МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

ИНЖЕНЕРНЫЕ КАДРЫ – БУДУЩЕЕ ИННОВАЦИОННОЙ ЭКОНОМИКИ РОССИИ

Материалы V Всероссийской
студенческой конференции

Йошкар-Ола, 5-8 ноября 2019 г.

Часть 4

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ – ОСНОВА СТРАТЕГИЧЕСКОГО ПРОРЫВА В СОВРЕМЕННОЙ ПРОМЫШЛЕННОСТИ

Йошкар-Ола
2019

УДК 378:62
ББК 74.48:30
И 62

Руководитель проекта
Андрианов Ю. С., начальник Управления
научной и инновационной деятельности ПГТУ

Редакционная коллегия:
Сидоркина И.Г., д-р техн. наук, профессор, декан факультета информатики и вычислительной техники ПГТУ;
Савинов А.Н., канд. техн. наук, доцент кафедры информационно-вычислительных систем, зам. декана по НИР факультета информатики и вычислительной техники;
Морохин Д.В., канд. техн. наук, доцент, и.о. зав. кафедрой информационно-вычислительных систем;
Кревецкий А.В., канд. техн. наук, профессор, зав. кафедрой информатики;
Бородин А.В., канд. экон. наук, профессор, зав. кафедрой информатики и системного программирования.

И 62 **Инженерные кадры – будущее инновационной экономики России:** материалы V Всероссийской студенческой конференции (Йошкар-Ола, 5-8 ноября 2019 г.): в 8 ч. *Часть 4: Информационные технологии – основа стратегического прорыва в современной промышленности.* – Йошкар-Ола: Поволжский государственный технологический университет, 2019. – 174 с.
ISBN 978-5-8158-2133-0
ISBN 978-5-8158-2137-8 (Ч. 4)

В рамках Всероссийской студенческой конференции представлены результаты научно-исследовательских работ студентов, магистрантов, аспирантов в области информационных технологий, компьютерных сетей, искусственного интеллекта, информационной безопасности, робототехники с перспективой их практического использования.

УДК 378:62
ББК 74.48:30

ISBN 978-5-8158-2137-8 (Ч. 4)
ISBN 978-5-8158-2133-0

© Поволжский государственный технологический университет, 2019

ПРЕДИСЛОВИЕ

Современные методы и подходы в области информационных технологий на основе широкого использования последних достижений науки и техники предъявляют сегодня новые требования к уровню подготовки инженерных кадров. Будущие специалисты-профессионалы должны быстро воспринимать передовые знания и воплощать их в практической деятельности. Помогает выработать необходимые навыки сочетание учебно-образовательной и научно-исследовательской деятельности.

В настоящем издании представлены материалы секции «Информационные технологии – основа стратегического прорыва в современной промышленности» Всероссийской студенческой конференции «Инженерные кадры – будущее инновационной экономики России», которая проходила в рамках одноименного форума 5-8 ноября 2019 года в Поволжском государственном технологическом университете.

Все студенты, магистранты, аспиранты ПГТУ и других вузов из различных регионов РФ своим участием в данной конференции внесли большой вклад в свое будущее и в будущее инженерных кадров Российской Федерации.

Тематика секции связана с применением информационных технологий в современном производстве. Материалы конференции отражают результаты молодежных исследований в актуальных областях:

- информационные технологии;
- компьютерные технологии;
- информационная безопасность;
- искусственный интеллект;
- робототехника.

Статьи, предложенные для публикации, рассмотрены программным комитетом конференции. Лучшие из них включены в настоящий сборник. По результатам представленных сообщений многие из авторов отмечены дипломами соответствующей степени.

Оргкомитет и редакционная коллегия сборника выражают искреннюю благодарность участникам конференции, их руководителям и консультантам за высокий уровень докладов. Будем рады видеть Вас в следующем году с новыми актуальными и интересными исследованиями.

УДК 836.2

Ахметзянова Лейсан Рустемовна
направление «Информационная безопасность» (специалитет), гр. БИ 41

Научный руководитель: **Сидоркина Ирина Геннадьевна**
доктор технических наук, профессор кафедры ИБ
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ИММУННАЯ СИСТЕМА ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

Одной из центральных проблем компьютерной безопасности является определение разницы между нормальной и потенциально вредной деятельностью разработчиков. В течение полувека разработчики защищали свои системы с помощью правил, которые могли идентифицировать и заблокировать определенные события. Тем не менее, характер нынешних и будущих угроз в сочетании с все более крупные ИТ-системами требуют срочной разработки автоматизированных и адаптивных средств защиты. И появляется перспективное решение в виде биологически мотивированных вычислений, в частности, искусственных иммунных систем.

Иммунная система человека может обнаруживать вредные вещества и защищаться от них ранее невиданных захватчиков, так что может ли подобная система быть построена для наших компьютеров? Сейчас мы это рассмотрим.

В последнее время появилось достаточно большое количество моделей, использующих иммунные системы в своей основе либо в качестве ключевых узлов. Иммунные системы часто применяются для решения задач оптимизации и классификации, также искусственные иммунные сети применяются для сжатия информации, машинного обучения, кластеризации, обработки неструктурированных данных, поиска аномалий и извлечения информации, компьютерной безопасности и адаптивного контроля. Если сравнивать с популярными ныне генетическими алгоритмами, которые обычно имеют тенденцию к изменению всей популяции, иммунные алгоритмы используют только лучшие найденные решения, что может эффективно использоваться в задачах мультимодальной оптимизации.

Следует отметить, что направления исследований иммунных систем в данный момент можно формализовать как активную стадию

применений и исследований взаимосвязи природных и компьютерных систем.

В иммунной системе существует различные методы предотвращения вторжений, одним из которых являются системы обнаружения вторжений (СОВ), используемым для защиты компьютерных систем. Основной целью являются данные системы, они должны выявлять несанкционированное использование, неправомерное использование и злоупотребление компьютерными системами со стороны инсайдеров обеих систем и внешних злоумышленников. СОВ реализуют два основных подхода: обнаружение аномалий и обнаружение злоупотреблений.

Учитывая выше сказанное, показана аналогия (см. таблицу 1) между иммунной системы человека (ИСЧ) и системой обнаружения вторжений.

Таблица 1. Сравнение ИСЧ и СОВ.

Характеристика	ИСЧ	СОВ
1. Врожденный иммунитет	Воспаления	Обнаружение неизвестных вирусов
2. Адаптивный иммунитет	Реакция организма	Специфические механизмы распознавания вторжений
3. Распознавание вируса	Сбор данных образца вируса	Выделение и пересылка
4. Дальнейшая защита	Выработка вакцины	Выработка обновленной антивирусной базы

Таким образом, можно сделать вывод, что ИСЧ во многом послужила для создания и реализации СОВ, которое привело, в свою очередь, к актуальности данной темы. По принципу искусственной иммунной системы можно обнаруживать ранее невиданные и вредоносные вирусы и защищаться от них, что позволяет нам использовать эту систему для своих компьютеров.

Список литературы

1. Р. А. Голдсби, Т. Дж. Киндт, Б. А. Осборн и В. Х. Фриман. Куби Иммунология. У. Х. Фриман, 5-е издание, 2002.

2. Д. В. Ким. Интеграция искусственных иммунных алгоритмов для обнаружения вторжений. Кандидатская диссертация, университет Колледж Лондон, 2002.

3. У. Айккелин, Дж. Гринсмит и Дж. Твикросс «Подходы иммунной системы к обнаружению вторжений". В трудах ICARIS-2004, 3-я Международная конференция по искусственным иммунным системам LNCS 3239, стр. 316-329, Катания, Италия. 2004.
4. Ю.О. Чернышев, Г.В. Григорьев, Н.Н. Венцов «Искусственные иммунные системы: обзор и современное состояние», текст научной статьи по специальности «Кибернетика», с.137.
5. А.У. Актаева, Р. Ниязова, Н. Гагарина «Искусственной интеллектуальной системы для обнаружения вторжений», Текст научной статьи по специальности «Автоматика. Вычислительная техника», с.49-50.

УДК 004.05

Белоусов Константин Михайлович
направление Информатика и вычислительная техника
(магистратура), гр. ИВТм-22

Научный руководитель: **Кубашева Елена Сергеевна**
канд. техн. наук, доцент кафедра ИВС
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

РАЗРАБОТКА АЛГОРИТМА И МЕТОДИКА ОЦЕНКИ КАЧЕСТВА ПРОГРАММНОГО ПРОДУКТА

В статье рассматривается задачаусовершенствования методики оценки качества программного продукта.

Web-сайты являются специфическим видом информационных ресурсов, значение которых в вопросах удовлетворения информационных потребностей широкого круга пользователей, неуклонно возрастает. Разнообразные способы подачи и размещения информации «на просторах» сети, а также недостаточная научная проработка и систематизация соответствующего опыта, делает чрезвычайно актуальной разработку методов контроля, гарантирующих не только качество готового программного продукта (сайта), но и повышение эффективности его использования.

Любой пользователь информационного ресурса, будь это рядовой пользователь или генеральный директор крупной компании, заказавший сайт для своего бизнеса, хочет видеть качественный контент. Данная проблема уже затрагивалась не одним человеком. Одним из наиболее авторитетных специалистов в области исследования сайтов в США является профессор Джени Стоуэрс. В его работе:«Измеряя электронное правительство» основное внимание уделено разнообразию

методов, используемых для оценки правительственной веб-инфраструктуры [1]. Оценке качества сайта свое исследование посвятил Добрынин Сергей в работе:«Анализ сайта. Оценка сайта по качеству». Также существует ГОСТ Р ИСО/МЭК 25021-2014 «Информационные технологии (ИТ)» для оценки качества программных продуктов.

Анализ, предложенных разными авторами методов, показал отличие в пути оценивания сайта. Предложенная в работе методика качественно отличается от анализируемых тем, что основывается на существующем стандарте ГОСТ Р ИСО/МЭК 9126-93 «Оценка программной продукции» и содержит максимальное число оцениваемых параметров. Представленный алгоритм позволяет оценить сайт наиболее быстро и эффективно.

Целью представленной работы является поиск путей совершенствования методики оценки качества web-сайтов, путем оценивания всех качественных характеристик (функциональность, надежность, практичность, сопровождаемость и мобильность).

Функциональность содержит такие характеристики как: правильность, пригодность для применения, способность к взаимодействию, защищенность. Правильность предполагает корректное отображение данных на сайте. Пригодность для применения подразумевает собой полезность. Способность к взаимодействию означает работоспособность на любой аппаратной и программной платформе. Защищенность сайта показывает защиту от взлома.

Надежность детализируется следующими свойствами: уровнем завершенности и восстанавливаемостью. Уровень завершенности означает отсутствие на сайте ошибок. Восстанавливаемость отражает возобновление нормальной работы сайта после кратковременного отказа. Сайт должен максимально быстро восстановиться после ошибок, допущенных пользователем.

Следующим показателем для оценивания является практичность. Она описывается понятностью и простотой использования. Понятность предполагает легкое восприятие сайта пользователем. Простота использования означает удобство и быстрый поиск необходимой информации.

Сопровождаемость описывается стабильностью и изменяемостью. Стабильность характеризует сайт с точки зрения легкого возврата к прежней версии. В коде без особого труда можно убрать строки с модификацией. Изменяемость описывается простотой изменения сайта. Для мелких корректировок сайта можно обойтись простым текстовым редактором.

Показатель мобильности содержит такие характеристики, как: адаптируемость, простота инсталляции. Адаптируемость показывает возможность сайта работать на любом программном обеспечении. Простота инсталляции показывает возможность функционирования сайта при любом наборе программного обеспечения.

Новизна исследования заключается:

1. В разработке новой методики оценки качества программных продуктов, позволяющей оценить сайт, как со стороны дизайнерского решения, так и информационной полезности;

2. В обосновании целесообразности предложенного метода, отличающегося от рассмотренных более подробным рассмотрением (рассматриваются все качественные характеристики сайта любого профиля, не только правительственного), позволяющего разработчику узнать слабые стороны программного продукта (сайта).

Таким образом, с развитием информационных технологий и многообразием видов подачи информации, создание алгоритмов и методики оценки качества программных продуктов, в нашем случае сайтов, является актуальной задачей.

Список литературы

1. Добрынин С. Анализ сайта. Оценка сайта по качеству. - 2009.

2. ГОСТ Р ИСО/МЭК 25021-2014 «Информационные технологии (ИТ)». 2014.

3. ГОСТ Р ИСО/МЭК 9126-93 «Оценка программной продукции». 1994.

УДК 004.415.24

Бородин Андрей Викторович
направление Информационная безопасность (магистратура), гр. ИБм-11

Научный руководитель: **Чекулаева Елена Николаевна,**
канд. экон. наук, доцент кафедры информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ВАРИАНТ ПОСТАНОВКИ ЗАДАЧИ ПРОТИВОДЕЙСТВИЯ РЕВЕРС-ИНЖИНИРИНГУ КОДА В РАМКАХ ИМПЕРАТИВНОЙ ПАРАДИГМЫ ПРОГРАММИРОВАНИЯ

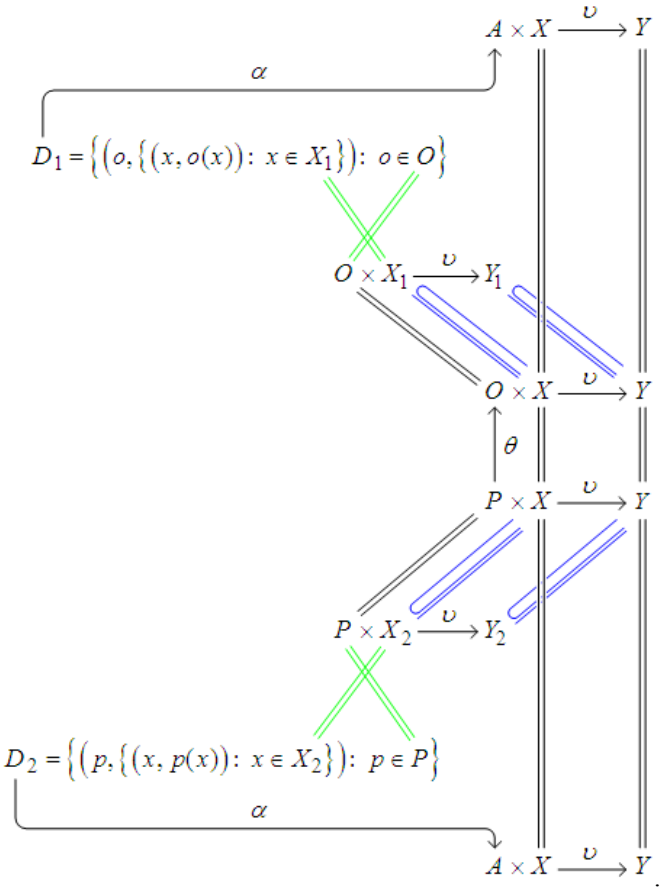
Проблема защиты интеллектуальной собственности в последние годы становится все более и более актуальной. Связано это, как с

взрывным ростом количества новых идей, продуктов и технологий, так и с упрощением процедур их описания и реализации. Информационные технологии здесь оказались катализатором инновационного процесса. Они предложили гигантское множество простых для пользователя инструментов поддержки инновационной деятельности и постарались, по возможности, предложить технологии защиты интеллектуальной собственности. В то же время, очевидно, что прогресс в развитии простых и удобных в эксплуатации инструментальных средств поддержки инноваций существенно опережает создание и развитие инструментария защиты интеллектуальной собственности [1]. В ряду инструментальных средств, для которых справедливо все выше сказанное, можно отметить продуктовую линейку Microsoft Office, многие популярные продукты компаний Corel, MindJet, CA Technologies и т. д. Эти программные средства благодаря поддержке языка программирования Visual Basic for Applications (VBA) [4] взяли на себя роль метасистем – инструментов создания инноваций в области программного обеспечения, в том числе со стороны прикладных специалистов, не считавших себя ранее специалистами в области программирования.

Другой связанной проблемой является задача снижения вероятности нарушения целостности программного обеспечения, функционирующего на недоверенных хостах некоторой вычислительной сети [2].

Обе описанные проблемы, так или иначе, связаны с решением злоумышленником задачи реверс-инжиниринга программного кода. При этом базовыми технологиями противодействия этой угрозе являются технологии обфускации. Исследование проблем обфускации, таким образом, является задачей крайне актуальной.

Рассмотрим классическое определение обфускации. Для этого, в начале, рассмотрим следующую коммутативную диаграмму [3]:



Здесь использованы следующие обозначения: P – множество программ; X – множество исходных данных для программ из множества P; Y – множество результатов выполнения программ из множества P с исходными данными из множества X; υ – отображение, реализуемое вычислителем (компьютером); O – множество обфусцированных программ; θ – отображение, реализуемое обфускатором (специальной программой некоторого вычислителя); X_1 – некоторое подмножество множества X, $X_1 \subseteq X$, на диаграмме это отношение представлено соответствующим удлиненным знаком; Y_1 – подмножество множества Y, $Y_1 \subseteq Y$, содержащее результаты выполнения обфусцированных программ из множества O с исходными данными из множества X_1; D_1 –

наблюдаемое атакующим субъектом множество обфусцированных программ с некоторой частью примеров их выполнения, определяемой множеством X_1; A – множество, реконструированных атакующим субъектом программ на основе исследования элементов множества D_1 (или D_2) с использованием алгоритма реконстукции (рефакторинга), представленного на диаграмме отображением α; X_2 – некоторое подмножество множества X, $X_2 \subseteq X$; Y_2 – подмножество множества Y, $Y_2 \subseteq Y$, содержащее результаты выполнения программ из множества P с исходными данными из множества X_2; D_2 – наблюдаемое атакующим субъектом множество исходных программ с некоторой частью примеров их выполнения, определяемой множеством X_2; две параллельные линии – суть биекция.

Введенная таким образом модель предметной области может быть использована для построения определения обфускации.

Определение. Алгоритм θ назовем обфускатором для класса программ P, если справедливы следующие три свойства.

1) Сохранение функциональности:

$$\forall p\,(p \in P)\,\forall x\,(x \in X)\left[\theta(p)(x) = p(x)\right].$$

2) Не более чем полиномиальное снижение эффективности:

$$\forall p\,(p \in P)\left[\left|\theta(p)\right| \le \pi_s\left(|p|\right)\right],$$

$$\forall p\,(p \in P)\,\forall x\,(x \in X)\left[\tau\left(\theta(p)(x)\right) \le \pi_t\left(\tau\left(p(x)\right)\right)\right],$$

где $|p|$ – сложность программы p по объему кода; $\pi_\bullet$ – некоторая полиномиальная функция; $\tau\left(p(x)\right)$ – время выполнения программы p с исходными данными x.

3) Стойкость к реконструкции:

$$\forall p\,(p \in P)\left[\tau\left(\alpha\middle|D_1, O = \{\theta(p)\}\right) >> \tau\left(\alpha\middle|D_2, P = \{p\}\right)\right],$$

где $\tau\left(\alpha\middle|D_1, O = \{\theta(p)\}\right)$ – время исполнения сужения отображения α на множество D_1 для случая, когда множество O содержит один элемент – результат обфускации программы p; $\tau\left(\alpha\middle|D_2, P = \{p\}\right)$ – время исполнения сужения отображения α на множество D_2 для случая, когда множество P содержит один элемент – программу p.

Прорывная работа [5] ознаменовала новый этап в создании стойких обфускаторов. Однако в практическое русло эти разработки вплоть до настоящего времени не вошли.

В настоящей статье предлагается модификация приведенного определения обфускации в части третьего условия – стойкости к реконструкции:

$$\exists X_1, X_2 \left(X_1 \neq X_2\right) \ \forall p \left(p \in P\right) \ \exists \theta$$
$$\left[\tau\left(\alpha \middle| D_1 = \left\{\left(\theta(p), \left\{\left(x, o\left(\theta(p)\right)\right) : \ x \in X_1\right\}\right)\right\}\right) >>$$
$$\tau\left(\alpha \middle| D_2 = \left\{\left(p, \left\{\left(x, p(x)\right) : \ x \in X_2\right\}\right)\right\}\right)\right].$$

Представляется, что в контексте нового варианта определения возможно существование стойких обфускаторов, которые могут быть относительно легко реализованы на практике в рамках императивной парадигмы программирования.

Список литературы

1. Бородин, А. В. Линейные конгруэнтные последовательности максимального периода в задачах обфускации программ / А. В. Бородин // Кибернетика и программирование. – 2016. – № 6. – С. 1-19. – DOI: 10.7256/2306-4196.2016.6.18499.

2. Бородин, А. В. О задаче контроля целостности программного обеспечения удаленного недоверенного хоста / А. В. Бородин, А. А. Старовойтов // Актуальные направления научных исследований: перспективы развития: материалы III Международной научно–практической конференции (Чебоксары, 8 октября 2017 г.). – Чебоксары: ЦНС «Интерактив плюс», 2017. – С. 119-123. – DOI: 10.21661/r-464620.

3. Львович, И. Я. Перспективные тренды развития науки: техника и технологии. Т. 1 / И. Я. Львович, В. А. Некрасов, А. П. Преображенский и др. – Одесса: КУПРИЕНКО СВ, 2016. – 197 с.

4. Михеев, Р. Н. VBA и программирование в MS Office для пользователей / Р. Н. Михеев. – СПб.: БХВ-Петербург, 2006. – 384 с.

5. Garg, S. Candidate indistinguishability obfuscation and functional encryption for all circuits / S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, B. Waters // 54th Annual Symposium on Foundations of Computer Science, FOCS 2013, October 2013. – Berkeley: IEEE Computer Society, 2013. – P. 40-49. – DOI: 10.1109/FOCS.2013.13.

УДК 629.7.05

Вагапова Регина Юнировна
направление Информатика и вычислительная техника (магистратура),
гр. ИВТм-12

Научный руководитель: **Васяева Елена Семеновна**
к.т.н., доцент
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ ИССЛЕДОВАНИЯ МОДЕЛЕЙ СИСТЕМ ОБРАБОТКИ ДАННЫХ

Цель работы– разработка архитектуры информационно-обучающего программного комплекса, для проведения компьютерныхэкспериментов и исследования различных моделей современныхвычислительных систем.

Актуальность.В настоящее время для обучения студентов активно используются электронные обучающие курсы и системы. Они позволяют представить нужный материал наглядно, проводить эксперименты и анализировать результат. Такой подход значительно облегчает процесс обучения для студентов и позволяет закреплять полученные знания.

На кафедре ИВС Поволжского государственного технологического университета почти 20 лет назад была разработана программа для выполнения лабораторных работ по дисциплинам, связанным с организацией ЭВМ и вычислительных систем. Однако современные подходы и требования к образованию и возможности нынешних средств разработки информационных систем сделали актуальной задачу создания новой версии данной программы, расширенной как по функционалу, так и концептуально. Можно сформулировать основное требование к новой системе – помощь студентам в овладении знаниями и навыками по созданию и исследованию на ЭВМ моделей вычислительных средств, проверки адекватности моделей исследуемым объектам при различных режимах работы ЭВМ и ВС, правильной интерпретации полученных результатов применительно к конкретным структурным решениям и заданным классам решаемых задач.

Анализ имеющейся системы проводился с точки зрения требований как студента, так и преподавателя, и выявил следующие недостатки:

- отсутствует возможностьувеличивать количество вариантов заданий и корректировать исходные данные для лабораторных работ;

• жёстко задан перечень графиков, которые можно построить при проведении исследований;

• невозможно корректировать диапазон и шаг исследуемых параметров при построении графиков;

• нет заданий для закрепления материала (хотя бы в виде теста);

• нет возможности автоматического оценивания работы студента в данной системе.

Исходя из недостатков имеющейся системы, были определены требования к разрабатываемому программному продукту:

• информационная система должна содержать блок настройки тестовых заданий, проведения тестирования и формирования промежуточных и итоговых отчетов о результатах усвоения материала;

• система должна обладать гибким функционалом для настройки графиков при проведении исследований, чтобы можно было оценить степень понимания студентом процесса проведения исследований от постановки цели до формулирования выводов;

• программный продукт должен предусматривать идентификацию пользователей в системе для реализации возможности одновременной работы нескольких пользователей;

• исходные данные по вариантам должны храниться в отдельном файле, который преподаватель сможет отредактировать при необходимости;

• должен быть реализован механизм ввода граф-схем алгоритмов (для увеличения количества вариантов работ) по таблице смежности.

На рис. 1 приведена структура информационной системы «Исследование моделей систем обработки данных». Для реализации системы был выбран язык программирования Python. Он поддерживает объектно-ориентированное программирование. Описание интерфейса осуществляется с помощью кроссплатформенного фреймворкаQt. Python позволяет запускать написанное с его помощью программное обеспечение в большинстве современных операционных систем путём простой компиляции программы для каждой системы без изменения исходного кода. Включает в себя все основные классы, которые могут потребоваться при разработке прикладного программного обеспечения, начиная от элементов графического интерфейса и заканчивая классами для работы с сетью, базами данных и XML. Является полностью объектно-ориентированным, расширяемым и поддерживающим технику компонентного программирования.

Рис. 1. Структура информационной системы «Исследование моделей систем обработки данных»

Выводы. Разрабатываемая система нацелена на устранение недостатков, выявленных при работе с имеющемся программным продуктом по исследованию моделей систем обработки данных.Разнообразие задач и тематики лабораторных занятий позволит активизировать познавательную деятельность студентов и использовать многообразие методов стимулирования эффективности усвоения комплекса знаний: учебный эксперимент, работу с книгой, обсуждение теоретических положений и применимости на практике результатов, полученных при выполнении лабораторных работ.

Список литературы

1. Исследование моделей систем обработки данных: лабораторный практикум / Е. С. Васяева, Н. С. Васяева, А. А. Власов. - Йошкар-Ола: Поволжский государственный технологический университет, 2019. – 148 с.

2. Основы теории вычислительных систем: Учебное пособие / Под редакцией С. А. Майорова. – М.: Высш. шк., 1978. – 408 с.

УДК 004.4'23

Ванясин Никита Вадимович
Направление:05.13.19, аспирант каф. ИБ

Научный руководитель: **Сидоркина Ирина Геннадьевна**
доктор технических наук, профессор кафедры ИБ
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ПОЛЬЗОВАТЕЛЬСКИЙ ИНТЕРФЕЙС ИНТЕГРИРОВАННОЙ СРЕДЫ РАЗРАБОТКИ СО СТРУКТУРНЫМ РЕДАКТОРОМ

Структурно любая программа представляется в виде иерархии, также известной как абстрактное синтаксическое дерево (АСД). Это дерево строится на основе исходного текста при помощи *сканера* и *парсера*. С улучшением программных языков и сред, укреплялось мнение, что синтаксическое дерево может быть показано на экране напрямую. АСД можно визуально изобразить в виде вложенных блоков, специальной разметки, а также отступов для выделения языковых конструкций. Так появилась концепция структурного редактора.

Структурный редактор позволяет пользователю взаимодействовать с АСД напрямую при помощи взаимодействия с узлами дерева – языковыми конструкциями. В этом случае, языковые конструкции становятся новыми “неделимыми частями” программы, в отличии от символов и строк текста. Также, в данном случае отсутствует шаг перевода исходного текста программы в АСД (для последующих действий) и обратно (для сохранения в виде файла).

В противовес современным текстовым редакторам, которые можно назвать “осведомленными о языке”, структурные редакторы являются “управляемыми языком”. Это накладывает более строгие ограничения на редактирование, потому что каждое изменение происходит над конкретной языковой конструкцией, а не над набором символов или строк. Синтаксис и грамматика языка определяют, какие языковые конструкции могут быть использованы в текущем контексте и редактор предоставляет выбор пользователю [1].

В ходе исследований [2][3] была предложена архитектура интегрированной среды разработки со структурны редактором и разработан прототип среды разработки для языка Go.

Интерфейс взаимодействия с пользователем

Пользовательский интерфейс для взаимодействия пользователя со средой разработки. Предоставляет собой структурный редактор для

исходного кода и широкий набор функциональных возможностей для разработки программного обеспечения: отладчик, средства рефакторинга, интерфейс для системы контроля версий, навигацию по исходному коду проекта, быстрый поиск, автодополнение и др. Внешний вид пользовательского интерфейса представлен на Рисунке 1.

На рисунке можно видеть основные компоненты пользовательского интерфейса:

- В верхней части расположено главное меню приложения. Позволяет пользователю запустить все возможные команды в рамках текущего контекста. Состоит из набора подменю, сгруппированных по логике действий: Проект, Редактирование, поиск, Вид, Код, Рефакторинг, Запуск, Помощь.
- В левой части расположено отображение «SolutionExplorer» (Обзор структуры проекта). Позволяет пользователю видеть и редактировать структуру проекта. Возможна организация модулей проекта в виде вложенных папок. При помощи двойного клика можно открыть модуль для редактирования.

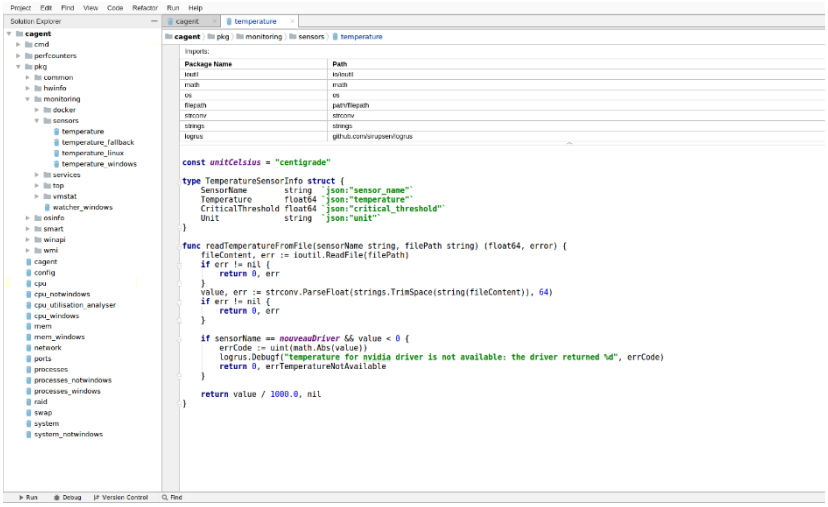


Рис. 1 - Внешний вид пользовательского интерфейса предложенной среды разработки со структурным редактором

- В центральной части видно основную рабочую область редактора – список вкладок с исходным кодом ПО. Каждая открытая вкладка с кодом состоит из:
  - Компонента «хлебные крошки» для отображения текущего

местоположения курсора в иерархической структуре модуля. Доступна навигация при помощи клика по элементам компонента.

- Таблицы импорта. Отображает список зависимых пакетов для текущего модуля. В основном формируется автоматически, но пользователь может задать альтернативное имя для импорта (alias), а также создать «пустой» импорт.
- Области редактирования. Содержит сам структурный редактор для АСД модуля. Навигация по дереву возможна при помощи клавиш клавиатуры, а также мыши. Все действия над грамматическими конструкциями можно выполнять как при помощи клавиатуры, так и кликов мышью.

- В нижней части расположена панель для управления отображением дочерних окон, таких как окно «Запуск», «Отладка», «Система Контроля Версий» и «Результаты поиска».

Предложенный пользовательский интерфейс структурного редактора обладает множеством преимуществ и выделяется среди известных аналогов[4]:

- **Атомарность изменений** гарантирует, что языковые конструкции добавляются, перемещаются, переименовываются или удаляются целиком, а не частично;
- **Соответствие грамматике.** Следование грамматики языковых конструкций гарантирует корректную вставку или вложенность узлов АСД – каждый узел может содержать только такие узлы, которые могут быть вставлены в соответствии с грамматикой языка;
- **Удобство использования**. Так как структурный редактор имеет больше знаний о редактируемой программе и семантике изменений [5], он может предложить более продвинутый обратный отклик для пользователя и перечислить только корректные варианты автодополнения в зависимости от текущего контекста [6];
- **Расширяемость и встраивание.**Структурный редактор может предоставлять платформу для расширения языка программирования аналогично макросам в таких языках как C++. Возможно внедрение блоков программного кода на другом языке программирования без ущерба читаемости и структуре кода;
- **Отслеживание семантики изменений**позволяет сохранять в системе контроля версий не изменения символов и строк файла, а изменений грамматических конструкций, например

переименование метода или факт осуществления рефакторинга [8];

- **Упрощение обучения языкам программирования** за счет расширенной осведомленности о контексте – пользователю не нужно обращаться к документации или справке, чтобы узнать, какие языковые конструкции он может использовать в данном конкретном узле синтаксического дерева.

