своими особенностями, специфическими характеристиками, подчиняющаяся своим правилам и законам. От грамотности специалистов транспортной компании и правильной оптимизации и организации процесса транспортировки груза будет зависеть его сохранность, соблюдение сроков доставки (особенно важный момент для продуктов и др. скоропортящихся товаров). В последние десятилетия стали особенно активно развиваться компании, которые предоставляют клиентам различные способы доставки грузов. В сфере грузоперевозок важна каждая мелочь, так как от этого зависит целостность вашего груза и своевременность доставки, так как бывает необходимо доставить скоропортящаяся продукты. В нашей стране, к сожалению, не стоит забывать о плохом качестве дорог и наличие пробок, поэтому необходим специалист, который подскажет наиболее оптимальный маршрут до точки назначения. Именно поэтому в данном деле очень важна логистика - наука, предмет которой заключается в организации рационального процесса движения товаров и услуг от поставщиков сырья к потребителям, функционирования сферы обращения продукции, товаров, услуг, управления товарными запасами и провиантом, создания инфраструктуры товародвижения. Также некоторые транспортные компании предлагают своим клиентам страхование грузов, таможенное сопровождение и др.

Сегодня существует множество различных транспортных компаний, так как выяснилось, это весьма доходный бизнес. Но не у всех предприятий есть свой сайт, который отвечал бы поставленным требованиям и предоставлял бы клиентам всю необходимую информацию. Для одной из таких компаний и разрабатывается веб-сайт.

Веб-ресурс должен предоставлять следующие возможности:

- Возможность регистрации новых клиентов;
- Возможность входа/выхода под своим логином и паролем;
- Хранение данных о клиентах ресурса;
- Возможность просмотра информации о предоставляемых услугах и ценах на них;
- Предоставление данных об автопарке транспортной компании;
- Возможность узнать последние новости из мира грузоперевозок;
- Разграничение прав пользователей;
- Предоставление конфиденциальной информации только для сотрудников транспортной компании;
- Предоставление данных о графике работы транспортной компании;
- Предоставление данных о способах связи с транспортной компанией;
- Адаптация для мобильных устройств;
- Возможность пользователям самостоятельно сделать заявку на грузоперевозку

Особенности разработки:

- Удобное представление информации;
- Не требуется установка сторонних скриптов, все действия выполняются на сервере;
- Новый пользователь может сам зарегистрироваться на сайте без вмешательств администратора;
- Возможность редактировать данные в исходной БД предоставлено только администратору.

В ходе разработки сайта было использовано следующее ПО:

- MySQL 5.5
- phpMyAdmin 4.5.2
- Apache 2.4
- PHP 5.6
- JavaScript
- Notepad ++

На рисунке 1 приведена структура разрабатываемого ресурса.

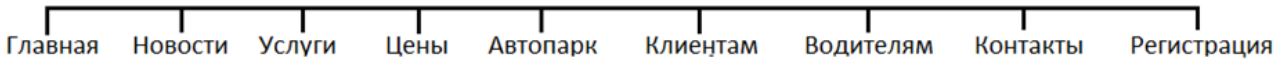


Рисунок 1 – Структура веб-сайта

При разработке сайта используются не сильно тусклые, но и не сильно яркие цвета, цвет и размер текста подобраны так, что он не сливается с фоном и не выглядит слишком мелким. Пользователь, зайдя на главную страницу сайта, может быстро перейти в необходимый для него раздел для получения более подробной информации. Навигационное меню приведено на рисунке 2.

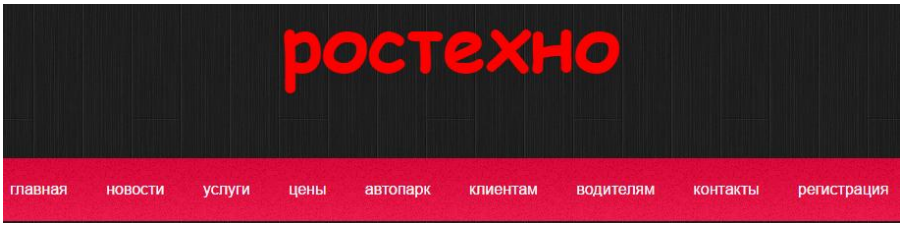


Рисунок 2 –Навигационное меню

Для разрабатываемого веб-сайта была создана база данных, в которую включены две таблицы: в одной таблице хранятся данные о зарегистрированных пользователях, а во второй таблице хранятся данные о заявках на грузоперевозку. Структура представлена на рисунке 3.

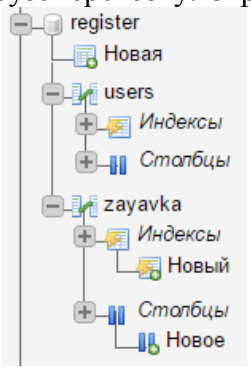


Рисунок 3 – Структура БД

В заключении следует отметить, что в результате проделанной работы, создан ресурс, который позволяет клиентам быстро и подробно узнать обо всех возможностях транспортной компании «Ростехно», узнать о порядке заключения договора на сотрудничество с данным предприятием и получить всю сопутствующую перевозке товара информацию.

Список использованных источников

1. Логистика [Электронный ресурс] - Режим доступа: https://ru.wikipedia.org/wiki/%D0%9B%D0%BE%D0%B3%D0%B8%D1%81%D1%82%D0%B8%D0%BA%D0%B0 –Загл. с экрана.
2. Немцова Т.И., Назарова Ю.В. Компьютерная графика и web-дизайн. Практикум: учебное пособие / под ред. Л. Г. Гагариной. — М.: ИД «ФОРУМ»: ИНФРА-Ь, 2010. — 228 с.: ил. — (Профессиональное образование).
3. Дунаев, В. Базы данных. Язык SQL для студента / В. Дунаев. - М.: БХВ-Петербург,2012.-320с.
4. Дунаев,В.В. HTML, скрипты и стили /В.В. Дунаев. -М.: СПб:БХВ, 2006. – 832 с
5. Кирсанов Веб-дизайн: Книга Дмитрия Кирсанова / Кирсанов, Дмитрий. - М.: СПб:Символ-Плюс,2004.-376с.
6. Петюшкин, А. HTML экспресс-курс / А. Петюшкин. - М.: СПб: БХВ-Петербург, 2004. - 250 с.
7. Кузнецов PHP. Практика создания Web-сайтов / Кузнецов, М.В. и. - М.: БХВ-Петербург, 2008. - 712 с.
8. Герберт, ШилдтJavaScriptv5.0 (Tiger). Новые возможности; СПб: БХВ-Петербург - Москва, 2005. - 208 с.
9. СтеймецPHP. 75 готовых решений для вашего сайта +CD / Стеймец, Ульям. - М.: СПб: Наука и Техника, 2009. - 256 с.
10. Транспортные компании. Зачем нужны? [Электронный ресурс] - Режим доступа: http://nk-trans.spb.ru/info/3-tramsportnaya-kompaniya–Загл. с экрана.
11. Транспортная компания груз-логистика [Электронный ресурс] - Режим доступа: http://gruz-logistika.ru/–Загл. с экрана.
12. Транспортная компания Пэк [Электронный ресурс] - Режим доступа: http://pecom.ru/–Загл. с экрана.
13. Кит - транспортная компания [Электронный ресурс] - Режим доступа: http://tk-kit.ru/–Загл. с экрана.

АНАЛИЗ ЭФФЕКТИВНОСТИ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЙ ДВУМЕРНЫХ ВХОДНЫХ СИГНАЛОВ В ЗАДАЧАХ РАСПОЗНАВАНИЯ ГРАФИЧЕСКИХ ОБЪЕКТОВ

Краснослободцев Р.А. – студент, Тушев А.А. – к.т.н., доцент
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

В последние десятилетия теория и методы цифровой фильтрации двумерных сигналов получили большое развитие и распространение. Это обусловлено как появлением новых математических методов, таких как перекрёстный оператор Робертса, оператор Собеля, детектор границ Кэнни, позволяющих создать эффективные алгоритмы фильтрации, так и возросшими требованиями к фильтрации, особенно в случае обработки изображений. При этом фильтрация в большинстве случаев является не конечным этапом обработки, а некоторой предобработкой, например, для последующего распознавания образов.

Как показывает практика, в реальных задачах в качестве фильтруемого сигнала выступает достаточно большой объем данных. В свою очередь, большинство методов цифровой фильтрации требуют больших вычислительных мощностей, что является причиной чрезмерно длительного преобразования. Очевидно, что в системах с критичным временем отклика, данные алгоритмы либо не применимы в принципе, либо подлежат тщательной оптимизации в зависимости от решаемой задачи.

Рассмотрим нейронную сеть обратного распространения ошибки, способную решать задачу распознавания лиц на фотографиях. Очевидно, что предварительная фильтрация входного сигнала методами выделения границ на фотографиях улучшит результат распознавания вследствие непосредственного упрощения сигнала [2]. Однако, подобная

обработка требует соответствующего времени для вычислений и актуальна лишь при наличии требований высокой точности классификации.

В данной работе, в качестве предварительной фильтрации предлагается использовать дискретное вейвлет-преобразование, которое, как предполагается, должно существенно ускорить время обработки, при этом ненамного ухудшить итоговую ошибку распознавания в сравнении с методами выделения границ.

В качестве обрабатываемых данных выступает база лиц The ORL DatabaseofFaces [3], часто используемая для тестирования алгоритмов распознавания (рисунок 1).

Кратко рассмотрим исходный алгоритм фильтрации. Вейвлет-преобразование – операция математической свертки «вейвлет-функции» с обрабатываемым сигналом. В данной работе в качестве вейвлет-функции используется вейвлет Хаара, в виду относительной простоты реализации (2).

Рисунок 1 – Пример входных данных для преобразования

$$\psi(x) = \begin{cases} 1, & 0 \le x \le 1/2 \\ -1, & 1/2 \le x \le 1 \\ 0, & x < 0, x \ge 1 \end{cases} \qquad (2).$$

Пусть имеется одномерный дискретный входной сигнал *S*. Каждой паре соседних элементов ставятся в соответствие два числа: $a_i = \frac{S_{2i} + S_{2i+1}}{2}$ и $b_i = \frac{S_{2i} - S_{2i+1}}{2}$. Повторяя данную операцию для каждого элемента исходного сигнала, на выходе получают два сигнала, один из которых является «огрубленной» версией входного сигнала — a_i, а второй содержит детализирующую информацию, необходимую для восстановления исходного сигнала.

Любое изображение можно интерпретировать как функцию двух переменных *f(x, y)*, которая в нашем случае является матрицей значений яркости пикселей обрабатываемой фотографии. Алгоритм вейвлет-преобразования двумерной функции аналогичен одномерному случаю:

1. Применим одномерное преобразования Хаара к каждой строке матрицы и получим две новые матрицы, строки которых содержат аппроксимированную и детализирующую часть строк исходной матрицы.

2. К каждому столбцу полученных матриц применим одномерное преобразование Хаара и на выходе получим четыре матрицы, одна из которых является аппроксимирующей составляющей исходного сигнала, а три оставшиеся содержат детализирующую информацию — вертикальную, горизонтальную и диагональную.

После применения двумерного вейвлет-преобразования Хаара к исходной выборке лиц, имеем результат, представленный на рисунке 2.

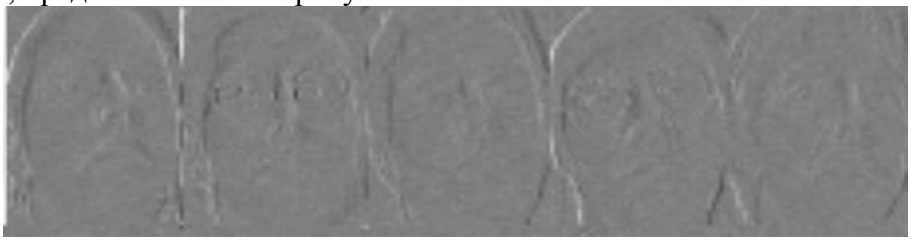


Рисунок 2 – Визуальное представление результата двумерного вейвлет-преобразования

В виду малого количества выполняемых операций, на физической машине алгоритм работает гораздо быстрее операторов выделения границ. Произведем обучение нейронной сети на обработанной выборке. На рисунке 3 представлен график обучения сети. По оси абсцисс отложено количество эпох обучения, по оси ординат ошибка распознавания.

Обучение прошло успешно, суммарная ошибка постепенно убывала и в итоге составила *0.035*. На основе полученных данных можем сделать вывод об актуальности применения двумерного вейвлет-преобразования для нейронной сети распознавания графических объектов.

Такая обработка не требует больших вычислительных мощностей, вместе с тем, путём упрощения исходного сигнала, уменьшается количество ошибочных активаций нейронов, точность классификации увеличивается.

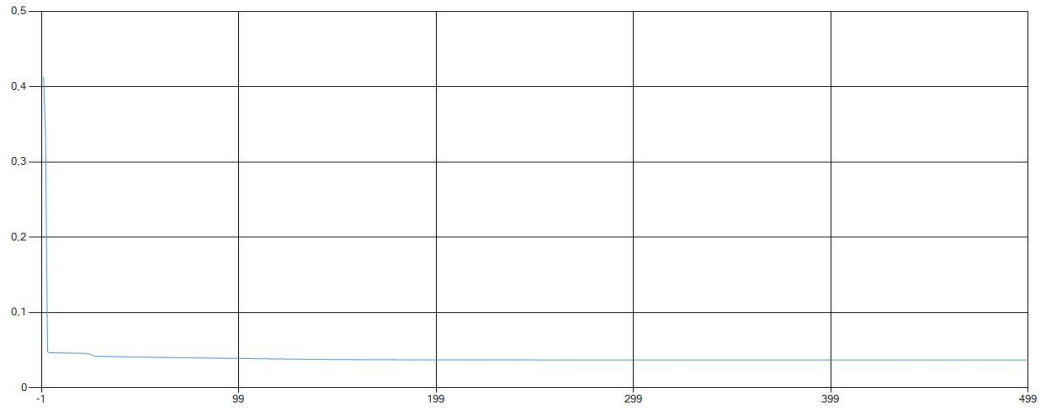


Рисунок 3 – График обучения сети после применения дискретного вейвлет-преобразования Хаара

Библиографический список.

1. Ю.Е. Воскобойников. Вейвлет-фильтрация сигналов и изображений (с примерами в пакете MathCAD) [Электронный ресурс], - Режим доступа: http://www.sibstrin.ru/files/kis/Воскобойников_Вейвлет_Монография_2015_часть_1.pdf

2. Краснослабодцев Р.А., Тушев А.Н. Исследование эффективности предварительной фильтрации двумерных входных сигналов искусственной нейронной сети для распознавания графических объектов. // Ползуновский альманах №2, - г. Барнаул. - 2016г. – с.38-42

3. Archive Cambridge University Computer Laboratory. [Электронный ресурс], - Режим доступа: http://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html

4. Малла, С. Вейвлеты в обработке сигналов. / С. Малла. – -М.: Мир, 2003.