Заключение

Предложенный пользовательский интерфейс позволяет добиться улучшения производительности разработчика программного обеспечения по множеству параметров. Экспериментальные исследования, проведенные в [8], подтверждают эффективность разработанной среды разработки со структурным редактором. Кроме того, разработанной структурный редактор прошел апробацию в организациях, занимающихся промышленной разработкой программного обеспечения и принят в качестве одного из инструментов разработки в рабочий процесс.

Список литературы

1. Ballance, Robert A.; Graham, Susan L.; Van De Vanter, Michael L. (1990). "Pan language-based editing system for integrated development". SDE 4: Proceedings of the fourth ACM SIGSOFT symposium on Software development environments. Irvine, CA: ACM Press. pp. 77–93.

2. Vaniasin N.V., Sidorkina I.G. Semantic source code editing in Integrated Development Environments // Economics, Management, Information and Technology EMIT. – 2018. Vol. 5. №2 – С. 48-53.

3. Ванясин Н.В., Сидоркина И.Г. Структурный редактор для семантического редактирования исходного кода // Труды Конгресса по интеллектуальным системам и информационным технологиям «IS&IT`18» Таганрог: Изд-во Ступина С.А., 2018. Т.2 – С. 127-134.

4. Voelter M. et al. Towards user-friendly projectional editors // International Conference on Software Language Engineering. – Springer, Cham, 2014. – С. 41-61.

5. Мучник Т.Г. Языково-настраиваемый структурный редактор со средствами семантического контроля // Программирование. – 1990. – № 2.

6. Clark T. A general architecture for heterogeneous language engineering and projectional editor support //arXiv preprint arXiv:1506.03398. – 2015.

7. FowlerM. Languageworkbench [Электронный ресурс] - [2008] - URL: https://martinfowler.com/bliki/LanguageWorkbench.html (дата обращения: 23.03.2019).

8. Ванясин Н.В., Сидоркина И.Г. Анализ функциональных возможностей структурных редакторов исходного кода программного обеспечения //. Вестник ПГТУ. Серия «Радиотехнические и инфокоммуникационные системы» —

Йошкар-Ола: Поволжский Государственный Технологический Университет, 2019. – С. 64-77.

УДК007.3

Варламова Татьяна Валерьевна
направление Прикладная информатика (магистратура), гр. ПИм-11

Научный руководитель: **Бородин Андрей Викторович**
к. э. н., профессор кафедры информационных систем в экономике
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

АНАЛИЗ РИСКОВ МОДЕРНИЗАЦИИ СИСТЕМЫ БЮДЖЕТИРОВАНИЯ ПРЕДПРИЯТИЯ

На сегодняшний день одним из путей повышения эффективности финансового планирования и управления на предприятии является внедрение и модернизация системы бюджетирования(СБ). Основу данной системы составляет бюджет движения денежных средств и бюджет доходов и расходов, где подробно отражена структура затрат предприятия, информационной базой для составления служат счета бухгалтерского и налогового учета. Внедрение и модернизацияСБ должна снизить нагрузку на контролирующий орган, избавиться от узких мест и уменьшить объем документооборота, что положительно скажется на времени операционного цикла выделения денежных средств. Проведение модернизации СБ будет способствовать ее эффективному функционированию, что позволит формировать более качественную информационную базу системы управления.

Для модернизации СБ необходим переходный период, который потенциально может быть источником проблем и, следовательно, убытков.Целью данной работы является разработка подходов к минимизации указанных издержек.

Процесс модернизации СБ можно рассматривать как процесс риска. Для построения модели управления риском будем использовать методологию, предложенную в цикле статей[1, 3].

Отправной точкой для автоматизированного построения имитационных моделей процесса внедрения может стать онтологическая модель процесса риска, включающая в себя не только факторы риска, но и описание системы мер по их снижению, и/или ограничению, и/или компенсации, и/или т. п. Для формального

представления такой расширенной онтологической модели удобно использовать нотацию IDEF5 [2]. Для нашего случая онтологическая модель процесса риска представлена на рисунке 1. Словарь модели представляет таблица 1.

Используя предложенную онтологическую модель, можно в автоматизированном режиме построить имитационную модель. Если в качестве критерия оптимальности выбрать совокупную стоимость владения объектом внедрения [4] и, учитывая случайный характер этой величины, использовать подходящую меру риска [5], то можно выбрать оптимальный вариант внедрения СБ. Таким образом, в данной работе выявлены и классифицированы риски процесса модернизации СБ предприятия, а также предложена система мер по компенсации этих рисков. Полученная онтологическая модель предметной области может быть использована в дальнейшем для построения соответствующей имитационной модели.

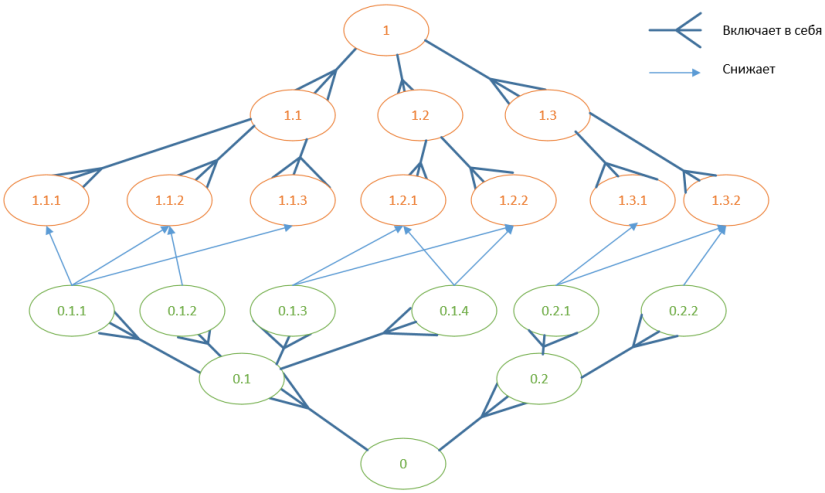


Рис. 1 – Онтологическая модель процесса риска модернизации системы бюджетирования предприятия

Таблица 1. Словарь модели процесса риска модернизации СБ предприятия

ID	Описание факторов риска / мер по компенсации риска
0	Меры по снижению рисков
0.1	Организационные мероприятия
0.1.1	Создание комитета по исполнению модернизации СБ

0.1.2	Формирование плана восстановления данных
0.1.3	Создание комитета по изменениям внешней и внутренней среды
0.1.4	Разработка сценариев работы по изменениям внешней и внутренней среды
0.2.	Инфраструктурная поддержка.
0.2.1	Обеспечение возможности параллельной опытной эксплуатации в ограниченном масштабе
0.2.2	Наличие ресурсов для параллельной эксплуатации
1	Риски модернизации СБ
1.1.	Риск исполнения
1.1.1	Риск обнаружения противоречивых требований
1.1.2	Риск потери данных
1.1.3	Риск нарушения сроков выпуска
1.2	Риск изменений
1.2.1	Риск изменений внешней среды
1.2.2	Риск изменений внутренней среды предприятия
1.3	Эксплуатационный риск
1.3.1	Риск отказа в обслуживании
1.3.2	Риск качества реализации

Список литературы

1. Бородин, А. В. Методологические основы моделирования в задачах экономики безопасности / А. В. Бородин // Современные проблемы и перспективы социально-экономического развития предприятий, отраслей, регионов. – Йошкар-Ола: Поволжский государственный технологический университет, 2014. – С. 217-222.

2. Бородин, А. В. Метод онтологического анализа IDEF5 в задачах структурного синтеза динамических моделей угроз / А. В. Бородин // Обозрение прикладной и промышленной математики. – 2006. – Т. 13. – № 3. – С. 474.

3. Бородин, А. В. Онтологические модели в экономике безопасности / А. В. Бородин // Труды Поволжского государственного технологического университета. Серия: Социально-экономическая. – Йошкар-Ола: Поволжский государственный технологический университет, 2014. – №2. – С. 14-19.

4. Уразаева, Т. А. Методология оценки эффективности оптимизационных моделей управления инвестициями / Т. А. Уразаева // Безопасность человека, общества, природы в условиях глобализации как феномен науки и практики. Девятые Вавиловские чтения: сборник статей. – Йошкар-Ола: МарГТУ, 2006. – С. 211-216.

5. Уразаева, Т. А. Риск и его измерение / Т. А. Уразаева // Актуальные проблемы современной экономики. – Йошкар-Ола: МарГТУ, 2006. – С. 259-266.

УДК 004.056

Васильева Елена Сергеевна
направление Информационная безопасность
автоматизированных систем (специалитет), гр. БИ-32

Научный руководитель: **Смирнов Владимир Иванович**
старший преподаватель кафедры информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ВОЗМОЖНОСТЬ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННЫХ ИСТОЧНИКОВ СВЕТА ДЛЯ ФОРМИРОВАНИЯ КАНАЛОВ УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ

Данная статья посвящена выявлению возможностей использования искусственных источников света для формирования каналов утечки речевой информации.

Введение

Добров М.С. и Фильчакова Ю.В. справедливо отмечают, что «нашу жизнь невозможно представить без искусственного освещения» [1]. Для жизни и работы человеку необходимо освещение с применением различных ламп. Наиболее часто встречаются лампы накаливания, люминесцентные и светодиодные энергосберегающие лампы. Искусственное освещение также используют в выделенных помещениях (ВП) или в защищаемых помещениях (ЗП). В помещениях, где ведутся конфиденциальные переговоры, утечка речевой информации возможна через осветительные приборы.

В настоящее время существует большое количество физических принципов, которые используются в создании каналов утечки информации, а также технических средств для перехвата информации. Каждое техническое средство потенциально может образовывать различные каналы утечки информации. Это обусловлено взаимосвязями технических систем: объекты внешней среды и результаты проявления физических эффектов (ФЭ), входящих в их состав.

Физические схемы (ФСх) лампы накаливания и лампы дневного света при воздействии на них акустического (звукового) поля

Соболев А.Н. и Кириллов В.М. выявили [2], что звуковое поле вызывает колебания стенок колбы лампы, проявляется эффект возникновения упругих колебаний (эффект Гука). В свою очередь, это вызывает изменение светопроводимости баллона лампы, результат

которого – модулирование звуковым полем светового потока. Таким образом, простейшая система (лампа накаливания) позволяет создавать канал утечки речевой информации (рис. 1).

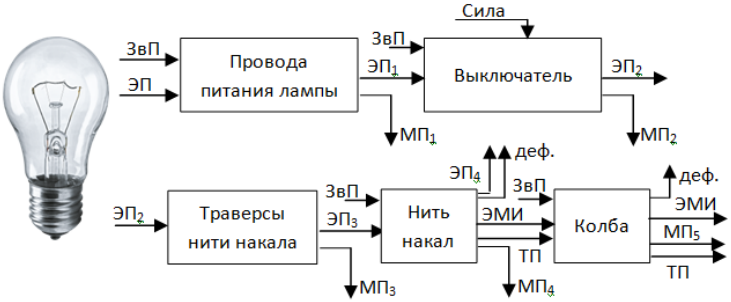


Рис. 1. - Лампа накаливания и её ФСх при воздействии на неё акустического (звукового) поля

Аналогично, лампы дневного света при воздействии на них звукового поля могут формировать канал утечки информации (рис. 2).

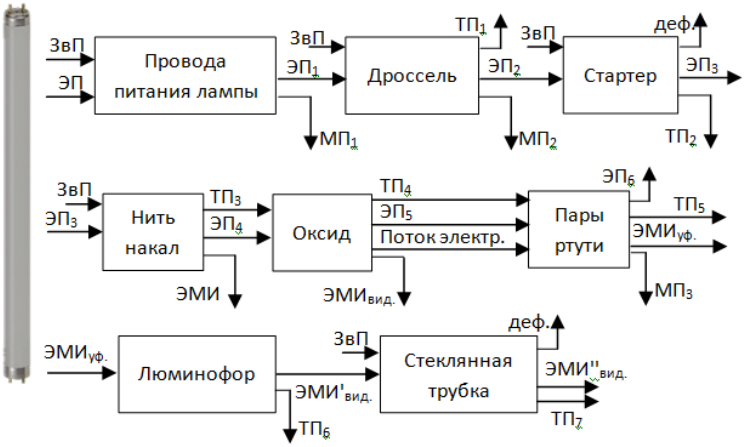


Рис. 2. - Лампа дневного света и её ФСх при воздействии на неё акустического (звукового) поля

Возможность применения других ламп для утечки информации

Внедрение мощных высокочастотных преобразователей привело к появлению потенциальных каналов утечки информации разных видов в нагревательных и осветительных устройствах, раннее бывшими вполне безопасными. Примером может служить широкое использование в настоящее время энергосберегающих ламп для освещения помещений.

Энергосберегающая лампа с защитными фильтрами на входе схемы (рис.3), фильтры позволяют предотвратить утечку несущего сигнала в сеть переменного тока. Элементная база влияет не только на технические характеристики, но и на возможность возникновения технического канала утечки речевой информации за счёт схемотехнических решений энергосберегающей лампы. Наиболее опасными элементами энергосберегающих ламп являются трансформатор и дроссель, которые могут влиять на частоту колебаний, а также обладают акустической чувствительностью [3].

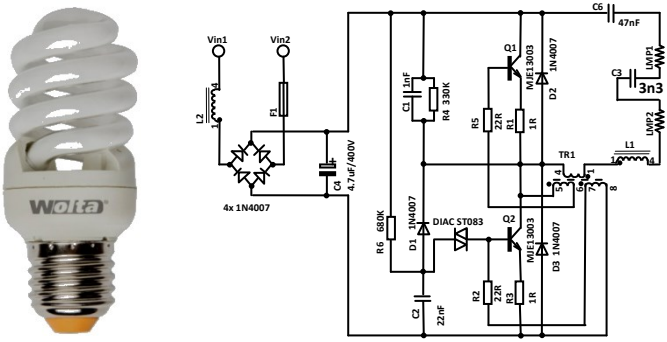


Рис. 3. - Энергосберегающая лампа Wolta и схема лампы на 11 Вт с защитными фильтрами

Anindya Maiti и Murtuza Jadliwala из Техасского университета в Сан-Антонио в работе [4] показали, что некоторые «умные» лампы можно использовать в качестве источника данных о их владельцах, а также в качестве скрытого канала передачи данных с изолированных от интернета устройств. В последние годы многие производители бытовых устройств стали оснащать их возможностью управления с внешнего устройства. Исследователи проверяли методы атак на популярных «умных» лампах Philips Hue и LIFX.

Кроме того, лампы принимают команды от любых устройств в локальной сети без авторизации. Во время эксперимента авторы кодировали данные с помощью амплитудной манипуляции, при которой уровням интенсивности излучения сопоставляются определённые значения. Они пришли к выводу, что от количества используемых уровней интенсивности сильно зависит доля ошибок при передаче данных. Исследователи показали, что «умные» лампы можно использовать для незаметной передачи данных.

Заключение

Все виды ламп создают разнообразные каналы утечки информации. Лампы накаливания являются наиболее защищёнными, а «умные»

лампы – самыми уязвимыми. Чем сложнее устроено устройство, тем сложнее обеспечить её безопасность. Разработка ФСх и их анализ позволяют выявлять потенциально возможные каналы утечки информации, а также спрогнозировать необходимые меры для того, чтобы уменьшить вероятность их появления.

Список литературы

1. Добров М.С., Фильчакова Ю.В. Сравнение характеристик энергосберегающих, люминесцентных и ламп накаливания, или как сохранить бюджет семьи? // Юный ученый. – 2017. – №2. – С. 37-39.
2. Соболев, А.Н. Физические основы технических средств обеспечения информационной безопасности: учебное пособие / А.Н. Соболев, В.М. Кириллов. – Йошкар-Ола: МарГТУ, 2004. – 232 с.
3. Кравченко В.Б., Матвеева С.В. Влияние схемотехники энергосберегающих ламп на возможность формирования канала утечки информации / В.Б. Кравченко, С.В. Тарасова // Межотраслевая информационная служба. – 2011. – С. 37-46.
4. Anindya Maiti, Murtuza Jadliwala. Light Ears: Information Leakage via Smart Lights. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2019; 3 (3): 1 DOI: 10.1145/3351256

УДК 004.056

Глозштейн Даниил Александрович
Направление Государственное и муниципальное управление (магистратура), гр. ГМУм-11(з)

Научный руководитель: **Сидоркина Ирина Геннадьевна**
доктор технических наук, профессор кафедры ИБ
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

СРАВНИТЕЛЬНАЯ ХАРАКТЕРИСТИКА СУЩЕСТВУЮЩИХ МЕТОДИК КОЛИЧЕСТВЕННОЙ ОЦЕНКИ РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Стандарты ISO 31000 определяют риск как результат неопределенности в отношении целей, где под результатом понимают отличие итога от предполагаемого, а неопределенность – состояние дефицита информации, которое напрямую связано с знаниями о событии, его последствиями или вероятностью [1]. Так как подавляющая часть рисков никогда не падает до нулевых значений,

основным способом борьбы с ними в любом масштабе действий является управление рисками. Однако эффективность принимаемых мер не превышает статистической погрешности распределения случайно величины, если действия по управлению рисками происходит раньше анализа рисков (а это особенно характерно для многих отечественных компаний).

Кроме того, даже при обстоятельном подходе к управлению рисками, стадия оценки ограничивается только качественным анализом, который мало того, что не дает конкретной информации для организации-заказчика оценки риска, но и с трудом воспринимается при взгляде со стороны, так как любое предприятие рассматривает вопросы, связанные с его бизнес-процессами, сквозь призму рентабельности. Поэтому более практичным (но и более сложным) подходом является количественная оценка рисков.

В основе количественного подхода является получение всеми элементами оценки рисков конкретных количественных значений, в соответствии с некоторым наглядным алгоритмом. В качестве объекта оценки обычно выбирают наиболее важные параметры, такие как стоимость защитных мер, вероятность реализации угрозы, ущёрб от неё, ценность актива в денежном эквиваленте и т.д. В результате количественной оценки рисков должны быть определены [3]:

- стоимость активов в численном выражении (ценность);
- наиболее детальный перечень всех угроз ИБ с расчетом однократного "срабатывания" каждой угрозы (возникновение инцидента ИБ);
- количество реализованных угроз за определенное время (частота);
- возможный ущерб от реализации;
- список рекомендуемых мер обеспечения безопасности и действий по нейтрализации каждой угрозы.

Рассмотрим наиболее часто применяемые и эффективные методы количественной оценки рисков ИБ:

1. К наиболее результативным методам количественного анализа относится метод RiskWatch. В основе метода лежит количественная оценка общих годовых потерь (Annual Loss Expectancy, ALE) и коэффициента возврата от инвестиций (Return on Investment, ROI) при внедрении средств защиты информации [5].

Реализация метода состоит из четырёх этапов:

А. Выявление предмета исследования. В ходе этого этапа проводится исследование типа организации, состава и структуры

исследуемой системы, основные требования в сфере информационной безопасности. В методе существует ряд стандартных моделей, соответствующих типу организации, категории защищаемых ресурсов объединены в соответствующие списки, потерь, угроз, уязвимостей и мер защиты информации.

Б. Описание конкретных характеристик системы с помощью ввода различных данных. Здесь требуется максимально подробно описать ресурсы, потери и классы инцидентов. которые образуются при сопоставлении категории потерь и категории ресурсов. RiskWatch включает в себя базы с оценками частот LAFE (Local Annual Frequency Estimate - показывает, сколько раз в среднем в год исследуемая угроза реализуется в исследуемом месте) и SAFE (Standard Annual Frequency Estimate - показывает, сколько раз в среднем в год исследуемая угроза реализуется в исследуемой области), которые помогают определить итоговую частоту возникновения для каждой угрозы.

В. На следующем этапе производится непосредственно количественная оценка рисков. Здесь каждому риску присваивается определённое значение и производится выбор мер обеспечения безопасности. Для каждой из контрмер определяется стоимость внедрения, стоимость поддержки, время жизни и текущий процент реализации. Риск ИБ оценивается как стоимость актива, умноженная на вероятность реализации угрозы.

Г. Последний этап заключается в построении различных видов отчетности по результатам оценки рисков.

2. Метод Digital Security рассматривает две основных модели оценки рисков: модель информационных потоков и модель анализа угроз и уязвимостей. В первой модели для оценки рисков осуществляется построение модели ИС организации. Защищенность каждого типа ресурсов во второй модели определяется путем анализа угроз, действующих на ресурс, и уязвимости, через которые угрозы имеют возможность себя реализовать [4].

3. Метод ISRAM был разработан Институтом Электроники и Криптографии совместно с Турецким Технологическим институтом Гебзе. В этой методике широко используется применение опросных листов как способа оценки факторов риска, а затем производится вычисление уровня риска в виде произведения вероятности реализации угрозы и ее последствий. Данный уровень риска находится в диапазоне от 1 до 25 и вычисляется по следующей формуле:

$$Risk = \left(\frac{\sum_m T_1(\sum_i w_i * p_{i)}}{m}\right) * \left(\frac{\sum_n T_{21}(\sum_j w_j * p_j)}{n}\right)$$

В (3) значение i показывает номер вопроса, используемого для оценки вероятности реализации угрозы, j – номер вопроса, используемого для оценки последствий от реализации угрозы, m и n – количество экспертов, участвующих в опросе, w_i и w_j - веса вопросов, p_i и p_j - количественные значения выбранных ответов на вопросы с номерами i и j, T_1 и T_{21} - порядковые шкалы для оценки вероятности реализации угроз и последствий.

4. Метод iRisk предлагает достаточно простой метод количественной оценки рисков ИБ в организациях. Данный метод может быть легко использован внутри различных моделей управления рисками.

В общем виде, оценка риска ИБ в данном методе осуществляется с помощью формулы^

$$iRisk = (Vulnerability * Threat) - Control$$

где Vulnerability - оценка уязвимости, Threat - оценка угрозы, Control - оценка мер безопасности.

Оценка уязвимости осуществляется на базе известного метода CVSS V2 «A Complete Guide to the Common Vulnerability Scoring System», используя только базовые метрики. При оценке угрозы выполняют оценку возможности реализации угрозы (likelihood) и степени её влияния (impact). Степень влияния угрозы оценивается через частные показатели ущерба. Оценка мер безопасности осуществляется с помощью определения типов и оценки эффективности используемых или планируемых мер безопасности в ИС.

Каждый из рассмотренных подходов к оценке рисков ИБ имеет свои особенности, достоинства и недостатки. В таблице проведен сравнительный анализ данных подходов по ряду критериев.

Таблица 1. Сравнительная характеристика количественных методов

-	Методология/Метод/Частная задача	Моделирование объекта защиты	Экспертные или статистические оценки	Учет различных показателей	Управление
RiskWatch	Метод	Да	Экспертные Статистические	Да	Нет
Digital Security	Метод	Да	Экспертные	Нет	Да
ISRAM	Метод	Нет	Экспертные	Да	Нет
iRisk	Метод	Нет	Экспертные	Да	Нет

Основными сложностями при решении задач количественной оценки и управления рисками ИБ являются:

- ✓ нечеткий и качественный характер большинства частных показателей, влияющих на возможность реализации угроз и использования уязвимостей, а также определяющих ущерб;
- ✓ неопределённость исходной информации о частных показателях.

Ниже представлены основные задачи, требующие решения для количественной оценки рисков ИБ и управления ими [2]:

1. Разработка формальной модели ИС, учитывающей взаимодействие активов, для решения задач количественной оценки рисков ИБ.
2. Разработка метода и алгоритмов для нечеткой количественной оценки ущерба от реализации угроз.
3. Разработка методов и алгоритмов нечетких количественных оценок возможности реализации угроз.
4. Разработка метода нечеткой количественной оценки рисков ИБ с учетом реализации множества защитных мер на основе сформированных нечетких количественных оценок факторов риска.
5. Разработка метода управления рисками ИБ, основанного на оценке эффективности реализуемых защитных мер, в условиях существующих финансовых ограничений.

Список литературы:

1. ISO 31000:2009, Международный стандарт, 1 издание, 2009-11-15
2. Аникин И.В. Метод оценки рисков для уязвимостей информационных систем, основанный на нечеткой логике // Информация и безопасность. 2014. Т. 17. № 3. С. 468-471.
3. А.В. Царегородцев, Е.В.Макаренко. Методика количественной оценки риска в информационной безопасности облачной инфраструктуры организации // Угрозы и безопасность, 1(233) - 2015
4. Вихляев С. А., Белов И. В., Кононова М. А. Применение программной системы Digital Security Office для проведения аудита безопасности информационной системы обработки персональных данных // Молодой ученый. — 2014. — №8. — С. 75-78
5. Carl S. Young. Information Security Threats and Risk // Information Security Science, 2016

УДК 004.056

Грачев Делявер Владимирович, Ясновская Кристина Валерьевна
направление Информатика и вычислительная техника (магистратура),
гр.ИВТм-12

Научный руководитель: **Мясников Владимир Иванович**
д-р техн.наук., доцент, заведующий каф. ИВС.
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

РАЗРАБОТКА КОНТРОЛЛЕРАИЗМЕРИТЕЛЯ ПЛОТНОСТИ ПОЧВЫ

Цель работы – разработка аппаратной части прототипа контроллера измерителя плотности почвы для измерения и мониторинга твердости почвы по глубине.

Одним из актуальных аспектов в сельскохозяйственной промышленности для исследования и улучшения является почва. Обработка почв является главным сельско-техническим мероприятием, которая способствует хорошей урожайности культурных растений, так как в результате ее происходит избавление от сорняков, и создаются благоприятные режимы для корней растений и для микроорганизмов почвы – воздушный, тепловой, водный, питательный и т.д.

Определение твердости почвы в полевых условиях является доступным способом получения информации о состоянии подпахотных слоев, тогда как изучение многих агрофизических свойств почвы трудоемко, а в производственных условиях невыполнимо. Поэтому **актуальным** является определение связей между основными агрофизическими показателями, в частности твердости почвы с традиционными и информативными показателями - плотностью почвы и ее влажностью.

Современная ситуация требует от участников АПК постоянных усилий по оптимизации введения хозяйства, экономии и рациональному использованию имеющихся ресурсов.

Для устранения и решения данных проблем была поставлена задача – разработать измеритель плотности почвы, который будет потреблять мало энергии и стоить не дорого.

Поскольку использование пенетрологгера возможно при разных условиях, необходимо предусмотреть альтернативу в питании устройства.

В схеме присутствует модуль питания. Так как микроконтроллер подключается к внешнему источнику питания, имеющий напряжение

питания не выше 20 В, от высоких уровней пульсаций в схему установлен стабилизатор.Данный модуль питает все датчики, индикатор, ЖКИ -экран и сам микроконтроллер.(Рис.1.). Для обеспечения схемы питанием на длительное время используется готовая сборка из 5-и параллельно соединенных аккумуляторов с суммарной емкостью 15000 mah (мАч).Высокая энергетическая плотность, низкий саморазряд, простота обслуживания, низкий удельный вес. Оптимальные условия хранения Li-ion-аккумуляторов достигаются при 40%-ом заряде от ёмкости аккумулятора при температуре около 5 градусов Цельсия. При этом низкая температура является более важным фактором для малых потерь ёмкости при долговременном хранении.

Используем дополнительный светодиоды (LED) для включения и выключения внешнего аккумулятора. Это самый простой и дешевый способ визуализации процесса работы измерительного устройства. [1]. Светодиод подключается к разъему микроконтроллера с номиналом 5 В.

Преимущество разработанного прототипа на базе микроконтроллера, является дешевизна его компонентов (Arduino, датчики, простой ЖК-дисплей, батареи) и минимальное потребление энергии. Еще одним явным преимуществом данного устройства является небольшой вес прототипа измерителя плотности почвы, что говорит о легкости в эксплуатации.

Модуль микроконтроллера (+ источник питания прототипа), который периодически собирает данные с датчиков, обрабатывает их и сохраняет в Flash-память.

По заданию требуется использовать микроконтроллер на базе серии AVR. Поэтому исходя из количества подключаемых к микроконтроллеру устройств и их параметров, был выбран микроконтроллер ATmega328pc платой расширения ArduinoNano. [3] В плате используется чип FTDI FT232RL для USB-Serial преобразования и применяется mini-USB кабель для связи с ардуино вместо стандартного. Связь с различными устройствами обеспечивают UART,I2C и SPI интерфейсы. Микроконтроллер прост в подключении и программирование, имеет ОЗУ в 2 Кб. Благодаря особой технологии можно выводить наборы символов и данных на дисплей, используя всего лишь 2 пина.

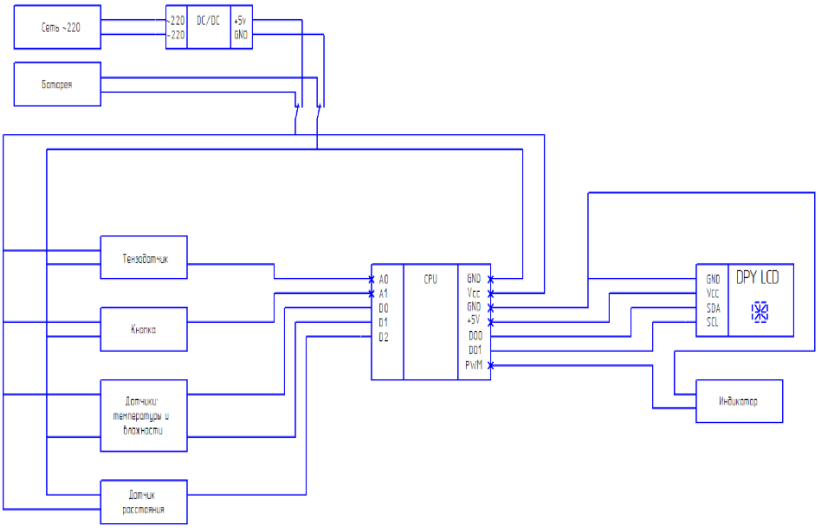


Рис.1. Функциональная схема контроллера измерителя плотности почвы.

Выводы

Преимущество разработанного прототипа на базе микроконтроллера, является дешевизна его компонентов и минимальное потребление энергии. Еще одним явным преимуществом данного устройства является небольшой вес прототипа измерителя плотности почвы, что говорит о легкости в эксплуатации.

Список литературы

1. Микропроцессорные системы: учебное пособие по курсовому проектированию / В. И. Мясников. – Йошкар-Ола: Поволжский государственный технический университет, 2018. – 200 с.

2. Старыгин, С.В. Схемотехника ЭВМ [Текст]: учеб. пособие для студентов специальности 220100 / С.В. Старыгин. - Йошкар-Ола: МарГТУ, 2000. – 188 с.

3. Мясников, В.И. Микропроцессорные системы [Текст]: лабораторный практикум В.И. Мясников. - Йошкар-Ола: Поволжский Государственный Технологический Университет, 2015. – 284 с.

УДК 004.056

Грачев Делявер Владимирович, Ясновская Кристина Валерьевна
направление Информатика и вычислительная техника (магистратура),
гр.ИВТм-12

Научный руководитель: **Мясников Владимир Иванович**
д-р техн.наук., доцент, заведующий каф. ИВС.
ФГБОУ ВО «Поволжский государственный технологический университет», г.Йошкар-Ола

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИЗМЕРИТЕЛЯ ПЛОТНОСТИ ПОЧВЫ

Цель работы – разработка трех алгоритмов для измерения плотности почвы пенетрологгером.

В данный момент все большее внимание в сельском хозяйстве получает аграрный комплекс. На его развитие направлены ресурсы, и особенно важно для этого иметь знание о состояние и о свойствах почвы, которые определяют ее плодородие, что является важнейшим фактором и источником для принятия объективных решений в усовершенствовании технологий агропромышленного и малого фермерства, что является **актуальным** почти во всех регионах России. Это касается таких ее свойств, как вязкость, влажность, текстура, содержание, т.е. плодородие почвы, питательных веществ и минеральный состав.

При обнаружении больших показаний твердости почвы зачастую значительно понижается прорастание семян, возможна гибель растения со временем, и это является препятствием для свободного роста и развития корней растений. Также происходит изменения свойств в почве, в частности, таких как содержание воды, количество кислорода и перепады температуры, которые отрицательно сказываются на условиях для развития самих растений. Исходя из этого важно следить за уровнем плотности почв, чтобы вовремя избежать потерю урожайности. Не смотря на развитие технологий, земельный комплекс не богат разнообразием удобного, легкого в процессе эксплуатации для пользователя и привлекающим по цене оборудования.

Для того, чтобы была возможность отслеживать изменения столь важногопараметра как плотность почвы, в настоящий момент используется большоеразнообразие цифровых измерительных устройств, позволяющие определять величину параметра по выбранным показаниям встроенных датчиков.

У каждого такого устройства есть свои недостатки и достоинства, но главный недостаток аналогов — это дорогая стоимость пенетрологгеров. Пользователь ориентируется при выборе на определенную сферу использования устройства и на точность измерений, от этого и существуют разница в измерительных устройствах не только в технических его параметрах, но и разница соответственно в программном обеспечении, в котором заложены определенные алгоритмы.

В каждом из трех алгоритмовнеобходимо определить влажность, которая играет важную роль, от нее зависят получаемые результаты сопротивления почвы. Для грунтовых почв, влажность которых ниже 40 % характерно повышение сопротивления пенетрации, что означает способность почвы препятствовать проникновению в нее различных объектов (агротехнических орудий, живых организмов, корней растений), соответственно возрастает плотность почвы. Повышение влажности почвы больше, чем на 60 % введет за собой значительное понижение сопротивления пенетрации, но грозит уменьшению пористости почвы, что ведет за собой соответственно уменьшение содержания кислорода в почве. [1] Получается, что оптимальная влажность равняется 40-60%, что позволит более точно снимать показания с датчиков и с меньшей вероятностью допустить погрешность измерений.

Как только влажность почвы становится оптимальной для более точного определения плотности, в разработанном алгоритме проверяется условие, в котором уточняется полученное значение сопротивление пенетрации ровняется или больше 3-3,5 МПа или нет, если ответ положительный, то подтверждается, что это значение является критическим, что дает важную информацию для фермера и помогает предпринять необходимые меры.

Для погружение стержня в почву на заданную глубину запускается датчик расстояния, который информирует пользователя о достигнутом расстоянии, и параллельно включается тензодатчик для определения силы, которое было оказано на устройства, что соответствует сопротивлении пенетрации, которое определяется по формуле[2]:

$$P_{\text{пен}} = \frac{m*g*h_1}{S*h_2}\,[\text{МПа}], \quad (1)$$

Где, в нашем случае, *mg* - сила направленная вниз, то есть оказанная на пенетрологгер;

h1- высота, с которой оказана сила давления;

h2- глубина проникновения стержня измерителя в почву;

S- площадь погруженного в почву наконечника стрежня($см^2$);

После определения сопротивления пенетрации происходит измерение влажности почвы по формуле (3), по которой находится относительная влажность почвы, по значению которой можно сказать и о степени увлажнения почвы:

$$W_0 = \frac{W_a}{W_n} * 100, [\%] \qquad (3)$$

где W_n- полевая влагоемкость почвы (%);

W_a- абсолютная влажность почвы (%).

После каждого определения плотности почвы задается условие для определения количества произведенных измерений в различных точках на испытуемом участке земли. В том случае если получено три измерения плотности почв, они выводятся на экран и алгоритм завершает свою работу, а в отрицательном- требуется провести дополнительные замеры на другом расстоянии. Увеличение данного расстояния связано с различными природными условиями в момент совершения измерения.

Выводы

Сбор данных о сопротивлении почвы осуществляется в период с мая по август, для заполнения базыданных и для наблюдения изменений параметров показаний, это можно было в дальнейшем при большом банке собранных данных для пользователя, который содержит земельный участок, определиться в каком месяце и в какие примерные числа целесообразно выполнять те или иные виды работ на участке (например, посадка семян, орошение почвы и т.п.).

Список литературы

1. О.В. Кормилицина, В.В. Бондаренко /Мониторинг состояния почвенно-грунтовых условий озелененных территорий. / Лесной вестник 1/2016 – Московская область. -2016г.

2. Влияние технологических систем возделывания ячменя на плотность почвы./ О.И. Горянин, Л.В. Пронович, И.Ф. Медведев// журн. Естественные науки ,№ 05, г. 2017- г. Самара, - с.1-4

УДК 004.056

Громов Дмитрий Владимирович
направление Информатика и вычислительная техника (магистратура),
гр.ИВТм-21

Научный руководитель **Мясников Владимир Иванович**

канд. техн. наук, зав. кафедрой информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ПРОЕКТИРОВАНИЕ СИСТЕМЫ ДИСТАНЦИОННОГО ИЗМЕРИТЕЛЯ CO2 В ПОТОКЕ МАШИН

Цель работы – построениеконтроллера дистанционного измерителя CO2 в потоке машин предназначен для измерения концентрации окиси углерода в выбросах автомобильного транспорта автоматически, без участия оператора, непосредственно в потоке движущегося автотранспорта

Актуальность.Автомобильный транспорт в Российской Федерации продолжает оставаться одним из основных загрязнителей атмосферного воздуха. В крупных городах его вклад в суммарные выбросы может достигать 90 %.

В системе государственного управления качеством окружающей среды методическое обеспечение для проведения расчётных оценок (инвентаризации) выбросов загрязняющих веществ и климатических газов от автомобильного транспорта занимает важное место.

Количественные оценки объёмов выбросов загрязняющих веществ автомобильным транспортом необходимы для решения целого ряда практических задач, направленных на повышение устойчивости функционирования транспортных систем, в частности для:

— проведения оценки экологической эффективности различных технических и организационных

решений в сфере автотранспорта, различных мер и решений в области транспортной политики;

— расчёта размеров платы за загрязнение окружающей среды для предприятий автомобильного транспорта и штрафов за сверхнормативное загрязнение окружающей среды.

Включение в систему экологических оценок модулей расчёта рассеивания выбросов загрязняющих веществ от автотранспорта, расчёта экспозиции их воздействия и оценки влияния на здоровье

позволяет решать широкий круг задач по управлению качеством окружающей среды (рис. 1).

В Российской Федерации первые методики инвентаризации выбросов от автотранспорта были утверждены и начали применяться ещё в восьмидесятых годах прошлого века. В табл. 1 представлена характеристика трёхуровневой системы действующих в настоящее время в России методикинвентаризации выбросов от автотранспорта, разработанных Научно-исследовательским институтом автомобильного транспорта (ОАО «НИИАТ»), Представленные методики широко используются в практической деятельности инженерами-экологами и гигиенистами, реализованы и растиражированы в виде коммерческих программных продуктов.

В настоящее время существуют приборы дистанционного зондирования выхлопных газов RSD –Remote Sensing Devices (Испания), BDH series－Remote Sensing equipments(Китай). Такие приборы обладают достаточно высокими параметрами быстродействия и чувствительности. Но в этих приборах, как правило, используются недисперсионные источники ИК и УФ излучения, приводящие к существенному уменьшению дальности зондирования и чувствительности. Китайские системы дистанционного зондирования выхлопных газов используют диодные лазеры ближнего ИК диапазона для регистрации CH4, CO2 и CO примесей но не обладают достаточной чувствительностью. Например, чувствительность определения CO варьируется в пределах 1-10%, что существенно выше уровня разрешенного выброса для европейских двигателей. Нужно отметить, что степень загрязненности автотрасс в Китае очень критична и намного превышает аналогичную в США и Европе.

Существующее в настоящее время газоаналитическое оборудование для дистанционного мониторинга газовых выбросов автомобилей имеет ряд недостатков:

1. Использование недисперсионных источников для детектирования выхлопов в ИК УФ диапазонах не обеспечивают необходимую чувствительность и существенно ограничивает область зондирования примесей.

2. Использование ИК-оптопар (светодиод – фотоприемник) так же не позволяет достичь высокой чувствительности и селективности к измеряемой компоненте из-за присутствия интерферирующих полос поглощения воды, и других газов.

3. Оптические схемы приема-передачи излучения: многозеркальные компоненты для разворота ИК-луча на трассе зондирования сложны в

настройке и обладают температурной и вибрационной нестабильностью при эксплуатации; Телескопические системы приема-передачи излучения имеют небольшую апертуру, недостаточную для уверенной регистрации выхлопного зондирующего облака движущегося автотранспортного средства.

Исследование применяемого аппаратного обеспечения в существующих контроллерах для измерения CO2, удовлетворяющих критериям энергосбережения и отказоустойчивости.

Транспортный комплекс является мощнейшим источником загрязнения природной среды, основным источником шума в городах и вносит значительный вклад в тепловое загрязнение среды. Оценка экологической обстановки на автомобильных трассах городов является актуальной задачей. Непрерывный мониторинг основных загрязняющих газовых компонент выбросов автомобилей на трассах невозможен без привлечения новых дистанционных средств зондирования.

Существующее в настоящее время газоаналитическое оборудование для дистанционного мониторинга газовых выбросов автомобилей имеет ряд недостатков:

1. Использование недисперсионных источников для детектирования выхлопов в ИК УФ диапазонах не обеспечивают необходимую чувствительность и существенно ограничивает область зондирования примесей.

2. Использование ИК-оптопар (светодиод – фотоприемник) так же не позволяет достичь высокой чувствительности и селективности к измеряемой компоненте из-за присутствия интерферирующих полос поглощения воды, и других газов.

3. Оптические схемы приема-передачи излучения: многозеркальные компоненты для разворота ИК-луча на трассе зондирования сложны в настройке и обладают температурной и вибрационной нестабильностью при эксплуатации; Телескопические системы приема-передачи излучения имеют небольшую апертуру, недостаточную для уверенной регистрации выхлопного зондирующего облака движущегося автотранспортного средства.

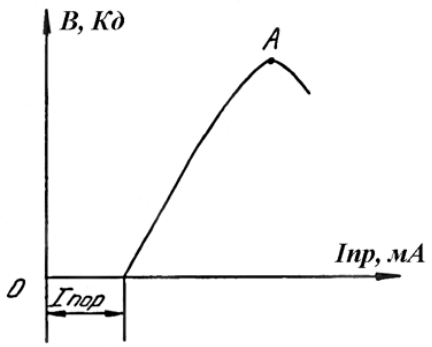


Рис. 1 – Излучательная характеристика светодиода.
В – яркость свечения;

Iпор – пороговое значение прямого тока при котором начинается свечение;

Iпр – прямой ток;

А – в точке А наступает насыщение центров люминесценции.

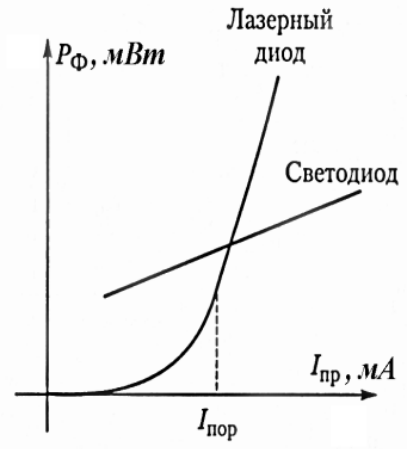


Рис. 2 – Характеристика лазерного диода.
Рф – мощность излучения

В этой связи наиболее актуальным является использование лазерных дистанционных абсорбционных методов измерения газовых примесей. Преимущество использования диодной лазерной абсорбционной спектроскопии в мониторинге примесей обусловлено высокой

селективностью к выбранной газовой компоненте, высокими параметрами спектральной яркости и мощности излучения диодных лазеров, достаточными для дистанционного газоанализа на больших трассах зондирования. Быстродействие и чувствительность при измерении концентрации примесей в сочетании с компактностью этих лазерных систем позволяет использовать современные методы сканирования ИК-луча (гальванометрические сканаторы, акустооптические дефлекторы) и проводить мониторинг примесей в режиме реального времени без изменения скорости потока движения автотранспортных средств.

Новизной предлагаемого решения по сравнению с упоминаемыми другими методами регистрации выхлопных газов является:

• Использование диодных лазеров с волоконным выводом излучения в ближнем ИК-диапазоне, а так-же квантовокаскадных лазеров среднего ИК-диапазона, работающих в нормальных условиях для регистраций примесей выхлопных газов: CO, CO2, NO, CH4 движущегося автомобиля.

• Применение оригинальной оптомеханической системы приема и регистрации ИК-излучения диодных лазеров с применением сканеров лазерного луча для увеличения зоны охвата при зондировании. Функциональное предназначение сканера (сканатора) лазерного луча – доставка лазерного излучения до объекта зондирования без существенного изменения потери мощности и увеличении зоны пространственного сканирования.

• Использование недорогих светоотражающих поверхностей для формирования отраженного ИК-луча, взамен сложной зеркальной оптики, применяемой западными партнерами и Китаем.

• Применение быстродействующих программно-аппаратных средств для регистрации зондирующего излучения и получения концентрации выхлопных газов в режиме реального времени.

Подобное сочетание преимуществ диодного лазерного зондирования позволит максимально эффективно решить задачу мониторинга загрязнения воздуха на автотрассах.

Разработка функциональной схемыконтроллера дистанционного измерения CO2.

Принципиальная блок-схема дистанционного сенсора измерения примесей Принципиальная блок-схема дистанционного сенсора измерения примесей на базе диодных лазеров представлена на рис.3

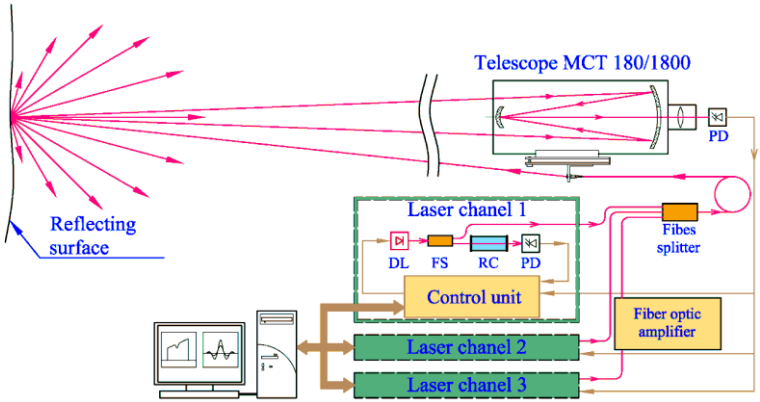


Рис.3 Принципиальная блок-схема дистанционного сенсора измерения примесей на базе диодных лазеров

Излучения диодных лазеров для каждой компоненты выхлопа с помощью телескопа МСТ (диаметр зеркала 180 мм, фокусное расстояние 1800) направляются на отражающее покрытие. Между отражателем и телескопом на расстоянии одной полосы движения проезжает автотранспортное средство на пониженной передаче и скорости не более 60 км/ч. Расположение телескопа и отражательного покрытия должно находиться на уровне выхлопной трубы автомобиля. Для оптимизации зоны охвата при зондировании можно использовать различного рода сканаторы.

Оптоэлектронные блоки для каждого канала регистрации примеси имеют модульную независимую структуру и содержат: диодный лазер, канал сравнения с реперной кюветой исследуемой примеси, электронные модули приема и регистрации излучения и т.д. В зависимости от типа диодного лазера эти блоки могут соединяться и согласовываться между собой с помощью оптоволокна или обычной оптики. Регистрация и прием излучения для всех лазерных источников синхронизовано на одном фотоприемнике, расположенном в коллиматорной части телескопа. Синхронизация вывода и приема излучения диодных лазеров организована по мультиплексной схеме, подразумевающую временную задержку импульсов излучения для лазеров при последовательной временной организации схемы излучения и приема сигнала. Расположение блоков в дистанционном сенсоре измерения примесей представлена на рис. 4.

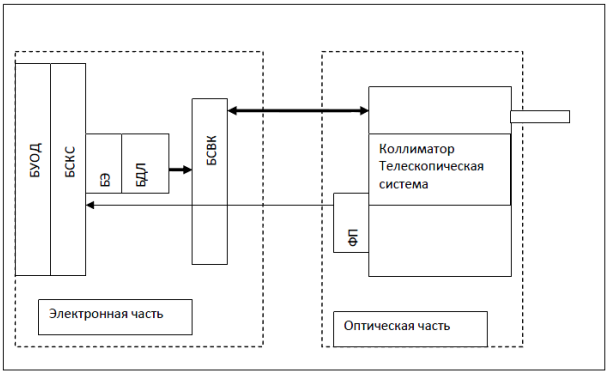


Рис. 4 Схема расположения блоков в дистанционном сенсоре измерения примесей. Жирные стрелки означают передачу оптического сигнала, тонкие - электрического.

В электронную часть дистанционного сенсора измерения примесей входят:

1. блок управления, обработки и документирования результатов измерений (БУОД) – состоит из компьютера (или индустриального компьютера) и монитора;

2. блок согласования и коммутации сигналов (БСКС) – состоит из контроллера, электронной платы ввода-вывода, размещенных либо внутри компьютера, либо отдельно в зависимости от типа плат и контроллера;

3. блок электроники (БЭ) – предназначен для усиления управляющих сигналов с БСКС;

4. блок диодного лазера (БДЛ) – состоит из собственно диодного лазера, разветвителя, реперной кюветы с фотоприемником. Заканчивается волоконным выходом лазерного излучения

5. блок сведения волоконных кабелей (БСВК). Состоит из Y – разветвителей, назначение которых - объединить излучение нескольких оптических сигналов в один волоконно-оптический выход.

В оптическую часть дистанционного сенсора измерения примесей входят:

6. Коллиматор

7. Телескопическая система

8. Фотоприемник (ФП) аналитического канала.

Заключение

1. Исследованы существующие контроллеры для измерения CO2;

2. Исследовано применяемое аппаратное обеспечение в существующих контроллерах для измерения CO2, удовлетворяющих критериям энергосбережения и отказоустойчивости;

3. Разработана функциональная схема контроллера дистанционного измерения CO2.

Список литературы

1. Грандарс [Электронный ресурс]: Загрязнения окружающей среды – электронные данные, – режим доступа http://www.grandars.ru/shkola/bezopasnost-zhiznedeyatelnosti/zagryazneniya-okruzhayushchey-sredy.html – дата доступа: сентябрь 2018.

2. Транспорт и окружающая среда: Учебник/М.М. Болбас, Е.Л. Савич, Г.М. Кухаренок, Р.Я. Пармон и др. – Мн.: Технопринт, 2003. – 262 с.

3. Устройство автомобиля [Электронный ресурс]: Загрязнение автотранспортом окружающей среды – электронные данные, – режим доступа http://ustroistvo-avtomobilya.ru/sistemy-snizheniya-toksichnosti/zagryaznenie-avtotransportom-okruzhayushhej-sredy/ – дата доступа: сентябрь 2018.

4. Горелик Д.О. Мониторинг загрязнения атмосферы и источников выбросов. Аэроаналитические измерения. 1992. – 432 с.

5. Сабельников Д.А. – Разработка электронной системы контроля выбросов автомобильного транспорта, 2011.

УДК 004.056

Гуров Артур Рустамович
направление: "Механизация сельского хозяйства" студент 4-ого курса 422 группы
Игнатьева Алина Николаевна
направление: "Ветеринария" студентка 3го курса 315 группы
ГБПОУ "Кемлянский аграрный колледж"
с.Кемля

Научный руководитель: **Абросимов Вячеслав Матвеевич**
Программист "Пензенского государственного технологического университета"
Пензенский государственный технологический университет, г.Пенза

СОВРЕМЕННЫЕ ХОСТИНГ СИСТЕМЫ, ДЛЯ МАЛОГО И СРЕДНЕГО БИЗНЕСА

Аннотация: Статья представляет собой описание хостинга и его видов. Приводятся примеры тарифов и критерии выбора в различных условиях. А так же затронуты вопросы безопасности использования подобных систем.

Ключевые слова: хостинг; виды хостинга; безопасность; защита данных

Введение:

В нашем современном мире, существенная роль принадлежит компьютерной технике. Область её применения чрезвычайно широка. Вычислительная техника всё больше внедряется в сферу производительной и научной деятельности человека. С каждым годом растут вычислительные мощности, требующиеся для реализации различного рода задач.

Современные компьютерные системы в настоящее время трудно представить без использования сервисов сети Интернет. Различные web-сайты, которые сейчас создаются не только компаниями, но уже и рядовыми пользователями, базы данных, виртуальные диски и с другие облачные сервисы которые сейчас располагаются в сети и помогают решать вопросы постоянного доступа к данным. И вопрос о том, где же размещаться свои данные, проводить различного рода вычисления, является как никогда актуальным.

В данной статье будут рассмотрены способы размещения данных в сети интернет, чтобы каждый пользователь мог получить доступ к определенной информации. Будут проанализированы возможности, и услуги различных хостинг провайдеров, их плюсы и минусы, рассмотрены способы самостоятельной организации подобной системы. А так же будут затронуты вопросы безопасности и защиты своей информации в сети интернет, способы обнаружения атак, и анализ подозрительной активности.

Хостинг

Для начала следует разобраться, что же такое хостинг. Хостинг – это услуга предоставления вычислительных ресурсов на сервере для размещения информации в сети Интернет. Чаще всего, для размещения каких либо сайтов. Обычно под хостингом подразумевается услуга размещения файлов сайта на заранее настроенном сервере с программным обеспечением, необходимым для обработки запросов к файлам сайта и сопутствующим сервисам (Веб-сервер, сервер баз данных, DNS-сервер, CGI-обработчик, FTP-сервер, почтовый сервер).

Но использование хостинга не ограничивается размещением сайтов. На нем так же можно размещать программы, требующие постоянного выхода в интернет, например 1С Бухгалтерия. Организовать файлообменник или попросту хранить файлы для личного пользования. Также можно создать и собственный сервер, например игровой, что в совокупности с быстро растущей игровой индустрией делает эту услугу

очень популярной, не только среди хостинг провайдеров, но и среди энтузиастов, работающих в данной области.

Хостинг провайдер – это компания, занимающаяся предоставлением услуг хостинга и сдающая оборудование в аренду. В данное время существует множество хостинг компаний, предоставляющих различные услуги, рекламирующие свои возможности и сервисы. В рамках данной научной работы будут рассмотрены лишь некоторые из них, но это позволит сформировать общее представление об оказываемых услугах и предоставляемых сервисах.

Виды хостинга

В реальной ситуации видов хостинга достаточно много, и все зависит от желаний и возможностей человека, или организации. Но все же рассмотрим основные виды хостинга, названия которых часто указываются в рекламах различных хостинг компаний:

Виртуальный хостинг - его особенностью является то, что все ресурсы сервера разделены между учетными записями хостинга, в каждой из которых может быть размещено несколько сайтов. На таком хостинге уже есть необходимое для работы сайтов программное обеспечение – веб-сервер, сервер баз данных, FTP–сервер, PHP–обработчик, а так же предусмотрены дополнительные опции, в виде автоматически развертываемой CMS для сайта или же различных конструкторов;

Реселлер-хостинг - готовое решение для перепродажи хостинга. Приобретая реселлер-хостинг, вы становитесь посредником между хостинговым провайдером и конечным пользователем;

Виртуальный сервер (VPS-сервер или VDS-сервер) - Эта услуга подразумевает, что на одном физическом сервере может быть запущено несколько виртуальных машин, каждая из которых полностью изолирована от остальных. Арендатор такого сервера получает полный доступ к управлению ВПС (на уровне администратора/root-пользователя) и может размещать там все необходимое;

Выделенный сервер - отдельный физический сервер или компьютер, все ресурсы которого находятся в вашем распоряжении. Такой вариант необходим для размещения ресурсоемкого проекта с большим количеством посетителей, например, среднего или крупного интернет–магазина. Владельцы такой услуги сами управляют выделенным сервером, могут устанавливать требуемые ОС, и другое программное обеспечение, что позволяет гибко настраивать машину под определенные задачи;

Колокация - размещение собственного выделенного сервера в дата-центре хостингового провайдера. Данная услуга похожа на «Выделеный сервер», за одним исключением. В данном варианте клиент сам размещает свое оборудование в дата-центре, оплачивая только место в стойке, интернет и потребляемую сервером энергию. Дата-центр в свою очередь берет на себя ответственность за сохранность данного оборудования, а так же за стабильный интернет и непрерывное энергоснабжение.

Из перечисленных вариантов самым распространенным является «виртуальных хостинг». Данная услуга чаще всего приобретается небольшими фирмами и частными лицами, которые хотят быстро и без особых затрат разместить информацию о себе в сети. Цена на данную услугу начинается от 100 рублей в месяц, а наличие конструктора сайтов у многих хостинг провайдеров, упрощает эту задачу.

Минусом данного варианта является его малая гибкость и адаптация под конкретные задачи. Как правило, хостинг провайдеры выделяют небольшие ресурсы одному клиенту, это от 4гб дискового пространства, ограничение исходящего интернет трафика, ограничение на использование процессора и количество одновременно размещаемых сайтов.

Для более гибкого варианта стоит обратить внимание на услуги выделенного сервера. Но то, на что стоит обращать внимание при выборе хостинга будет рассмотрено далее.

Выбор хостинга

Выбор хостинга, это один из ответственных моментов любой организации. Так как от принятого решения зависит дальнейшая судьба проектов организации, и ее работа в целом.

Первым делом следует определиться с минимальными системными требованиями, для какого либо проекта или проектов, планируется ли дальнейшее расширение и добавление функционала. Так как, если в планах, какой либо компании, предусмотрено создание нескольких крупных интернет ресурсов, то выбирать явно стоит услуги выделенного сервера, так как виртуальных хостинг не сможет обеспечить всех потребностей при развертывании. А если планируется только создать сайт визитку, с главной информацией об услугах компании, можно воспользоваться бюджетными тарифами на виртуальный хостинг.

Вторым пунктом, следует обратить внимание на географическое расположение оборудования провайдера. Так как быстрое время отклика и скорость загрузки, главные характеристики при работе с

любыми интернет сервисами. Если же планируется привлечение иностранных граждан, то компании следует задуматься о выборе дополнительных, зарубежных хостингов, чтобы сократить время доступа клиентов к данным.

После определения основных потребностей, уже можно задумываться о выборе какого либо хостинг провайдера, и его необходимых услуг.

Сами же хостинг провайдеры формируют свой рейтинг по следующим параметрам:

Надежность (uptime) – отношение времени работы ко времени простоя. Данный параметр является одним из основных при выборе провайдера;

Быстродействие – данный параметр определяет скорость работы всего хостинга в целом, что важно при размещении ресурсоемких проектов;

Время отклика (ping) – показывает время ответа сервера после обращения клиента к нему. Чем ниже данный параметр, тем лучше;

Выдерживаемая нагрузка – параметр схож с быстродействием, но показывает общее состояние хостинга при массовых и длительных запросах к серверу;

Безопасность – надежность сохранности данных при размещении.

По данным параметрам пятерку лидеров в России возглавляют: Макхост, Евробайт, HostMan, appletec, WebHost1. Тарифы непосредственно на сам хостинг не сильно различаются. Так например тарифы на «Виртуальный хостинг» сравнивают и описывают по следующих количественным и качественным ограничениям:

поддержка CGI: Perl, PHP, Python, ASP, Ruby, JSP, Java;

модули и фреймворки;

размер дискового пространства под файлы пользователя;

количество месячного трафика;

количество сайтов, которые можно разместить в рамках одной учётной записи;

количество FTP пользователей;

количество E-Mail ящиков и объём дискового пространства, предназначенного для почты;

количество баз данных и размер дискового пространства под базы данных;

количество одновременных процессов на пользователя;

количество ОЗУ, и максимальное время исполнения, выделяемое каждому процессу пользователя;

Выбор между данной линейкой тарифов стоит осуществлять лишь из цены на тариф и предоставляемых возможностей. В некоторых хостинг компаниях, бонусом к таким тарифам идет SSL сертификат и домен для сайта.

Если говорить о тарифах на виртуальный сервер или выделенный сервер, то ограничений не так много, но они более весомые, так основное отличие данных тарифов в выделяемых клиенту ресурсах:

объем жесткого диска;

объем оперативной памяти

количество ядер процессора и его частота.

Цена на данные тарифы начинается от 500 рублей в месяц, но клиенту предоставляется полный доступ к серверу без каких либо ограничений, как в случае с виртуальным хостингом. Клиент самостоятельно может выбирать операционную систему, которая будет установлена на сервере, а так же сам может устанавливать и настраивать под себя необходимое программное обеспечение.

Опционально к таким тарифам идут следующие услуги:

Интернет канал 100мбитсек с выделенным IPv4 адресом;

Контрольная панель управления сервером – для контроля непосредственно за самим сервером, которая включает мониторинг потребляемых ресурсов, создание резервных копий системы с возможностью возвращения к ним в случае неполадок и автоматическую установку операционных систем;

Панель управления ISPmanager – для управления конфигурацией сервера, которая позволяет устанавливать в автоматическом режиме пользовательское программное обеспечение, добавлять домены, почтовые ящики и так же создавать резервные копии.

При выборе между данными тарифами следует опираться только на системные требования разворачиваемого приложения и выбирать тариф с соответствующими характеристиками.

Услуга «Колокация», является менее популярной из описанных выше. В большинстве случаев, компании, имеющие собственное дорогостоящее оборудование, предпочитают размещать его у себя, и самостоятельно конфигурировать. Так как цены на данную услугу начинаются от 5000 рублей в месяц, и дополнительно клиент самостоятельно оплачивает расходы на электроэнергию, пользоваться данной услугой нецелесообразно, для размещения маломощного компьютера или сервера.

В случаях, когда требуется полный контроль над оборудованием, данными и программным обеспечением, следует задуматься о

самостоятельном конфигурировании какого либо компьютера в качестве сервера. Так как все необходимое программное обеспечение является бесплатным и находится в свободном доступе.

Размещение и конфигурирование собственного сервера

В случаях, когда имеется свободный компьютер, и желание избежать дополнительных расходов на хостинг, следует задуматься о конфигурировании собственного сервера, для размещения всех данных организации.

Основным требованием для данного решения, является наличие выделенного IPv4 адреса, по которому клиенты будут обращаться к серверу. Большинство интернет провайдеров предоставляют эту услугу за небольшую плату. А в некоторых случаях он выделяется бесплатно. Если данная услуга предоставляется, то дальнейшим действием необходимо просто установить необходимое программное обеспечение на собственный компьютер. В настоящие время, различное серверное программное обеспечение имеет собственные конфигураторы, что освобождает обычного пользователя от долгого редактирования конфигурационных файлов, и без привлечения дополнительных сотрудников для этих целей.

Главное преимущество такого метода размещения интернет сервисов, является гибкость, которая ограничивается лишь желанием фирмы заниматься данным вопросом. Из минусов можно отметить то, что самой фирме придется заниматься администрированием и поддержкой данного сервера. Это требует некоторых трудовых, временных, а в некоторых случаях и финансовых затрат. Но данное решение, при грубых расчетах, в среднем окупит себя через год. Так как не потребуется, выделять средства на сторонний хостинг, а при возникновении проблем, решать их с технической поддержкой самого хостинга, что иногда отнимает много времени.

Так же в качестве дополнительного дохода можно сдавать часть вычислительных ресурсов сервера в аренду. В России, с юридической точки зрения, услуга хостинга не относится к телематическим услугам связи в силу различия определения телематических услуг связи и сути хостинга.

Безопасность и защита данных

Далее речь пойдет о безопасности, при использовании услуг хостинг провайдеров. Каждый раз, при принятии решения об использовании какого либо хостинга, стоит помнить следующее высказывание: «Все, что было загружено в интернет, остается там навсегда». Конечно,

различные хостинг провайдеры предоставляют множество услуг по защите данных.

Из программных, доступных для управления пользователю:

SSL сертификаты для сайта;

Автоматические резервные копии;

Антивирусная защита.

Из аппаратных, реализованных на уровне оборудования провайдера, это использование RAID массивов, фаерволов и пакетных фильтров используемых для защиты от DDoS атак.

Но как показывает практика использования данных услуг, они все являются ненадежными, а об некоторых услугах упоминается лишь в маркетинговых целях, для привлечения клиентов.

Автоматические резервные копии не всегда помогают решить проблему, иногда они просто оказываются поврежденными, либо же не содержат нужной информации в связи с введенными ограничениями. Встроенная антивирусная защита не может обнаружить простейшие бекдоры в скриптах сайта, а так же она не защищает от проникновения злоумышленника на сервер. Конечно, некоторые хостинг провайдеры предоставляют услуги двухэтапной аутентификации, но и они не всегда бывают надежными. Что касательно защиты от DDoS атак, если данная функция и реализована, то она обычно распространяется на некоторые часто используемые протоколы, http, ftp, ssh. Но если требуется реализация подобной защиты для собственного приложения, то все упирается в ограничения, наложенные хостинг провайдером.