5. Гонсалес Р., Вудс Р. Цифровая обработка изображений. М., Техносфера, 2005 г., 1070 с.

ТЕМПОРАЛЬНАЯ МОДЕЛЬ ГРУППЫ ГЕОМЕТРИЧЕСКИХ ПАТТЕРНОВ ДЛЯ ДАННЫХ МОНИТОРИНГА

Колдин И.Ю. - студент, Сучкова Л.И. - д.т.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова(г. Барнаул)

В природе существует множество циклических процессов, параметры которых постоянно измеряются и регистрируются датчиками. Многие организации и службы собирают данные о таких процессах с целью контроля и управления сложными объектами, системами. В таких системах, огромные объемы данных быстро прибывают и их значения изменяются с течением времени.

В настоящее время актуально развитие методов обработки и анализа измерительной

информации, отражающей нестационарное поведение сложных динамических объектов, причем данным, описывающим функционирование таких объектов, зачастую свойственна большая размерность в силу возможности одновременной регистрации нескольких сигналов различной природы [1-5].

Основной проблемой при обработке данных измерений является большой объем исследуемых выборок. Поэтому актуальной задачей является сжатие данных измерений без потери заключенной в ней важной информации. Решение задачи осуществляется путем выявления в них закономерностей и выделения повторяющейся части – периода. Для этого можно использовать такой формальный метод описания, как геометрические паттерны. Они представляют собой некоторый повторяющийся шаблон или образец. Геометрическому паттерну визуально соответствует кривая зависимости измеряемых данных от времени. Этой зависимости, с алгебраической точки зрения, соответствует функция, имеющая тип и набор коэффициентов. Пример геометрического паттерна приведен на рисунке 1.

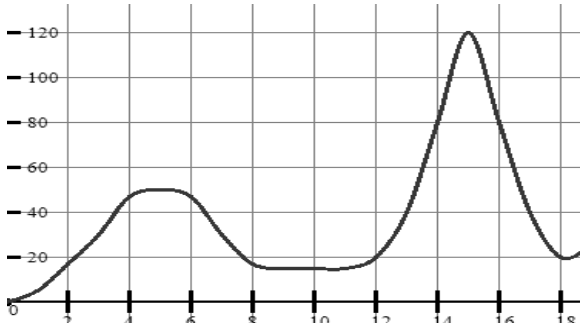


Рисунок 1 –Геометрический паттерн

Представляют интерес геометрические паттерны, описывающие периодические данные. Периодические данные повторяются на промежутках времени – периодах, причем допускается вариабельность данных внутри периода и вариабельность границ периода для различных временных интервалов [6-10].

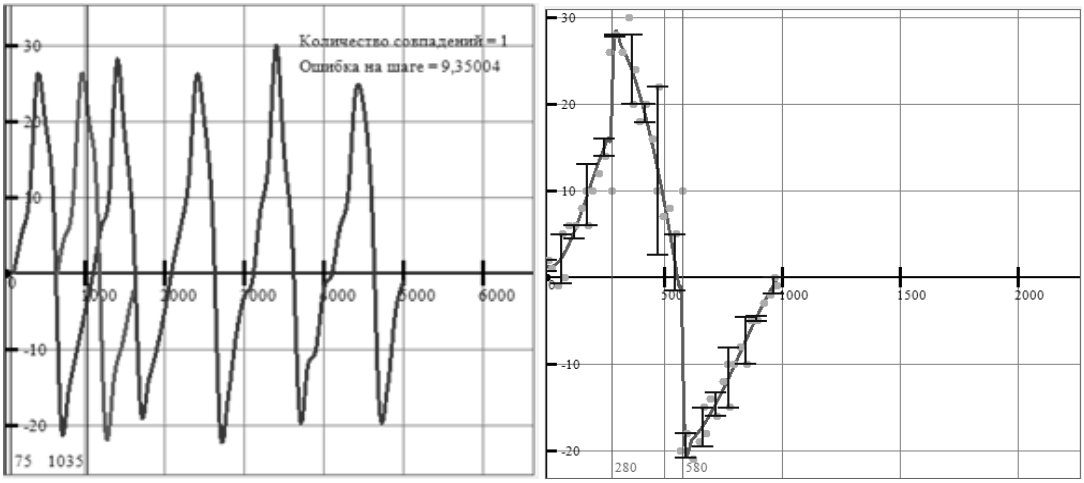
Основными этапами при анализе данных измерений с применением геометрических паттернов являются:

1. Сбор данных за некоторый промежуток времени.
2. Выявление закономерностей в данных и выделение периодов.
3. Построение геометрического паттерна.

Опишем каждый этап подробнее.

Сбор данных осуществляется на основе сигналов, регистрируемых установленными на объекте автономными датчиками. Требования к хранению информации основаны на обеспечении достоверности вычислений при одновременном компактном хранении данных. Важным является уменьшение времени обработки большой по объему базы данных, так как предполагается, что программа будет работать в режиме реального времени.

На основе анализа данных для выделенных периодов строится геометрический паттерн, представляющий собой усредненный шаблон для любого из периодов. Он способен охарактеризовать цикличность сигнала. При его формировании используются такие способы, как аппроксимация методом наименьших квадратов и интерполяция кубическим сплайном. Пример сформированного геометрического паттерна на основе тестовых данных приведен на рисунке 2.



а) б)

Рисунок 2 – Пример сформированного геометрического паттерна на основе тестовых данных. а) – тестовые данные, б) – геометрический паттерн.

При выявлении закономерностей в данных измерений необходимо их описать с помощью функциональных зависимостей от времени, а затем выделить периоды, на которых применим шаблон выбранного вида. Для этого можно использовать подход PatternGrowthGraph (PGG)[11]. В потоковой обработке изменения обнаруживаются путем сравнения старых данных с поступающим потоком с помощью сопоставления последовательностей. Для эффективного представления потока бесконечный поток разделяется на сегменты и формируется волновой шаблон для получения значимой информации об изменениях данных. С помощью алгоритма «SlidingWindowAndBottom-up» строится волновой шаблон, который затем принимает и обрабатывает PGG для получения информации об изменениях данных и их компактификации. Затем каждый новый шаблон сравнивается с ранее сформированными, и изменения сохраняются в двунаправленный связанный список, который включает информацию о частоте и времени каждого появления шаблона. Таким образом, можно хранить и отслеживать историю изменений потока данных за один проход. С помощью PGG также можно обеспечить такие функции, как восстановление потока и обнаружение аномальных ситуаций. Кроме того, статистическая информация PGG помогает системе отличать значащие изменения данных измерений от шума. Данный метод тестировался на реальных наборах данных, и полученные результаты продемонстрировали его эффективность и целесообразность использования.

В итоге комплексное использование PGG и геометрических шаблонов формирует темпоральную модель группы геометрических паттернов, которая способна охарактеризовать особенности измерений за определенный промежуток времени при одновременном обеспечении компактного хранения информации. Это позволяет увеличить эффективность обработки и анализа измерительной информации.

Список использованных источников

1. Клионский Д.М. Методы выявления аномальных событий в многокомпонентных измерительных сигналах на основе мультимасштабных и спектральных методов высокого разрешения. [Текст]: Автореф. дис. канд. техн. наук. — Санкт-Петербург: СПГЭУ «ЛЭТИ» им. В.И. Ульянова (Ленина), 2012. — 18 с.

2. Марчук В.И., Токарева С.В. Способы обнаружения аномальных значений при анализе нестационарных случайных процессов// Монография. ГОУ ВПО «Южно-российский государственный университет экономики и сервиса», 2009. – 60 с.

3. Марчук В.И., Уланов А.П. Методы обнаружения и отбраковки аномальных результатов измерений// Изв. вузов. Сев.-Кавк. регион. Техн. науки. 2001. №2. –С.7–8.

4. Орешко Н.И., Геппенер В.В., Клионский Д.М. Применение гармонических вейвлетов в задачах обработки осциллирующих сигналов // Цифровая Обработка Сигналов, № 2, 2012,

С. 6-14.

5. Сучкова Л.И. Подход к прогнозированию нештатных ситуаций в системах мониторинга с использованием паттернов поведения группы временных рядов / Л.И. Сучкова // Ползуновский вестник. – 2013. – №2. Режим доступа: http://elib.altstu.ru/elib/books/Files/pv2013_02/pdf/088 suchkova.pdf.

6. Minos N. Garofalakis, Rajeev Rastogi, Kyuseok Shim. Data Mining and the Web: Past, Present and Future / VLDB '94 Proceedings of the 20th International Conference on Very Large Data Bases. – 1994. – С. 487-499.

7. Rakesh Agrawal, RamakrishnanSrikant Fast Algorithms for Mining Association Rules /WIDM '99 Proceedings of the 2nd international workshop on Web information and data management. – 1999. – С. 43-47.

8. Sheng Ma and Joseph L. Hellerstein. «Mining Partially Periodic Event Patterns With Unknown Periods»// International Conference on Data Engineering. 2000.

9. Faraz Rasheed, Mohammed Alshalalfa, and RedaAlhajj, Associate Member, IEEE. «Efficient Periodicity Mining in Time Series Databases Using Suffix Trees»// IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 23, NO. 1, JANUARY 2011.

10. Johannes Assfalg, Thomas Bernecker, Hans-Peter Kriegel, Peer Kroger, Matthias Renz. «Periodic Pattern Analysis in Time Series Databases»// 14th International Conference, DASFAA’09, Brisbane, Australia, pp. 354-368, 2009.

11. L Tang, B Cui, H Li, G Miao, D Yang, X Zhou «Effective variation management for pseudo periodical streams» // Proceedings of the 2007 ACM SIGMOD international conference on Management of data, Brisbane, Australia, pp. 257-268, 2007.

ОПРЕДЕЛЕНИЕ УСЛОВИЙ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ, СОЗДАВАЕМОГО НА ОСНОВЕ АВТОМАТИЗИРОВАННЫХ И ИНФОРМАЦИОННЫХ СИСТЕМ

Кудрявцев В.А. - студент, Загинайлов Ю.Н. - к.в.н., доцент
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Государственный стандарт России по проектированию автоматизированных систем в защищённом исполнении (АСЗИ) [1], АСЗИ, относящихся к одному из типов объектов информатизации (ОИ), в качестве одного из требований к проектированию, включает требование того (п.5.3, абз.3), что «…система защиты информации АСЗИ должна создаваться с учетом обеспечения возможности формирования различных вариантов ее построения, а также расширения возможностей ее составных частей (сегментов) в зависимости от условий функционирования АСЗИ…». Это выполняется на стадии «Формирование требований кАС» (п.6.1) и этапе этой стадии «Обследование объекта и обоснование необходимости создания АС» (п.6.1.1. абз.1). Состав таких условий рассматривался в целом для объекта информатизации в работах [2, 3], однако в них не учтены специфические особенности таких АСЗИ, которые предусмотрены требованиями ФСТЭК России к государственным информационным системам (ГоИС) [4] и информационным системам персональных данных (ИСПДн) [5], автоматизированным системам управления технологическими и производственными процессами, что делает актуальным этот вопрос в контексте современной теории и практики комплексного обеспечения защиты информации объекта информатизации. В настоящей работе рассмотрены условия для всех объектов информатизации и определены условия функционирования систем защиты информации для объектов информатизации типа ГоИС и ИСПДн.

Анализ стандарта [1], , учебно-научных трудов [2,3], требований ФСТЭК России[4-6], позволил систематизировать условия функционирования различных информационных систем, как ОИ. Все условия разделены на три группы (рисунок 1):

1) Условия, определяющие особенности защиты информации ограниченного доступа;

2) Условия, оказывающие влияние на построение системы защиты;

3) Условия, определяющие особенности конкретного типа автоматизированной (информационной) системы.

Условия, определяющие особенности защиты информации ограниченного доступа, характерные для любых объектов информатизации, будут включать:

1) форма собственности;
2) организационно-правовая форма предприятия;
3) характер основной деятельности предприятия;
4) состав, объекты и степень конфиденциальности защищаемой информации.

Условия, оказывающие влияние на построение системы защиты, характерные для любых объектов информатизации, будут включать:

1) структура и территориальное расположение предприятия;

2) режим функционирования предприятия;

3) конструктивные особенности предприятия;

4) количественные и качественные показатели ресурсообеспечения;

5) степень автоматизации основных процедур обработки защищаемой информации.

6) количество и технологические особенности технических средств обработки, хранения, передачи информации (средств автоматизации, связи и т.п);

7) количество и уровень подготовки персонала связанного с использованием, обработкой, хранением, передачей информации вообще и ценной (конфиденциальной) в частности;

8) угрозы безопасности всем видам защищаемой информации, информационным ресурсам, системам и средствам их обработки, передачи, хранения расположенным в помещении где расположена АС.

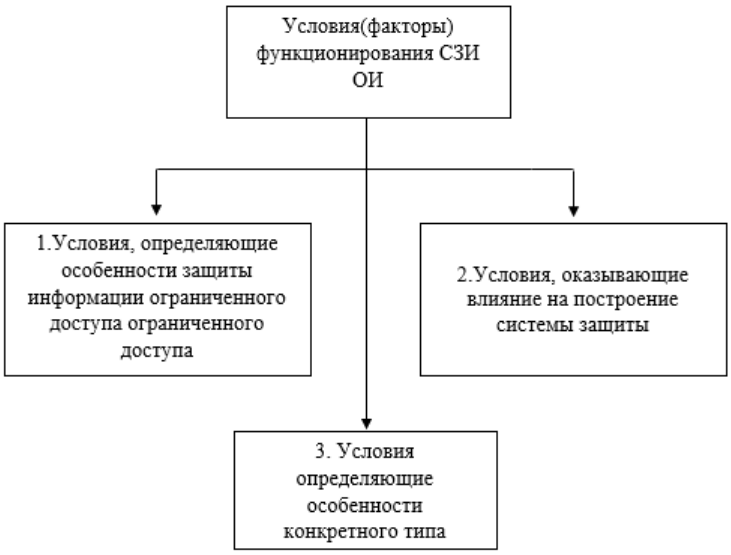


Рисунок 1- Условия функционирования системы защиты информации ОИ

Специфические условия функционирования СЗИ ИСПДн, С учётом анализа требований по организации защиты персональных данных [5], к специфическим особенностям функционирования СЗИ ИСПДн следует отнести:

1) Вид персональных данных (специальные, биометрические, общедоступные, иные);

2) Типы актуальных угроз;

3) Объём и количество субъектов персональных данных, не являющихся сотрудниками оператора (менее 100000 субъектов персональных данных, более 100000 субъектов персональных данных

Специфические условия функционирования СЗИ ГоИС, С учётом анализа требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах по организации защиты [6], к специфическим условиям функционирования СЗИ ГоИС следует отнести:

1) значимость обрабатываемой в ней информации;

2) масштаб информационной системы;

3) структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы.

4) физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, с иными информационными системами и информационно-телекоммуникационными сетями.

5) режимы обработки информации в информационной системе и в ее отдельных сегментах.

6) иные характеристики информационной системы, применяемые информационные технологии и особенности ее функционирования.

Уровень значимости информации определяется степенью возможного ущерба для обладателя информации (заказчика) и (или) оператора от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации. Для определения степени возможного ущерба от нарушения конфиденциальности, целостности или доступности могут применяться национальные стандарты и (или) методические документы, разработанные и утвержденные ФСТЭК России.

Рисунок 2 – Специфические условия функционирования ГоИС и ИСПДн

Полученные в результате исследования материалы планируется использовать в учебной и учебно-методической литературе для учебных дисциплин образовательной программы подготовки бакалавров по направлению «Информационная безопасность» в АлтГТУ.

Список использованных источников

1.ГОСТ Р 51583-2014.Защита информации. Порядок создания автоматизированных

систем в защищенном исполнении. Общие положения.

2. . Комплексная система защиты информации на предприятии: учеб.пособие для студ. высш. учеб. заведений / В. Г. Грибунин, В.В.Чудовский. — М.: Издательский центр «Академия», 2009. — 416 с.

3. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557

4.Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утвержденны приказом ФСТЭК России от 11 февраля 2013 г. N 17 [Электронный ресурс]. - URL: http://fstec.ru/normotvorcheskaya/akty/53-prikazy

5.Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Приказ N 21 ФСТЭК России от 18 февраля 2013 г. [Электронный ресурс]. - URL: http://fstec.ru/normotvorcheskaya/akty/53-prikazy;

6.Требованиями к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, Приказ N 31 ФСТЭК России от 14 марта 2014 г. [Электронный ресурс]. - URL: http://fstec.ru/normotvorcheskaya/akty/53-prikazy.

АНАЛИТИЧЕСКИЙ ОБЗОР СУЩЕСТВУЮЩИХ ФОТОСЕПАРАТОРОВ

Кузнецов С.А. – магистрант, Якунин А.Г. – д.т.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Современному фермеру, сельскохозяйственному предприятию или заводу по переработке пластмасс с их различными нуждами по сортировке всевозможных материалов, будь то посадочные семена, сушеные пищевые продукты или же пластмасса не обойтись без современного фотосепаратора для достижения наилучших результатов сортировки.происхождения. Фотосепаратор является электронным оборудованием для сортировки сыпучих материалов, особенно зерна и семян, по цвету, структуре, размеру, форме. В основном применяется для очистки исходного продукта от примесей.

Общий принцип работы фотосепаратора приведен ниже на рисунке 1.

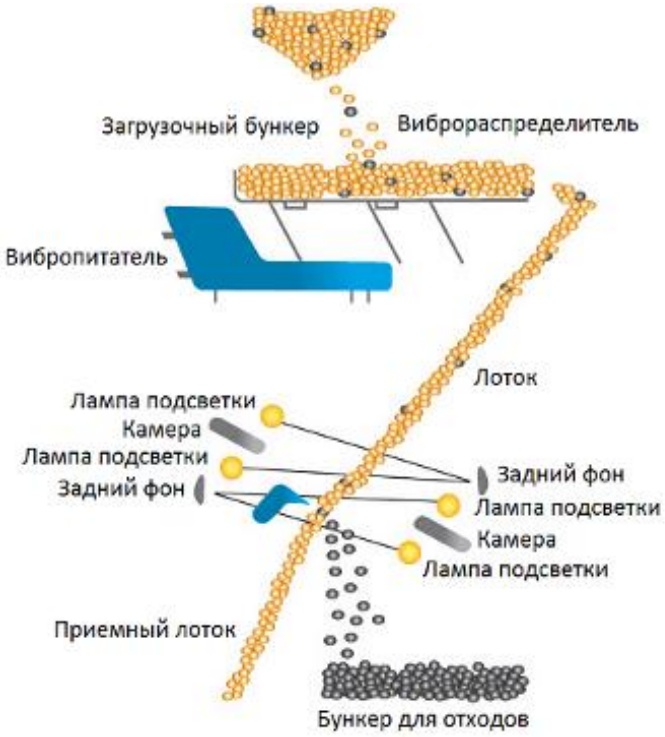


Рисунок 1 - Схема работы фотосепаратора

Из загрузочного бункера продукт (например, зерно) поступает на виброраспределитель, где равномерно распределяется по всей его площади. Затем очищаемый продукт поступает на подающий лоток – своего рода доска из специального сплава, разрешенного к применению в пищевой промышленности, с направляющими канавками определенной глубины и ширины для каждого продукта, с антифрикционным износостойким покрытием, исключающим «кувыркание» продукта. Последнее может затруднить идентификацию полезного продукта или примеси. Составляющие продукта должны без кувырканий с большой скоростью двигаться одно за другим по канавке лотка фотосепаратора. Когда продукт попадает в зону осветителя, собственно и начинается процесс сортировки продукта. Согласно заданным настройкам, зерно определяется фотосепаратором как годное или уходит в отход.

Фотоэлектронный сепаратор делится на виды по следующим принципам [1]:

1) по оптической схеме и источнику излучения;
2) по типу видеорегистратора или анализатора сигнала;
3) по механической схеме;
4) по очищаемому или сортируемому материалу;
5) по производительности.

По оптической схеме и источнику излучения различают фотосепараторы:

1) полихроматический – на основе белого света (присутствуют практически все длины волн видимого спектра), излучаемого люминесцентной или галогенной лампы;
2) монохроматический – на основе лазера: чаще всего полупроводникового и иногда - гелий неонового;
3) бихроматический – на основе двух лазерных светодиодов, обычно красного и синего спектра;
4) инфракрасный – на основе монохроматического или полихроматического источника излучения с длинами волн в диапазонах инфракрасного света – от 0.7 до 2 мкм;
5) ультрафиолетовый – на основе источника ультрафиолетового излучения;
6) рентгеновский – на основе рентгеновской трубки. Такие фотосепараторы применяются тогда, когда требуется сортировать частицы в зависимости от внутренней структуры сортируемого материала.

По типу фотоприемникафотосепараторы бывают следующих модификаций:

1) на фотоэлектронном умножителе (ФЭУ) – применяются при необходимости точной регистрации слабого сигнала) или телевизионной передающей трубки;

2) на основе полихромных фотоэлементов;

3) на основе фотодиодов, соответствующих по максимальной спектральной чувствительности оптимальной зоне спектрограммы кондиционного материала или примеси;

4) на основе фотодиодной линейки;

5) на основе двумерной фотодиодной или ПЗС – матрицы [2];

6) на основе инфракрасной или другой видеокамеры.

В настоящее время в мире основными являются два вида фотосепараторов: на сенсорах и ПЗС – матрицах. Сенсор — это, по сути кремниевая пластинка, способная накапливать заряды. Фотосепараторы на основе сенсоров используют в качестве анализатора светового потока. При этом анализ зерновки происходит по всей площади (общим пятном) зерновки. ЫВ фотосепартарох на основе ПЗС или фотодиодных матриц используется интеллектуальная обработка изображений, в том числе – использованием нейросетевых технологий [3].

Современные сепараторы отличаются также по механической схеме. Самыми распространенными на данный момент по принципу перемещения отсортированного материала являются пневматические.

В большинстве своем требования к системе анализа, материалам покрытия канавки лотка и ряд других конструктивных и технологических особенностей фотосепаратора определяет сортируемый (очищаемый) материал. Так, сортировка продуктов содержащих камешки, стекло и примеси, одинаковые по цвету с годным продуктом, возможна при наличии камеры, работающей в ИК [4]. Для замороженных продуктов нужно переоборудовать фотосепаратор так, чтобы он мог стабильно функционировать при низких температурах - от 0°С. А также он должен быть выпущен в "открытом" исполнении - для удобства очистки от остатков сортировки. Поэтому производители выпускают не только "универсальные" фотосепараторы, но и специализированные, направленные для сортировки какого либо конкретного продукта - чай, рис, орехи, пластиковые отходы, замороженные продукты.

В то же время, как уже отмечалось ранее, общая схема функционирования для большинства изделий отличается незначительно, и поэтому для перехода на сортировку нового вида зернопродукта бывает достаточно просто модифицировать программное обеспечение фотосепаратора. Поэтому большинство исследований в области сортировки с применением фотосепараторов ведется именно в этом направлении [3]. Так, например, для Алтайского края весьма актуальна задача сортировки семян подсолнечника. В целом такая задача уже решена [3] и, тем не менее, и на сегодняшний день для черной семечки еще сохраняется проблема отделение от нее склероциев – вредной примеси грибкового происхождения. Проведенные исследования показали, что для ее решения можно использовать простейшие алгоритмы, основанные на сопоставлении геометрических размеров семечки и склероции в двух ортогональных направлениях.

Список использованных источников

1. Фотосепараторы – технические характеристики [Электронный ресурс] // Режим доступа: http://promplace.ru/fotoseparator-rabochie-harakteristiki-i-ekspluatatciya-551.htm.

2. Бузанова Л.К., Глиберман А.Я. Фотоприемники - М., 1976.

3. Фотосепаратор [Электронный ресурс] // Режим доступа: https://ru.wikipedia.org/wiki/Фотосепаратор

4. Основы оптики. - С.А. Родионов - М.: Санкт-Петербургский государственный институт точной механики и оптики (технический университет), 2000.

МЕТОДЫ И СРЕДСТВА ИЗМЕРЕНИЯ СКОРОСТИ ВЕТРА

Кузнецов С.А. – магистрант, Якунин А.Г. – д.т.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

В настоящее время проблема определения направления и измерения скорости воздушных масс актуальна во многих областях: в синоптике, экологии, медицине, а также военном деле [1-4]. Основной величиной, характеризующей силу ветра, является его скорость. Скорость ветра отличается большим непостоянством: она изменяется не только за продолжительное время, но и за короткие промежутки времени (в течение часа, минуты и даже секунды) на большую величину [1]. Все эти особенности необходимо учитывать при выборе метода и средства измерения.

Существует несколько методов измерения скорости потока воздуха, основанных на различных физических принципах. Среди них наибольшее распространение получили следующие методы, использующие:

- перепад давления;
- крутящий момент;
- тепловые изменения;
- акустические свойства перемещаемой среды;
- оптические свойства перемещаемой среды;

Метод перепада давления является одним из старейших методов измерения скорости воздуха. Его недостатком является чувствительность к загрязнениям и небольшая чувствительность при измерении небольших скоростей потока.

У метода крутящего момента основной недостаток – наличие движущихся частей. Акустические и оптические методы наиболее дорогостоящие.

Тепловые методы, в свою очередь, делятся на термоанемометрические и термокаталитические.

Каждый из них перечисленных методов имеет свои области наиболее эффективного применения.

Отдельно стоит отметить акустические анемометры, принцип работы которых основан нап использовании эффекта Доплера. На их базе возможно создание прибора для определения направления воздушного потока в трехмерном пространстве, что крайне важно при проведении климатических исследованиях. Кроме того, в отличие от флюгеров, в их конструкции отсутствуют вращающиеся механические части. Для определения скорости воздушного потока акустические анемометры используют ультразвук. Ультразвуковая (УЗ) волна вследствие высокой её частоты распространяется в виде лучей, т.к. из-за малой длины волны можно пренебречь её волновыми свойствами. Такие лучи можно фокусировать с помощью специальных акустических линз и достигать, таким образом, большой интенсивности УЗ-волны. Кроме того, поскольку интенсивность волны пропорциональна квадрату частоты и амплитуды колебаний, то высокая частота УЗ-волны даже при малых её амплитудах предопределяет возможность получения УЗ-волн большой интенсивности [2]. В качестве первичных преобразователей в акустических анемометрах для излучения и приема ультразвуковых волн обычно используют пьезоэлектрические преобразователи (ПЭП), имеющие рабочий диапазон ультразвука в области 15-100 кГц, т.к. именно на таких частотах звуковые волны имеют наименьшее затухание при прохождении через воздушную среду. Для применения анемометра в уличных условиях на открытом воздухе УЗ датчики должны быть герметичны и иметь широкий диапазон рабочих температур. Если диаграмма направленности ПЭП достаточно широка, можно создавать достаточно простые конструкции, когда при малом числе ПЭП можно осуществлять контроль по всем трем декартовым координатам.

Список использованных источников

1. Анемометры – разработчики и изготовители. [Электронный ресурс] // Режим доступа: http://www.anemometers.ru;

2. Аэрология горных предприятий. / Ушаков К.З [и др.] - М.: Недра, 1987;

3. Красильников В. А., Звуковые и ультразвуковые волны в воздухе, воде и твердых телах [Текст], 3 изд. - М., 1960;

4. Метеорологическое оборудование. [Электронный ресурс] // Режим доступа: http://www.raimet.ru/?p=catalog&c=402;

5. Шкундин, С.З. Состояние и перспективы развития анемометрии в угольной промышленности. [Электронный ресурс] / С.З. Шкундин, О.А. Кремлёва, А. Л. Иванников // Режим доступа: http://www.sirsensor.ru/art_3.htm.

6. Плотников, А.Д. Сравнительный анализ приборов и методов измерения скорости и направления ветра/ А.Д.Плотников, Л. И. Сучкова. Ползуновский альманах. – 2010, №2, С 119 – 122.

ИССЛЕДОВАНИЕ СВОЙСТВ ИЗОБРАЖЕНИЙ СЕМЯН ПОДСОЛНУХА И СКЛЕРОЦИЕВ

Кузнецов С.А. – магистрант, Якунин А.Г. – д.т.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Фотоэлектрические сепараторы в последнее время широко используются для очистки семян различных видов зерновых продуктов не только в лабораторных, но и в производственных условиях, причем качество их работы и номенклатура очищаемых зернопродуктов во многом определяется заложенным в системе алгоритме обработки изображений [1]. В данной работе были проведены исследования свойств изображений семян подсолнечника и склероциев с целью разработки алгоритма, пригодного для работы в фотоэлектрическом сепараторе. Изначально исследования выполнялись при помощи высокоскоростной черно-белой камеры "Видеоскан 2000", для чего была разработана и изготовлена экспериментальная установка, схема которой приведена на рисунке 1.

Суть эксперимента заключалась в сопоставлении средних уровней сигналов отсемечки и склероция в различных спектральных диапазонах, для чего применялись узкополосные спектрозональные и обычные светофильтры типа КС-13, КС-15, КС-17, КС-19, ХССС-1, ЗС-10, ЖЗС-1, ЖЗС-5, ЖЗС-6, СЗС-9, СЗС-17, СЗС-20 [2]. Кроме того, изображение формировалось еще и с применением ИК – подсветки. Сравнение выполнялось по трем строкам изображения, взятым в верхней части, в центре, и нижней части наблюдаемых объектов. Пример их изображений и видеосигнала с одной из строк приведен на рисунке 1.