Из вышесказанного следует, что безопасности, является еще одним из главных критериев при выборе хостинг провайдера. Но как показывает практика, несмотря на рекламные обещания, не везде хорошо с безопасностью. И в случаях, когда речь идет о каких либо ценных корпоративных данных, следует задуматься о размещении собственного сервера на месте. Так как этот способ, при грамотной настройке сети и прав доступа, сможет гарантировать высокую безопасность данных компании.

Но если бюджет компании ограничен, и не предусматривается привлечение дополнительных сотрудников, для обеспечения безопасности, то достаточно следовать некоторым правилам, чтобы избежать потери или кражи данных:

Следует всегда обновлять антивирусное программное обеспечение, так как большинство современных антивирусов, умеют находить и вылечивать, вредоносное содержимое даже в .php скриптах сайта.

Всегда требуется устанавливать сложные пароли, не привязанные к какой либо дате, или знакомому числу, а при возникновении подозрительной активности

сразу их менять.

Создавать индивидуальные учетные записи для каждого пользователя, с разграничением полномочий, это позволит предотвратить случайное изменение конфигураций каким либо пользователем, а так же упросит сбор информации о действии всех пользователей

Открывать только целевые порты в фаерволе. А при возможности, менять стандартные порты. Например по умолчанию SSH-сервер открывает для входящих соединений 22 TCP-порт, и тем самым вызывает потенциальную угрозу bruteforce-атак, поскольку злоумышленник обнаружив на сервере такой открытый порт, пытается подобрать пароль к удалённому серверу при помощи специальных средств автоматизации. Поэтому его следует сменить на любой другой, но следует помнить, что диапазон не должен превышать число 65535, а так же не должен перекрывать прослушиваемые порты других приложений, это может привести к сбоям в работе некоторых сервисов или к их полной остановке. Список уже прослушиваемых портов можно узнать различными средствами мониторинга сети. Начиная с Windows 7 для этих целей можно воспользоваться монитором ресурсов.

Так же всегда стоит раз в неделю просматривать лог файлы на предмет подозрительной активности, это позволит проанализировать безопасность сервера и принять дополнительные меры для устранения уязвимостей в системе.

Заключение

В ходе исследования были рассмотрены различные виды услуг хостинга, а так же хостинг провайдеры. Данная услуга является очень популярной для тех, кто желает арендовать готовую платформу для размещения интернет приложений, в основном для размещения сайтов, а небольшие цены на некоторые тарифы, делают данный вид услуги распространенным не только среди корпоративных клиентов. Так же, встроенные инструменты, позволяют без особых трудовых затрат, развернуть уже готовый сайт, или создать простейший макет сайта визитки.

Несмотря на простоту использования и доступность, у данного вида услуг есть проблемы с безопасностью, что не всегда гарантирует целостность и защиту данных от утечек. Поэтому, все чаще, организации предпочитают размещать данные на своих собственных

серверах. Это обеспечивает им полный контроль и гибкость при развертывании, а так же, при должной конфигурации, защищает от утечек и несанкционированного проникновения. Данное решение будет так же полезным, при продаже лишних мощностей, и привлечении дополнительной прибыли. Так как в России, с юридической точки зрения, услуга хостинга не относится к телематическим услугам связи и не требует лицензирования.

Услуги хостинг провайдеров, будут полностью оправданы в случае, если компания намерена привлечь иностранных клиентов. Поэтому для удобства, сокращения времени доступа к данным, а иногда из-за определенных законов, следует воспользоваться решениями, расположенными в конкретном регионе, для размещения уже готовых интернет приложений.

Список литературы

1. Хостинг // Wikipedia [электронный ресурс]. Режим доступа https://ru.wikipedia.org/wiki/Хостинг (Дата обращения: 03.06.19)

2. Хостинг и виды хостинга // HostIQ [электронный ресурс]. Режим доступа https://hostiq.ua/wiki/about-hosting/ (Дата обращения: 03.06.19)

3. Рейтинг хостинг-провайдеров // hosting-ninja [электронный ресурс]. Режим доступа https://hosting-ninja.ru/rating/ (Дата обращения: 03.06.19)

4. Смена порта как способ защиты от брутфорса // Putty [электронный ресурс]. Режим доступа https://putty.org.ru/articles/change-default-sshd-por.. (Дата обращения: 03.04.19)

УДК 004.056.55

Гущина Евгения Вячеславовна
направление Информационная безопасность (специалитет), гр. БИ-51

Научный руководитель: **Чекулаева Елена Николаевна,**

канд. экон. наук, доцент кафедры Информационная безопасность
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ОСНОВНЫЕ ВИДЫ УГРОЗ И ФАКТОРЫ ИНФОРМАЦИИ ИНФОРМАЦИОННОЙ И ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

В статье рассматриваются основные виды угроз с точки зрения информационной безопасности, выделена классификация угроз экономической безопасности согласно сферам их появления. Отражены

факторы информационной и экономической безопасности, а также учтены источники ЭБ, обеспечивающие финансовую защиту как средство преодоления угроз.

На сегодняшний день увеличивается значимость и заинтересованность к экономической и информационной безопасности как к аспекту функционирования предприятия. В современных условиях обеспечение безопасности является основой существования отдельных хозяйствующих субъектов (предприятий, фирм), различных форм собственности. Существует множество определений экономической безопасности предприятия, но в общем, под ней понимается способность предприятия наиболее эффективно достигать основной цели (получать прибыль) в рыночной экономике, за счет четкого выполнения предприятием своих функций в условиях воздействия внутренних и внешних угроз. Понятие «угрозы безопасности» предполагает изменение во внешней и внутренней среде субъекта, которые приводят к негативному изменению предмета безопасности.

Существует большое число различных классификаций угроз с точки зрения экономической и информационной безопасности.

Рассмотрим классификацию угроз информационной безопасности [1]:

- по характеру нарушений:
  - нарушение конфиденциальности данных
  - нарушение работоспособности ЭВМ
  - незаконное вмешательство в функционирование ЭВМ и т.д.
- по тяжести нарушения:
  - незначительные ошибки
  - мелкое хулиганство
  - серьезные преступления/природные и техногенные катастрофы
- по предвидению последствий нарушителем:
  - намеренные нарушения
  - ненамеренные нарушения
- по мотивации:
  - злонамеренные нарушения
  - незлонамеренные нарушения
- по месту возникновения:
  - внешние угрозы
  - внутренние угрозы (угрозы со стороны инсайдеров)
- по законченности:
  - реализованные
  - нереализованные

- по объекту воздействия:
  - угрозы, нацеленные на всю ИС
  - угрозы, нацеленные на отдельные компоненты ИС
- по причине возникновения:
  - угрозы, возникшие из-за недостаточности средств технической защиты
  - угрозы, возникшие из-за недостаточности организационных мер
- по каналу проникновения:
  - угрозы, проникающие через уязвимости ПО, бесконтрольные съемные носители
  - угрозы, проникающие через бреши в системах авторизации, недостатки систем хранения документов и т.д.
- по виду реализации угрозы:
  - вредоносные программы, спам-письма, программные закладки, хакерские атаки
  - уязвимые процедуры авторизации и другие регламенты ИБ
  - стихийные бедствия
- по происхождению:
  - антропогенные
  - техногенные
  - природные
- по размеру ущерба:
  - незначительные
  - значительные
  - критичные

Следует почеркнуть, что классификация угроз экономической безопасности по сфере их возникновения, во-первых, имеет лучшее на сегодняшний день теоретическое обоснование и, во-вторых, нашла наибольшее практическое применение (таб.1) [2].

Таблица 1 Классификация угроз ЭБ

Признак	Содержание
Расположение угроз относительно объекта	Внешние и внутренние
Момент существования	Актуальные и потенциальные
Частота воздействия	Постоянные и случайные
Степень очевидности	Явные и скрытые
Воздействия на объект	Актуальные и пассивные
Сфера возникновения	Правовые, экономические, культурные, социальные, технические

По мнению, авторов лучшая классификация ЭБ актуальна согласно сферам их появления, а именно:

1. Разглашение - это умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним.

2. Утечка - это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.

3. Несанкционированный доступ - это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам. Сравнительно источника появления угрозы экономической безопасности предприятия можно разделить на объективные и субъективные. Объективные источники возникают без участия и помимо желания предприятия или его служащих, независимо от решений, действий, принятых менеджером – это состояние финансовой конъюнктуры, научные открытия, форс-мажорные обстоятельства. Субъективные источники появляются из-за действий людей, умышленные или неумышленные, различных органов и организаций, в том числе государственных и международных предприятий, конкурентов. Объективные источники необходимо уметь распознавать и обязательно учитывать в управленческих решениях. Предотвращение субъективных источников во многом связано с воздействием на субъекты экономических отношений.

В качестве источников угроз экономической безопасности могут выступать [3]:

1) внешние источники:

- рынок – изменение спроса, курсов валют, продуктовой линейки, стоимости кредитов, повышение конкуренции;
- недобросовестная конкурентная борьба либо незаконные воздействия третьих лиц, нацеленные против предприятия;
- угрозы репутации компании по политическим, религиозным и иным мотивам, идущие от органов государственной власти и общественных организаций;
- промышленные катастрофы, аварии, террористические акты, стихийные бедствия.

2) внутренние:

- служащие предприятия – оглашение конфиденциальных данных, целенаправленные нарушения контрольных процедур с целью хищения, безответственность, саботаж;

• недоработка процессов контрольных процедур (отсутствие требуемого контроля, неосведомленность их персоналом).

К внешним источникам угроз информационной безопасности относятся [4]:

• деятельность иностранных структур, направленная против интересов Российской Федерации в информационной сфере;

• стремление ряда стран ущемить интересы России в мировом информационном пространстве, вытеснить ее с внешнего и внутреннего информационных рынков;

• обострение международной конкуренции за обладание информационными технологиями и ресурсами;

• деятельность международных террористических организаций;

• увеличение технологического отрыва ведущих держав мира;

• деятельность разведки иностранных государств;

• разработка рядом государств концепций информационных войн, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранность информационных ресурсов, получение несанкционированного доступа к ним.

К внутренним источникам угроз информационной безопасности относятся [4]:

• недостаточная экономическая мощь государства и недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;

• критическое состояние отечественных отраслей промышленности;

• отставание России от ведущих стран мира по уровню информатизации всех видов человеческой деятельности;

• недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере;

• получение криминальными структурами доступа к конфиденциальной информации, усиление влияния организованной преступности на жизнь общества;

• недостаточная координация деятельности по формированию и реализации единой государственной политики в области обеспечения информационной безопасности;

• неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;

• снижение эффективности системы образования, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;

• недостаточная активность федеральных органов государственной власти субъектов РФ в информировании общества о своей деятельности.

Факторы экономической безопасности предприятия – это совокупность окружающих обстоятельств, которые влияют на характеристики безопасности. Факторы финансовой защищенности делят на внутренние и внешние. Внешние факторы можно разбить на три подгруппы [5]:

1) макроэкономические: этап формирования экономики государства, устойчивость хозяйственного законодательства, уровень инфляции, соотношение валют, покупательская способность населения, положение финансовой системы, государственная политика (антимонопольная, инвестиционная, налоговая, инновационная, регуляторная, внешнеэкономическая, ценовая);

2) рыночные: потребительский и производственный спрос, уровень цен на сырьевые материалы и готовую продукцию, динамика конкурентной борьбы в регионе и отрасли, действия конкурентов, емкость рынка, платежеспособность контрагентов;

3) прочие: темпы научно-технического прогресса, демографические тенденции, криминогенная ситуация, природно-климатические условия и др.

Совокупность внутренних факторов финансовой защищенности можно разбить на следующие группы:

1) финансовые: состав и ликвидность активов, состав капитала, обеспеченность собственным оборотным капиталом, степень рентабельности, прибыльность инвестиционных проектов, дивидендная политика;

2) производственные: применение оборотных и основных средств, положение и состав основных фондов, система контроля качества, состав себестоимости;

3) кадровые: организационная структура управления, мотивирование персонала, наличие стратегии развития, квалификация и состав персонала, параметры оплаты труда, степень рационализаторской инициативности, социальные мероприятия;

4) материально-технического обеспечения: уровень диверсификации поставок сырья, качество поставляемого сырья, периодичность поставок, применение современных технологий;

5) инвестиционно-технологические: НИОКР, наличие вкладываемых ресурсов, уровень инновационной активности;

6) сбытовые: выбор продукции, ценовая политика, набор заказов, степень диверсификации покупателей, политика расчетов с потребителями, готовность отправляемой продукции, осуществление маркетинговых исследований;

7) экологические: введение новых технологий, реализация природоохранных мероприятий.

В заключении хочется отметить, что для обеспечения экономической и информационной безопасности необходимо учесть все возможные варианты защиты экономических данных и обеспечить полную конфиденциальность всей информации. Тем самым защита экономической безопасности - это комплекс мероприятий, направленных на обеспечение экономической безопасности, которая обеспечит предприятию необходимый аспект ведения бизнеса в условиях агрессивной рыночной экономики, а информационная безопасность - это защита информации от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб ее владельцу или пользователю.

Список литературы:

1. https://www.arinteg.ru/articles/ugrozy-informatsionnoy-bezopasnosti-27123.html

2. Гладышев В.А. Классификация угроз экономической безопасности предприятия. - Экономика, система управления. - с. 27-31

3. Горбачев, Д.В. Комплексный подход к организации деятельности службы экономической безопасности предприятия / Д.В. Горбачев, М.В. Кононова // Интеллект. Инновации. Инвестиции. – 2014. - № 1.

4. Доктрина информационной безопасности РФ

5. Чекулаева Е.Н. основные виды и важность факторов угроз информации в информационной и экономической безопасности. - сборник статей Международной научно-практической конференции (23 мая 2019 г.) – Петрозаводск: МЦНП «Новая наука», 2019. –с. 19-25.

УДК 004.056

Дмитриев Александр Сергеевич, Алексеев Павел Олегович,
направление Информатики и вычислительной техники (бакалавриат),
гр. ИВТ-11-16, ИВТ-22-16

Научный руководитель **Галанина Наталия Андреевна**,
д-р техн. наук, профессор кафедры математического и аппаратного обеспечения информационных систем
ФГБОУ ВО «Чувашский государственный университет им. И. Н.Ульянова», г. Чебоксары

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ КООРПОРАТИВНОГО ОБУЧЕНИЯ СОТРУДНИКОВ

Актуальность. Сегодня обучение сотрудников и повышение их квалификации является необходимостью для функционирования компаний. Как правило, необходимых компании специалистов на рынке не хватает, астуденты, проходящие практику или стажировку в компаниях, не имеют прикладных навыков для работы, вследствие чего компаниям приходится проводить свои собственные курсы или полностью оплачивать обучение.Составленная внутри компании программа обучения не всегда является эффективной, кроме того, с уходом сотрудников, проводящих обучение, программа обучения теряется. Не всем стажерам бывает удобно проходить обучение в офисе из-за учебы или работы.

Целью работы является разработка платформы, способной решить вышеуказанные проблемы.Предлагаемая платформа представляет собой клиент-серверное приложение. В отличие от сайтов с коммерческими курсами и готовыми программами,разрабатываемая платформа позволяетсоздаватьсобственный контент, что позволяет компаниям реализовывать любую программу обучения. В ходе разработки были выделены основные критерии эффективности программы по разным параметрам, что позволяет рассчитать эффективность курса и его отдельных частей. Таким образом, компания сможет «оттачивать» свои программы, доводя их до совершенства, а стажеры с каждым следующим набором будут лучше и эффективнее обучаться.

Приложение реализует следующие основные функции: авторизация и аутентификация пользователей; регистрация компаний; создание курсов, шагов, тестов, опросников и блоковобучения;оценка эффективности составленной программы; выделение слабых сторон программы обучения; статистика по прохождению.

Выбор средств разработки. Разработка платформы проводилась в три этапа. На первом этапе былоспроектировано будущее приложение, на втором - написание серверной части приложения, на третьем - реализация клиентского приложения.

В качестве серверного языка был выбран язык PHP, в качестве фреймворка - Laravel, так каку него отличная архитектура и он представляет весь функционал, необходимый современным веб-приложениям, такие как: сокеты, ORM, resourses и т. д. В качестве СУБД была выбрана MySQL, так как она является нереляционной. Веб-сервер -nginx, так как он обеспечивает высокую производительность работы веб-приложения при высоких нагрузках. Серверное приложение представляет собой API-сервер, с которым взаимодействует клиентское приложение. Такой подход является современным подходом разработки и максимально инкапсулирует части платформы.

Клиентское приложение разработано с помощью JavaScript-библиотекиReact. Использование этого инструмента упрощает процесс разработки и поддержки пользовательских интерфейсов. На стороне клиента только генерируетсяразметка, что положительно сказывается на производительности сервера и обеспечивает большую безопасность приложения.

Вывод. На сегодняшний день платформа тестируется. Пример пользовательского интерфейса платформы приведен на рисунке. Реализован весь задуманный функционал, но по мере работы над проектом возникли новые идеи, которые будут реализованы в скором времени. Например: продажа собственных курсов для получения дополнительной прибыли, покупка курсов других компаний для внутреннего использования, система оценок курса, система достижений и уровней для пользователей, авторизация через социальные сети, мобильное приложение.

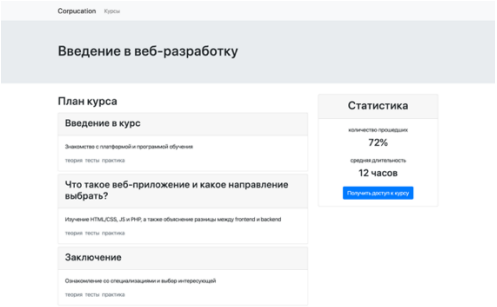


Рис 1. - Страница курса приложения

Список литературы
1. Laraveldocumentation[Электронный ресурс]. – Режим доступа:https://laravel.com/docs/6.x (дата обращения 20.10.2019).
2. Документация – React [Электронный ресурс]. - Режим доступа:https://ru.reactjs.org/docs/ (дата обращения 20.10.2019).
3. Nginx: документация [Электронный ресурс]. - Режим доступа:https://nginx.org/ru/docs/ (дата обращения 20.10.2019).
4. React-router: DeclarativeRoutingforReact.js [Электронныйресурс]. - Режимдоступа: https://reacttraining.com/react-router/ (датаобращения 20.10.2019).

УДК 004.056

Ильин Кирилл Юрьевич,
Направление Информатика вычислительная техника (бакалавриат),
гр. ИВТ-11-16

Научный руководитель **Галанина Наталия Андреевна**,
д-р техн. наук, профессор кафедры математического и аппаратного обеспечения информационных систем
ФГБОУ ВО «Чувашский государственный университет им. И.Н. Ульянова», г. Чебоксары

ИСПОЛЬЗОВАНИЕ 3D-ГРАФИКИ ПРИ РАЗРАБОТКЕ WEB-ПРИЛОЖЕНИЙ

Цель работы –проведение анализа современных подходов к созданию анимированной компьютерной трёхмерной графики при разработке клиент-серверного приложения и предложение возможных идей её использования.

Актуальность темы заключается в том, что развитие трехмерной графики в WEB с выходомAPI WebGL[4] позволяет создавать производительные и кроссплатформенные браузерные приложения[3].На текущий момент временииспользование 3D-графики в веб-приложениях,несмотря на то, что условия для использования библиотеки созданы, не получило широкогораспространения в готовых проектах.

Использования трехмерной графики без фреймворков WebGL. На её основе разработчики могут создавать совершенно новые пользовательские интерфейсы, трехмерные игры и использовать трехмерную графику для визуализации различной информации [1]. На данный момент этот стандарт является единственновозможным и

рекомендуемым для отображения полноценной трехмерной графики в браузере. По данным наиболее «свежей» на момент написания работы статистики специализированной организации около 97% веб-браузеров пользователей [2] поддерживают WebGL. Но по-прежнему технология используется в проектах избирательно по следующимпричинам:

1. Создание 3D - это непростая задача и онаиногда выходит за пределы компетенций рабочей группы. Простейшие работы требуют знаний и навыков в области 3D-моделирования, дизайна и программирования [3];

2. Клиенты не заказывают 3D-графику, поскольку не знают, что существуют в этой области доступные решения и не представляют ее возможности [3];

3. Наличие сложной графики в приложении не всегда приводит к достижению коммерческих целей.

Перечисленные проблемы традиционны для растущих технологий.

Подход использования WebGL с помощью фреймворков.Технология WebGL использует низкоуровневое API, этот аспект облегчает внедрение технологии разработчиками браузеров в свои продукты, но создает достаточно большие трудности при создании интерфейсов[1].Поэтому были созданы библиотеки и фреймворки, которые упростили работу разработчикам приложений.Они помогают сосредоточиться на конечном результате с минимумом кода. Наиболее популярные из них -Three.js, Babylon.js, Processing [5].

Предлагаемые идеи использования трехмерной графики в web-приложенияхмогут выглядеть следующим образом:

1. онлайн - конструкторы, позволяющие сразу увидеть результат взаимодействия с элементами конструктора;
2. презентация продукта;
3. описание устройства продукта;
4. визуализация данных;
5. карты и геолокация.

Заключение. Таким образом, в настоящее время существует развивающаяся технология WebGLдля работы с трехмерной графикой в клиент-серверных приложениях, которая поддерживается у 97% браузеров пользователей. Исходя из рассмотренныхподходов, можно сказать, что для работы с WebGLлучше выбирать использование библиотек и фреймворков, так как они позволяют «миновать» низкоуровневое API, а это в свою очередь уменьшает время разработки. Исходя из рассмотренных причинвозможной неэффективности использования трёхмерной графики в проектах, можно сказать, что

необходимо выбирать использование технологии целесообразнопроекту.Для этого в работе предложены возможные идеиреализации 3D-графики в проектах.

Список литературы

1. Трехмерная графика в вебе [Электронный ресурс] / habr.com – URL: https://habr.com/ru/post/325646 (дата обращения: 23.10.2019)
2. WebGLStats [Электронный ресурс] / Webglstats.com. – URL: http://webglstats.com (дата обращения: 23.10.2019)
3. Использования трехмерной графики в веб-разработке [Электронный ресурс] / blog.techart.ru – URL: https://blog.techart.ru/idei-ispolzovaniya-trehmernoi-grafiki-v-veb-razrabotke/ (дата обращения: 23.10.2019)
4. WebGL [Электронный ресурс] / ru.wikipedia.org– URL: https://ru.wikipedia.org/wiki/WebGL/ (дата обращения: 23.10.2019)
5. Выбираем библиотеку для работы с WebGL [Электронный ресурс] / ru.wikipedia.org– URL: https://habr.com/ru/post/278731/ (дата обращения: 24.10.2019)

УДК 004.772

Канатеева Анастасия Владимировна
направление Информатика и вычислительная техника (магистратура),
гр. ИВТм – 22

Научный руководитель: **Васяева Наталья Семеновна**
к.т.н., доцент каф.ИВС
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ИССЛЕДОВАНИЕ АЛГОРИТМА ШИФРОВАНИЯ БЕСПРОВОДНЫХ СЕТЕЙ WPA

Рассматривается задача исследования алгоритма шифрования WPA, выявления его недостатков и предложения модификации методов шифрования.

Таблица 1 [1].

Свойство	**Статический WEP**	**Динамический WEP**	**WPA**	**WPA 2 (Enterprise)**
Идентификация	Пользователь, компьютер, карта WLAN	Пользователь, компьютер	Пользователь, компьютер	Пользователь, компьютер
Авторизация	Общий ключ	EAP	EAP или общий ключ	EAP или общий ключ
Шифрование	Статический ключ	Сессионный ключ	Попакетный ключ через TKIP	CCMP (AES)
Алгоритм	RC4	RC4	RC4	AES
Целостность	32-bit Integrity Check Value (ICV)	32-bit ICV	64-bit Message Integrity Code (MIC)	CRT/CBC-MAC Part of AES
Распределение ключей	Однократное, вручную	Сегмент Pair-wise Master Key (PMK)	Производное от PMK	Производное от PMK
Вектор инициализации	Текст, 24 бита	Текст, 24 бита	Расширенный вектор, 65 бит	48-бит номер пакета (PN)
Длина ключа, бит	64/128	64/128	128	до 256
Требуемая инфраструктура	Нет	RADIUS	RADIUS	RADIUS

WEP (WiredEquivalentPrivacy) – первый стандарт шифрования данных. Алгоритм использует перемножение блоков исходных данных на псевдослучайную последовательность такой же длины, что и блок шифруемых данных (соответствует кадру MAC-уровня).

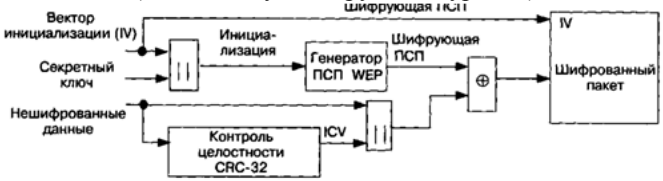


Рис. 1. Протокол WEP

WPA (Wi-FiProtectedAccess) — современная технология защиты беспроводной Wi-Fi-сети, заменившаяWEP.В нем используется 48-битный вектор инициализации, и изменены правила построения вектора, также для подсчета контрольной суммы используется MIC (MessageIntegrityCode), который используется вместо менее надёжного CRC32 Для управления ключами существует специальная иерархия, которая призвана предотвратить предсказуемость ключа шифрования для каждого кадра. Благодаря TKIP ключ шифрования для каждого кадра данных генерируется таким образом, что они не повторяют друг друга, пусть даже частично [2].

Рис. 2. Протокол TKIP

WPA2 — усовершенствованный вариант WPA. Существенным отличием его от WPA является то, что каждое устройство имеет свои ключи шифрования для обмена данными с точкой доступа. Основное отличие от TKIP и WEP – это централизованное управление целостностью пакетов, которое выполняется на уровне AES [2].

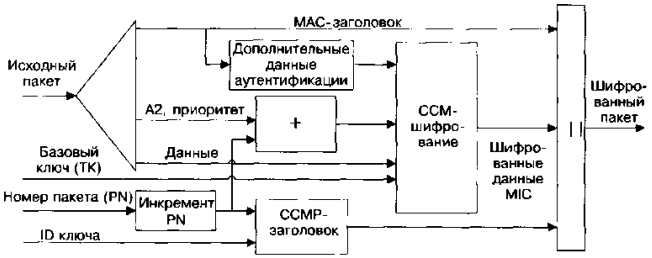


Рис. 3. Протокол CCMP

WPA2 является самым надежным соединением, но уязвим для атаки «человек посередине». Чтобы обезопасить от такого вида атак беспроводную сеть, необходимы мониторинг системы для выявления слабых звеньев сети, локализация несанкционированных точек доступа, использование УРМ-клиентов для защиты передаваемых данных в открытом режиме работы сети.

Список литературы

1. https://habr.com/ru/post/150179/
2. http://mgupi-it.ru/Tech/wireless/wifisecurity_part2.html
3. https://ru.wikipedia.org/wiki/WPA
4. Визавитин О. И., Логинова Д. А., Таякин С. Д. Применение современных алгоритмов шифрования при обеспечении информационной безопасности беспроводных локальных сетей // Молодой ученый. — 2016. — №10. — С. 138-142. — URL https://moluch.ru/archive/114/29954/ (дата обращения: 28.01.2019).

УДК 004.772

Кардаков Денис Алексеевич
Направление "Управление в технических системах", гр. УТС/б - 16-1-о

Научный руководитель: **Кабанов Алексей Александрович**
К.т.н доцент, заведующий кафедрой ИУТС
ФГБОУ ВО "Севастопольский государственный университет"
г. Севастополь

РАЗРАБОТКА СИСТЕМЫ УПРАВЛЕНИЯ МАНИПУЛЯТОРОМ С ИЗБЫТОЧНЫМ КОЛИЧЕСТВОМ ЗВЕНЬЕВ

Одним из важных разделов современной теории автоматического управления является разработка систем управления многозвенными роботами-манипуляторами. Вызвано это высоким спросом на подобные

системы со стороны промышленности. Манипуляционные роботы, как правило, характеризуются большей стоимостью в сравнении с традиционными устройствами, но за счет гибкой конфигурируемости способны выполнять широкий круг всевозможных задач в условиях промышленного производства, в том числе те, которые раньше мог выполнять только человек. Возможность перенастройки с целью выполнения различных функций позволяет использовать роботы-манипуляторы в течении длительного времени для решения разных задач без необходимости закупки дорогостоящего специализированного оборудования, что ведет к экономии средств в перспективе.

Целью данной работыявляется разработка системы управления и автономной работы манипулятора для решения различных производственных задач (захват, перемещение, сортировка объектов). Основой для разработки стал робот-манипулятор Optima-2 компании «Зарница». Данный манипулятор создан на базеArduino, что позволяет свободно «прошивать» его собственными программами управления. Для того, чтоб успешно управлять манипулятором требуется произвести следующие шаги: рассчитать и построить математическую модель захвата, перенести её в компьютерную программу для симуляции, создать канал управления реальным манипулятором, придумать интерфейс для взаимодействия симуляции и реального манипулятора. Выполнив все эти шаги мы получим платформу идеально подходящую для тестирования и разработки автоматизированной системы управления роботом.

Для того, чтоб создать модель манипулятора нужно для начала построить представление Денавита–Хартенберга, которое описывает вращательные и поступательные связи между соседними звеньями устройства. Манипулятор Optima 2 имеет 5 степеней свободы (5 звеньев), следовательно, представление Денавита–Хартенбергадля него будет выглядеть следующим образом (рисунок 1).

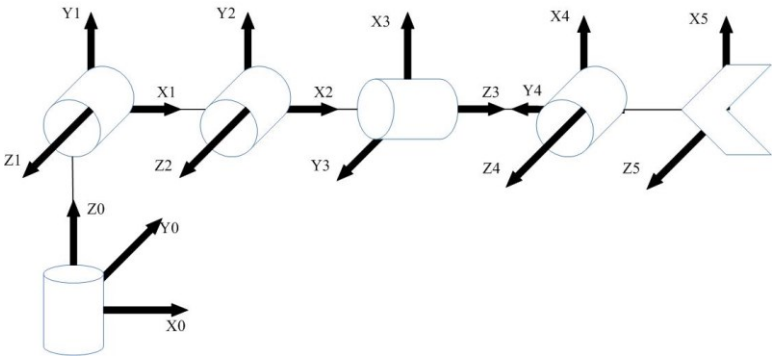


Рис. 1. Кинематическая схема манипулятора Optima 2

При помощи метода ДХ мы создали кинетическую модель нашего манипулятора. Теперь можно приступить к решению задач прямой и обратной кинематики, без которых невозможно управление манипулятором. Задача прямойкинематики заключается в вычислении положения рабочего органа манипулятора по его кинематической схеме и заданной ориентации его звеньев. Обратнаязадача — это вычисление углов по заданному положению рабочего органа и опять же известной схеме его кинематики.

Т.о., решение прямой задачи говорит — где будет находиться рабочий орган манипулятора, при заданных углах его суставов, а обратная задача, наоборот, говорит: как нужно «вывернуться» манипулятору, чтобы его рабочий орган оказался в заданном положении.

Для их решения требуется составить матрицу преобразования нашей модели. Однородная матрица преобразования может быть разбита на четыре подматрицы:

$$T = \begin{bmatrix} R_{3\times3} & \vdots & p_{1\times3} \\ f_{1\times3}\text{a} & \vdots & 1\times1 \end{bmatrix} = \begin{bmatrix} \text{Поворот} & \vdots & \text{Сдвиг} \\ \text{Перспектива} & \vdots & \text{Масштаб} \end{bmatrix}$$

$R_{3\times3}$ – представляет собой матрицу вращения системы $x_n y_n z_n$относительно$x_0 y_0 z_0$

$p_{1\times3}$ - вектор линейного смещения начала координат системы $x_n y_n z_n$относительно$x_0 y_0 z_0$

$f_{1\times3}$ -подматрица размерностью 1x3 задает преобразование перспективы;

четвертый диагональный элемент является глобальным масштабирующим множителем.

Дополнительно для решения ОЗК требуется учесть рабочую зону манипулятора. Рабочая зона — это множество всех точек в трехмерном пространстве, которые может достичь захват. Знание границ оболочки робота позволяет судить о возможностях и произвольности робота.