Аналогичные эксперименты были выполнены и с заменой черно-белой видеокамеры на цветную. На рисунке 2 и в таблице 1 приведены отдельные фрагменты такого эксперимента

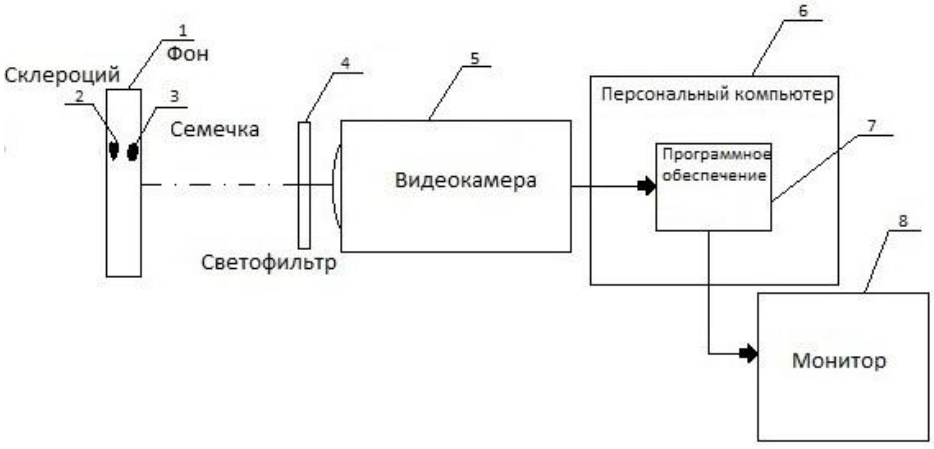


Рисунок 1 - Схема экспериментальной установки. 1 - фон; 2 - семя подсолнуха; 3 - склероций; 4 - светофильтр; 5 - видеокамера; 6 - персональный компьютер; 7 - ПО; 8 - монитор

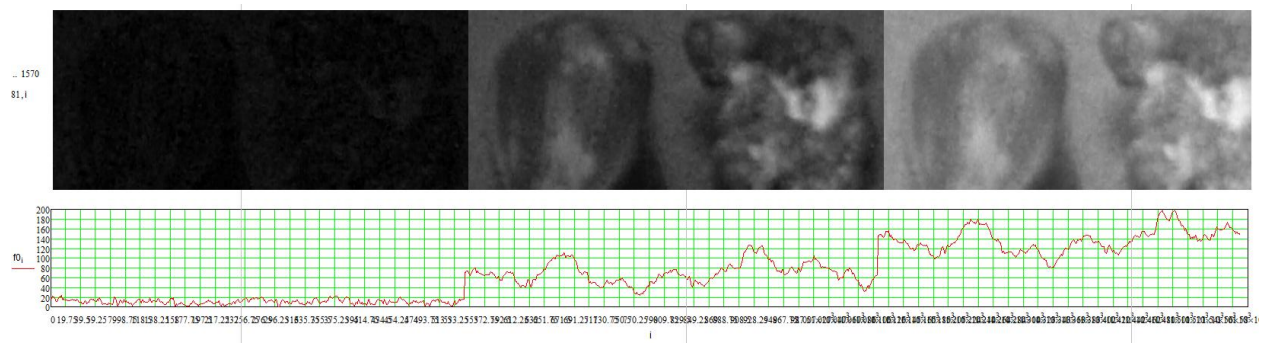


Рисунок 1 - Графики полученной интенсивности пикселей RGB строки 181 при использовании фильтра СЗС- 20 и красного фона

Таблица 1 Средние значения и значения доверительного интервала, полученные для средней строки изображения, полученного с использованием цветной видеокамеры и светофильтра СЗС-17.

Семечка	Склероций	Семечка	Склероций	Семечка	Склероций
R-канал		G- канал		B- канал	
42,07±4,86	39,22±9,25	49,00±4,46	39,55±19,35	55,43±3,61	46,19±19,23

Проанализировав результаты эксперимента, было установлено, что для всех рассмотренных вариантов доверительные интервалы сигналов черной семечки и склероция, пересекаются, а значит сортировка по порогу яркости пикселя в объекте невозможна.

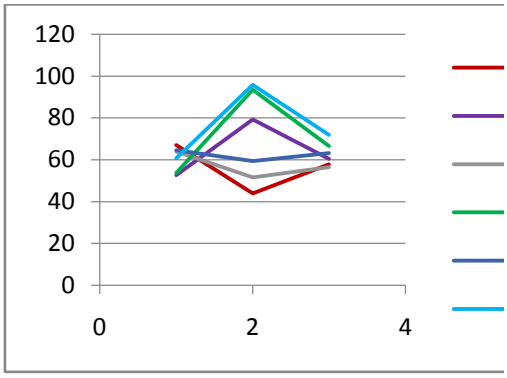


Рисунок 2 - Диаграмма значений RGB сигнала с трех строк 1,2 и 3 изображения при использовании светофильтра СЗС-20.Ряды 1-R,3-G,5-B - составляющие семечки;ряды 2-R,4-G,6-B -

Далее была исследована возможность использования в качестве идентифицирующего признака соотношения геометрических размеров контролируемых объектов в двух ортогональных направлениях, для чего искались отношения максимального числа занимаемого изображением строк к максимальной протяженности строк. Результаты данного эксперимента приведены в таблице 2, откуда видно, что при углах ориентации семечки в пределах 90º±15º, можно с высокой вероятностью идентифицировать контролируемые объекты. Приэто важно отметить, что данное условие хорошо соблюдается в существующих системах полдачи семян, поскольку семечки подсолнечника имеют протяженную форму и всегда ориентируются в лотке подачи по направлению лотка.

Таблица 2 - Значения отношений максимального количества строк(n) в объектах к максимальному количеству пикселей(k) в j-ой строке (M) в зависимости от угла поворота объекта

Объект	Отношение M при различных углах поворота объекта						
	0º	15º	30º	45º	60º	75º	90º
Семечка	1,92±0,13	1,82±0,14	1,56±0,09	1,24±0,06	0,9±0,03	0,6±0,02	0,53±0,04

Склероций	1,12	1,15	1,10	0,99	0,97	1,00	0,88

Список использованных источников

1. Галкин Е.В. Умные фотосепараторы: нейронный алгоритм в решении нестандартных задач сортировки.// Журнал «Хлебопродукты». №5/2016.

2. Хеймен Р., Светофильтры (RexHayman.Filters) [Текст] – М., Focal Press. London&Boston. 1984..

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ПОСТРОЕНИЯ ЛОПАСТИ ВОЗДУШНОГО ВИНТА В СРЕДЕ SOLIDWORKS

Лен С.А. - студент, Гребеньков А.А. – к.ф.-м.н., доцент
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

В наше время не существует единой методики для определения параметров воздушного винта. Ввиду большого количества условий, влияющих на работоспособность воздушного винта, конструкторы по всему миру разрабатывают алгоритмы их расчетов, как теоретических, так и практических. Зачастую подбор характеристик воздушного винта ведется методом выбора из числа уже имеющихся воздушных винтов, т.е. винтов, испытанных в аэродинамических установках. В большинстве случаев таким методом исследуются воздушные винты для «большой» авиации, связанной с использованием крупных самолётов, способных нести большую нагрузку. Для транспорта сверхлегкой авиации винты изготавливаются индивидуально для конкретного средства. Таким образом, для выбора воздушного винта в настоящее время ставится задача его последовательного расчета и проектирования [1].

В основном расчет параметров воздушного винта ведется по вихревой теории, ручной расчет по которой занимает значительное время. В настоящее время существуют алгоритмы расчета, ориентированные под численные методы [2].

На рисунке 1 представлена схема обтекания сечения лопасти в обращенном движении, на которой показаны характерные углы и компоненты скоростей, где: V – поступательная скорость винта; ω – угловая скорость вращения; v_a и v_t – осевая и тангенциальная составляющие индуктивной скорости v; W – скорость притекания потока; c – хорда сечения лопасти; α – угол атаки; α_i – угол индуктивного скоса потока; γ – угол установки сечения; β – угол притекания невозмущенного потока; φ – угол притекания возмущенного потока. Индуктивная скорость v перпендикулярна результирующей скорости W.

В работе Н. В. Левшонкова «Методика проектировочного расчёта и рациональный выбор параметров воздушного винта при разработке многорежимных летательных аппаратов» приводится формула для расчета параметров воздушного винта с использованием безразмерных характеристик:

$$N_b \bar{c} C_y \overline{W}^2 = 8\pi r F(\varsigma + \varsigma^2 \cos\varphi), \quad (1)$$

где N_b – количество лопастей, $\bar{c} = c/R$ – относительная хорда лопасти, $\overline{W}^2 = 3\varsigma^2 + \chi^2 + 1$, N_b – число лопастей винта, $\varsigma = v/V$ - отношение индуктивной скорости к поступательной, $r = y/R$ – относительный радиус, F – функция потерь Прандтля [3], которая вычисляется по формуле:

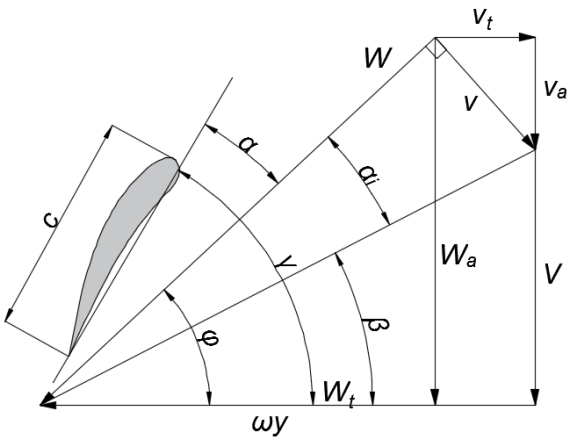


Рисунок 1 – Схема обтекания лопасти

$$F = \frac{2}{\pi}\arccos(e^{-f}), f = \frac{N_b(1-r)}{2\sin\varphi_T}, \quad (2)$$

где φ_T – значение угла φ на конце лопасти.

Величина ς является критерием эффективности воздушного винта. Данная величина связана с углом φ через формулу:

$$\cos\varphi + \varsigma = \chi\sin\varphi \quad (3)$$

где $\chi = \frac{\omega y}{V}$.

Используя равенство (4) можно вычислить угол притекания возмущенного потока при заданных остальных значениях величин, а задав проектное значение угла атаки каждого сечения лопасти α, можно вычислить угол установки γ (геометрическую крутку) $\gamma = \varphi + \alpha$.

В ходе расчета задается величина ς первого приближения. Далее, используем уравнение:

$$dT = dY cos\varphi(1 - \varepsilon tg\varphi), \quad (4)$$

где $\varepsilon = \frac{C_x}{C_y}$, C_x – коэффициент аэродинамического сопротивления, C_y – коэффициент подъемной силы. После интегрирования по радиусу лопасти:

$$T - \int_0^R dT = 0, \quad (5)$$

Получим уравнение вида:

$$A\varsigma^2 + B\varsigma + C = 0, \quad (6)$$

решение которого даст некоторое значение ς. Полученное значение ς не будет совпадать с заданным в начале вычислений. Поэтому проводим серию итерационных расчетов ς, пока задаваемая и получаемая из уравнения величины ς не окажутся равными.

Используя приведенные выше формулы, было написано программное обеспечение, позволяющее строить лопасть воздушного винта по заданным параметрам в среде SolidWorks. На рисунке 2 представлена блок схема макроса.

Форма имеет простой интуитивно понятный интерфейс. После нажатия кнопки «Построить» по заданным параметрам строится модель лопасти воздушного винта. В дальнейшем данную модель можно использовать в проектировочных сборках, а также для расчета аэродинамических параметров с использованием среды SolidWorks. Приведенный алгоритм тесно связан с осевой индуктивной скоростью, что позволяет анализировать картину обтекания, наиболее приближенную к реальной.

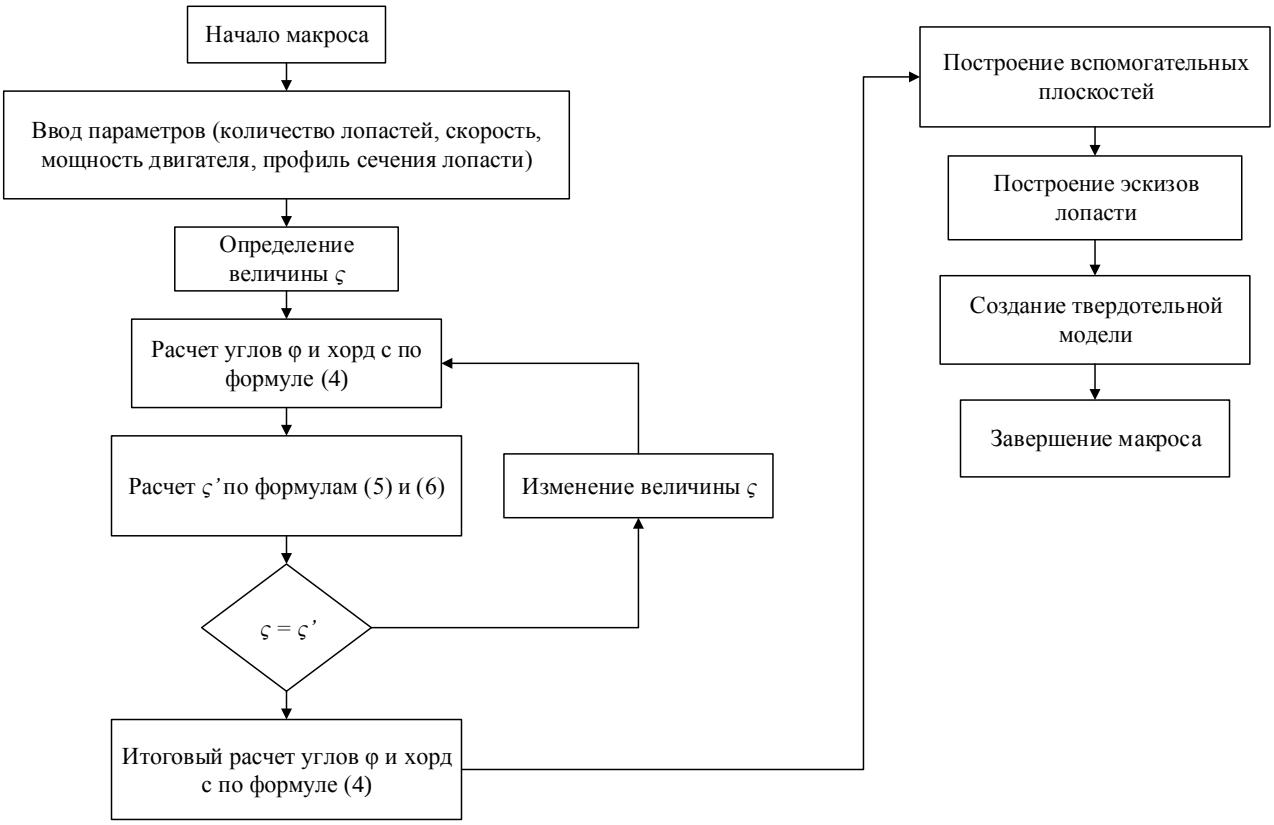


Рисунок 2 – Блок-схема макроса

На рисунке 3 представлено главное окно макроса для ввода параметров пользователем.