Теперь, построив мат. модель манипулятора, можно переходить к созданию симуляции. Для это была собрана URDFмодель манипулятора, которая содержит в себе всю информацию, полученную нами при расчете мат. модели. Она требуется для построения 3Dсимуляции в таких программах как RvizиGazebo. Далее будем использовать программу-планировщик движений робота – Moveit, для генерации и исполнения траекторий движения симуляции манипулятора. Теперь переходим к управлению реальным роботом.Манипулятор Optima 2 представлен на рисунке 2.

Рис. 2. Манипулятор Optima 2

За движения звеньев робота отвечают шаговые двигатели и сервопривод. Для управления ими в среде Arduinoиспользовались библиотеки AccelStepperи Servo. Написав прошивку для запуска двигателей переходим к созданию интерфейса для взаимодействия симуляции и реального манипулятора.

Для реализации взаимодействия будем использовать ROS (Robot Operation System). Основной идеей интерфейса было следующее: передвигать манипулятор в симуляции, и реальный манипулятор должен отразить это движение в режиме реального времени.Для этого был создан rosnode, который преобразовывал вращение (в градусах) каждого сустава на моделируемом роботе в шаги. Этими шагами было фактическое количество шагов, необходимых для перемещения

манипулятора робота в желаемое положение. Затем, чтобы отправить данные шагов в Arduino, было написано собственное сообщение ROS, которое структурировало данные шагов. В итоге был создан rostopic (канал передачи данных), в котором с одной стороны симуляция публиковала данные, а с другой стороны Arduinoих считывала. Таким образом, всякий раз, когда движение выполнялось в симуляции, оно отражалось на реальном роботе.

Выводы. Основным результатом является разработка алгоритма по созданию системы управления многозвенным манипулятором с практически любой конфигурацией звеньев. Также была разработана платформа для тестирования и разработки автоматизированной системы управления манипулятором Optima 2, что позволит расширить класс решаемых роботом задач, ввиду возможности его перепрограммирования. В дальнейшем планируется добавить камеру для реализации нахождения и распознавания объектов и перемещения их в заданную точку.

Список литературы

1. Siciliano, B. Robotics: Modeling, PlanningandControl [Электронныйресурс] / B. Siciliano, L. Sciavicco, L. Villani, G. Oriolo**.** – Режимдоступа: https://epdf.pub/robotics-modelling-planning-and-control.html.

2. Борисов О.И. Методы управления робототехническими приложениями [Электронный ресурс] / О.И. Борисов, В.С. Громов, А.А. Пыркин. — Режим доступа: https://books.ifmo.ru/file/pdf/2094.pdf

УДК 004.772

Кардаков Денис Алексеевич
Направление "Управление в технических системах", гр. УТС/б - 16-1-о

Научный руководитель: **Кабанов Алексей Александрович**
К.т.н доцент, заведующий кафедрой ИУТС
ФГБОУ ВО "Севастопольский государственный университет"
г. Севастополь

РАЗРАБОТКА СИСТЕМЫ УМНОГО МИКРОКЛИМАТА

Микроклимат жилых и рабочих помещений является важнейшей составляющей здорового и продуктивного ритма жизни человека. Мы не часто задумываемся о том, каким образом виляют на наш организм

различные факторы окружающей среды в помещении, в то время как они могут сильно повлиять на состояние здоровья человека.

Целью данной работыявляется разработка системы умного микроклимата, котораяспособна измерять и оценивать качество окружающей среды, а также корректировать ее состояние для повышения комфорта человека.В нашей работе мы ориентируемся на глобальные тренды цифровизации и создания умного пространства.

Схема работы устройства представляет собой следующий алгоритм: сбор данных о состоянии окружающей среды, передача этих данных на сервер, их обработка и представление в приложении, сбор обратной связи от пользователя, корректировка на её основе «комфортных» показателей факторов окружающей среды, подстройка микроклимата под эти показатели для создания условий максимального комфорта и продуктивности пользователя.

Сбор данных осуществляется при помощи датчиков под управлением платформы ArduinoMega2560. В тестовый образец входят датчики: температуры, влажности, уровня CO2, пыли, уровня освещенности и давления. Для передачи данных по сети Wi-Fiиспользуется плата ESP-01 на базе чипа ESP8266. Также для цветовой индикации состояния окружающей среды в прототипе используется светодиодная лента. Принципиальная схема представлена на рисунке 1.

Для представления информации на смартфоне было создано приложение (на базе Blynk), которое обрабатывает полученные данные и показывает их в виде графиков и диаграмм, а также информирует пользователя о превышении какого-либо из показателей окружающей среды. Экран приложения представлен на рисунке 2.

Далее по алгоритму следует сбор обратной связи от пользователя, корректировка на её основе «комфортных» показателей факторов окружающей среды. Этот пункт будет реализован на основе технологии нейронных сетей. Созданная нами сеть, каждый раз после получения обратной связи будет переобучаться и синтезировать новые весовые коэффициенты «комфортных» показателей факторов окружающей среды. Последний пункт будет реализован путем внедрения нашего устройства в экосистему умного дома, что позволит ему управлять техникой, регулирующей параметры микроклимата помещения (кондиционер, приточная вентиляция и тд.).

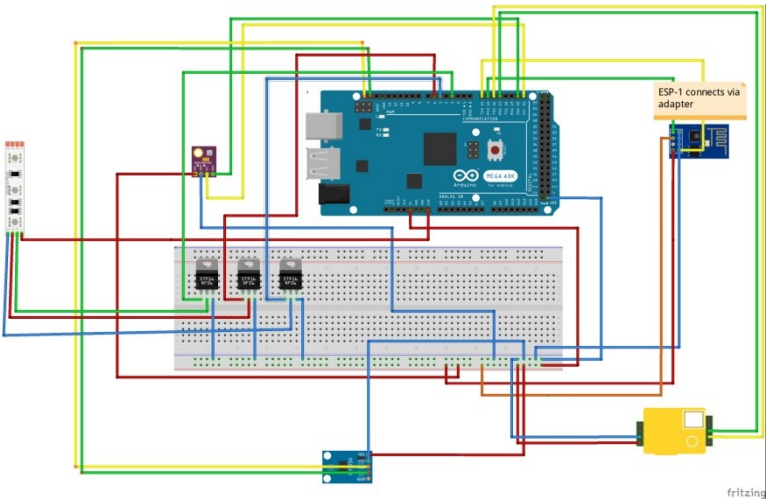


Рис. 1. Принципиальная схема устройства

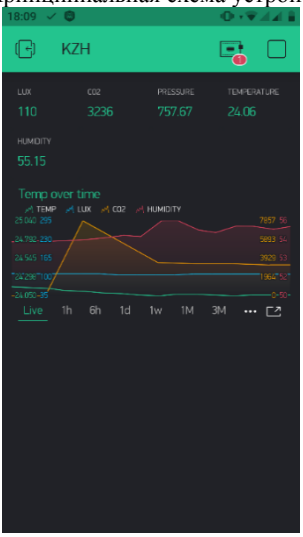


Рис. 2. Окно приложения

На данном этапе прототип устройства выглядит следующим образом (рисунок 3).

Рис. 3. Прототип устройства

Выводы. Ввиду ухудшения глобального климата на планете, контроль за личным микроклиматом является одной из приоритетных задач современного человека. Созданное в ходе работы устройство поможет людям в контроле и поддержании комфортного состояния окружающей среды у них дома или на работе.

Списоклитературы

1. Страуструп, Б. Программирование. Принципы и практика с использованием C++ / Б. Страуструп. – 2-е изд. – М.: Додэка XXI. – 1328 с.

2. Блум, Дж. Изучаем Arduino. Инструменты и методы технического волшебства: пер. с англ. / Дж. Блум. – СПб.: БВХ-Петербург, 2015. – 336 с.: ил.

УДК 004.056.53

Карманова Екатерина Владимировна
Информационная безопасность автоматизированных систем(специалитет),
гр. БИ-32

Научный руководитель: **Сидоркина Ирина Геннадьевна,**
доктор технических наук, профессор, декан факультета информатики и вычислительной техники,
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

СИСТЕМА ЗАЩИЩЕННОЙ СВЯЗИ НА ОСНОВЕ СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ

Информация всегда являлась одним из самых дорогостоящих товаров, причем ее ценность зачастую определяется кругом лиц,

допущенных к ней. В современном мире, характеризующимся колоссальными объемами, скоростьюи географической рассредоточенностьюинформационных потоков, наряду с конфиденциальностью информации, особенно остро стоит вопрос актуальности и доступности.В связи с этим большой интерес представляют системы защищенной связи в режиме реального времени.

Исторически сложилось так, что при построении подобных систем в подавляющем большинстве случаев используются криптографические методы защиты информации. Целью же данной работы является показать преимущества применения стеганографии в системах защищенной связи.

Обобщенная система передачи информации состоит из 5 основных компонентов: источник информации, передатчик информации, канал связи, приемник информации и получатель информации. С точки зрения информационной безопасности наиболее предпочтительным является использование выделенного канала связи в распределенной вычислительной системе[2]. Но подобный подход имеет ряд недостатков:

1. Сложность и высокая стоимость реализации;
2. Сложность внесения изменений в конфигурацию;
3. Низкая отказоустойчивость.

Таким образом, несмотря на значительные преимущества при обеспечении конфиденциальности информации, существенно страдает актуальность и доступность, а значит необходимо использование широковещательной среды передачи, например, сети Интернет, чтобы адресат смог вовремя получить необходимую информацию, где бы он ни находился.

Для безопасной передачи информации по открытой транспортной сети используются различные технологии защищенного канала, который подразумевает выполнение следующих функций[3]:

1. Взаимная аутентификация абонентов при установлении соединений;
2. Защита передаваемой по каналу информации от несанкционированного доступа;
3. Подтверждение целостности поступающей информации.

В настоящее время самым распространенным и сложно идентифицируемым разрушающим информационным воздействием на систему является удаленная сетевая атака [2], осуществляемая по каналам связи, что предъявляет дополнительные требования к

обеспечению их безопасности.Этот вопрос решается с помощью различных криптографических методов.

Стойкость большинства криптоалгоритмов базируется на вычислительной сложности решения конкретных задач за полиномиальное время, например в основе системы RSAлежитзадача факторизации больших чисел [4].

Развитие технологий заостряет внимание на следующих проблемах современной криптографии:

1. Ограниченность числа задач, на которых базируются криптоалгоритмы;

2. Постоянный рост размеров блоков данных и ключей;

3. Решение задачиNP –сложной задачи.

Данные проблемы несут несомненную угрозу стойкости криптоалгоритмов, в связи с этим возрастает интерес к стеганографии.

Большое количество разнородной информации, обилие и скорость каналов передачи предоставляют отличный плацдарм для применения различных методов компьютерной стеганографии, при этом значительным преимуществом обладает тот, кто скрывает информацию. А возможность интеграции криптографических алгоритмов в стеганографические системы повышает степень защищенности информации [5].

Несмотря на то, что методы стеганографии становятся все более востребованными в современном мире, степень теоретических изысканий в этой области достаточно мала для успешного развития этого направления [1].В частности,применение стеганографии в системах защищенной связи создает объективные трудности для идентификации канала связи и выявления конечного адресата, что позволяет, если не избежать, то значительно усложнить проведение атак на систему связи, а значит существенно повышает стойкость подобных систем.

Список литературы

1. Грибунин В.Г., Костюков В.Е., Мартынов А.П., Николаев Д.Б., Фомченко В.Н. Стеганографические системы. Атаки, пропускная способность каналов и оценка стойкости: Учебно-методическое пособие // Под ред. В.Г. Грибунина. Саров:ФГУП"РФЯЦ-ВНИИЭФ", 2015.

2. Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака на Internet // ДМК, 1999.

3. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. – СПб.: Питер, 2017.

4. Фергюсон Н., Шнайер Б. Практическая криптография. : Пер. с англ. – М. : Издательский дом «Вильямс», 2005.

6. Карманова Е.В., Сидоркина И.Г. Влияние факторов стегосистем и оценка стегостойкости с использованием потокового навязанного контейнера: Труды Международного научно-технического конгресса «Интеллектуальные системы и информационные технологии - 2019» («ИС& ИТ-2019», «IS&IT'19»). Научное издание в 2-х т. Т. 2. – Таганрог: Изд-во Ступина С.А., 2019.

УДК 004.9

Кириллов Игорь Геннадьевич
направление Информатика и вычислительная техника (магистратура), гр. ИВТм– 22

Научный руководитель: **Кубашева Елена Сергеевна**
к.т.н., доцент каф.ИВС
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ ТИПОГРАФИЕЙ СПЕЦИАЛИЗИРОВАННОГО НАЗНАЧЕНИЯ

Аннотация
Статья описывает основные положения автоматизированной системы контроля и управления производственным процессом. Приводятся новые решения, функции, с помощью которых автоматизированная система имеет большую функциональность.

Ключевые слова: CRM, PHP, MySQL, информационная система.

За последние несколько лет объем и оборот информационных данных в различных сферах деятельности человека – экономической, политической, духовной, экономической, значительно возрос. Сам же процесс обработки, использования и накопления информации значительно ускоряется с каждым годом. Многие ученые говорят, что через десять лет объем используемой информации увеличится вдвое. Именно поэтому возникает необходимость использования автоматизированных средств обработки, хранения и распределения данных и информации.

Автоматизированных систем управления имеется целое множество. Недостатки многих автоматизированных решений в том, что типографии придется подстраиваться под возможности данной системы, хотя должны быть наоборот – автоматизированная система должна быть адаптирована под потребности компании.

Так как данная система управления разрабатывается для конкретного предприятия, соответственно она будет индивидуализирована под конкретные бизнес-процессы. Также будет реализована более полная интеграция системы в существующие базы данных типографии.

Целью работы является уменьшение времени обслуживания, повышение эффективности принятия решений при оперативном управлении взаимоотношениями с клиентами. Исходя из поставленной цели, в данной работе решаются следующие задачи:

1. Провести системный анализ предметной области для обоснования функциональности разрабатываемой системы управления взаимоотношениями с клиентами.
2. Разработать модель управления процессом взаимодействия с клиентами.
3. Разработать структуру системы управления взаимоотношениями с клиентами.
4. Разработать модуль для оперативного отслеживания оборота документов и расчетов по нему.
5. Разработать программное обеспечение для управления процессом взаимодействия с клиентами.

Методы исследования заимствованы из областейобщей теории систем и системного анализа, факторного анализа, теории управления и теории принятия решений, системного моделирования, моделирования информационных систем.

Предметом исследования является модель управления процессом взаимодействия с клиентами.

Новизна исследования заключается в том, что предложены механизмы для обработки данных, которые отличаются от известных большей интеграцией системы, позволяющей загружать и выгружать информацию о покупателях; разработанная структура веб-интегрированной системы, в отличие от известных, осуществляет интеллектуальное обеспечение: ведение статистики заказов, в соответствии с которой формируется информация о наличии или отсутствии необходимых для производства материалов, и в дальнейшем, автоматическое пополнение, заказ всего необходимого для производства, что позволяет достичь автоматизации базовых процессов.

Практическую ценность работы составляет разработка прототипа веб-интегрированной системы управления взаимоотношениями с клиентами, позволяющей повысить эффективность при обработке

данных клиентов в процессе оперативного управления взаимоотношениями с клиентами.

Одна из основных задач, которую решает данная система - организация работы с клиентами с возможностью составлением отчетов. Во многих системах данные возможности присутствуют, но одновременно вместе с необходимыми в пакете программного обеспечения имеются и многие другие, которыми, возможно, так и не воспользуются, так как одни функции явно избыточны, другие продублированы уже используемым программным обеспечением.

Предложенная система представляет из себя веб-интегрированную автоматизированную систему управления. Данная система управления имеет несколько блоков, которые представляют структуру системы.

№ п/п	**Наименование модуля**	**Функции модуля**
1)	ПМ Авторизация	Выполняет авторизацию пользователей при их доступе в систему
2)	ПМ Главное меню	Производит вызов меню, для каждого вида пользователей - своего
3)	ПМ работы со справочниками	Содержит определенные процедуры, позволяющие осуществлять редактирование справочников
4)	ПМ Работа с отчетами	Формирует документы в соответствии с заданными критериями, регистрирует документы, добавляет записи
5)	ПМ получения отчетов	Содержит заранее определенные процедуры формирования отчетных документов
6)	ПМ вывода на печать	Выводит результатные документы на печать

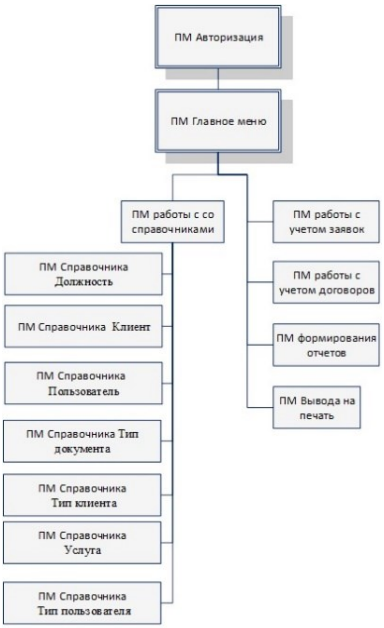


Рисунок 1 Программные модули системы

Также предложены несколько модулей, которые не реализованы во многих автоматизированных системах. Модуль для работы с клиентами в принципе имеется во многих подобных системах. В данном же случае предлагается расширить его функционал, добавив большей полей для обработки данных пользователей, а неиспользуемые поля, которые реализованы в готовых системах, не добавлять в данную систему.

Также предлагается модуль статистики ведения заказов. Данный модуль встречается не так часто в подобных системах, а его эффективность может быть недооценена. Одна из необходимых функций, которая может использоваться при реализации данного модуля заключается в том, что можно автоматизировать процесс заказа материалов для печати. В данном случае система самостоятельно отслеживает какие материалы расходуются на производстве, и в дальнейшем может самостоятельно отправлять сообщения поставщикам о необходимости доставки какого-либо материала для печати. Также на основе заказов можно предполагать какие виды заказов более предпочтительны в различное время года.

Для реализации данной системы выбран язык программирования php и СУБД MySql.

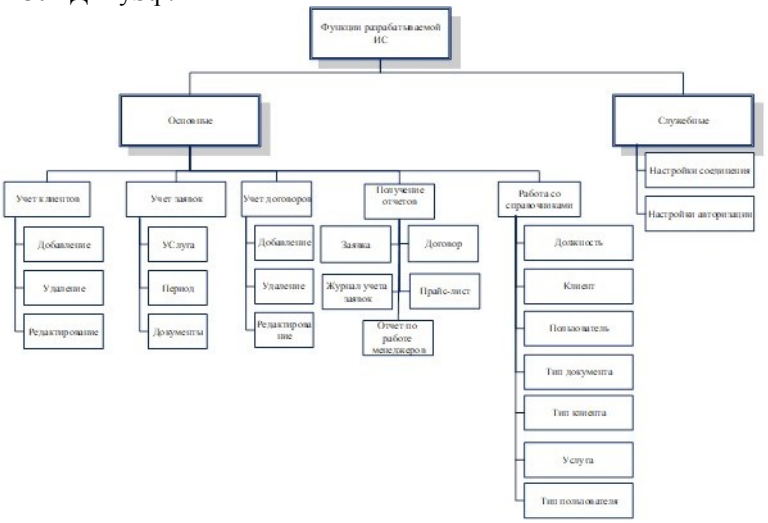


Рисунок 2 Дерево функций

Данная система может использоваться типографиях, так как разрабатывалась под данный тип предприятий. При доработке данной системы она может использоваться и в других отраслях.

Список литературы

1. Алистер Коберн, Современные методы описания функциональных требований к системам, М., Лори, 2017 г., 288 с.

2. Васильев Р.А, Калянов Г.А., Левочкина Г.А., Стратегическое управление информационными системами, М, Интернет-университет информационных технологий, Бином. Лаборатория знаний, 2017 г, 512с.

3. Демин В. CRM нельзя купить, CRM – это стратегия вашего бизнеса. М., 2001 г.

4. Друкер П. Ф. Задачи менеджмента в 21-ом веке.: Пер. с англ. – М.: Изд. Дом «Вильямс», 2000 г.

5. Картышев С.В., Кульчитская И.Н., Поташников Н.М. Управление комплексом маркетинга на предприятии на основе CRM-технологии // Маркетинг в России и за рубежом. – 2002 г. - №2

УДК 004.91

Логинова Эльвира Владимировна
направление Информатика и вычислительная техника (магистратура),
гр. ИВТм– 22

Научный руководитель: **Кубашева Елена Сергеевна**
К.т.н., доцент каф.ИВС
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ИНТЕГРИРОВАННАЯ АВТОМАТИЗИРОВАННАЯ СИСТЕМА СКЛАДСКОГО УЧЁТА И УПРАВЛЕНИЯ СКЛАДОМ

Аннотация

В статье рассмотрена задача слияния Автоматизированной системы складского учета (АСУ ММЗ) с автоматизированной системой управления складом (управление штабелером).Выявлены проблемы, встающие при автоматизации складского комплекса.

Ключевые слова: склад, складская система, управление складом, автоматизация склада, автоматизированная система управления складом, управление штабелером, реинженеринг.

Повышение эффективности промышленного производства в любое время и при любых условиях является важной, актуальной задачей. Существенную роль в ее решении играет внедрение комплексных автоматизированных систем складского учета, основанных на новейших средствах получения и обработки информации в режиме реального времени, что позволяет снизитьвременные и трудовые затраты.

Также значимую роль в производстве играет применение автоматизированных складских комплексов, предназначенных для хранения иобработки товаров, обеспечивающих быструю и безошибочную приемку ивыдачу грузов. Внедрение таких комплексов позволяет решать проблемы, связанные с уплотнением хранения, повышением культуры производства,предотвращением несанкционированного доступа, снижением времени доступак хранимым грузам и т. д.

Автоматизация складского хозяйства как с точки зрения внедрения аппаратных систем, так и с точки зрения развертывания программных комплексов способствует развитию предприятия за счет сокращения площадизанимаемой складом, ускорения операций по работе с грузами, увеличениюточности и обеспечению безопасности грузов при их

хранении, а четкий учетпомогает сэкономить средства и избавить от увеличения складских запасов.

Целью исследовательской работы является повышение уровня автоматизации и механизации складских операций Марийского Машиностроительного завода путем слияния автоматизированной системы складского учета и управления автоматизированным штабелером. Обеспечить переход от бумажных карточек к автоматизированным рабочим местам. Исходя из поставленной цели, в данной работе решаются следующие задачи:

- Исследование функциональных возможностей различных комплексных автоматизированных систем складского учета;
- Исследование существующей автоматизированной системы предприятия управления складом(управление штабелером) и исследование АСУ ММЗ;
- Интеграция системы управления складом с АСУ ММЗ, с учетом особенностей используемого контроллера ПЛК 110-64 фирмы ОВЕН и языка программирования Delphi;
- Проверка корректности работы автоматизированной системы складского учета на действующей системе управления складом;
- Внедрение в производство предприятия.

Первоочередная задача, которую следовало решить перед проектированием и разработкой АСУ складским комплексом, – проведение обследования процессов предметной областивнедрения автоматизированной системы и выявление критичных функциональных требований к АСУ ММЗ. В рассматриваемом случае такиетребования свелись к обеспечению совместимости с уже существующей информационной инфраструктурой складского хозяйства. Необходимо реализовать работу с заданием на комплектацию и обеспечить возможность работы одновременно с двумя различными системами.

Методы исследования:информационного поиска; эмпирические методы (методы анализа литературы); изучение и анализ автоматизированных систем складского учета; структурный анализ и проектирование информационных систем, моделирование с использованием языка UML,методы объектно-ориентированного анализа, проектирования и программирования.

Объектом исследования является процесс автоматизации управления складом в Марийском Машиностроительном Заводе.

Предметом исследования является средства автоматизации процессов управления складом и складского учета.

Новизна исследования заключается в том, что предложена архитектура автоматизированной системы управлениясскладским комплексом, позволяющая без использования сторонних средствинтеграции обеспечить складской учет и комплектование сборок с выдачейинформации в корпоративную информационную систему предприятия.Разработаны модели анализа складских процессов Марийского Машиностроительного завода, позволяющие проводить реинжиниринг ипоследующую автоматизацию работы складов предприятия в целом.

Практическую ценность работы составляетреализация интеграции автоматизированной системы складского учета (АСУ ММЗ) с автоматизированной системой управления складом (управление штабелером).

Внедрение в производство реализованной системы позволит повысить уровень автоматизации на заводе, и достичь следующих количественных показателей:

- сокращение времени, затрачиваемого на складские операции, в 1,5-2 раза;
- увеличение точности выполнения работ;
- возможность управления складом через ПК;
- значительное сокращение возможных ошибок в базе данных;

На рынке множество решений, предлагаемые как крупными отечественными производителями ПО, так и зарубежными создателями специализированного ПО, помимо этого свои решения предлагают и небольшие фирмы – разработчики. Решения, предлагаемые такими фирмами, как Microsoft, Oracle и SAP, являются более привлекательными для автоматизации «с нуля», но они в основном предназначены для оптимизации складских комплексов торговых организаций. Также отличительным недостатком данных систем является высокая стоимость услуг и внедрения таких систем в производство.

Стоимость представленной системы значительно отличается от предложений других компаний. Отличительной особенностью является то, что система подстраивается уже под имеющуюся систему управления складом, разработанной инженерами завода и дополняет уже существующую систему АСУ ММЗ. Так же это является и недостатком системы, так как система требует доработки под другие складские комплексы.

Список литературы

1. Капулин, Д. В. Автоматизация планирования мелкосерийного производства сетевыми методами / Д. В. Капулин, М. В. Винниченко, Д. И. Винниченко // Прикладная информатика. – М.: Университет «Синергия», 2016. – Т.11. – №6(66). – С.6–18.

2. Кульга, К. С. Автоматизация технической подготовки и управленияпроизводством на основе PLM-системы / К. С. Кульга. – М.: Машиностроение, 2008. – 265 с.

3. Чемидов, И. В. Особенности применения автоматизированныхскладских комплексов в радиоэлектронном производстве / И. В. Чемидов, М. А. Казанцев, Д. В. Капулин // Системы связи и радионавигации : сб. тезисов / науч.ред. В. Ф. Шабанов ; отв. за вып. А. Ю. Строкова. – Красноярск : АО «НПП«Радиосвязь»», 2016. – С. 428–431.

4. Лифтовые автоматизированные складские системы [Электронныйресурс] : Официальный сайт компании Компания инноваций и технологий. –Режим доступа: http://www.kiit.ru/katalog/avtomatizirovannye-sklady/liftovyesklady/ (дата обращения: 12.05.2017).

УДК 004.422

Лоскутов Павел Олегович
направление Информатика и вычислительная техника (магистратура), гр. ИВТм– 21

Научный руководитель: **Савинов Александр Николаевич**
К.т.н., доцент каф.ИВС
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

АРХИТЕКТУРА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СИСТЕМЫ СБОРА И АНАЛИЗА ФЕНОЛОГИЧЕСКИХ ДАННЫХ

На данный момент актуальной является задача восстановления фенологических наблюдений на территории РФ и расширения сети добровольных корреспондентов-фенологов РГО с целью сбора уникальных наземных фенологических наблюдений. Совершенно необходимо создать структуру, способную на современном уровне координировать и направлять наблюдения и исследования в определенное русло хозяйственных и научных интересов общества. Структурой, позволяющей достигнуть практических результатов, мог бы стать разрабатываемый портал сбора фенологических наблюдений.

Разработанное программное обеспечение позволит решить следующие задачи:

1. Сбор и накопление возможно более полной информации о сезонных событиях в явлениях живой и неживой природы, с последующим сравнением хода сезонных явлений и исследованием корреляции между ними.

2. Формирование с помощью Интернет разветвленной сети добровольных наблюдателей (корреспондентов-фенологов), которая позволит детально описывать фенологические процессы, корректировать невольные ошибки и снизить риск пропуска явлений.

3. Определение и прогнозирование оптимальных сроков проведения сельскохозяйственных работ, работ в лесной отрасли, охотничьих, рыбоводческих и прочих хозяйствах.

Предложено разработать описываемую систему в виде веб-портала и веб-приложения. Разработана структура и архитектура Системы сбора и анализа фенологических данных. Разработанная архитектура представлена в виде UML диаграммы развертывания (см. рис. 1).

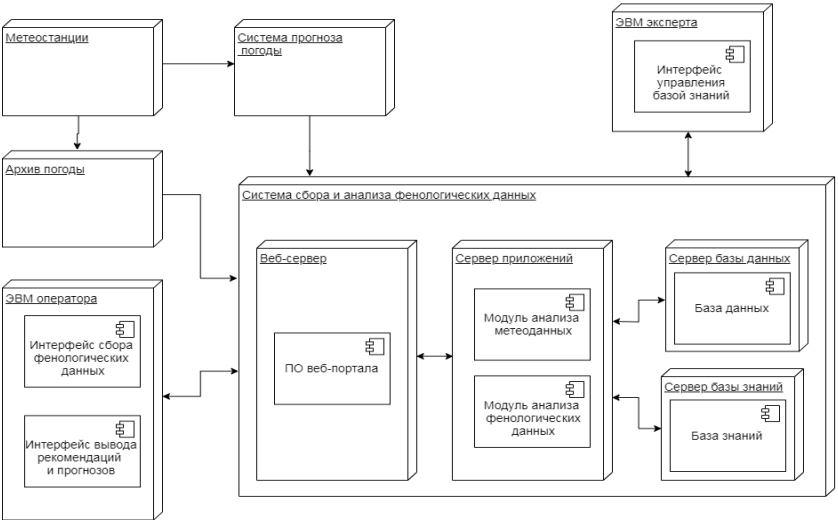


Рисунок 1 – UML диаграмма развёртывания. Архитектура Системы сбора и анализа фенологических данных.

В состав предложенной системы входят:

1. Метеостанции, архивы погоды и системы прогноза погоды. Являются внешним звеном Системы. В разработанной Системе должны быть реализованы интерфейсы взаимодействия с указанными

объектами, выполняющие функции получения данных о текущем и прогнозируемом состоянии погоды в природе в конкретном географическом районе. Состояние природы описывают следующие переменные: текущая температура, количество осадков за последний период наблюдения, солнечная активность.

2. Модуль анализа метеоданных. Данное программное обеспечение реализовано с целью анализа текущих метеоданных для конкретной местности и расчета на их основе агрометеорологических и фенологических показателей, таких как сумма эффективных/активных температур, количество осадков и накопление солнечной энергии за последний период.

3. База данных. Реляционная база данных, выполняющаяся на сервере СУБД MySQL. Поддерживает подключение по HTTP. Содержит в себе таблицы для сохранения учетной информации о наблюдаемых метеорологических и фенологических явлениях в конкретной местности. В базе данных планируется хранение регистрационной информации о пользователях всероссийской сети добровольных корреспондентов-фенологов.

4. База знаний. Служит для хранения правил сопоставления метеорологических показателей со сроками наступления фенологических явлений. Является основой экспертной системы анализа фенологических данных. Обеспечиваются возможности ручного обучения и автоматического самообучения системы.

5. Модуль анализа фенологических данных. Реализует экспертную систему сбора и анализа фенологических данных. Определяет сроки наступления фенологических явлений по полученным метеорологическим данным и прогнозам погоды. Выявляет сроки зависимости сроков наступления фенологических явлений и их корреляцию с метеорологическими показателями для конкретной местности.

6. Веб-сервер. Служит для генерации веб-страниц с интерфейсом, пользователя Системы. Служит для соединения всех компонентов Системы в единое целое. Отвечает за процедуры регистрации и авторизации пользователей, сбор и предварительный анализ данных. Для выполнения данных функций разработано ПО на языках PHP и Python, устанавливаемое и выполняемое на Apache-сервере. Пользователь подключается к веб-серверу системы через Интернет по протоколу HTTP, используя свой браузер или мобильное программное обеспечение.

7. Интерфейс сбора фенологических данных. Специальный интерфейс, разработанный для пользователей добровольной сети корреспондентов-фенологов.

8. Интерфейс рекомендаций и прогнозов. Позволяет просмотреть в интерактивной форме сроки наступления ближайших фенологических явлений в конкретном географическом районе.

9. Интерфейс управления базой знаний. Позволяет в ручном режиме редактировать правила корреляции метеорологических и фенологических явлений.

Разработанная архитектура системы сбора и анализа фенологических данных позволит получить эффективное веб-приложение, позволяющее обеспечить высокую доступность для пользователей системы. Разработанная архитектура позволит справится с высокой нагрузкой, которая будет связана с анализом большого объёма метеорологических и фенологических данных.