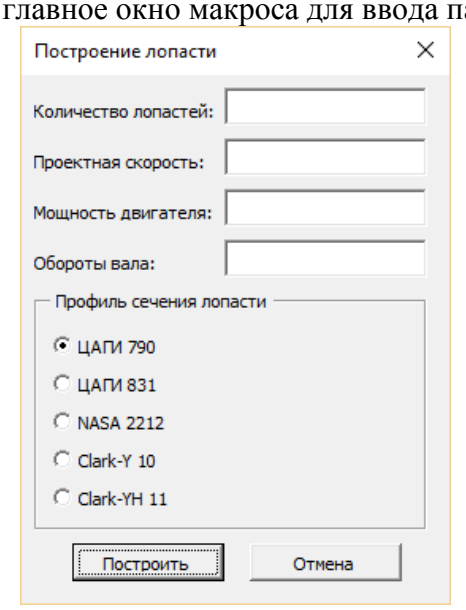


Рисунок 3 – Главное окно макроса

Список использованных источников

1. Гайнутдинов В.Г. О проектировании лопастей воздушного винта повышенной эффективности – Изд-во Казан.гос. тех. университета. – Казань, 2013.

2. Ковалев Е.Д. Аэродинамическое проектирование воздушного винта – Харьков.-№6. - 1999.

3. Ветчинкин В.П. Теория и расчет воздушного гребного винта. / В.П.Ветчинкин, Н.Н. Поляков. – М.: Оборонгиз, 1940. – 520 с

4. Жуковский Н.Е. Вихревая теория гребного винта. / Н.Е. Жуковский. – М: Гос. изд-во техн.-теорет. лит., 1950. - 240 с

5. Александров В.Л. Воздушные винты / В.Л. Александров. – М.: Оборонгиз, 1951. – 475 с.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ PHP-ФРЕЙМВОРКОВ, ИСПОЛЬЗУЕМЫХ В РАЗРАБОТКЕ WEB-РЕСУРСОВ

Менделев Д.В. – магистрант, Якунин А.Г. –д.т.н., профессор
Алтайский государственный технический университет им И.И. Ползунова (г. Барнаул)

Фреймворк — это инструмент, который во многом определяет архитектуру будущего web - приложения и существенно ускоряет процесс его разработки. Фреймворк содержит в себе отлаженный код для решения часто используемых задач web-разработчика, и, в частности, таких, как работа с формами, базой данных, шаблонами.

Выбор фреймворка на сегодняшний день один из самых сложных вопросов, которые необходимо решать при создании web-приложения. В зависимости от технологии разработки, фреймворки делятся на следующие наиболее популярные типы:

- фреймворки с java-script;
- фреймворки с PHP;
- фреймворкиRuby;
- CSS — фреймворки;

PHP — наиболее популярный серверный скриптовый язык программирования. С тех пор как он появился, а произошло это в 1995 году, сложность веб-проектов возросла настолько, что уже просто невозможно писать код для всего приложения с нуля. Поэтому, чтобы повысить эффективность процесса разработки, и были созданы фреймворки.

Выделим основные преимущества PHP-фреймворков:

- ускорение процесса разработки;
- возможность легко масштабировать проекты;
- соблюдение парадигмы разработки MVC;
- упрощение написания структурированного кода;
- поддержка современных практик разработки, например ООП.

В таблице 1 на основании приведенных на [1-5] данных приведено сравнение пяти самых популярных PHP-фреймворков по следующим основным пунктам.

Таблица 1 — сравнение возможностей PHP-фреймворков.

Критерий / название	**Laravel**	**Symfony2**	**Yii2**	**CakePHP**	**Zend Framework 2**
Требуемая версия PHP	5.5.9	5.5.9	5.1.0	5.5.9	5.3
Типы поддерживаемых баз данных	MySQL Postgress SQLite SQL Server	MySQLPostgressSQLite Oracle	MySQLPostgressSQLite Oracle	MySQL Postgress SQLite Oracle SQL Server	MySQL SQLite SQL Server Oracle Postgress
Документация на официальном сайте	Пошагов ое руководс	Пошаговое руководство, справка по API	Пошаговое руководство, справка по API	Пошагов ое руководс	Пошаговое руководств о,

Критерий / название	**Laravel**	**Symfony2**	**Yii2**	**CakePHP**	**Zend Framework 2**
	тво, справка по API, видеоуроки			тво, справка по API	подробная справка по API с комментариями пользователей
Автоматическаяустановка расширений	Да	Да	Да	Да	Да
Сложность установки и настройки	Средняя	Высокая	Средняя	Низкая	Высокая

1) Требуемая версия PHP. Один из самых важных критериев, так как в зависимости от версии будет и разный набор функций языка программирования.

2) Типы поддерживаемых баз данных. В web-приложении самым важным и уязвимым местом является база данных. К выбору базы данных нужно подходить особенно внимательно. От БД будет зависеть скорость работы всего проекта.

3) Наличие документации на официальном сайте. Так как любой сложный продукт нуждается в инструкции, так и фреймворк нуждается в понятной, структурированной, и самое важное, актуальной документации.

4) Автоматическая установка расширений. В современном мире все стремится к автоматизму процессов. Поэтому автоматизация процесса установки освободит разработчика от излишних временных затрат.

5) Простота установки и настройки. Очень важно сразу правильно установить и настроить новый продукт, чтобы в дальнейшей работе не иметь проблем и неудобств.

Исходя из приведенной в таблице информации, следует, что основное различие во фреймворках заключается в используемой версии PHP и в сложности установки и настройки. Отдельно стоит вынести такой показатель, как цикломатическая сложность программы (рисунок 1).

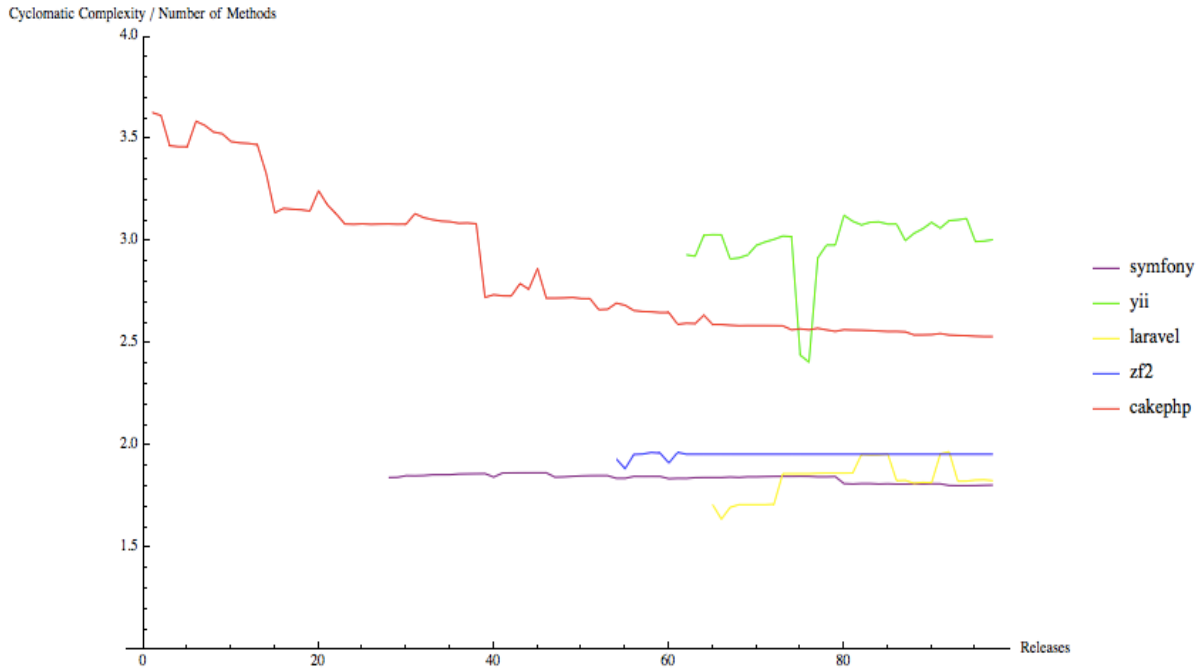


Рисунок 1 –График изменение отношения цикломатической сложности к количеству методов для всех релизов соответствующих фреймворков

Для нахождения цикломатической сложности можно воспользоваться библиотекой Себастьяна Бергмана “phploc” [6]. Из приведенного на рисунке графика видно, что Symfony [2] выигрывает у ZF [1] по качеству алгоритмов. Laravel [5] занимает промежуточное место между ними, и тоже держится на хорошем уровне.CakePHP [3] стал гораздо лучше, чем в момент своего появления, однако, похоже, он достиг своей асимптоты.Yii [4] пока тоже не показывает хороших результатов. Однако, цикломатическая сложность лишь косвенно позволяет судить об эффективности работы программы, поскольку, например, время выполнения программного кода зачастую определяется не числом циклом и переходов, а целым рядом других факторов. Среди них важнейшими являются статистика использования фрагментов программного кода, содержащего большое число циклов и ветвлений, а также количество повторного использования таких фрагментов и протяженность циклов в зависимости от решаемых фреймворком функций и характера исходных данных. Отсюда следует, что для однозначного решения вопроса о выборе инструмента для автоматизации разработки web-приложений необходимо провести целый ряд дополнительных исследований, направленных как на формирование дополнительных квантификационных критериев для сравнения фреймворков, так и на оценку их зависимости от перечисленных факторов.

Список использованных источников

1. ZendFramework[Электронный ресурс] : https://framework.zend.com
2. Symfony[Электронный ресурс] :https://symfony.com
3. CakePHP[Электронный ресурс] :https://bakery.cakephp.org
4. Yiiframework[Электронный ресурс] : http://www.yiiframework.com
5. Laravelframework[Электронный ресурс]: https://laravel.com
6. Библиотека Себастьяна Бергмана[Электронный ресурс] : https://github.com/sebastianbergmann/phploc

РАЗРАБОТКА МЕТОДА ИССЛЕДОВАНИЯ ЭФФЕКТИВНОСТИ РАБОТЫ ФРЕЙМОВРКА С БАЗОЙ ДАННЫХ

Менделев Д.В. – магистрант, Якунин А.Г. –д.т.н., профессор
Алтайский государственный технический университет им И.И. Ползунова (г. Барнаул)

Разработка web-приложения представляет собой достаточно трудоемкий процесс [1]. Нужно учитывать все аспекты используемой при разработке системы автоматизации создания программного кода и реализуемых приложением функций, чтобы максимально быстро и грамотно реализовать продукт. Чем быстрее отрабатывает и грузится сайт, тем лучше он работает. На его быстродействие влияет много факторов. Одно из самых уязвимых мест в быстродействии web-приложения является качество его работы с базой данных. Если не оптимизировать этот процесс, то сайт может потерять свою актуальность. В связи с этим был разработан метод для исследования эффективности работы фреймворка с базой данных.

Алгоритм предлагаемого метода включает следующие этапы.

1. Установка утилиты “AB” (ApacheBenchmark) [2] на компьютер, с которого будут проводиться тестирование. Утилита AB предназначена для тестирования веб-сервера Apache на предмет его производительности. Ее создали для того, чтобы была возможность определить производительность текущей настройки Apache. Данная утилита показывает, сколько запросов в секунду Apacheспособен обслужить.
2. Установка «чистого» фреймворка, подвергаемого тестированию (без оптимизаций или каких либо дополнений)
3. Написание с использованием тестируемогофреймворка страницы, на которую должны приходить запросы к базе данных и которая будет выводить ответ на эти запросы.
4. Проведение тестирования с помощью утилиты AB и расчет среднего времени цикла обращения приложения к базе данных.
5. Повторение п.2-4 для сопоставляемыхфреймворков
6. Сравнение полученных результатов.

Для более получения корректных и точных данных, можно дополнительно рассчитывать и вычитать из общего времени цикла среднее время работы SQL – сервера, затрачиваемое им на обработку одного поступающего запроса с использованием, например, встроенного в СУБД специального механизма, каковым для СУБД MySQL является механизм profiling [3,4].

Ниже приведен пример выдачи результатов тестирования при помощи утилиты AB:

```
    Benchmarking    localhost (be patient)
    Completed               600     requests
Completed           1200    requests
Completed           1800    requests
Completed           2400    requests
Completed           3000    requests
Completed           3600    requests
Completed           4200    requests
Completed           4800    requests
Completed           5400    requests
Completed           6000    requests
Finished            6000    requests
    Server Software: Apache/2.2.16
    Server Hostname: localhost
    Server Port: 8080
    Document Path:/
    Document Length: 16521 bytes
    Concurrency Level: 10
    Time taken for tests: 37.622 seconds
```

Complete requests: 6000
Failed requests: 0
Write errors: 0
Total transferred: 73905880 bytes
HTML transferred: 78464087 bytes
Requests per second: 135.93 [#/sec] (mean)
Time per request: 78.665 [ms] (mean)
Time per request: 7.976 [ms] (mean, across all concurrent requests)
Transfer rate: 1693.50 [Kbytes/sec] received
Connection Times (ms)

	min	**mean**	**[+/-sd]**	**median**	**max**
Connect:	0	0	0,9	0	30
Processing:	19	80	15,9	79	229
Waiting:	0	59	16,8	59	159
Total:	19	80	15,9	79	229

Percentage of the requests served within a certain time (ms)
50% 79
66% 86
75% 90
80% 92
90% 99
95% 106
98% 115
99% 123
100% 220 (longestrequest)

А так выглядит, например, выдача результата обращения на выполнение запроса с помощью функционала profiling:

```
+----------+-----------+----------------------------+
| Query_ID | Duration  | Query                      |
+----------+-----------+----------------------------+
|        1 | 0.00012700 | select count(*) from comment |
|        2 | 0.00014200 | select count(*) from message |
+----------+-----------+----------------------------+
```

2 rows in set (0.00 sec)

Таким образом, с помощью предложенного метода планируется протестировать такие наиболее распространенные на сегодняшний день PHP – фреймворки, как Symfony [5], ZendFramework [6], CakePHP [7,] Yii [8] и Laravel [9]

Список использованных источников

1. Web-приложение [Электронный ресурс]: https://ru.wikipedia.org/wiki/Веб-приложение
2. Официальная документация Apache[Электронный ресурс]: http://httpd.apache.org/docs/2.0/programs/ab.html
3. Как узнать время выполнения MySQL запроса? [Электронный ресурс]: http://yournet.kz/blog/mysql/kak-uznat-vremya-vypolneniya-mysql-zaprosa
4. MySQLProfiler: простой и удобный инструмент профилирования запросов [Электронный ресурс]: https://habrahabr.ru/post/70435
5. Symfony[Электронный ресурс] :https://symfony.com
6. ZendFramework[Электронный ресурс] : https://framework.zend.com
7. CakePHP[Электронный ресурс] :https://bakery.cakephp.org
8. Yiiframework[Электронный ресурс]: http://www.yiiframework.com

9. Laravelframework[Электронный ресурс]: https://laravel.com

ОПРЕДЕЛЕНИЕ СОСТАВА НОРМАТИВНОГО И МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ АНАЛИЗА УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ РАЗЛИЧНЫМ ТИПАМ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Мизгирев А.Ю. - студент, Загинайлов Ю.Н. - к.в.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Формирование профессиональной компетенции по анализу и оценке угроз безопасности информации (УБИ) для объектов информатизации (ОИ) предприятия у студентов, обучающихся в вузе по направлению «Информационная безопасность», является в последние годы нетривиальной задачей. Это обусловлено расширением в период 2013-2016 годов типов защищаемых объектов информатизации, принятием новых стандартов и нормативных документов, содержащих методы оценки угроз. В связи с этим стала актуальной задача совершенствования методического обеспечения дисциплин образовательной программы этого направления, включающих темы по оценке угроз безопасности информации, и, в первую очередь, определение состава нормативного и методического обеспечения для анализа УБИ различным типам объектов информатизации.