Список литературы:

1. Коржов В.С. Многоуровневые системы клиент-сервер. Издательство Открытые системы, 1997. – 200 с.

2. Ананченко И.В. Проектирование современных инфокоммуникационных сетей с использованием технологий программно - конфигурируемых сетей и виртуализации сетевых функций Ананченко И.В., Щербович - Вечер А.В. Символ науки. 2015. № 12 - 1. С. 11 - 13.

УДК 004.5

Лоскутова Светлана Сергеевна
направление Прикладная математика иинформатика (магистратура), гр. 4199

Научный руководитель: **Валитова Наталья Львовна,**
канд.техн. наук, доцент кафедры прикладной математики и информатики
ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ»,
г. Казань

РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ РЕШЕНИЯ ОБРАТНЫХ ЗАДАЧ ПРОЧНОСТИ АВИАКОНСТРУКЦИЙ С ПРИМЕНЕНИЕМ МЕТОДА АНАЛИЗА ЧУВСТВИТЕЛЬНОСТИ

Цель работы – разработка алгоритма чувствительности и программного обеспечения для вычисления ошибки измерений

деформаций жесткости продольных ребер на растяжение-сжатие в сечениях, полученных путем проведения экспериментов с использованием четырехпоясного кессона квадратного сечения, один конец которого жестко закреплен, а на другом – приложена осевая нагрузка на два противоположных ребра.

В области авиастроения в настоящее время остаются **актуальными** вопросы обеспечения безопасности конструкций авиатранспорта. Рассчитываются диаграммы и графики деформирования материалов элементов тонкостенных конструкций. Приближенность математических данных достаточно велика от данных, полученных методом экспериментов с реальными материалами.

Таким образом, возникает вопрос о разработке методики измерения деформаций жесткости материалов не для прообразов конструкций, а для реальных элементов.

Решением задачи является восстановление жесткости продольных ребер на растяжение-сжатие в сечениях.

На рисунке представлен четырехпоясный кессон квадратного сечения, один конец которого жестко закреплен, а на другом – приложена осевая нагрузка на два противоположных ребра (рис.1).

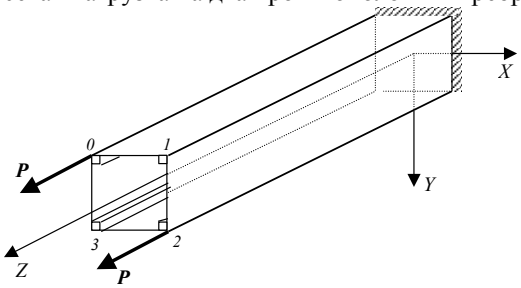


Рис. 1. Квадратный кессон с осевой нагрузкой на противоположные ребра

Математическая часть поставленной задачи состоит из:

1. Решения задачи оптимизации, для получения общего вида.
2. Решения задачи с помощью метода интегрирующих матриц, для применения численных методов.
3. Определения алгоритма чувствительности.
4. Решение прямой задачи прочности, для получения экспериментальных данных.
5. Нахождение приближений деформации, для определения вычисления целевой функции, полученной в п.3.

6. Рассчитывается ошибка в идентификации жесткостей ребер с применением данных из п.6.

Разработка рабочей программы основана на языке программирования C# и базы данных MicrosoftSQL.

Модули, которые должны присутствовать в программной части:

1. Расчетный, в котором отображается расчет формул.

2. Графический, в котором отображаются графики приближений.

База данных при взаимодействии спрограммной частью должна сохранять и выгружать при необходимости расчетные данные для дальнейшего их использования.

Программа дает возможность получать результаты расчетов без применения физических усилий, помогает в точности получать графические результаты измерений и сохранять или выгружать данные из единой базы данных.

Выводы

Программа с подобным алгоритмом вычисления деформаций поможет в короткий срок провести измерения и получить экспериментальный результат.

Список литературы

1. Баничук Н.В. Введение в оптимизацию конструкций. М.: Наука, 1986. 302 с.

2. Дегтярев Г.Л., Сиразетдинов Т.К. Теоретические основы оптимального управления упругими космическими аппаратами. М.:Машиностроение,1986. 214с.

3. Костин В.А., Валитова Н.Л. Идентификация изгибной жесткости балки с использованием функции чувствительности // Новые технологии, материалы и оборудование российской авиакосмической отрасли: Сб. докл. Всерос. науч.-практ. конф. с международным участием. Казань: АН РТ, 2016. Т.1. С. 86–91.

4. Костин В.А., Хуан Ш., Валитова Н.Л. Применение дискретно-континуальной модели расчета на прочность для решения задачи идентификации теплонагруженной конструкции // Изв. вузов. Авиационная техника. 2017. №3. С. 3–7.

5. Костин В.А., Хуан Ш., Валитова Н.Л. Численные методы анализа чувствительности в задачах идентификации конструкций // Вестник КГТУ им. А.Н. Туполева. 2017. Т. 73.№1. С. 78–83.

6. Костин В.А., Хуан Ш., Валитова Н.Л. Решение обратной задачи прочности тонкостенных конструкций с использованием алгоритма чувствительности // Изв. вузов. Авиационная техника. 2018. №1. С. 123–127.

УДК 622.323

Матвеев Илья Александрович
направление Радиоэлектронные системы и комплексы (специалитет), гр. РСК-61

Научный руководитель: **Смирнов Алексей Владимирович**
к. т.н, доц. каф. Информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

РЕЗОНАНСНЫЙ МЕТОД ОПРЕДЕЛЕНИЯ УРОВНЯ ЗАТРУБНОЙ ЖИДКОСТИ НЕФТЕДОБЫВАЮЩИХ СКВАЖИН

Рассматриваетсязадача определения уровня затрубной жидкости нефтедобывающих скважинпо известной эхограмме акустического шума.

Актуальность. При разработке добывающих скважинкрайне важно контролировать такой параметр как уровень затрубной жидкости. Острая необходимость контроля возникает в случае ремонта скважин и для скважин с высокой подачей. Существующий на данный момент волнометрический метод определения уровня обладает рядом недостатков, а именно:

- отсутствиеполной автоматизации процесса определения;
- необходимость стравливания затрубного газа с целью создания зондирующего акустического импульса;
- невозможность определения малых уровней скважинной жидкости.

Цель работы:

- обеспечение автоматизации определения уровня;
- повышение уровня безопасности труда персонала при обслуживании скважин;
- увеличение степени защиты окружающей среды путем уменьшения вероятности утечек нефти;
- минимизация рисков выхода из строя устьевого и насосного оборудования.

Решаемые задачи:

1. разработать алгоритм определения уровня скважинной жидкости, использующий метод определения резонансной частоты акустического шума в затрубном пространстве;

2. проверить работу алгоритма на эхограммах, зарегистрированных на действующих скважинах с известными параметрами, с целью выставления требований к реализации алгоритма и существующему регистратору шума.

Техника решения (описание проекта). В реальном мире практически недостижима полная звукоизоляция – окружающее пространство заполнено разнообразными шумами. Так в нефтедобывающей скважине основными источниками возникновения акустического шума являются элементы работающего насосного оборудования, движение нефтеносных пластов, течение жидкости по стенкам насосно-компрессорных труб, промышленные шумы и прочие.

Представим скважинув виде отрезка трубы, закупоренного с двух сторон и находящегося под давлением не ниже атмосферного, тогда можно говорить о нем как об объемном резонаторе. Предположим, в нем возникает стоячая волна между устьем скважины и жидкостью в затрубном пространстве, вызванная совокупностью всех факторов существования шума. В таком случае для определения уровня жидкости необходимо определить основную частоту стоячей волны и затем с помощью известной скорости звука в исследуемой скважине произвести вычисления. Часто бывает невозможно определить первую гармонику резонансной частоты.Однако достаточно определить расстояние между соседними гармониками, дабы получить необходимое значение основной частоты.

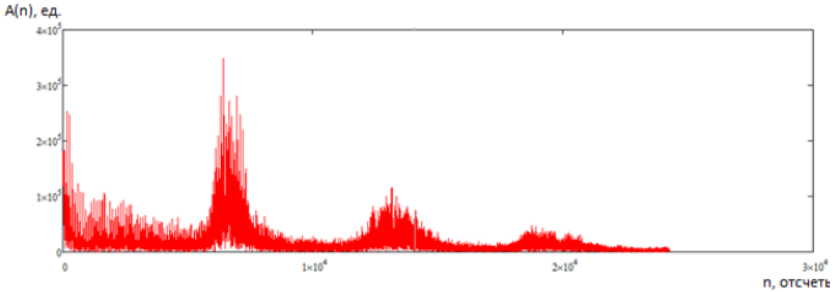


Рис. 1 – Пример выделенного диапазона амплитудного спектра

Путем последовательного разбиения амплитудного спектра исходного сигнала на поддиапазоны, предлагается выделить из него диапазон (рисунок 1), в котором сосредоточена большая часть энергии сигнала. Дополнив найденный диапазон до необходимого разрешения и подвергнув его повторному преобразованию Фурье, определим номер

отсчета, соответствующего максимальному пику. С учетом разрешения вычислим значение уровня скважинной жидкости. Для контроля правильности обнаружения будем использовать отношение абсолютных величин найденного пика к величине второго по значению пика.

Анализ результатов определения уровня по имеющимся эхограммам, снятых с действующих скважин устройством с полосой пропускания до 4 Гц, показал на данном этапе существование систематической критической ошибки (больше 10 м) для некоторых скважин.

Выводы.Таким образом, существует принципиальная возможность определения уровня затрубной жидкости с помощью резонансного метода. Однако для повышения точности определения следует произвести предварительную ВЧ-фильтрацию сигнала и изменить характер поиска поддиапазона. Кроме того полоса пропускания существующего регистратора шума может быть расширена до 20-30 Гц, дабы точно исключить наводки на промышленной частоте.

Список литературы

1. Ржевкин С.Н. Курс лекций по теории звука. – М.: Изд-во МГУ,1960. – 216 с.

2. Акустика в задачах: учеб. рук-во для вузов / под ред. С.Н.Гурбатова, О.В.Руденко. – М.: Физматлит, 1996. – 336 с.

УДК 004.7

Морохина Дарья Дмитриевна
направление Информатика и вычислительная техника (бакалавриат),
гр. ИВТ-11

Научный руководитель: **Морохин Дмитрий Витальевич,**
к.т.н., доцент кафедры информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

СИСТЕМА ВИЗУАЛИЗАЦИИ АНАЛИЗА ПОГРЕБЕНИЙ

Изучение археологических объектов основано на анализе артефактов. При более глубоком анализе количество атрибутов и связей между ними значительно возрастает, что сильно увеличивает трудоемкость процесса исследований.

Рассмотрим данную проблему на примере изучения могильников. Возникает две наиболее актуальные и интересные задачи этой области. Во-первых, это автоматизация процесса определения взаимосвязи между объектами, в том числе скрытых, не явных или второстепенных связей. Во-вторых, визуализация этих связей, позволяющая более наглядно представить результаты исследований.

Могильники состоят из некоторого количества погребений, жертвенных комплексов и заупокойных даров, которые в свою очередь включают в себя другие объекты (одежда, оружие, орудия труда, украшения и т. п.). Эти объекты могут разделяться на типы и под типы, например, перстень усатый, перстень витой и т. п., а также повторяться в разных погребения разных могильников. Определяя совпадения атрибутов объектов можно установить наличие или отсутствие связи между погребениями разных могильников и объединять несколько погребений в определенные группы (Рис.1).

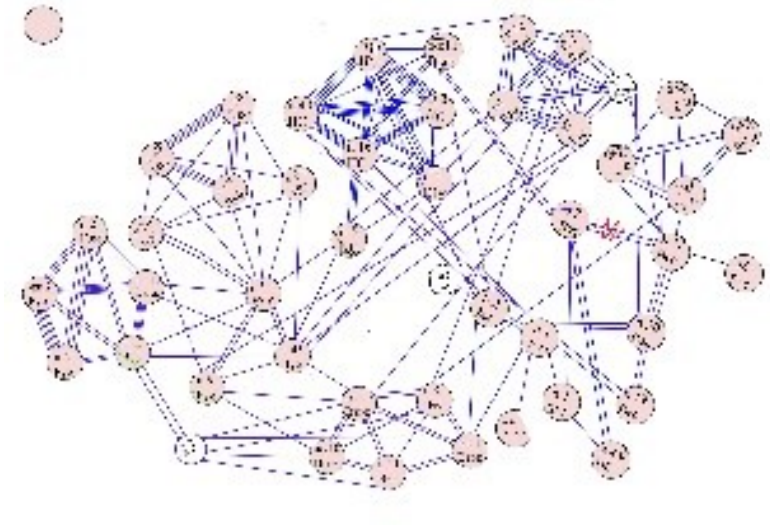


Рис.1. Связи между погребениями

Однако одиночных или множественных связей может быть много, и обрабатывать большое количество погребений по большому количеству объектов достаточно проблематично. Связи накладываются друг на друга, пересекаются и так далее. В такой 'паутине' довольно сложно разобраться, следовательно, требуется автоматизация и визуализация

данного процесса исследований. Одним из первых шагов можно убрать из визуализации малозначащие связи (Рис.2).

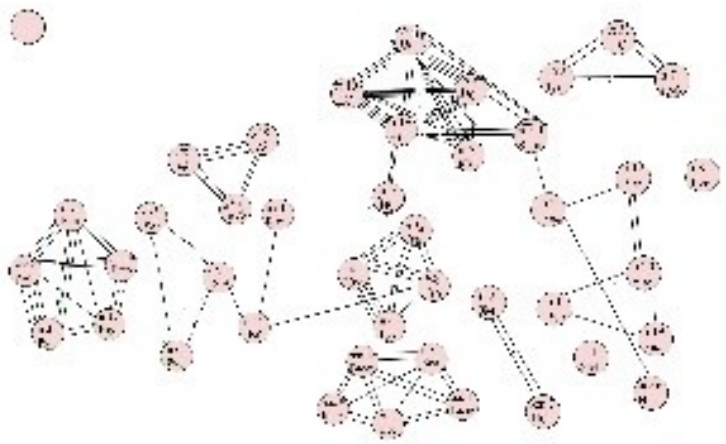


Рис.2. Связи между погребениями (после удаления 2 связей)

Для выявления взаимосвязей можно использовать метод статистического анализа, в частности расчет коэффициентов корреляции таблицы совместимости. Целесообразным видится проведение исследований несколькими методами независимо для поверхностного и более глубокого анализа. Например, методом машинного обучения для решения задачи кластеризации, в частности нейронные сети Кохона, при избыточном количестве нейронов карты способны выявлять скрытые группы внутри больших классов.

На начальном этапе работы над проектом требуется решить две задачи. Первая - определение значимости входных параметров для оптимизации размерности входных данных. Вторая - подбор наиболее подходящих средств и алгоритмов для кластеризации и работы с картографическими данными (Рис.3).

Рис.3. Начальная схема работы системы

УДК 004.7

Николаев Роман Геннадьевич
направление Информационная безопасность автоматизированных систем (специалитет), гр. БИ-51

Научный руководитель: **Смирнов Владимир Иванович,**
старший преподаватель кафедры ИБ
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ ПО РАСПОЗНАВАНИЮ РИСУНКА ВЕН ЛАДОНИ ЧЕЛОВЕКА: ПЕРСПЕКТИВЫ И ПРЕИМУЩЕСТВА

За последние годы одним из наиболее интенсивно развиваемых методов идентификации и аутентификации личности является идентификация по биометрическим характеристикам. На сегодняшний день существует большое разнообразие методов идентификации. Так, системы контроля и управления доступом (СКУД) представляют собой один из развитых сегментов рынка безопасности как за рубежом, так и в России.

СКУД представляет собой комплекс программно-технических средств и организационно-методических мероприятий, назначением которых является контроль помещений, оперативный контроль перемещения персонала, управление доступом посещения помещений [1, с. 49]. Общая схема СКУД представлена на рисунке 1.

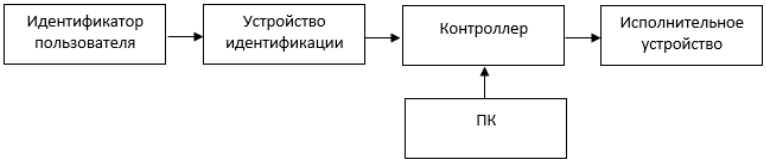


Рис. 1 - Общая схема СКУД

Следует отметить, что существует два основных вида СКУД – автономные и сетевые, которые можно различить по способу управления ими. Если автономные системы не требуют централизованного управления с применением компьютерных технологий, то сетевые СКУД управляются непосредственно центральным компьютером, что, в свою очередь, предоставляет возможность не только оперативно, но и единовременно менять ключи доступа для всех преграждающих устройств (проходных, дверей, ворот). В настоящее время существует много разновидностей СКУД разных производителей, а также ее компонентов [2, с. 14].

Развитие биометрических технологий и, прежде всего, их интеграция с системами контроля доступа способствовали росту рынка СКУД в целом. Крупные предприятия все чаще стали устанавливать системы безопасности, которые позволяют проводить аутентификацию, к примеру,по отпечаткам пальцев, радужной оболочке глаза, а также по распознаванию рисунка вен человеческой ладони.

Подробнее остановимся на идентификации по рисунку вен ладони человека. СКУДна основе данной технологии появились совсем недавно. В связи с тем, что данное новшество позволило существенно повысить безопасность предприятий и других защищаемых объектов, эксперты всего мира признают такие СКУД эффективными.

Помимо этого, система, основанная на идентификации по рисунку вен ладони человека, является наиболее практичной и удобной по сравнению с другими устройствами, которые обеспечивают доступ на предприятие по отпечаткам пальцев или специальным именным картам.

Прежде всего, рисунок вен – это биометрическая характеристика. Основой идентификации по венам ладони выступает сканирование инфракрасными лучами рисунка кровеносных сосудов. Важно то, что, во-первых, у каждого человека свой уникальный рисунок вен ладони, а, во-вторых, такая биометрическая характеристика намного сложнее отпечатков пальцев или радужной оболочки глаза, потому что она скрыта от стороннего наблюдателя и определяется только сканированием в ИК-освещении. Таким образом, данные особенности

позволяют существенным образом повысить точность процедуры распознавания.

Необходимо учитывать, что определенные трудности в работе считывателя могут вносить некоторые болезни человека. К примеру, некоторые формы анемии. Однако, если сопоставить метод распознавания по рисунку вен с другими биометрическими методами идентификации, такой недостаток, скорее, является технологической особенностью.

При этом важно отметить, что основой всех биометрических методов выступают вероятностные и статические методы [3, с. 15]. Для оценки надежности методов существует несколько способов, однако наиболее распространенным является подход, за основу которого принимаются ошибки первого и второго рода.

Ошибкапервогорода (FRR) – это вероятность ложного отказа в доступе пользователю, который имеет право доступа. Ошибка второго рода (FAR) – это вероятность ложного доступа, когда систему ошибочно опознает чужого как своего. Данные характеристики получают расчетным путем с помощью методов математической статистики: чем ниже эти показатели, тем точнее распознавание объекта.

В таблице 1 представлены средние значения FAR и FRR для популярных в настоящее время методов биометрической идентификации [4]. Как можно видеть из таблицы, биометрия ладони является достаточно точной: хотя по FAR уступает многим методам биометрии, однако по FRR является наилучшим методом.

Таблица 1 –Средние значения FAR и FRR

Метод биометрической идентификации в СКУД	FAR	FRR
Отпечаток пальца	0,001%	0,6%
Распознавание лица 2D	0,1%	2,5%
Распознавание лица 3D	0,0005%	0,1%
Радужная оболочка глаза	0,00001%	0,016%
Сетчатка глаза	0,0001%	0,4%
Рисунок вен	0,0008%	0,01%

Кроме того, статистика говорит о том, что мировой рынок биометрических систем достаточно активно применяет технологии, которые основаны на распознавании и использовании следующих биометрических данных [5]: отпечатки пальцев (более 50% всего объема рынка), изображение лица (21,6%), изображение радужной оболочки глаза (10,2%), голос (4%), рисунок вен (3%); геометрия ладони, ДНК и иное (около 7%).

При этом наиболее перспективными являются такие технологии, как идентификация по изображению радужной оболочки глаза и по рисунку вен ладони человека. Соответственно, можно предположить, что они станут самыми быстрорастущими сегментами рынка СКУД в ближайшие 5-10 лет. Так, согласно прогнозу среднегодового темпа роста рынка биометрических систем, в разрезе технологий до 2020 года [5], ситуация будет следующей (рисунок 2).

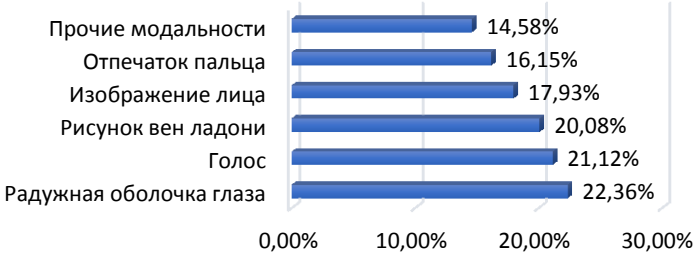


Рис. 2 - Прогноз среднегодового темпа роста рынка до 2020 года

Говоря о российском рынке СКУД, необходимо отметить, что аутентификация по рисунку вен представляет перспективное направление. Кроме того, рынок России в сравнении с мировым значительно отличается, так за последние четыре года в общем объеме российского биометрического рынка доля технологии идентификации по отпечаткам пальцев уменьшилась в два раза, а доля технологии распознавания по венам стала гораздо выше по сравнению с мировой тенденцией. В формирование спроса на данную технологию у нас в стране основой вкладвнеслакомпания «Прософт Биометрикс».

В заключение отметим, что технология распознавания рисунка вен ладони человека является сравнительно простой в реализации, а также довольно точной.Кроме того, метод не требует столь дорогого оборудования, как, например, методы распознавания по геометрии лица или радужной оболочке глаза. Реализация данной технологии позволяет существенно повысить уровень защищенности СКУД в целом.

Список литературы

1. Капинос И.С. Современные тенденции в построении систем контроля и управления доступом // Молодой ученый. - 2019. - № 22. - С. 49-51.

2. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом // М.: Горячая линия-Телеком, 2010. – 272 с.

3. Сабанов А.Г., Смолина С.Г. Сравнительный анализ методов биометрической идентификации личности // Труды ИСА РАН. – 2016. - № 3. – С. 11-20.

4. Технологии и методы биометрической идентификации [Электронный ресурс] // Режим доступа: http://www.techportal.ru/security/biometrics/tekhnologii-biometricheskoy-identifikatsii/ (дата обращения: 09.10.2019).

5. Обзор международного рынка биометрических технологий и их применение в финансовом секторе [Электронный ресурс] // Режим доступа: https://www.cbr.ru/content/document/file/36012/rev_bio.pdf (дата обращения: 28.09.2019).

УДК 534.014.2/534. 111/ 378.147

Попова Ирина Андреевна
направление Строительство (бакалавриат), гр. 314

Научный руководитель: **Белкин Александр Анатольевич,**
доктор физ.-мат. наук, заведующий кафедрой теоретической механики
«Новосибирский Государственный Архитектурно-Строительный Университет (Сибстрин)»,
г.Новосибирск

ЭЛЕКТРОННОЕ ОБУЧАЮЩЕЕ СРЕДСТВО «ИЗУЧЕНИЕ КОЛЕБАНИЙ НАНОРАЗМЕРНОГО ОСЦИЛЛЯТОРА МЕТОДОМ МОЛЕКУЛЯРНОЙ ДИНАМИКИ»

Электронные обучающие системы, включающие электронные учебники, тренажеры, тесты, лабораторные работы на ЭВМ, получают сегодня широкое распространение при подготовке квалифицированных инженерных кадров. Они позволяют излагать материал в наглядной форме, изучать его самостоятельно, в том числе дистанционно, реализовывать интерактивные технологии. Также они дают возможность познакомить студента с современными методами моделирования. Одним из них является метод молекулярной динамики основанный на моделировании веществ (газов, жидкостей, кристаллов) набором молекул с заданным законом взаимодействия между ними [1]. **Цель** данного исследования – МД моделирование колебаний наноразмерного поршня в цилиндре с плотным газом и создание на базе результатов моделирования электронной лабораторной работы.

Актуальность работы обусловлена несколькими факторами. Колебания широко распространены в природе и технике, поэтому изучаются во многих дисциплинах технических университетов.

Примененный метод МД является уникальным инструментом изучения нанообъектов, и в частности наножидкостей [2]. Их свойства уникальны и изучены далеко не до конца. Строго говоря, описываемая ниже изучаемая система также представляет собой наножидкость, поэтому полученные результаты имеют, помимо образовательной, и научную ценность. Таким образом, спектр использования разработанного программного обеспечения в образовательном процессе (ознакомление с колебательными системами, основами метода МД, методиками изучения наножидкостей) достаточно широк.

В ходе работы было решено несколько основных задач. Первая – изучение метода МД и программного пакета LAMMPS [3]. Пакет LAMMPS имеет встроенную базу потенциалов взаимодействия, а также набор функций для управления системой молекул и измерения ее характеристик. Он находится в открытом доступе и может быть установлен на любом современном ПК.

Второй задачей было создание МД модели наноразмерного газового осциллятора. Он состоит из заполненного молекулами газа цилиндра с подвижной твердым непроницаемым поршнем, поршень делит газ на две области (рисунок 1). Искусственно сдвинув его из положения равновесия, можно инициировать колебания поршня. Движение молекул газа сопровождается вязким сопротивлением, что будет приводить к затуханию колебаний.

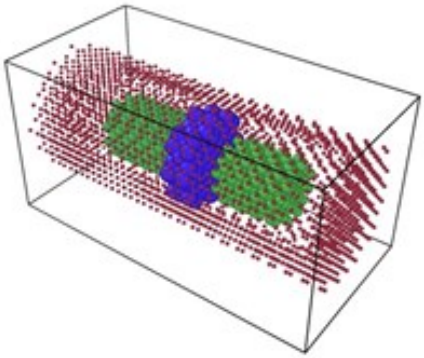


Рис. 1 – Ячейка моделирования. Красный цвет имеют неподвижные молекулы стенок, зеленый – подвижные молекулы газа, синий – движущиеся вместе молекулы поршня

Для реализации описанной выше модели был написан и отлажен программный код на собственном языке программирования пакета LAMMPS. Параметры потенциала взаимодействия молекул всех типов

соответствовали аргону, система изучалась при комнатной температуре, давление газа при неподвижном поршне составляло около ста атмосфер.

Наконец, последней задачей было определение закона движения поршня и зависимостей характеристик колебаний (в частности, частоты и декремента затуханий) от массы поршня. Эта задача также была решена, данные моделирования сопоставлены с известными аналитическими формулами. Такое исследование может быть предложено студенту при выполнении электронной лабораторной работы.

Дифференциальное уравнение линейных затухающих колебаний осциллятора имеет следующий вид

$$\ddot{x} + 2b\dot{x} + k^2 x = 0, \qquad b = \mu / 2m,\ k^2 = c/m, \tag{1}$$

где m – масса, c – коэффициент жесткости газовой «пружины», μ – коэффициент вязкого сопротивления. Решение уравнения (1) в случае слабого сопротивления имеет вид

$$x = Ae^{-bt}\cos(k^* t + \alpha), \tag{2}$$

где $k^* = \sqrt{k^2 - b^2}$ – не зависящая от времени частота колебаний, A, α – начальные амплитуда и фаза колебаний.

В первую очередь необходимо было ответить на вопрос, описывается ли закон движения поршня в системе, изображенной на рисунке 1, уравнением (2).

На рисунке 2 представлена зависимость от времени координаты одной из молекул поршня. Попытка аппроксимировать данные зависимостью (2), показанной пунктирной линией, не приводит к успеху. Видно, что удовлетворительно формула (2) работает примерно до первого минимума (на первом полуколебании системы). Далее частота колебаний поршня увеличивается, что не соответствует уравнению (2) с постоянной величиной k^*.

Для того, чтобы построить аппроксимацию, описывающую закон движения наноразмерного поршня, были построены зависимости от времени значений периода его колебаний при различных массах поршня. Мы варьировали отношение массы молекулы поршня M к массе молекулы газа m. Полученные данные представлены на рисунке 3.

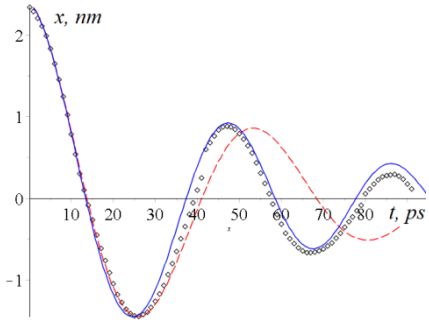


Рис. 2 – Закон движения поршня (метки), его аппроксимации уравнением (2) с постоянным периодом колебаний (штриховая линия) и с периодом, определяемым формулой (3) (сплошная линия)

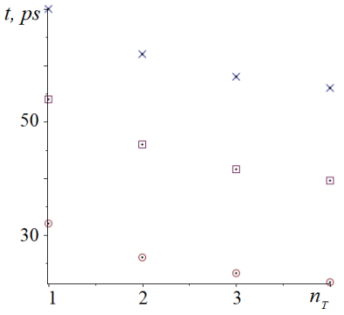


Рис. 3 – Зависимость значений периода колебаний от номера полуколебания, на котором он измерялся, для различных масс поршня M/m =100 (×), 50 (□), 15 (○)

Для разных масс поршня справедлива универсальная зависимость периода колебаний от времени вида

$$T = T_0(1 - t/B), \qquad (3)$$

где T_0 – начальный период, B – константа, зависящая от параметров системы.

Выводы

В работе написана и отлажена программа МД моделирования движения нано-поршня в плотном газе. Установлено, что закон движения не описывается решением уравнения линейных затухающих колебаний, период колебаний уменьшается с течением времени. Построена аппроксимация (3) для описания зависимости периода от времени.

На базе созданного программного обеспечения и полученных результатов мы предлагаем электронную лабораторную работу, которая позволит студенту наглядно изучить основные свойства затухающих колебаний и научиться определять их характеристики.

План лабораторной работы зависит от уровня подготовки обучаемого и может включать следующие основные действия:

1. Ознакомление с программой и ее запуск.
2. Определение положения поршня в разные моменты времени.
3. Сопоставление с уравнениями (2), (3), подбор параметров.

4. Изучение зависимости характеристик осциллятора от массы.
5. Оформление результатов.

Ясно, что этот план нужно варьировать в зависимости от изучаемой дисциплины, так, при изучении информационных технологий акцент должен быть сделан на работу с программой. Лабораторная работа может выполняться на персональном компьютере в удобное для студента время, что позволяет использовать ее в дистантном обучении.

Работа выполнена при частичной поддержке гранта РФФИ №19-01-00399 с использованием программного пакета LAMMPS и программы визуализации движения молекул OVITO.

Список литературы

1. Allen M.P., Tildesley D.J. Computer simulation of liquids. – Oxford : University Press, 1989.
2. Рудяк В.Я., Белкин А.А. Моделирование коэффициентов переноса наножидкостей. Наносистемы : физика, химия, математика. – 2010. – Т.1. № 1. – С. 156-177.
3. https://lammps.sandia.gov
4. https://www.ovito.org

УДК 621.396

Порфирьев Александр Игоревич
направление «Информационная безопасность» (специалитет), гр. БИ-41

Научный руководитель: **Сидоркина Ирина Геннадьевна,**
д-р техн. наук, профессор, кафедра информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ОСОБЕННОСТИ УТЕЧКИ ИНФОРМАЦИИ ЧЕРЕЗ АКУСТООПТИЧЕСКИЙКАНАЛУТЕЧКИИНФОРМАЦИИ НА ОСНОВЕ ФИЗИЧЕСКИХ ЭФФЕКТОВ

Под акустической информацией обычно понимается информация, носителями которой являются акустические сигналы. В том случае, если источником информации является человеческая речь, акустическая информация называется речевой.Первичными источниками акустических сигналов являются механические колебательные системы, например, органы речи человека, а вторичными - преобразователи различного типа, например, громкоговорители.Под утечкой информации по техническому каналу понимается неконтролируемое

распространение информации от носителя защищаемой информации через физическуюсреду до технического средства, осуществляющего перехват информации. [1]

Рассмотрим схему съема информации, осуществляющегося с плоской поверхности, колеблющейся под действием акустической волны, лазерным лучом в ИК-диапазоне.Это обеспечивает невидимость его невооруженным глазом. В качестве поверхности, на которую оказывает воздействие акустическая волна, используется внешнее стекло окна. Стекло облучается источником лазерного излучения с внешней стороны (из окна соседнего дома). На поверхности соприкосновения лазерного луча со стеклом происходит модуляция лазерного луча акустическими сигналами, генерируемыми в помещении (речь, звуковые колебания работающих технических систем).

Лазерные системы наиболее эффективны для прослушивания разговоров в помещениях небольшого размера, которые по своим акустическим характеристикам близки к объемному резонатору, когда все двери и окна помещения достаточно хорошо герметизированы. Эффективны они и для подслушивания разговоров, ведущихся в салонах автомашин. [2]

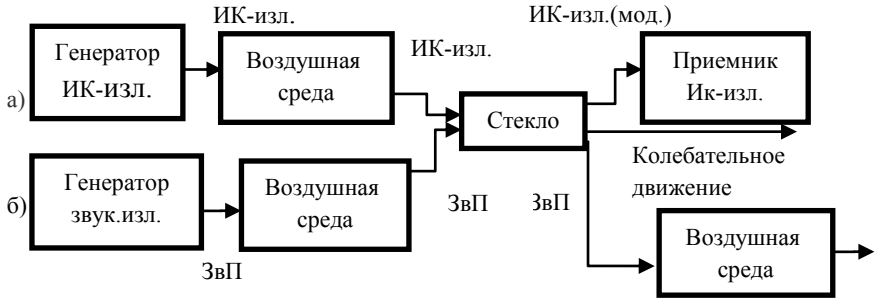


Рис. 1. - Физическая схема лазерной системы

Физические эффекты, используемые в физической схеме (ФСх)(рис.1):

а) 1) эффект отражения света;
2) эффект поглощения света;
3) эффект светопроводимости;
4) эффект модуляции света звуковыми колебаниями;

б) 1) эффект отражения звука;
2) эффект поглощения звука;

3) эффект звукопроводимости;

4) эффект преобразования звукового поля (ЗвП) в механические колебания стекла;

Для преобразования акустического сигнала в оптический могут бытьиспользованы следующие физические эффекты (ФЭ)(рис.1): эффект изменения светопроводимости под действием силы, деформирующей световод; эффект звуколюминесценции; эффект модуляции оптического (лазерного) луча поверхностью отражения, деформируемой звуковыми колебаниями и др.

На эффективность работы лазерной системы существенное влияние оказывает воздушная среда, через которую проходит прямой (мощный) и отраженный (маломощный) оптический сигнал. В воздушной среде проявляется эффект светопроводимости. Увеличение дальности прослушивания может быть осуществлено либо увеличением мощности генератора ИК-излучения, либо повышением чувствительности приемника, либо тем и другим вместе [3].

Эффекты поглощения света и светопроводимости уменьшают мощность отраженного луча ИК-излучения. Для повышения коэффициента отражения в определенном направлении поверхность стекла должна быть гладкой и чистой. Эти же качества будут улучшать светопроводимость, то есть уменьшать мощность отраженного сигнала.

Использование колеблющихся поверхностей объектов, сходящихся внутри помещения, для получения отраженного луча ИК-излучения существенно уменьшает расстояние прослушивания, так как прямой и отраженный лучи должны проходить через три среды как в прямом, так и в обратном направлении: воздушная среда (внешняя) – стекло – воздушная среда внутри помещения[2].

Заключение

Таким образом, уменьшить эффективностьакустооптического канала утечки информации можно следующим образом:

Установлено что, звукоизоляции одинарного остекления недостаточно для надежной защиты информации в помещении. Таким образом, для повышения звукоизоляции рационально использование окон с остеклением в раздельных переплетах с шириной воздушного промежутка более 200 мм или с тройным комбинированным остеклением и шумоизоляцией. Нужно установить жалюзи, заделать имеющиеся в окне щели звукопоглощающим материалом , а также покрыть окна металлизированной пленкой.

Окна должны быть чистыми и гладкими, для усиления светопроводимости, а значит и для уменьшения мощности отраженного

сигнала, или же наоборот, грязной и неровной, для уменьшения коэффициента отражения.

Список литературы

1. П.Н. Девянин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербаков Теоретические основы компьютерной безопасности: Учебное пособие для ВУЗов. – М.: Радио и связь, 2000. – 192с.

2. Хорев А.А. Техническая защита информации: учеб.пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. - М.: НПЦ «Аналитика», 2008. - 436 с.

3. Герасименко В.А., Малюк А.А. Основы защиты информации. – М.: "Инкомбук", 1997. – 540с.

УДК 004.056(075.8)

Порфирьев Александр Игоревич
направление «Информационная безопасность» (специалитет), гр. БИ-41

Научный руководитель: **Сидоркина Ирина Геннадьевна,**
д-р техн. наук, профессор, кафедра информационной безопасности
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

СОКРЫТИЕ ИНФОРМАЦИИ В ФАЙЛАХ ФОРМАТА PDF

Сокрытие информации в файлах формата PDF. Есть несколько способов сокрытия такой информации.Например, т.к. этот формат строится из блоков, состоящих из ключевых слов, между ключевыми словами можно вставлять непечатаемые символы, не опасаясь разрушения внешнего вида документа. Еще один способ сокрытия информации в файлах формата PDF заключается в использовании словаря.

Стеганография - это способ передачи или хранения информации с учетом сохранения в тайне самого факта такой передачи. Методы, которыми можно скрыть информацию в файлах, например,картинок, аудио- и видео- файлов, не повреждая их содержимое и оставляя эти файлы работоспособными. Да, в криптографии существуют методы с большими ключами, которые практически невозможно взломать, но использование таких “массивных” ключей запрещено для публичного применения, так что прятать информацию как раз в данном случае удобнее. А если такое сообщение еще и зашифровать, то это будет еще один дополнительный уровень защиты. Или же, например, если кто-то

пытается украсть данные, то они могут скрывать, тот же троян, в другом файле, например, в рисунке, и отсылать их, не привлекая внимания, по электронной почте или просто при передаче данных.

PDF формат поддерживает интегрированные шрифты и возможность шифрования текстовой информации, растровую и векторную графику. Документы этого формата внешне выглядят как статьи из журнала, в которых содержатся текст и фотографии.PDF файл состоит из таких элементов, как:<header> - заголовка;<body> -самого тела файла, включающего в себя object, последовательность объектов с идентификаторами objectnumber и generationnumber (номер объекта и номер поколения);

Кроме того, файл формата PDF содержит закрывающий тег, называющийся %EOF. Непечатными символами, такими как пробел и табуляция, можно кодировать информацию. Отображаемый документ от этого не изменится.

Есть еще один способ сокрытия информации в документах PDF формата. Между ключевыми словами можно вставлять непечатаемые символы, не опасаясь повреждения внешнего вида документа.

Другой способ сокрытия информации заключается в использовании словарей.Объекты состоят из streamdata и streamdictionary (потока данных и словаря потока). В словаре содержится описание атрибутов объекта. Он также указывает, что объект из себя представляет: текст, изображение, шрифты, информацию о шифровании и его алгоритме. Можно шифровать информацию с помощью словаря, скрывая её в номере объекта. Включив в документ объекты, имена которых соответствуют словарю и не несут в себе информации для вывода на экран монитора, то можно скрыто передавать информацию/ Например: 92= «Привет»,

Скрытая информация также может быть зашифрована. Совместное использование стеганографии и шифрования многократно повышает сложность обнаружения и раскрытия конфиденциальной информации. Методом шифрования называется совокупность обратимых преобразований, в соответствии с алгоритмом шифрования, открытой информации в закрытую информацию. Современные методы шифрования должны выполнять следующие требования:

1. Вскрытие шифра возможно только при полном переборе ключей;

2. Криптостойкость шифра обеспечена секретностью ключа. Криптостойкость измеряется временем или стоимостью тех средств, которые необходимы для получения исходной информации по шифротексту, при условии, что ключ неизвестен;

3. Зашифрованный текст не должен превосходить по объему исходный вариант текста;

4. Ошибки при шифровании не должны приводить к потере или искажению информации;

Время шифрования должно быть как можно короче.

Определяют два класса криптосистем:

Симметричные (одноключевые) криптосистемы, т.е. пользователи должны совместно выбрать единый математический алгоритм, который будет использоваться для шифрования и расшифрования данных. Но такие ключи трудно защищать и их необходимо часто менять, ведь есть риск их случайного раскрытия;

Асимметричные (двухключевые) криптосистемы (с открытым ключом). В них используются разные, но взаимно дополняющие друг друга ключи (один ключ зашифровывает информацию, а другой ее расшифровывает) и алгоритмы шифрования и расшифровки;

Среди наиболее известных алгоритмов открытых ключей можно назвать RSA (Rivest-Shamir-Adleman). При использовании алгоритма RSA можно не только использовать открытый ключ для шифрования, а секретный для расшифрования, но и наоборот: данные можно зашифровать с помощью секретного ключа, а открытый ключ применять при расшифровывании данных.

Однако на этом пути много ещё нерешенных проблем, связанных с разрушительным воздействием на криптосредства таких составляющих информационного оружия как компьютерные вирусы, логические бомбы, автономные репликативные программы и т.п. Объединение методов компьютерной стеганографии и криптографии явилось бы хорошим выходом из создавшегося положения. В этом случае удалось бы устранить слабые стороны известных методов защиты информации и разработать более эффективные новые нетрадиционные методы обеспечения информационной безопасности.

Список литературы

1. О.И. Шелухин, С.Д. Канаев, «Стеганография. Алгоритмы и программная реализация.», 2017г., 592 стр.

2. Барсуков Вячеслав Сергеевич, Романцов Андрей Петрович, статья «Компьютерная стеганография вчера, сегодня, завтра.», 2001г.

3. Сингх Саймон,«Книга шифров», 448 стр., 2007г.

УДК 004.4'23

Пуртов Дмитрий Николаевич
Направление:05.13.12, аспирант каф. ИБ

Научный руководитель: **Сидоркина Ирина Геннадьевна**
доктор технических наук, профессор кафедры ИБ
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

МЕТОДЫ ИЗВЛЕЧЕНИЯ КЛЮЧЕВОЙ ИНФОРМАЦИИ ИЗ ТЕКСТА

Качество извлечения ключевой информации из текста напрямую зависит от методов с помощью которого происходит извлечение той самой информации. Первое что стоит отметить это то, что само понятие ключевой информации не имеет четкого определения. Одной из возможных интерпретаций того, что такое ключевая информация может быть то, что ключевая информация - наиболее важная информация в тексте, которая не может быть подсказана контекстом, обязательно должна быть воспроизведена.**[1]**

Существует много различных задач в которых есть необходимость находить и извлекать только нужную информацию. Можно выделить такие группы задач как: распознавание именованных элементов, выделение терминологии, создание электронных автоматический перевод текстов, создание вопросно-ответных систем, информационный поиск и т.д. Для решения подобных задач как правило используются следующие группы методов: статистические методы, структурные методы, графовые методы, синтаксические методы, методы на базе искусственного интеллекта и др. **[6]**

Все перечисленные методы работают с так называемой единицей информации. Под единицей информации может пониматься буква, слово, словосочетание, предложение, часть текста или весть текст. Данный параметр показывает минимальную долю информации, которая необходима при реализации метода.

В основе статистических методов лежит то, что распределение слов естественного языка может подчиняется определенному закону, который можно сформулировать,учитывая относительные частоты встречаемости морфологических, лексических, синтаксических единиц информации.Представителями статистических методов являются: частотный анализ, контент-анализ, ранжирование данных и т.д. В качестве примера можно взять один из базовых методов в данной группе, а именно, расчет для каждой единицы информации, его

важности на основе частоты его употребления. Таким образом, зная статистические данные единицы информации можно уже делать вывод о том, насколько информация важна и является ли ключевой.**[2],[7]**

Структурированные методы базируются на том, что текст представляет собой комплекс внутренних связей, которыми обеспечивается единство и функциональность текста. При структурном анализе, текст разделяется на логические составные блоки связанные друг с другом. Причем каждый блок несет определенный смысл. **[3]** В общем виде процесс извлечения информации с использованием структурах методов выглядит следующим образом:

1. Деление текста на составные элементы (введение, заключение, основная часть и т д.);
2. Изучение отдельных элементов и их взаимосвязей;
3. Извлечение ключевой информации от отдельного элемента с учетом особенностей элемента.

В чистом виде как правило данная группа методов не используется, но используется в сочетании с другими методами. **[7]**Можно рассмотреть ситуацию, когда, текст, например, состоит из введения, основной части и заключения. В данном случае структурированные методы могут находить наиболее важные части текста, а именно в данной ситуации — это заключение, и отдавать текст с заключением другим методам, например, статистическим методам. Статистические методы уже с меньшей погрешностью, так как не анализируют весь текст, могут найти ключевою информацию.

Графовые методы как правило работают совместно с другими методами, как например структурными, статистическими и т.д. Методы данной группы базируется на том, что текст обладает признаками целостности и связанности. Задача графа с помощью матрицы смежности упростить анализ текста, разделив его на смысловые части и уже дальше извлечь ключевую информацию, используя другие методы при необходимости. В ряде случаев только графовые методы могут быть единственным способом для упрощения анализа.**[3]**

Графовые методы, как и структурированные методы определяют значимую область текста и уже другие методы завершают поиск ключевой информации.

Синтаксические методы базируются на том, что тексты имеют определенную синтаксическую структуру. Синтаксическая структура текста позволяет строить графы зависимостей единиц информации тем самым определить ключевую информацию. При синтаксическом анализе довольно часто встает задача, связанная с классификацией

единиц информации. Для решения этой задачи используют искусственный интеллект. В качестве примера можно рассмотреть ситуацию, когда для поиска ключевой информации строиться дерево зависимостей единиц информации, элементы которых связаны дугами, обозначающими синтаксическое подчинение. Опираясь на эти связи можно сделать выводы о том, какой из элементов дерева является ключевой. **[4]**

Методы искусственного интеллекта(ИИ) базируется на абстрактных правилах, полученных в ходе обучения. Особенность такого подхода в том, что ИИ может в ходе работы продолжать обучаться, что дает увеличение точности в каждым последующим его применением. Как правило методы ИИ работает совместно с другими методами, обучаясь на результате их работы. **[3],[5]** Одним из возможных способов реализации нейросетевых методов ИИ может быть ситуация, когда вначале ИИ обучается на работе синтаксических и структурных методов, а уже пройдя обучение находит ключевую информацию в нужном текст. При реализации же абстрактного логического вывода с использованием правил продукций в ИИ наиболее эффективные решения получаются при использовании метода (или теоремы) Байеса [8].

При рассмотрении таких методов как: статистические методы, структурные методы, графовые методы, синтаксические методы, методы на базе искусственного интеллекта можно сделать вывод о том, что на практике как правило не используются чистые методы, а реализуется их комбинация. Это подтверждает то, что нужно использовать различные комбинации методов для получения наиболее эффективного результата при извлечении ключевой информации из текста. Недостатком такого решения является то, что эффективность комбинации можно выяснить только, смоделировав ситуацию.Для быстрого анализа эффективности комбинаций методов можно прибегнуть к автоматическому тестированию. Для этого нужно подготовить входные данные и ожидаемые данные, причем так как работа ведется с неявными данными стоит сразу же определиться с уровнем погрешности при тестировании. Уровень погрешности необходим, так как всегда будут тесты, которые будут не пройдены. Благодаря автоматическому тестированию можно создать стенд с автоматической оценкой эффективности комбинации методов. Получившийся стенд позволит быстро оценивать комбинации методов, а также сравнивать новые комбинации с предыдущими, для поиска наиболее эффективных комбинации.

Список литературы

1. Словарь методических терминов и понятий [Электронный ресурс] – Режим доступа: https://methodological_terms.academic.ru/632/ключевая_информация.

2. О.В. Митина, А.С. Евдокименко Методы анализа текста: методологические основания и программная реализация [Электронный ресурс] – Режим доступа: http://dspace.susu.ru/xmlui/bitstream/handle/0001.74/3143/3.pdf

3. А.В. Ганичева, А.В. Ганичев Графовый метод анализа текстов [Электронный ресурс] – Режим доступа: https://docplayer.ru/60748824-Grafovyy-metod-analiza-tekstov-graph-method-of-text-analysis.html

4. И.В. Смирнов, А.О. Шелманов Семантико-синтаксический анализ естественных языков [Электронный ресурс] – Режим доступа: http://www.isa.ru/aidt/images/documents/2013-01/41_54.pdf

5. К.А. Найденова, О.А. Невзорова Машинное обучение в задачах обработки естественного языка: Обзор современного состояния исследования [Электронный ресурс] – Режим доступа: https://cyberleninka.ru/article/v/mashinnoe-obuchenie-v-zadachah-obrabotki-estestvennogo-yazyka-obzor-sovremennogo-sostoyaniya-issledovaniy

6. М.А. ПавленкоАнализ методов решения задачи извлечения информации из текстов[Электронный ресурс] – Режим доступа: http://www.hups.mil.gov.ua/periodic-app/article/11169

7. А.С. Ванюшкин, Л.А. Гращенко Методы и алгоритмы извлечения ключевых слов [Электронный ресурс] – Режим доступа: https://cyberleninka.ru/article/v/metody-i-algoritmy-izvlecheniya-klyuchevyh-slov

8. В. В. Чередниченко, Т. С. Бутакова Использование теоремы Байеса в HelpDesk системе [Электронный ресурс] – Режим доступа: https://storage.tusur.ru/files/53537/АОИ-1601_Чередниченко.Бутакова.pdf

УДК 004.725

Рогачева Ирина Сергеевна
направление Программная инженерия (бакалавриат), гр. ПС-12

Научный руководитель: **Бородин Андрей Викторович,**
канд. экон. наук, заведующий кафедрой информатики и системного программирования
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

МОДЕРНИЗАЦИЯ СТЕНДА ДЛЯ ИССЛЕДОВАНИЯ ТЕХНОЛОГИЙ ДИСТРИБУЦИИ ТОЧНОГО ВРЕМЕНИ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

Синтез оптимальных технических решений для дистрибуции точного времени в мультисервисных сетях передачи данных (МСПД) в качестве первого шага алгоритма оптимизации предполагает построение множества возможных технических решений. Это множество часто строится на комбинаторной основе и не все

конфигурации оборудования из этого множества могут хорошо (или плохо) выполнять свою функцию. Работоспособность многих конфигураций, как исходных, так и оптимальных, требует всестороннего тестирования. Испытания конфигураций на реальном оборудовании затруднено, а часто и невозможно, ввиду большого количества задействованных разнородных компонент (специализированные сервера и сервера общего назначения, коммутаторы и маршрутизаторы, линии связи и т. п.) [3]. В этих условиях значительный интерес представляют среды виртуализации разнородного оборудования и создание на этой основе испытательного стенда.

Рассмотрим следующую постановку задачи. Стенд, разработанный на базе технологий виртуализации, созданных в рамках проектов с открытыми исходными кодами, на основе IBM PC-совместимых компьютеров общего назначения, необходимо модернизировать для тестирования и отладки систем дистрибуции точного времени нового поколения. В качестве внешнего оборудования по отношению к стенду допускаются лишь специализированные NTP-сервера и (GPS- и радиочастотные) приемники, поддерживающие протокол NMEA, а также односторонние мультипликаторы последовательных интерфейсов. Стенд должен поддерживать эмуляцию сетевого оборудования компании Cisco и серверов с операционными системами семейств Microsoft Windows, Linux и QNX. Стенд должен поддерживать функции автоматического конфигурирования типовых элементов МСПД. В качестве базового сетевого оборудования рассматривается продукция компании Cisco Systems, Inc.

В базовом варианте в качестве средства виртуализации маршрутизаторов компании Cisco был выбран проект Dynamips, в частности была использована версия 0.2.7 [3]. Эмулятор Dynamips в рамках данной работы используется в режиме гипервизора. Для виртуализации серверов общего назначения в новой версии стенда используется программный продукт Oracle VM VirtualBox версии 6.0.12. Для перехвата и инжекции сетевого трафика на различных интерфейсах компьютеров-хостов используется программный продукт WinPcap версии 4.1.3. Диалог с гипервизором осуществляет система скриптов, написанная на языке программирования VBA, которая по описанию варианта технического решения, представленному в виде листа книги Microsoft Excel, формирует необходимую топологию сети, создает файловое окружение для виртуальных маршрутизаторов и осуществляет их запуск. Эта же система скриптов посылает команды

системе виртуализации Oracle VM VirtualBox по запуску виртуальных машин, эмулирующих сервера общего назначения, включенные в вариант технического решения. В ручном режиме запускаются лишь виртуальные машины, предназначенные для эмуляции атак. (Эти сценарии ориентированы на исследование устойчивости будущего релиза МСПД по отношению к различным видам активных действий злоумышленников.) Использование объектной модели Microsoft Excel на верхнем уровне программного обеспечения стенда обусловлено тем, что для пакета прикладных программ «МультиМир» [4], используемого для оптимизации технических решений в проекте, частью которого является данная работа, эта модель является «родной» (по среде).

Рассмотрим полученные результаты. Продолжение испытаний различных технических решений в области дистрибуции точного времени в рамках модернизированного стенда показало рост удобства его использования. На одном компьютере с ранее использованной типовой конфигурацией [3] и ОЗУ, увеличенным до объема в 32Gb, адекватно (с точки зрения тайминг-сервиса операционных систем) эмулируется одновременно до 12 маршрутизаторов и 2 серверов общего назначения. Возможное наращивание топологии МСПД желательно реализовывать, подключая дополнительные хост-компьютеры, соответственно из расчета один компьютер, не хуже выше указанной конфигурации, на 10…12 типовых маршрутизаторов.

Дальнейшее развитие проекта связано, во-первых, с модернизацией на стенде программного обеспечения поддержки типовых источников точного времени на базе GPS-приемников точного времени, поддерживающих протокол NMEA [2], во-вторых, с поддержкой аппаратных решений одностороннего дублирования последовательных интерфейсов, и, наконец, с обеспечением поддержки ряда продуктов, выпускаемых отечественными производителями [1]. На этом пути требуются дополнительные исследования по выбору параметров виртуальных машин Oracle VM VirtualBox, к которым предполагается физическое подключение приемников по интерфейсам RS-232 и/или USB.

Другим направлением развития проекта является интеграция в подсистему оптимизации обсуждаемого стенда визуального языка описания сценариев развития экономик [6] технических подсистем (в первую очередь источников точного времени), а также развитие механизма интерактивного пересчета показателей MTBF оборудования в вероятностные характеристики визуальных моделей подсистем [5].

Список литературы

1. Бородин, А. В. Об импортозамещении при создании систем дистрибуции точного времени в мультисервисных сетях передачи данных / А. В. Бородин // Кибернетика и программирование. – 2015. – № 2. – С. 78-97. – DOI: 10.7256/2306-4196.2015.2.14036.

2. Бородин, А. В. Стоимость владения как критерий архитектуры первичного NTP-сервера на основе GPS-приемников коммерческой точности / А. В. Бородин // Обозрение прикладной и промышленной математики. – 2009. – Т. 16. – С. 507.

3. Бородин, А. В. Учебно-испытательный полигон отработки технологий дистрибуции точного времени / А. В. Бородин, А. С. Варламов, Д. В. Кораблев // Кибернетика и программирование. – 2015. – № 3. – С. 11–23. – DOI: 10.7256/2306-4196.2015.3.15438.

4. Уразаева, Т. А. Алгебраические методы анализа риска в развивающихся экономиках / Т. А. Уразаева. – Йошкар-Ола: Поволжский государственный технологический университет, 2017. – 276 с.

5. Уразаева, Т. А. Модели риска в технико-экономическом обосновании инфраструктурных решений / Т. А. Уразаева // Современные проблемы и перспективы социально-экономического развития предприятий, отраслей, регионов: сборник статей. – Йошкар-Ола: Поволжский государственный технологический университет, 2015. – С. 161-164.

6. Уразаева, Т. А. Синтаксическая модель языка визуального представления развивающихся экономик / Т. А. Уразаева // Обозрение прикладной и промышленной математики. – 2006. – Т. 13. – С. 147.

УДК 620.179.16

Сафина Регина Рифатовна
направление Информатика и вычислительная техника (магистратура),
гр. ИВТм-22

Научный руководитель: **Смирнов Алексей Владимирович**,
канд. техн. наук, доцент кафедры информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственных технологический университет», г. Йошкар-Ола

АДАПТИВНЫЙ АЛГОРИТМ РАБОТЫ СТАЦИОНАРНОГО ИЗМЕРИТЕЛЯ УРОВНЯ ЗАТРУБНОЙ ЖИДКОСТИ НЕФТЕДОБЫВАЮЩЕЙ СКВАЖИНЫ

Актуальность работы. В настоящее время актуальной задачей является повышение эффективности работы нефтедобывающих скважин, в частности – повышение точности определения уровня

затрубной жидкости нефтедобывающих скважин при их исследований. Одним из направлений повышения точности определения уровня является адаптация алгоритма работы стационарного измерителя уровня к текущим параметрам нефтедобывающей скважины.

Цель работы – разработка адаптивного алгоритма работы стационарного измерителя уровня затрубной жидкости нефтедобывающей скважины.

Волнометрические методы определения динамических и статических уровней в скважинах основаны на измерении времени прохождения акустического импульса от устья скважины до измеряемого уровня затрубной жидкости и обратно [1].

Задача повышения точности определения уровня жидкости в межтрубном пространстве скважины сводится к повышению точности определения скорости звука в газе межтрубного пространства[2].

Известно[3],что можно повысить достоверность определения уровня жидкости путем определения скорости звука в газе межтрубного пространства скважины в соответствии с информацией о показателе адиабаты газа межтрубного пространства скважины, молекулярной массе газа межтрубного пространства скважины и средней температуре газа межтрубного пространства скважины.

Кроме того, возможно уточнение определенной скорости звука в газе межтрубного пространства скважины на основании информации:

- о среднем давлении газа межтрубного пространства скважины;
- о вязкости газа межтрубного пространства скважины;
- о молярной массе газа межтрубного пространства скважины;
- о конструкции скважины;
- о несущей частоте отраженного от жидкости акустического сигнала.

Рис. 1. Адаптивный алгоритм работы стационарного измерителя уровня затрубной жидкости нефтедобывающей скважины

Возможно определение скорости звука в газе межтрубного пространства скважины путем прямого измерения на устье скважины с последующей корректировкой в соответствии с информацией о средней температуре газа межтрубного пространства скважины.

На основе данной методики разработан адаптивный алгоритм работы стационарного измерителя уровня затрубной жидкости нефтедобывающей скважины, который представлен на рис. 1.

На начальном этапе работы прибора происходит загрузка входных параметров, таких как ориентировочный уровень затрубной жидкости нефтедобывающей скважины, способ добычи, значения требуемой точности обнаружения уровня. Так же производится измерение давления и температуры в затрубном пространстве.

После начала автономной работы измерителя осуществляется настройка модели затрубного пространства нефтедобывающей скважины.

Если параметры затрубного газа известны, то производится определение скорости звука в газе межтрубного пространства скважины в соответствии с информацией о показателе адиабаты газа межтрубного пространства скважины, молекулярной массе газа межтрубного пространства скважины и средней температуре газа межтрубного пространства скважины.

Если параметры газа известны не в полном объеме, то скорость звука определяется в газе межтрубного пространства скважины путем прямого измерения на устье скважины. Затем производится уточнение определенной скорости звука в газе межтрубного пространства скважины на основании информации о среднем давлении газа межтрубного пространства скважины, о вязкости газа межтрубного пространства скважины, о молярной массе газа межтрубного пространства скважины, о конструкции скважины, о несущей частоте отраженного от жидкости акустического сигнала.

Если уровень обнаружен, происходит расчет уровня с учётом определенной скорости звука.

Выводы.Предложен к использованию адаптивный алгоритм работы стационарного измерителя уровня затрубной жидкости. Адаптивность полученного алгоритма заключается в возможности расчета параметров модели затрубного пространства для каждой скважины в отдельности и с учетом параметров затрубного газа.

Список литературы

1. Лавров, В.В. Оборудование для глубинных и устьевых исследований скважин / В.В. Лавров, Г.П. Налимов, С.В. Тюрин, П.О. Гаус // Нефтяное хозяйство. – 2014. – №9. – С. 104-106.

2. Борминский С.А., Скворцов Б.В. Повышение точности электронно-акустических устройств измерения уровня жидкости // Измер. техн. 2016. № 8. С. 53–56.

3. Пат. № 2704082 РФ. Способ определения уровня жидкости в межтрубном пространстве скважины/ С.А. Павловский, А.В. Смирнов, Р.Р. Сафина. Заявлено 18.01.2018.

УДК 004.056

Смиренский Андрей Романович
направление Программная инженерия (магистратура), гр. ПСм-21

Научный руководитель: **Бородин Андрей Викторович,**
канд. экон. наук, заведующий кафедрой информатики и системного программирования
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

О ТРАНСФОРМАЦИИ ДОКУМЕНТООБОРОТА СУБЪЕКТОВ ЭКОНОМИКИ В СФЕРУ ЗАЩИЩЕННОЙ МОБИЛЬНОЙ КОММУНИКАЦИИ

Сегодня технологии электронной цифровой подписи (ЭЦП) распространены во всех сферах бизнеса и востребованы в основном юридическими лицами. Постепенно они внедряются и в практическую деятельность физических лиц. При наличии ЭЦП для физического лица открывается ряд новых и интересных возможностей [2]:

1) быстрый доступ к полному объему сервисов Единого портала государственных услуг;

2) дистанционная подача заявления на поступление в высшее учебное заведение;

3) участие в электронных торгах на поставку товаров и оказание услуг;

4) регистрация юридического лица или индивидуального предпринимателя;

5) быстрое дистанционное оформление заявки на получение патента на изобретение.

Год от года этот список расширяется.

Однако использование ЭЦП требует от физического лица наличия определенной технической культуры и понимания основных принципов обеспечения безопасности в области информационных технологий. С другой стороны, если посмотреть на перечень субъектов обеспечения этих новых возможностей, то там оказываются в основном государственные структуры или организации, аффилированные с этими

структурами, что связано, в частности, с особенностями правоприменения закона «Об электронной подписи» [4].

Существенно более широкое распространение технологий ЭЦП в сфере электронного документооборота по сравнению с сегодняшним днем предполагает наличие интуитивно понятного интерфейса у соответствующих продуктов при надлежащем уровне безопасности их использования, а также миграцию базовых технологий защиты на мобильные платформы. Последний тезис определяет актуальность темы настоящей работы.

В основу принципов формирования интуитивно понятного интерфейса системы поддержки ЭЦП можно положить концепцию «рабочих столов руководителя» [1], реализованную в среде операционной системы OS/2 еще на заре внедрения технологий подобного рода в Российской Федерации. В рамках этой концепции было реализовано визуально идентичное двум столам («на подпись» и «подписанные документы») окружение, где процедура подписания реализовывалась в рамках Drag-and-drop-операции с иконкой документа на иконку «Подписать». При этом автоматическая подпись или диалог с приглашением предъявить внешний носитель информации с секретным ключом определялись настройками политики безопасности и/или метками конфиденциальности документа. Соответствующее мобильное приложение может реализовать «столы с документами» в виде домашних папок приложений, поддерживающих соответствующие методы обработки документов: подписание документа, отправка, получение документа, проверка подписи. Для обеспечения поддержки приложением инфраструктуры открытых ключей очевидна потребность в реализации следующих базовых операций: получение и сохранение корневых сертификатов, генерация ключей ЭЦП, их сертификация, отзыв и (при необходимости) удаление.

Итак, настоящая работа посвящена разработке семейства мобильных приложений семейства «КриптоАРМ», позволяющих защитить документы при помощи шифрования и ЭЦП, а также быстро и достоверно проверить электронные подписи на документах. В приложениях семейства, в том числе, поддерживаются новые российские криптографические алгоритмы формирования и проверки электронной подписи ГОСТ Р 34.10-2012 и функции хэширования ГОСТ Р 34.11-2012. Использование данных алгоритмов станет обязательным для отдельных сфер применения со следующего года, взамен предыдущих алгоритмов 1994 и 2001 годов. Соответствующее

приложение семейства, использующее названные стандарты, получило название «КриптоАРМ ГОСТ».

В качестве методики оценки и обоснования экономической эффективности разработки данного проекта, а также тиражирования соответствующего продукта, использован подход, основанный на дискретно-событийных моделях жизненного цикла [3]. Для повышения эффективности вычислений риска эксплуатации приложения использованы методы алгебраической теории риска [5] и соответствующий пакет прикладных программ [6].