В настоящее время фактически можно выделить 2 вида и 4 типа в этих видах объектов информатизации [1]. В качестве первого типа, с учётом документов ФСТЭК России и [1] могут быть обозначены автоматизированные и информационные системы. К объектам 1 типа (в качестве подтипов) можно отнести следующие автоматизированные и информационные системы:

– АСЗИ обрабатывающие сведения, составляющие государственную тайну (АСЗИ ГТ);

– государственные информационные системы не обрабатывающие сведения, составляющие государственную тайну (ГоИС);

– информационные системы персональных данных (ИСПДн);

– автоматизированные системы управления технологическими производствами (АСУ ТП);

– информационные системы в банковском секторе (БИС);

– информационные (автоматизированные) системы коммерческих предприятий (ИСКП).

Каждый подтип ОИ имеет своё нормативное и правовое обеспечение, методики оценки УБИ. В результате проведенного исследования определены необходимые для изучения УБИ и проанализированы соответствующие документы. А также составлены рекомендации по их использованию при построении комплексной системы защиты объектов информатизации предприятия (организации) с учётом [2] и [3]. Структура нормативного и методического обеспечения для каждого типа ОИ включает следующие элементы: 1) федеральные законы (если включают нормы, связанные с угрозами); 2) стандарты; 3) методические документы (рисунок 1). Основные нормативные и методические документы приведены в таблице 1.

Таблица 1 - Нормативные и методические документы для оценки УБИ различных ОИ

Тип ИС (АС)	**Нормативные и методические документы для оценки УБИ**
АСЗИ ГТ	1. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения 2. СТР-97. 3. Другие.
ГоИС	1.Методический документ. Методика определения угроз безопасности информации в информационных системах. Проект. ФСТЭК России. 2. ГОСТ Р 56546-2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем.

Тип ИС (АС)	Нормативные и методические документы для оценки УБИ
	3. Специальные требования и рекомендации СТР-К. ФСТЭК России. 4.Банк данных угроз. Сайт ФСТЭК России. 5. ГОСТ Р ИСО/МЭК 27033-3-2014. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления
ИСПДн	1.Федеральный закон «О персональных данных». 2. Постановление Правительства 1119 2012г. Об утверждении требований к защите ПДн при их обработке в информационных системах ПДн. 3.Методика определения актуальных угроз безопасности ПДн при их обработке в информационных системах ПДн (утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г.) 4. Базовая модель угроз безопасности ПДн при их обработке в ИСПДн (утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.)
АСУ ТП	-
БИС	1.РС БР ИББС-2.2-2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности» 2.РС БР ИББС-2.4-2010 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Отраслевая частная модель угроз безопасности персональных данных при их обработке в ИСПДн организаций БС РФ"
ИСКП	1.ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства Обеспечения безопасности. Менеджмент риска информационной безопасности. 2. ГОСТ Р ИСО/МЭК 27033-3-2014. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления

Для ИСПДн источниками угроз, реализуемых за счет НСД к БД, являются субъекты:

1) нарушитель;

2) носитель вредоносной программы;

3) аппаратная закладка.

Для технических средств характерны угрозы, связанные с их умышленным или неумышленным повреждением, ошибками конфигурации и выходом из строя:

– вывод из строя;

– несанкционированное изменение конфигурации активного сетевого оборудования и приемо-передающего оборудования;

– физическое повреждение технических средств, линий связи, сетевого и каналообразующего оборудования;

– проблемы с питанием технических средств;

– отказы технических средств;

– установка непроверенных технических средств или замена вышедших из строя аппаратных компонент на неидентичные компоненты;

– хищение технических средств и долговременных носителей конфиденциальной информации вследствие отсутствия контроля над их использованием и хранением.

Особенностью нормативно технического обеспечения угроз ИСПДн является то, что технология оценки угроз рассматривается в законе о персональных данных, а все остальные объекты информатизации в стандартах ФСТЭК.

Поскольку объекты информатизации можно разделить на несколько типов, их необходимо рассматривать отдельно. На рисунке 2 приведена схема алгоритм определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

В результате данной работы были систематизированы учебные материалы по тематике угроз безопасности информации различным типам объектов информатизации. Была составлена обобщенная таблица угроз различных типов объектов информатизации. В дальнейшем результат данной работы планируется использовать для формирования учебного контента по дисциплинам направления «Информационная безопасность».

Список использованных источников

1. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю.Н. Загинайлов. - М.; Берлин: Директ-Медиа, 2015. - 253 с.: ил. - Библиогр. в кн. - [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557

2. Комплексная система защиты информации на предприятии: учеб.пособие для студ. высш. учеб. заведений / В. Г. Грибунин, В.В.Чудовский. — М.: Издательский центр «Академия», 2009. — 416 с.

3.Александров, Антон Владимирович. Оценка защищенности объектов информатизации на основе анализа воздействий деструктивных факторов: диссертация ... кандидата технических наук: 05.13.19. - Москва, 2006. - 219 с.: ил. РГБ ОД, 61 06-5/1697

Рисунок 2 - Алгоритм определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных

ОБУЧАЮЩАЯ ПРОГРАММА ПО МОДУЛЮ «ОПТИМИЗАЦИЯ ВНУТРЕННЕГО КОДА» ДИСЦИПЛИНЫ «ОСНОВЫ ЛИНГВИСТИЧЕСКОГО АНАЛИЗА»

Мухортов Д.Д. - студент, Сучкова Л.И. - д.т.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Эффективность исполнимой программы во многом зависит от оптимальности промежуточного кода, формируемого в процессе анализа исходного модуля. В АлтГТУ в рамках изучения дисциплины «Основы лингвистического анализа» изучаются методы преобразований внутреннего кода. Единственный способ получения практических знаний по данной теме – это выполнение лабораторных работ с последующей проверкой результата преподавателем, выявление ошибок и их последующее устранение. Данный процесс занимает большое количество времени как у преподавателя, так и у самих студентов.

Целью данной работы являлась разработка программного обеспечения, которое включает в себя следующий функционал:

- предоставляет пользователю теоретически й материал на темы, связанные с внутренним представлением кода и его оптимизацией;
- обеспечивает тестирование студентов по изученному материалу;
- выполнение автоматической проверки корректности многоадресного кода с неявно именуемым результатом (далее триадам);
- выполнение оптимизации кода, представленного в виде триад, с визуальным отражением данного процесса.

Оптимизация внутреннего кода реализовалась для следующих его элементов:

- линейные промежутки;
- логические выражения;
- циклы;
- вызовы процедур и функций.

Для линейных промежутков были рассмотрены:

- свертка объектного кода.
- удаление одинаковых триад на линейных участках;
- удаление бесполезных присваиваний.

Для предопределенных логических выражений осуществлялось игнорирование построений в коде, не влияющих на результат логического выражения.

Для инлайновых функций рассматривалась подстановка кода функции в точку вызова.

При оптимизации циклов осуществлялись следующие преобразования:

1) вынесение за пределы цикла триад, операнды которой в цикле не изменяются.

2) замена операций с индуктивными переменными.

Все описанные методы оптимизации внутреннего кода реализованы в среде MS VisualStudio. Графический интуитивно-понятный интерфейс разработан с использованием стандартных средств платформы WindowsForms, а функционал реализован на языке программирования C++.

Данная обучающая программа актуальна для учебного процесса кафедры «Информатика, вычислительная техника и информационная безопасность» АлтГТУ.

Список использованных источников

1. Ахо А., Ульман Дж. Теория синтаксического анализа, перевода и компиляции. – М.: Мир, 1978. – т.1,612 с. – т.2,487с.

2. Гордеев А.В. Операционные системы: учебник для вузов. – СПб.:Питер, 2004.–416 с.

3. Молчанов А.Ю. Системное программное обеспечение: Учебник для вузов, 3-е изд. – СПб.: Питер, 2010. – 400 с.

МОДЕЛИРОВАНИЕ НЕЙРОСЕТЕВЫХ ДЕТЕКТОРОВ ИММУННОЙ СИСТЕМЫ ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ ВТОРЖЕНИЙ

Ребро И.В. – студент, Шарлаев Е.В. – к.т.н., доцент
Алтайский государственный технический университет им. И.И. Ползунова(г. Барнаул)

Проблема защиты информационных ресурсов сети от несанкционированной деятельности хакеров, воздействий вирусов, обеспечения конфиденциальности, целостности и доступности данных является одной из актуальнейших и в то же время наиболее сложных проблем нашего времени.

При решении задач, связанных с диагностикой и защитой сетевых ресурсов, центральным вопросом является оперативное обнаружение состояний сети. Для обнаружения используется большой спектр специализированных систем: средства систем управления, анализаторы сетевых протоколов, системы нагрузочного тестирования, системы сетевого мониторинга и системы обнаружения вторжений. [1]

Концепция искусственных иммунных систем зародилась при исследовании принципов работы иммунной системы позвоночных, которая защищает их организм от влияния бактерий и вирусов. Биологическая иммунная система представляет собой надёжный механизм обнаружения аномалий, которыми являются болезнетворные вирусы и бактерии. При этом система обладает способностью анализировать и классифицировать неизвестные ранее объекты по различным классам. [2]

Эти особенности иммунной системы позволяют применять эту концепцию в области обработки массивов данных и использовать при защите информации и доказывают её перспективность при решении сложных задач. При построении искусственной иммунной системы для решения задач обнаружения и классификации сетевых аномалий обычно используется типовая схема работы иммунной системы, представленная на рисунке 1.

Система содержит в себе набор детекторов являющихся аналогами клеток иммунной системы – лимфоцитами. [3]

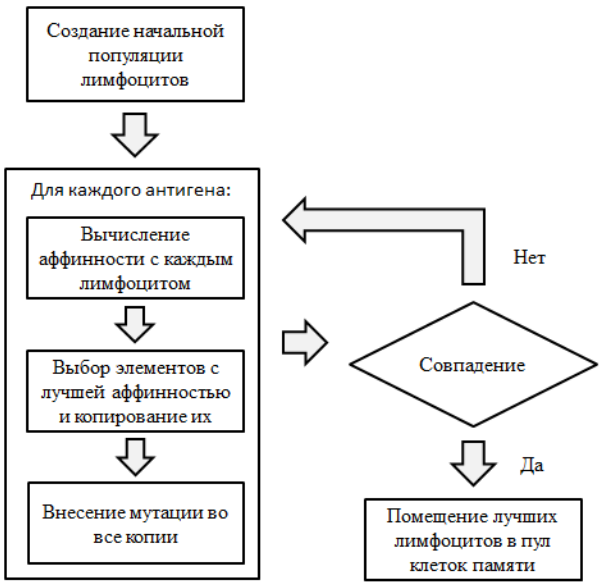


Рисунок 1 – Жизненный цикл детекторов (лимфоцитов) искусственной иммунной системы

Весь первоначальный набор иммунных детекторы генерируется по случайному алгоритму, что дает возможность создания большого количества не шаблонных разнообразных по структуре детекторов, способных отреагировать на любую возникшую аномалию. Лимфоцит проходит стадию обучения и тщательного отбора с помощью алгоритма отрицательного отбора, приобретая способность корректно реагировать на чужеродные объекты или явления и не осуществлять ложные срабатывания на родные объекты системы.

Детекторы, не обучившиеся корректно классифицировать входящие объекты (рисунок 2), удаляются. Отобранные детекторы допускаются к функционированию в реальных условиях с выделенным лимитированным количеством времени жизни. По истечению выделенного периода времени детекторы, не обнаружившие никаких аномалий, удаляются. Детекторы, обнаружившие аномалию, помещаются в иммунную память антигена (рисунок 3) и получают большее время жизни и доверие.

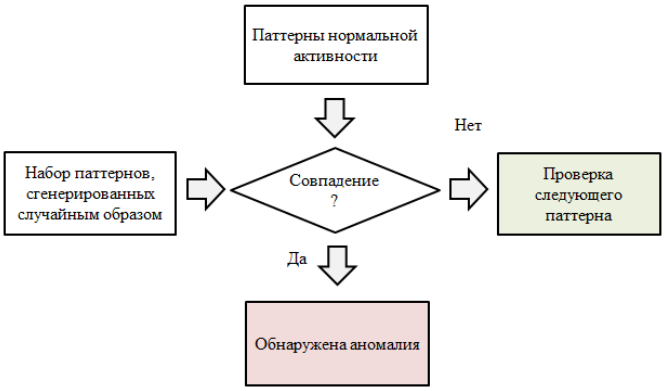


Рисунок 2 – Алгоритм отрицательного отбора. Генерирование детекторов.

Искусственные иммунные системы имитируют основные процессы, протекающие в биологической иммунной системе, и их взаимодействие, отличаясь в способе представления информации и структуре лимфоцита.

Для улучшения свойств адаптированного механизма искусственной иммунной системы и повышения качества обнаружения сетевых атак можно использовать нейросетевые детекторы.

Нейронная сеть характеризуется разделением по разным классам нейронов в скрытом слое Кохонена (рисунок 4). Выделяется два вида классов – сетевые атаки и нормальные соединения. [5]

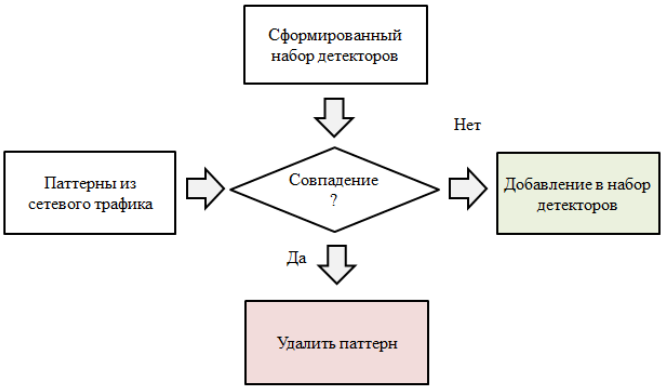


Рисунок 3 – Алгоритм отрицательного отбора. Обнаружение аномалий

Для корректного выполнения задач классификации входящего сетевого трафика детекторы лимфоцитов должны пройти процесс контролированного конкурентного обучения по правилу «победитель берёт всё». [4]

Для этого выбираются параметры сетевого трафика, характеризующие соединение с трёх сторон:

1. Внутренние параметры – данные полученные из заголовков пакетов, такие как число указателей срочности или флаги TCP.

2. Параметры содержимого – сюда входят такие показатели, как количество полученных сеансов суперпользователя, попыток авторизации, создания файлов и т.п.

3. Параметры трафика – к этой категории относятся параметры, которые описывают характеристики, присущие трафику устройства-отправителя, например, число соединений к одному узлу или порту.

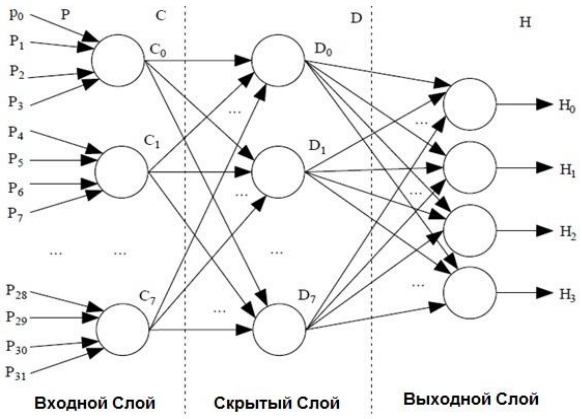


Рисунок 4 – Модель работы искусственной нейронной сети

Вторая группа параметров требует знания устройства сети, наличие профилей приложений, запускаемых на рабочих станциях.

Для минимизации возникновения ложных срабатываний, когда нормальное соединение принимается за сетевую атаку. Все обученные иммунные нейросетевые детекторы проходят проверку на классификацию с помощью заранее созданной тестовой выборки, состоящей из параметров нормального соединения (рисунок 5).

Таким образом, в рамках данной статьи была рассмотрена концепция, позволяющая повысить точность обнаружения сетевых вторжений и уменьшить количество ложных срабатывания.

Список использованных источников**:**

1. Аграновский, А.В. Обучаемые системы обнаружения и защиты от вторжений [Текст] / А.В. Аграновский // Искусственный интеллект. – 2001. – № 3. – с. 440-444.

2. Марков, Г.А. Использование технологий нейронных сетей при решении задач информационной безопасности [Текст] / Г.А. Марков // Молодежный научно-технический вестник. – 2014. – № 3.

3. Шелухин, О.И. Обнаружение вторжений в компьютерные сети (сетевые аномалии): учеб.пособие [Текст] / Д.Ж. Сакалема, А.С. Филинова, О.И. Шелухин. – М.: Горячая линия – Телеком, 2013.

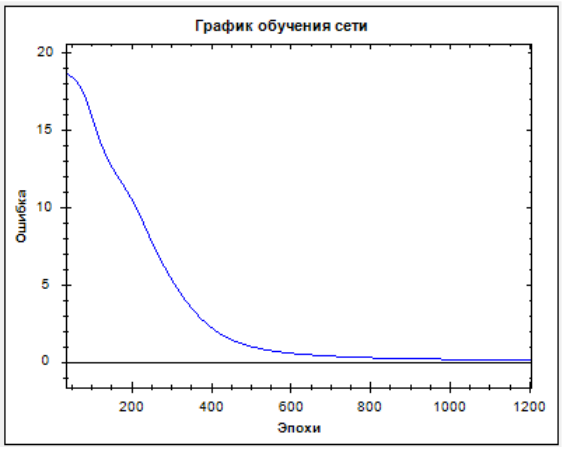


Рисунок 5 – Процесс обучения нейронных детекторов лимфоцитов

4. Новиков, Е.А. Сравнительный анализ методов обнаружения вторжений [Текст] / Е.А. Новиков, А.А. Краснопевцев // «Безопасность информационных технологий». – 2012. – № 1. – С. 47-50.

5. Покровский, П. Развертывание системы обнаружения вторжений [Электронный ресурс] / П. Покровский // «Журнал сетевых решений/LAN», №06, 2003. Режим доступа: http://www.osp.ru/lan/2003/06/137726.

ИССЛЕДОВАНИЕ МЕХАНИЗМОВ РАБОТЫ СРЕДСТВА ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ WEBAPPLICATIONFIREWALL

Теплюк П.А. – магистрант, Шарлаев Е.В.- к.т.н., доцент
Алтайский государственный технический университет им. И.И.Ползунова (г. Барнаул)

Современная Web-разработка приложений направлена на увеличение количества сервисов и большее вовлечение в информационный обмен числа пользователей сети интернет. В настоящее время в веб пространстве встречаются веб-приложения различной сложности: от простых веб-сайтов – блогов до сложных порталов, включающих поисковые системы, системы медиаконтента, социальные сети, приложения-поставщики облачных услуг и т.д.

С распространением таких приложений и технологий любой пользователей имеет возможность создать свой сайт всего в несколько «кликов». Поскольку порог вхождения в веб-разработку становится все ниже, следовательно возникает проблема, что многие веб-приложения оказываются достаточно уязвимы к атакам злоумышленников. Эксплуатируя уязвимости системы, злоумышленник может выполнять несанкционированные действия, например, производить deface веб-страниц, модифицировать / удалять таблицы базы данных, распространять вредоносный код.

Одним из ключевых решений для предотвращения вторжений в веб-приложение посредством эксплуатации уязвимостей является Webapplicationfirewall (WAF). WAF рассматривается как подмножество систем обнаружения вторжений (IDS) и направлен на обнаружение и предотвращение атак на веб-приложения [1], описываемых в проекте OWASPTopTen. В целом, целью данного проекта является повышение осведомленности о безопасности приложений при помощи определения наиболее критичных рисков, угрожающих организациям.

Основные защитные механизмы, присущие современнымWAF, описали в своем исследовании Баранов Б. А. и Бейбутов Э.Р. [2]. К ним следует отнести:

- проверка протокола;
- сигнатурный анализ;
- машинное обучение форматов идентификаторов доступа;
- защита от инъекций и XSS;
- пользовательские правила выявления несанкционированных запросов;
- защита от DoS- и DDoS-атак;
- интегрированность в ландшафт информационной безопасности организации.

Особое внимание заслуживают такие механизмы работы WAF, как защита от инъекций и XSS, а также предотвращение DoS-атак.

Защита от инъекций и XSS

Атаки посредством инъекций происходит в случаях, когда веб-приложение посылает непроверенные данные, содержащиеся в клиентском запросе, в командный интерпретатор конечной системы управления ресурсами. Такой системой может быть СУБД, ОС, сервер LDAP, XPath и др. Передача такого запроса может позволить злоумышленникам манипулировать с соседствующими с сервером приложений функциональными системами [3].

С целью предотвращения инъекций используются следующие механизмы:

- токенизация;
- контроль ответов веб-приложения;
- сигнатурный анализ.

Другой тип угроз – это попытки межсайтового выполнения сценариев (Cross-sitescripting, XSS). Атака данного типа становится возможной, если при формировании ответа веб-приложение использует клиентские данные без проведения надлежащей проверки. Благодаря возникающей уязвимости злоумышленник может красть

идентификаторы сеанса пользователя (cookie), производить deface веб-страниц и перенаправлять клиентов к произвольным ресурсам.

Для обнаружения XSSприменяются следующие механизмы:

– токенизация;

– внедрение политики безопасности контента;

– анализ ответов;

– внедрение в ответы Javascript-кода, предназначенного для контроля отображения страницы в браузере клиента;

– сигнатурный анализ.

Защита от DoS- и DDoS-атак

Обеспечение доступности информации не менее важная задача, как и обеспечение конфиденциальности и целостности обрабатываемых веб-приложением данных.

WAF реализует несколько уровней защиты от атак типа «отказ в обслуживании» (DoS, DDoS):

1. Первый уровень защиты – это механизм определения инфицированных клиентов. Проверка реализуется с помощью внедрения в ответы веб-приложения специального Javascript-кода, который сканирует окружение клиентского браузера на наличие потенциальных вредоносных программ. Данный уровень защиты больше направлен на предотвращение распределенныхDoS-атак (DDoS).

2. Второй уровень защиты – это механизм обнаружения аномалий трафика в контексте пользовательский сессий приложения. Клиенты, участвующие в аномально высокой нагрузке к объектам веб-приложения, автоматически ограничиваются или блокируются.

3. Третий уровень защиты – использование «капчи» (captcha). Разрешаются только те сессии клиентов, которые прошли испытание.

Анализ реализуемых в WAF механизмов позволяет сделать вывод, что средства этого класса являются серьезными сдерживающими контрмерами, усложняющими процесс взлома веб-приложений со стороны злоумышленников.

В настоящее время, наряду с комплексными методами защиты объекта информатизации, актуальными остаются частные задачи защиты конкретных приложений, направленные на закрытие и контроль уязвимостей присущих используемых в них IT-технологий. Поэтому наряду с разработкой непосредственно самого веб-приложения целесообразно внедрять WAF-модули, работающие с целевым приложением в одном окружении и обеспечивающим закрытие уязвимости такового. Важнейшим этапом разработки является исследование эффективности механизмов WAF методом тестирования на проникновение, который подразумевает под собой моделирование и непосредственно попытки реализации атаки злоумышленником.

Список использованных источников

1. Asrul H. Yaacob. Moving Towards Positive Security Model For Web Application Firewall // International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:6, No:12, 2012.Режимдоступа: http://waset.org/publications/14960/moving-towards-positive-security-model-for-web-application-firewall, свободный.

2. БарановП.А., БейбутовЭ.Р. Обеспечениеинформационнойбезопасностиинформационныхресурсовспомощьюмежсетевых экрановдлявеб-приложений // Переводстатьи: Baranov P.A., Beybutov E.R. Securing information resources using web application firewalls Business Informatics. 2015. No. 4 (34). P. 71–78. Режим доступа:https://bijournal.hse.ru/data/2016/03/18/1127231431/Баранов%20Бейбутов%20РУС.pdf, свободный.

3. Moosa A., “Artificial Neural Network based Web Application Firewall for SQL Injection,” // World Academy of Science, Engineering and Technology, no. 64, pp. 12–21, 2010.

ОРГАНИЗАЦИЯ ВНЕШНЕГО АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ

Фещенко Д.Н. - студент, Загинайлов Ю.Н. - к.в.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Одной из важных тем, изучаемых студентами АлтГТУ направления подготовки «Информационная безопасность», в рамках учебной дисциплины «Комплексное обеспечение защиты информации объекта информатизации», является тема, связанная с аудитом информационной безопасности объектов информатизации предприятия. При этом с учётом нового профиля подготовки для этого направления «Организация и технология защиты информации», актуальной становится задача формирования компетенций по организации аудита информационной безопасности [1], и, соответственно, формирования учебного контента и методического обеспечения этой темы.

Для решения этой задачи были проанализированы существующие научные и учебные материалы по теме, стандарты, сформированы схемы аудита и апробированы применительно к ИС, не обрабатывающей сведения, составляющие государственную тайну, органа государственной власти г. Барнаула.

Среди научных трудов, материалы которых взяты для формирования учебного контента, следует выделить [2], включающего анализ проблемы аудита на этапе оценки вариантов реализации угроз безопасности информации. Среди учебных материалов (пособий), следует выделить [3], материалы которого взяты за основу учебного контента по теме.

Аудит информационной безопасности в организации: Периодический независимый и документированный процесс получения свидетельств аудита и объективной оценки с целью определить степень выполнения в организации установленных требований по обеспечению информационной безопасности [4].

Целями работ по аудиту состояния информационной безопасности АС исполнительных органов государственной власти являются [7]:

1. проверка соответствия установленным правовым и договорным требованиям, а также иным требованиям и связанным с ними последствиям для безопасности;
2. достижение и поддержка уверенности в возможностях менеджмента риска проверяемой организации.

Аудит безопасности органов государственной власти должен рассматриваться как конфиденциальный инструмент управления, исключающий в целях конспирации возможность предоставления информации о результатах его деятельности сторонним лицам и организациям.

При проведении аудита информационной безопасности существующие методики проведения аудита невозможно использовать без адаптации, в связи с этим, решая конкретную задачу по проведению внешнего аудита информационной безопасности органа государственной власти, была проведена формализация этого процесса (рисунок 1), в соответствии с рекомендациями, изложенными в [6].

При проведении аудита информационной безопасности необходимо учитывать следующие рекомендации:

1. требования аудита должны быть согласованы с соответствующим руководством;
2. область проверок следует согласовывать и контролировать;
3. при проведении проверок доступ к программному обеспечению и данным должен быть ограничен только чтением;
4. другие виды доступа, кроме доступа только для чтения, могут быть разрешены только в отношении изолированных копий файлов системы, которые необходимо удалить по завершению аудита или обеспечить соответствующей защитой, если необходимо хранить такие файлы в соответствии с требованиями документального оформления аудита;
5. ресурсы, необходимые для выполнения проверок, должны быть четко определены и сделаны доступными;

6. требования в отношении специальной или дополнительной обработки данных следует определить и согласовать;

7. весь доступ необходимо отслеживать и регистрировать для создания прослеживаемых ссылок;

8. все процедуры, требования и обязанности следует оформлять документально;

9. лицо(а), проводящее(ие) аудит, должно(ы) быть независимым(и).

В настоящее время существует три главных практических подхода к анализу и оценке текущего состояния информационной безопасности организации [3].

Для апробирования на практике сформированной схемы проведения аудита, в соответствии с указанными в данной работе рекомендациями, был выбран первый поход к анализу и оценке текущего состояния информационной безопасности организации, использующийся при определении так называемого базового уровня информационной безопасности организации, когда достаточно проверить соблюдение на практике действующих специальных требований и рекомендаций по технической защите конфиденциальной информации [3].

Был составлен перечень из 30 вопросов для проверки соответствия системы защиты информации организации:

1. требованиям к организации работ по защите информации;

2. требованиям к защите речевой информации;

3. требованиям к защите конфиденциальной информации, обрабатываемой в ИС.

После согласования с руководителем организации срока и порядка проведения аудита, был проведен внешний аудит информационной безопасности организации, в процессе которого были получены сведения о текущем состоянии безопасности организации в ходе анализа которых были выявлены 3 потенциальные угрозы, характерные как для внутренних, так и для внешних нарушителей. Был составлен итоговый отчет по результатам аудита, а также были разработаны рекомендации по устранению выявленных угроз.

В целях конспирации, в данной работе не раскрываются полученные сведения о текущем состоянии информационной безопасности организации и характер выявленных угроз.

Рисунок 1 – Схема проведения внешнего аудита информационной безопасности организации

Список использованных источников

1. Основная профессиональная образовательная программа высшего образования. Направление подготовки (специальность) 10.03.01 «Информационная безопасность». Профиль «Организация и технология защиты информации». АлтГТУ, г.Барнаул., 2016.-122 с. [Электронный ресурс].:http://www.altstu.ru/sveden/oop/0532/

2. Александров Антон Владимирович. Оценка защищенности объектов информатизации на основе анализа воздействий деструктивных факторов: диссертация ... кандидата технических наук: 05.13.19. - Москва, 2006. - 219 с.: ил. РГБ ОД, 61 06-5/1697

3. Аверченков В.И. Аудит информационной безопасности органов исполнительной власти: учеб. Пособие [электронный ресурс] В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин,

М.В. Рудановский. – 3-е изд., стереотип. – М. : ФЛИНТА, 2011. – 100 с. – (Серия «Организация и технология защиты информации»). https://docviewer.yandex.ru/view/0/?*=nIRwQkyJ7lsIGagJsSYuvzm

4. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения [Текст]. –Введ. 2008–02–01. – М.: Стандартинформ, 2008. – 10 с.

5. С. Симонов. Аудит безопасности информационных систем/ С. Симонов // JetInfo - 1999. - №9(76).

6. ГОСТ Р ИСО/МЭК 27002—2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента безопасности. – М.: Стандартинформ, 2007. – 63 с.С.84-85

7. ГОСТР ИСО/МЭК 27007-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности. – М.: Стандартинформ, 2015. –23 с.

8. ГОСТ Р 56045-2014. Информационная технология. Методы и средства обеспечения безопасности. Рекомендации для аудиторов в отношении мер и средств контроля и управления информационной безопасностью. © Стандартинформ, 2015.

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ИССЛЕДОВАНИЯ ВАРИАНТОВ ХРАНЕНИЯ И ОБРАБОТКИ ДАННЫХ В СИСТЕМАХ BIGDATA

Яковенко Р.А. – студент, Сучкова Л.И. – д.т.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Одним из значимых и перспективных направлением в области разработки высоконагруженных распределенных систем хранения и обработки данных (далее, систем BigData) является предварительное моделирование их функционирования с целью проведения экспериментов без ее физической реализации. Потребность в имитационных системах возникает при создании и развертывании сложных быстродействующих информационных систем в областях, где тестирование затруднено или невозможно по причине высокой стоимости, а сбои и отказы могут привести к серьезным или даже к катастрофическим последствиям [1]

Специализированные программные средства для имитационного моделирования работы систем BigData (SCADA ZetView, Tossim, NetWizard, OpnetModeler и др.), имеют следующие недостатки: высокая стоимость (до 70 000$), отсутствие средств обработки нештатных ситуаций и оценки характеристик работоспособности системы в зависимости от параметров данных, выполняющихся на узлах системы. Кроме того, многие из перечисленных программных комплексов ориентированы на оборудование конкретного производителя.

Главной особенностью BigData систем является то, что количество типов запросов известно заранее, и разработчик может самостоятельно указать все особенности оптимального выполнения каждого из них.

В подавляющем большинстве высоконагруженные распределенные системы обработки и хранения данных являются системами массового обслуживания (далее, СМО), в которых в произвольные моменты времени появляются заявки на обслуживание от клиентов (запросы), а также присутствует устройство (комплекс устройств) для обработки таких заявок (сервера) [2].

Разработана имитационная модель, а также её программная реализация, для исследования вариантов хранения и обработки данных в системах BigData, позволяющей учитывать различные конфигурации архитектуры хранения и обработки данных.

Имитационной системы имеет следующие этапы работы:

1) Переход от реляционного представления базы данных к NoSQL- представлению (JSON).

2) Генерация множества вариантов логической структуры данных в

нереляционномпредставлении.

3) Распределение данных по машинам кластера.

4) Тестирование выбранного варианта архитектуры данных на множестве клиентских типовых запросов.

Результатом первого этапа работы системы при переходе от SQL к NoSQL-представлению данных, является JSON-данные запроса. Например, типичный SQL-запрос «SELECTid, nameFROMuserASu» можно трансформировать в формат JSON:

```
{
   select: [‘user.id’, ‘user.name’],
   from: [‘user’]
}
```

SQL-запрос, представленный в таком формате, имеет большую наглядность и с ним удобнее работать программисту.

На основании полученного JSON-представления структуры табличных данных генерируется множество вариантов логической структуры в нереляционном представлении. Одним из способов отображения логической структуры данных на физическую является представление данных в виде множества строк и столбцов. Каждая строка и столбец определяются уникальным ключом (rowkey и columnkey соответственно). Данные в NoSQL структуре данных хранятся в виде: (Table, RowKey, Family, Column, Timestamp) ->Value, где левая часть образует ключ, а правая – значение [3]. Значение строки при моделировании работы BigData систем большой роли не играет и для удобства хранит размер данных. От ключа напрямую зависит скорость доступа к данным. Поэтому способ выбора ключевых полей определяет распределение данных по кластеру и, как следствие, скорость доступа к ним при выполнении запросов.

Ключ строки может быть сформирован различными способами:

1) первичный ключ или уникальное поле;

2) конкатенация нескольких полей из таблиц;

3) хэш-функция от полей.

Поля, которые не вошли в ключ строки, должны быть распределены между семейства колонок (columnfamilies). Такой подход обосновывается облегчением управления и манипуляции данными. Так как все данные каждой columnfamily хранятся в определенном наборе файлов, то выбор распределения столбцов напрямую влияет на скорость выполнения запросов. Таким образом, поля, которые встречаются вместе в запросе разумно выделить в одну columnfamily.

Генерация NoSQL-структуры может быть произведена полным перебором вариантов выбора columnfamily, либо пользователем. В данной имитационной системе нереляционные структуры генерируются на основании пользовательского способа группировки полей.

Математическая модель оценки времени на выборку данных для одной пары Key-Value описывается формулой (1):

$$T = T_{read(key)} + kT_{read(value)} + (1 - k)(T_{parse(key)} + T_{read(value)}) + T_{transfer} \quad (1)$$

где $T_{read(key)}, T_{read(value)}$ – времячтения Key и Value из Row;

$T_{parse(key)}$ – время выделения поля из RowKey для сравнения;

$T_{transfer}$ – время передачи row между узлами системы;

k– коэффициент, равный 1, если все поля запроса находятся в RowKey, иначе 0.

Существует множество вариантов физической организации хранения информации. Распределение данных по машинам кластера можно производить различными способами [4]:

1) по первичным ключам (хеш-кодам);

2) по атрибутам данных (например, данные 2015-2017 годов находятся на одной машине, а данные 2014-2015 годов – на другой);

3) по композитным ключам;

4) по таблицам;

5) по столбцам и записям таблиц.

Основной единицей масштабируемости и балансировки нагрузки является регион (region). Регион является непрерывным диапазоны строк, имеющих одно место хранения. При добавлении новых данных в регион, система проверяет, чтобы общий объем не превысил допустимый размер. Когда объем данных в регионе достигает максимального значения, регионы динамически расщепляются (split) системой на две части. Один из новых регионов останется на прежнем сервере, а второй может быть перенесен на другой, менее загруженный. Каждый регион обслуживается одним регион-сервером. Регион-сервер – это сервера хранения данных, ответственные за все операции чтения и записи по отношению к обслуживаемым регионам. Каждый из таких серверов обрабатывают множество регионов в одно время.

В любой BigData системе, как правило, имеется мастер-сервер [5]. В его задачу входит управление множеством подчиненных регион-серверов. Также, главный сервер ответственен за назначение регионов регион-серверам и за распределение данных по регион-серверам. Также он отвечает за баланс нагрузки между регион-серверами. При записи данных на регион-сервер запросы от клиента на запись сначала поступают намастер-сервер, который имеет реестр с информаций о регионах. Далее главный сервер перенаправляет данные на нужный регион-сервер.

Так как для моделирования выполнения процессов использован аппарат теории СМО, то в роли обслуживающих устройств выбраны мастер и регион-сервера, а в качестве событий различных типов – запросы на запись или выборку данных.

В ходе данной работы был проведен обзор различных способов организации очередей в СМО [6]. В разработанной имитационной системе комбинируются следующие модели работы с очередями:

1) модель очередь задач;
2) модель маршрутизации;
3) модель RPC.

Использование модели очередь задач предоставляет возможность мастер-серверу получать запросы от клиентов. Модель маршрутизации позволяет мастер-серверу распределять события по регион-серверам. Благодаря реализации модели RPC всегда существует обратная связь с клиентом после сделанного им запроса, а также связь между главным и регион серверами, до момента потери необходимости.

Для имитационной модели выделены следующие этапы сбора входных данных:

1) Создание и конфигурация узлов хранения и обработки данных.
2) Создание логической структуры хранения данных (таблицы, поля, индексы).
3) Настройка сегментирования данных (Partitioning).
4) Описание набора SQL запросов, указание числа клиентов в системе и других параметров СМО [10].

Результаты имитационного моделирования работы распределенной высоконагруженной системы отображаются графически (рисунки 1,2).

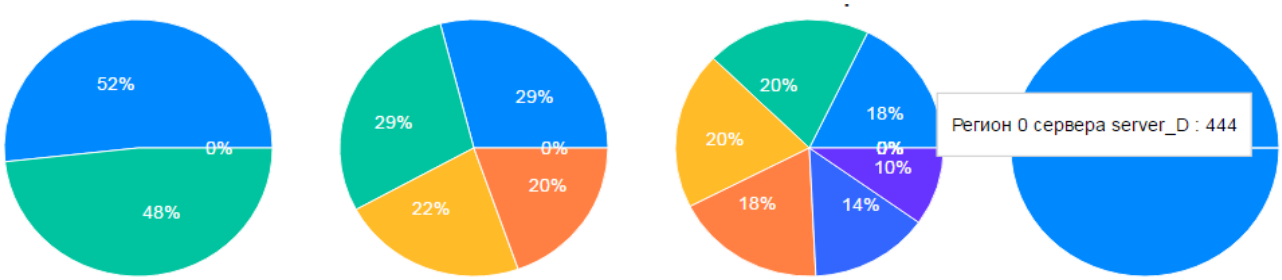


Рисунок 1 – Результат заполнения мастер-сервером регионов четырех регион-серверов

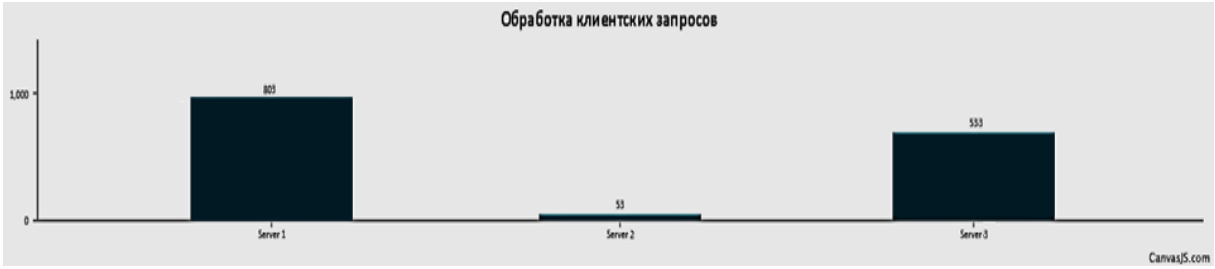


Рисунок 2 – Диаграмма количества обработанных клиентских заявок

Данная имитационная система позволяет рассмотреть результат распределение данных и клиентских запросов по регион серверам. Такой подходит для исследования различных вариантов архитектур хранения и обработки данных в системах BigData, а также позволяет найти оптимальный вариант.

Список использованных источников

1. Стигнеева, М. Техногенные катастрофы / М.Стигнеева // Тайны XX Века. – 2007.– № 49.

2. Гильмутдинов Р.Ф., Кирпичников А.П. Математическая модель замкнутой одноканальной системы массового обслуживания // Вестник Казанского государственного технологического университета – Казань: Изд-во Казан.гос. технол. ун-та, 2011 - № 6 - с. 18

3. Fay Chang, Jeffrey Dean, Sanjay Ghemawat, Wilson C. Hsieh, Deborah A., Wallach, Mike Burrows, Tushar Chandra, Andrew Fikes, Robert E. Gruber. Bigtable: A Distributed Storage System for Structured Data – Google Inc. 2006, 14c.

4. HrishikeshKarambelkar. Scaling Big Data with Hadoop and Solr – Packt 2013, 144 c.

5. TypicalHadoopCluster [Электронный ресурс] – 2015. Режим доступа: https://docs.hortonworks.com/HDPDocuments/HDP2/HDP-2.3.6/bk_cluster-planning-guide/content/typical-hadoop-cluster-hardware.1.html

6. Обзор способов организации очередей заявок для решения задач имитационного моделирования функционирования распределенных систем сбора и обработки большого объема данных [Текст] / Р.А. Яковенко, Л.И. Сучкова // Ползуновский альманах: Виртуальные и интеллектуальные системы обработки информации в студенческих работах. – Барнаул. Изд-во АлтГТУ, 2016 - №2 – С. 215-218.

7. Part 1: RabbitMQ for beginners - What is RabbitMQ? [Электронный ресурс] – 2015. – Режим доступа: https://www.cloudamqp.com/blog/2015-05-18-part1-rabbitmq-for-beginners-what-is-rabbitmq.html

8. Dr. Michael Eichberg. Software Engineering: The Observer Design Pattern - Department of Computer Science, 2009 - 36c.

9. Имитационное моделирование работы распределённой вычислительной системы на основе принципов теории массового обслуживания / Е.В. Бочкарева, И.М. Кулагин, Л.И. Сучкова // Измерение, контроль, информатизация ИКИ-2010: материалы XI Международной научно-технической конференции. – Барнаул: Изд-во АлтГТУ, 2010. – С. 41-44

10. Харламов, А.И. Исследование схем хранения информации в распределенных системах с учетом основных закономерностей доступа к данным [Текст] / А.И.Харламов, Л.И. Сучкова, Е.В. Бочкарёва // Ползуновский вестник: измерение, информатизация, моделирование: проблемы и перспективы технологической разработки и применения. – Барнаул: Изд-во АлтГТУ, 2012. – №3/ 2. – С. 81 – 86