В целом, с учетом оценки экономической эффективности проекта, разработку семейства приложений «КриптоАРМ» следует признать целесообразной и перспективной в рамках цифровизации российской экономики.

Дальнейшее развитие семейства приложений «КриптоАРМ» предполагает разработку языка описания сценариев применения криптопримитивов продукта и интеграцию соответствующего интерпретатора в разработанные приложения.

Список литературы

1. Бородин, А. В. Открытая система визуального документооборота со встроенной поддержкой электронной цифровой подписи / А. В. Бородин // Труды Марийского государственного технического университета. Вып. 2: Материалы научной конференции профессорско-преподавательского состава, докторантов, аспирантов, сотрудников Марийского государственного технического университета 27-31 мая 1996 г. Ч. III. – Йошкар-Ола: Марийский государственный технический университет, 1996. – С. 20–22.

2. Бородин, А. В. Синтез политики безопасности для процессов отчужденной обработки информации на основе онтологического анализа предметной области / А. В. Бородин // Инновационное развитие российской экономики: IX Международная научно-практическая конференция. Т. 3: Информационно-коммуникационные технологии. – М.: ФГБОУ ВО «РЭУ им. Г. В. Плеханова», 2016. – С. 14-16.

3. Бородин, А. В. Технико-экономическое обоснование внедрения технологии обеспечения целостности и подлинности информации на бумажном носителе при отчужденной обработке документов / А. В. Бородин // Кибернетика и программирование. – 2017. – № 1. – С. 30-47. – DOI: 10.7256/2306-4196.2017.1.22192.

4. Об электронной подписи: федеральный закон от 06.04.2011 № 63-ФЗ: по состоянию на 23.06.2016. – URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=220806&dst=100006%2C1&date=21.10.2019. Дата обращения: 21.10.2019.

5. Уразаева, Т. А. Алгебраические методы анализа риска в развивающихся экономиках / Т. А. Уразаева. – Йошкар-Ола: Поволжский государственный технологический университет, 2017. – 276 с.
6. Уразаева, Т. А. О функциональности пакета прикладных программ «МультиМИР» / Т. А. Уразаева // Современные проблемы и перспективы социально-экономического развития предприятий, отраслей, регионов. – Йошкар-Ола: Поволжский государственный технологический университет, 2014. – С. 261-265.

УДК 621.3.084.2

Смирнов Егор Александрович
направление Информатика и вычислительная техника (бакалавриат), гр. ИВТ-41

Научный руководитель: **Смирнов Алексей Владимирович**
канд. техн. наук, доцент кафедры информационно-вычислительных систем
ФГБОУ ВО«Поволжский государственный технологическийуниверситет», г.Йошкар-Ола

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ MEMS АКСЕЛЕРОМЕТРА В ДАТЧИКЕ ВИБРАЦИИ

Основная функция акселерометра – определение ускорения по одной из осей системы координат. Наиболее распространённые примеры применения акселерометра:

1. в системах навигации,
2. в смартфонах для определения положения в пространстве,
3. в системах вибродиагностики.

Существуют два основных вида акселерометров: пьезоэлектрические и микроэлектромеханические (MEMS). В настоящее время для задач мониторинга уровня вибрации обычно используют пьезоэлектрические акселерометры. Их основные преимущества – широкий диапазон рабочих частот с сохранением высокой точности измерения виброускорения. Основной недостаток – высокая стоимость.

В сравнении с пьезоэлектрическими, у MEMS акселерометров частотадискретизации и точность определения ускорениянише, при этомих стоимость также существенно ниже. В статье исследованыособенности применения MEMS акселерометров для датчиков вибрации.

Для проведения исследования был выбран трехосевой, программируемый акселерометр IIS2DH компании

STMicroelectronics.Калибровка данного акселерометра осуществляется производителем. Максимальная частота дискретизации - 5376 Гц. Для взаимодействия с акселерометром предусмотрено два интерфейса:SPIи I2C. Дляпрограммирования акселерометра, получения и обработки значений ускорения нужно использовать микроконтроллер. К нему выдвигается требование по быстродействию, для обеспечения скорости работы акселерометра на частоте 5376 Гц. За промежуток времени равный $5376\ с^{-1}, \approx 0{,}2$ мс контроллер должен вычитать данные из акселерометра, обработать, то есть перевести в физическую величину, и отправить на компьютер по интерфейсу UART. С этой задачей справится система на кристалле NRF52 с процессором, работающем на частоте 64 МГц.

Первой задачей в исследовании датчика стала разработка драйвера для взаимодействия с акселерометром. Основные функции драйвера:

1. передача на ПК значения ускорения для дальнейшего анализа
2. приём и установка настроек для акселерометра от пользователя

Драйвер включает в себя обработчик прерываний, предназначенный для обработки событий на специальной линииDATAREADY. Линия служит для сообщения контроллеру о готовности данных для чтения.

Второй задачей являлось оценка шума системы.Для этого был собран специализированный стенд, обеспечивающий снижение воздействий внешних вибраций. Эксперименты проводились для разных настроек акселерометра: изменялись частота дискретизациии коэффициент усиления аналогового тракта. В результатеэкспериментов выяснилось,что шум укладывается в диапазон, заявленный производителем, но для повышения точности измерений его можно снизить двумя способами:

1. используя встроенный фильтр низких частот;
2. усреднение с шагом от 2 до 128значений (скользящее среднее).

Первый эксперимент – исследование влияния фильтра низких частот на СКО выборки.Результат представлен в таблице.Можно заметить, чтоиспользование полосы фильтрацииулучшает эффективную разрешающую способность примерно на 40%.

Таблица 1 –Влияние фильтра на СКО выборки

Номер эксперимента	1	2	3	среднее
Без фильтра	51.7	57.2	51.2	53.4
С фильтром	37.9	33.9	38.2	36.7

Далее исследовалось влияние усреднения по 2, 4, 8, 16 и 128 точкам.Результат эксперимента представлен в таблице 2.

Таблица 2 –Влияние усреднения на СКО выборки

Окно усреднения	1	2	4	16	128
Без фильтра	51.7	40.9	32.0	16.8	6.2
С фильтром	37.9	35.1	30.5	17.1	7.2

Выбор количества точек усреднения зависит от частоты колебаний, Например, усреднение по двум точкам снижает частоту поступления значений в 2 раза, следовательно, в 2 раза снижает максимальную частоту колебаний, которую можно зарегистрировать.

Дальнейшей задачей являетсяпроведение испытаний акселерометра на вибростенде. В ходе испытаний планируется установить максимальную частоту колебаний, которую акселерометр способен регистрировать с последующим расчетом величин виброскорости и виброперемещения.

В целях подготовки к данным испытаниям реализован адаптивный алгоритм работы акселерометра, снижающий влияние его основного недостатка –понижение точности регистрации значений ускорения при увеличении частоты дискретизации. В основу работы алгоритма заложен механизм определения в реальном масштабе времени несущей частоты сигнала виброускорения с последующим выбором текущей частоты дискретизации.

Список литературы

1. Ultra-low-power high-performance 3-axis accelerometer with digital output for industrial applications. Datasheet - productiondata. [Электронный ресурс] URL: https://www.st.com/resource/en/datasheet/iis2dh.pdf (дата обращения: 1.11.2019).

2. С. И. Баскаков.Радиотехнические цепи и сигналы. [Учеб.для вузов по специальности "Радиотехника"] – 3-е изд., перераб. и доп. – М. : Высш. шк., 2000. – 462 с.

УДК 621.3.084.2

Смоленцева Юлия Алексеевна
направление Информатика и вычислительная техника (магистратура),
гр. ИВТм-23

Научный руководитель: **Малашкевич Василий Борисович**
канд. техн. наук, доцент кафедры информационно-вычислительных систем
ФГБОУ ВО «Поволжский государственный технологическийуниверситет», г. Йошкар-Ола

ИССЛЕДОВАНИЕ ПОДСИСТЕМЫ ФОРМИРОВАНИЯ ДЕСКРИПТОРОВ ПОЛЬЗОВАТЕЛЬСКИХ ПРЕДПОЧТЕНИЙ НА ОСНОВЕ АНАЛИЗА БОЛЬШИХ ДАННЫХ

Большие данные относятся к потоку цифровых данных от многих цифровых источников, включая датчики, сканеры, численное моделирование, мобильные телефоны, интернет, видео, электронная почта и социальные сети. Типы данных включают тексты, геометрию, изображения, видео, звуки и комбинации каждого из них. Эволюция технологий и понимание человеком данных сместили обработку данных с традиционного статического режима на ускоряющуюся арену данных, характеризующуюся объемом, скоростью, разнообразием, достоверностью и ценностью. Первый объем относится к объему данных, который стремительно растёт и выходит за пределы нашей способности обрабатывать большие наборы данных. Объем является наиболее распространенный дескриптор больших данных (например, Hsu, Slagter и Chung). Скорость относится к быстрой генерации и передачи данных через Интернет на примере сбора данных от социальных сетей, огромное количество датчиков от микро (атомных) до макро (глобальных) уровней и передача данных от датчиков к суперкомпьютерам и лицам, принимающим решения. Разнообразие относится к различным формам данных, в которых модели и структурные данные архивируются. Правдивость относится к разнообразию качества, точности и достоверности данных. Все четыре V важны для достижения пятой V, которая фокусируется на конкретных предложениях исследований и поддержки принятия решений, которые улучшают нашу жизнь, работу и процветание.

Развитие больших данных, особенно их внедрение промышленностью, расширяет содержание и значение больших данных. Исходное определение на основе объема теперь включает в себя сами данные, соответствующие технологии и опыту, чтобы помочь генерировать, собирать, хранить, управлять, обрабатывать,

анализировать, представлять и использовать данные, а также полученную информацию и знания. Например, Big Earth Data Initiative определяет большие данные, как инвестиционную возможность и «визитную карточку» для развития науки о Земле с использованием больших данных и соответствующих технологий обработки. В геопространственной области большие данные развивались по пути от чисто данных к более широкой концепции, включая данные, технологии и рабочую силу. Особое внимание уделяется географическому аспекту больших данных из социальных сетей, исследование Земли и сервис данных с датчиков, кибер-инфраструктуры, социальные сети и бизнес. Например, исследование Земли генерирует терабайты изображений ежедневно; моделирование климата МГЭИК (Межправительственная группа экспертов по изменению климата) производить сотни петабайт для будущего анализа климата, сервис данных с датчиков производит еще больше из сенсорной сети. Социальные сети и бизнес - это данные, которые генерируются быстрее с определенными географическими и временными следами (то есть пространственно-временными данными).

С точки зрения бизнеса, в отчете McKinsey (2011) эра «больших данных» представлялась следующей границей инноваций, конкуренции и производительности, учитывая ее потенциальные возможности получения доходов от бизнеса и создания новых возможностей. Например, Наджар и Кеттингер (2013) использовали четырехэтапную стратегию для анализа возможности монетизации больших данных. Климатическая корпорация Monsanto использует большие геопространственные данные для анализа сложного и многослойного поведения погоды, чтобы помочь фермерам всего мира адаптироваться к изменению климата. McKinsey предсказал, что «Большие данные» улучшат 60% существующих предприятий и позволят создать большое количество нового бизнеса в следующем десятилетии. Таким образом, арена больших данных открывает широкие возможности и меняет сферу искоренения земного шара в отношении того, как мы живем, думаем и работаем, включая персонализированную медицину, индивидуальные рекомендации по продукту и варианты путешествий. В последние несколько лет произошла эта трансформация из концепции в реальность, благодаря множеству технологических инноваций (например, Uber).

Прошлые исследования по обработке больших данных, сосредоточенные на распределенной и потоковой обработке. Хотя облачные вычисления появились немного раньше, чем Big Data, это новая вычислительная парадигма для предоставления вычислений в

качестве пятой утилиты (после воды, электричества, газа и телефония) с функциями эластичности, объединенных ресурсов, доступа по требованию, самообслуживания и оплаты. Эти функции позволили облачным сервисам стать инфраструктурой как сервисом, платформой как сервисом и программным обеспечением как сервисом .

Таким образом, облачные вычисления предлагают новый способ ведения бизнеса и поддержки инноваций. Интеграция облачных вычислений, больших данных, экономии товаров и цифровых услуг способствует обсуждению связанных с ИТ услуг, большой доли нашего ежедневного потребления. Предполагается, что эти приложения больших данных с функциями и задачами 5 V будут и будут приводить к взрывному развитию соответствующих технологий облачных вычислений в различных направлениях.

Список литературы

1. Визуализация данных: сделать большие данные доступными и ценными . Обзор информации визуализация: последние достижения и проблемы. По состоянию на 25 ноября 2015 г. https://www.sas.com/content/dam/

2. SAS / en_us / doc / whitepaper2 / sas-data-visualization-marketpulse-106176.pdf

3. « Большие данные: раскрытие информации.» Журнал систем науки и инженерных систем 22 (2): 127 - 151.

4. Triguero, I., D. Peralta, J. Bacardit, S. García, and F. Herrera. 2015. “MRPR: A MapReduce Solution for Prototype Reduction in big Data Classification.” Neurocomputing 150: 331–345

УДК 004.056

Сосорева Анна Игоревна
направление Информационная безопасность автоматизированных систем(специалитет), гр. БИ-32

Научный руководитель: **Сидоркина Ирина Геннадьевна**
д.т.н., профессор, декан Факультета информатики и вычислительной техники
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола.

ХАРАКТЕРИСТИКИ ЭФФЕКТИВНОСТИ БАЗОВЫХ МЕТОДОВ СТЕГАНОГРАФИИ

Известны [1,2,3] несколько методов сокрытия информации в тексте: метод хвостовых пробелов, знаков одинакового начертания, метод

изменения кода пробела, изменения порядка следования маркеров конца строки, а также форматирование.Исследованию выделенных методов будет посвящена данная работа.

Первый метод, который будет рассмотрен — это метод хвостовых пробелов. Он заключается в дописывании пробела в конце каждой строки, если нужно закодировать один бит стеганосообщения. Если же нужно закодировать нулевой бит, то в этом случае пробел не дописывается. Далее, чтобы расшифровать сообщение, текстовый файл считывается построчно, из конца строки удаляются пробельные символы и затем в зависимости от значения текущего бита принимается решение о дописывании пробела в конец строки, далее преобразованная строка записывается в отдельный файл. Однако данный метод не удобен при распечатке файла с результатом. Так как на бумаге или другом носителе нельзя выявить пробелы в конце строки[2].

Второй метод, который мы рассмотрим - метод знаководинакового начертания. Он предполагает замену символов русского алфавита на символ того же начертания латинского алфавита, если нужнозакодировать 1 бит. Если нужно закодировать 0, то такая замена пропускается. Следует отметить, что меняться может и символ латинского алфавита на русский. Для извлечения стеганосообщения, файл считывается посимвольно и каждый символ проверяется, был ли он заменен[2].

Следующий метод сокрытия информации в текстовых файлах — это метод изменения кода пробела. Дело в том, что в кодовой странице Windows-1251 пробел может кодироваться как кодом 32, так и кодом 160. Для сокрытия стеганосообщения в тексте, можно заменять код пробела 32 на 160 для кодирования 1 бита, а пробелы с кодом 32 будут кодировать 0 бит. Данный метод является наиболее эффективным в использовании, так как заметить подмену кода символа «пробел» практически невозможно [2].

Последним, рассмотренным методом является метод изменения порядка следования маркеров конца строкиCR/LF. Данный метод предполагает безразличность следования символа перевода строки (CR) и перевода каретки (LF). Для того, чтобы закодировать 0в стеганосообщении, используют порядок CR/LF, а LF/CR для кодирования 1. Данный метод можно использовать для секретной передачи информации, однако многие редакторы Windows некорректно обрабатывают порядок LF/CR[2].

Таблица 1 – Сравнение характеристик эффективности базовых методов стеганографии

Метод	Пропускная способность	Способ обнаружения
Метод хвостовых пробелов	0,15%	При открытии файла в текстовом редакторе MicrosoftOfficeWord, и при использовании функции «отобразить все знаки», факт скрытой информации будет обнаружен
Метод знаков одинакового начертания	3,2%	При использовании MicrosoftOfficeWord с автоматической проверкой орфографии, будут выявлены все замены символов
Метод изменения кода пробела	2,1%	Текст с примененным методом изменения кода пробела успешно отображается во многих текстовых редакторах и обнаружить стеганосообщение практически невозможно
Метод изменения порядка следования маркеров конца строки CR/LF	0,15%	Так как многие редакторы Windowsнекорректно обрабатывают порядок LF/CR, то вероятность заподозрить, что в файле имеется скрытая информация возрастает

Под пропускной способностью каналов передачи скрываемых сообщенийбудем понимать максимальное количество информации, которое может быть вложено в один элемент контейнера[3].

Таким образом, на основе выделения характеристик методов показано, чтонаиболее эффективным методом сокрытия информации в текстовых файлах является метод изменения кода пробела. При использовании данного метода обнаружить, что в файле содержится информация практически невозможно. Это делает данный метод наиболее надежным и эффективным в использовании.

Список литературы

1. Аграновский А. В., Балакин А. В., Грибунин В. Г. Стеганография, цифровые водяные знаки и стеганоанализ - М.: Издательский дом “Вузовская книга”, 2009.

2. Беляев А. Стеганограмма: скрытие информации // Программист, 2002, №1 (электронная версия).

3. Грибунин В.ГОков И.Н., Туринцев И.В. Цифровая стеганография - Москва «СОЛОН-ПРЕСС», 2009, 272с.

УДК 004.056

Терентьева Дарья Александровна
направление Информатики и вычислительной техники (бакалавриат),
гр. ИВТ-11-16

Научный руководитель **Галанина Наталия Андреевна**,
д-р техн. наук, профессор кафедры математического и аппаратного обеспечения информационных систем
ФГБОУ ВО «Чувашский государственный университет им. И. Н.Ульянова», г. Чебоксары

САПР И PLM – СТРАТЕГИЯ СОВРЕМЕННОЙ ЭКОНОМИКИ

Цель работы. Работа посвящена изучению и анализу систем автоматизированного проектирования и PLM-систем в современной экономике и выявлению отраслевого спектра использования САПР и PLM.

Актуальность проекта. В современном проектировании ключевой компетенцией стала способность к автоматизированному проектированию. Информационно-коммуникационный уровень развития страны, в основном, отражает наличие собственных систем автоматизированного проектирования и управления жизненным циклом сложных изделий (САПР и PLM).

Основная часть. Системы автоматизированного проектирования (САПР) — это основной рабочий инструмент, используемый проектными и строительными организациями. Это сложные платформы, включающие не только программное и информационное обеспечение, но и мощный математический аппарат, необходимый для разработки физических объектов. Заложенные в САПР широкие функциональные возможности позволяют использовать их в различных отраслях экономики. В сами системы закладывается определенная специализация, позволяющая наиболее эффективно использовать их для выполнения поставленных задач. Выбор конкретного программного продукта зависит от того, что именно проектируется: здания, объекты инфраструктуры, механизмы.

Системы САПР можно разделить на 3 уровня:

1. Системы низкого уровня с закрытой математической моделью построений. Их логика очень проста — пользователь берет карандаш и рисует, только не на бумаге, а в векторном пространстве. Вся логика построений исходит исключительно из его соображений. Чтобы

работать в этих программах, следуетпервоначально определиться с размерами объектов, их характеристиками и геометрией.

2. Системы среднего уровня. Они имеют открытую математическую модель (дерево модели). Т.е. на любом этапе рисования пользователь может отследить предыдущие шаги построения. Данные системы своей логикой принципиально отличаются от систем низшего уровня. В математику модели заложена целостность геометрии объектов построения и любые пересечения или не соответствия «твердости» невозможны. Отсюда и термин «твердотельное моделирование». По факту работая в этих программах, инженер обращается с электронными копиями настоящих моделей, что позволяет применять к проектированию сборочную логику.

3. Системы высшего уровня с открытой математической моделью построений с возможностью сквозного анализа модели по установленным критериям (прочность, технологичность, геометрические ограничения и т.д.). Полные возможности данных систем используют только очень продвинутые пользователи и, как правило, только в отраслях с высокими ограничениями и сложными задачами (авиационная, космическая, атомная и т.д.). Т.е. эти системы - передовой край систем проектирования они самые совершенные и сложные. Сложность их заключается в том, что при моделировании программа «заставляет» четко определять связь геометрических объектов.

Основная задача систем САПР - это сокращение времени проектирования. Для этого используется три основных инструмента:

1. Создание библиотек решений в рамках ограничений, норм и правил проектирования.

2. Создание адаптивных сквозных моделей, способных к адаптации.

3. Создание коммуникативных сред проектирования (Windchill или Teamcenter и др.).

Все это позволило максимально сократить время проектирования и модернизации изделий. Если в рамках существующей системы проектирования и производства планируется создать что-то принципиально новое, следует четко понимать, что именно ограничения в проектировании создают возможность выработки устойчивых принципов и рекомендаций к проектированию. Что в свою очередь ограничивает поле возможных решений.

Управление жизненным циклом изделия (PLM – ProductLifecycleManagement) – система для управления всей информацией об изделии на протяжении всего его жизненного цикла.

Раньше под PLM чаще всего понимали то, что имело отношение к жизненному циклу материальных изделий, начиная от запуска в производство, регулирования объемов выпуска, определения времени выпуска новых или обновленных изделий, и, конечно же, сопровождение и сервис. Принципиальные изменения PLM произошли буквально в последние несколько лет. Теперь под PLM понимают автоматизацию всех видов работ, составляющих основу выпуска любой продукции — от проектирования изделия до его сбыта.

Программное обеспечение для определенного рода производств требуетспециализированных PLM-технологий. Основная часть PLM-платформ была рассчитана на производства другого типа: больше всего эта технология применяется в автомобилестроении, судостроении, авиакосмической промышленности. Однако в последнее время создается все больше платформ, рассчитанных на конкретные сферы непрерывного производства или обрабатывающей промышленности.

Выводы.Таким образом, для современного предприятия, стремящегося к росту и развитию, реализация концепции систем автоматизированного проектированиястановится необходимой составляющей бизнеса. Функциональные возможности САПР являются необходимым звеном для реализации информационной поддержки PLM.

Список литературы

1. Антонов А.В. Системный анализ. Методология. Построение модели: Учеб. пособие. — Обнинс: ИАТЭ, 2001. — 272 с.

2. Козырев А. Ю., Клочков А. Я. История развития систем проектирования Технические науки: традиции и инновации: материалы Международная научная конференция (г. Челябинск, январь 2012 г.). — Челябинск: Два комсомольца, 2012. — С. 64-66. — URL https://moluch.ru/conf/tech/archive/6/1575.

3. А.В. Петров. Проблемы и принципы создание САПР. Москва «Высшая школа», 1990.

4. URL https://habr.com/ru.

5. URL https://www.plm-ural.ru/resheniya/upravlenie-zhiznennym-ciklom-izdeliya-koncepciya-plm

6. URL https://borlas.ru/press/395_document.pdf

УДК 371.693.4

Томуров Павел Дмитриевич, Ульянкин Никита Алексеевич,
направление Информатика и вычислительная техника (бакалавриат), гр. ИВТ-41

Научный руководитель: **Танрывердиев Илья Оруджевич,**
канд. техн. наук, доцент, кафедра проектирования и производства ЭВС
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

СПОСОБ ДЛЯ ОБУЧЕНИЯ ДЕТЕЙ СПОРТИВНЫМ БАЗОВЫМ ЭЛЕМЕНТАМ С ПРИМЕНЕНИЕМ VR-СИСТЕМ

Цель работы – разработать технологию для обучения детей спортивным базовым элементам и реализовать её в виде аппаратно-программного комплекса.

Изобретение относится к области учебных моделей и тренажеров, отличающиеся обеспечением записи или измерения характеристик обучаемого.Способ для обучения детей спортивным базовым элементам с применением VR-систем – это аппаратно-программный комплекс, который в виртуальной среде имитирует тренировки с условиями, максимально близкими к реальным. Технология призвана обеспечить отсутствие травм в процессеосвоения детьми спортивных базовых элементов, при этом как можно сильнее вовлечь их в тренинг и добиться максимального результата в короткие сроки. Методика работы системы основана на выполнении пользователем комплекса упражнений, разработанных действующими тренерами, врачами, педагогами по физической культуре, и максимально точно представленных в среде виртуальной реальности, с созданием окружающего мира и физики. Помимо этого технология предусматривает систему помощи пользователю в выполнении упражнений, а также оценки качества выполнений физических упражнений.

В настоящее время в России стоит проблема развития детского и юношеского спорта. К сожалению, физическая культура у детей и молодых людей не в приоритете: они предпочитают вести «сидячий образ жизни». Именно в юности формируется образ поведения, определяющий физическое здоровье человека.

Проблема решается: открываются региональные и муниципальные центры спортивной подготовки секции по всяческим видам спорта, ведётся пропаганда здорового образа жизни. Молодёжь постепенно начинает проявлять интерес к спорту и здоровому образу жизни,

некоторые даже начинают заниматься спортом профессионально.Во время обучения часто возникают проблемы с освоением юными спортсменами базовых элементов, часто приводящие к травмам, что само по себе неприятно и опасно, так ещё и может отбить желание заниматься спортом в самом начале.

Технический результат предлагаемого решения заключается в исключении проблемы травматизма детей и юношей на этапе освоения спортивных базовых элементов и сокращении сроков обучения детей и юношей спортивным базовым элементам за счет формирования устойчивых когнитивных структур.

Указанный технический результат достигается тем, что испытуемый погружается в виртуальный мир посредствомVR-систем, после чего начинает взаимодействовать с написанным приложением, являющимся частью данного проекта.

Сначала нужно выбрать режим:

1. Режим обучения.В нём можно прочитать/прослушать инструкцию работы с приложением. Также можно посмотреть видеодемонстрацию упражненийвыполняемых виртуальным человеком, предусмотренных алгоритмами, имитирующими тренировки. Там же есть информация обо всех опциях приложения.

2. Режим тренировки. В данном режиме испытуемому предстоит выбрать комплекс упражнений, после чего начать обучение. Во время выполнения каждого упражнения испытуемый будет получать голосовые и письменные (они будут написаны в виртуальном пространстве, перед глазами сверху) распоряжения. Также при необходимости можно будет запустить видеодемонстрацию данного на тот момент действия с виртуальным человеком. В системе существует система оценки качества выполнения физических упражнений. После каждого упражнения пользователю будет объявлен результат оценки качества выполнения им данного упражнения. Обучаться придётся постепенно: система не даст испытуемому доступ к этапу, содержащего ключевые моменты другого этапа, пока тот этап не будет завершён на «Хорошо» или «Отлично» определённое количество раз.

3. Режим совместной тренировки. В данном режиме содержится комплекс групповых тренировок, позволяющих выполнять некоторые упражнения из Режима тренировки нескольким людям одновременно при этом, взаимодействуя друг с другом. Этот режим поможет испытуемым оперативно работать в команде, применяя приобретённые навыки в Режиме тренировки.

Упражнения выполняются с применением 3D-модели того или иного спортивного инвентаря (например, мяча), с учётом веса и физики движения моделируемого объекта.

Список литературы

1. Заявка на изобретение № 2013105987 РФ A63B69/00. Способ имитации игры в футбол для игровой тренировки футболистов, для игры в футбольное караоке и непосредственного проведения виртуальных футбольных матчей и устройство для его реализации // Пермяков А.М. (РФ), КузнецовН.П. (РФ).Заявка: 2013105987/12, 12.02.2013Опубл. 20.08.2014, Бюл. № 23.

2. Патент № 2149667РФA63B69/00, A63B22/02, A63B24/00, G06T15/70. Устройство для тренировки и соревнований, преимущественно в спортивных локомоциях и играх// Рязанов А.Г. (РФ). Заявка: 99114166/12, 05.07.1999Опубл. 27.05.2000, Бюл. № 15.

3. Патент № 160084 РФ G09B 9/02. Водительский тренажер виртуальной реальности с дополнением реальными объектами// Горбунов А.Л. (РФ), Зелинский А.Ю. (РФ), Кауров А.И. (РФ).Заявка: 2015129501/11, 20.07.2015Опубл. 27.02.2016 Бюл. № 6.

4. Патент № 2689445 РФ A63B69/00. Способ имитации участия спортсмена биатлониста или лыжника в соревнованиях любого уровня, в тренировках и устройство для его реализации // Кузнецов Н.П. (РФ), Симонова В.А. (РФ), Симонова Л.А. Заявка: 2018100381, 09.01.2018Опубл. 28.05.2019 Бюл. № 16.

УДК 004.942

Угрюмов Станислав Сергеевич
направление Информационные системы и технологии (бакалавриат),
гр. 5838

Научный руководитель: **Угрюмов Сергей Алексеевич**,
д-р техн. наук, профессор кафедры технологических процессов и машин лесного комплекса
ФГБОУ ВО «Санкт-Петербургский государственный лесотехнический университет имени С.М. Кирова»,
г. Санкт-Петербург

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ОПТИМИЗАЦИИ ПОДБОРА ЛЕСОЗАГОТОВИТЕЛЬНОГО ОБОРУДОВАНИЯ

Введение. Лесозаготовительное производство характеризуется разнообразием применяемых технологий и оборудования, которые зависят от характеристики древостоя, природных факторов, объемов

заготовки и переработки лесопродукции, уровня организации и технической оснащенности производства [1]. В последние годы в практику работы лесозаготовтельных предприятий широко внедряются и эффективно используются высокопроизводительные многооперационные машины, при этом применение бензиномоторных пил остается весьма значимым.Основным инструментом малых предприятий на валке леса по-прежнему является бензиномоторная пила [2].

При заготовке древесины бензиномоторные пилы могут применяться в различных системах машин (в сочетании с процессором, форвардером, трелевочным трактором), при этом в процессе организации лесозаготовок важно подобрать оптимальный комплекс лесозаготовительной техники, как наиболее эффективный в конкретных условиях [3]. На рынке бензиномоторных пил предлагается большая номенклатура инструмента, что позволяет лесозаготовителям выбирать технику различных фирм для реализации разнообразных технологий производства.

Выбор марки бензиномоторной пилы производят по мощности двигателя, при этом оптимальная мощность бензиномоторных пил определяется лесотаксационными показателями древостоев и условиями лесоэксплуатации [4]. Расчет мощности бензиномоторной пилы требует временных затрат, кроме этого он бывает затруднен поиском необходимых для расчета параметров в технической и справочной литературе. Поэтому на этапе выбора оптимальной марки пилы целесообразно максимально автоматизировать расчеты, что приведет к сокращению затрат времени и удешевлению комплекса трудоемких предпроектных работ, а также повысит точность расчета.

Целью работы является применение информационных технологий для автоматизации расчетов мощности пил и выбора марки пилы на основе расчетной мощности.

Результаты работы.В рамках данной работы для автоматизации расчетов была использована программа VisualStudio 2019, которая позволяет создать приложение для Windowsи оптимизировать процесс подбора технологического оборудования.

При создании программного кода были заведены формулы расчета оптимальной мощности пилы, используемой только на валке древесины; на валке древесины и обрезке сучьев; на валке древесины, обрезке сучьев и раскряжевке.

В качестве примера в данной работе приведены результаты оценки оптимальной мощности двигателя бензиномоторной пилы,

используемой на валке древесины, обрезке сучьев и раскряжевке, которую рассчитывали по формуле [5]:

$$N = \sqrt{\frac{1050\ (K_O K_п b d_k^2 \left(1+\frac{h}{l_c}\right)+0{,}5\ F)}{60\ d\sqrt{\frac{h}{\lambda}+h}}}, \qquad (1)$$

где K_O – удельная работа при поперечном пилении древесины цепными пилами, кДж/м^2;

$K_п$ – коэффициент учитывающий наличие преобладающей породы;

b – ширина реза пильной цепи, м;

d_k– диаметр дерева в месте спиливания, м;

h – высота древостоя, м;

λ – запас древесины на 1 га, м^3/га.

l_c– длина выпиливаемых сортиментов, м;

F – суммарная площадь обрезаемых сучьев, м^2.

В код программы были заведены необходимые для расчета эмпирические данные для пиления основных пород древесины, расчетные формулы по определению диаметра дерева в месте спиливания и суммарной площади обрезаемых сучьев, а также заведена база данных по паспортной мощности основных марок бензиномоторных пил отечественного и импортного производства.

В качестве примера на рис. 1 приведен фрагмент листинга разработанного приложения.

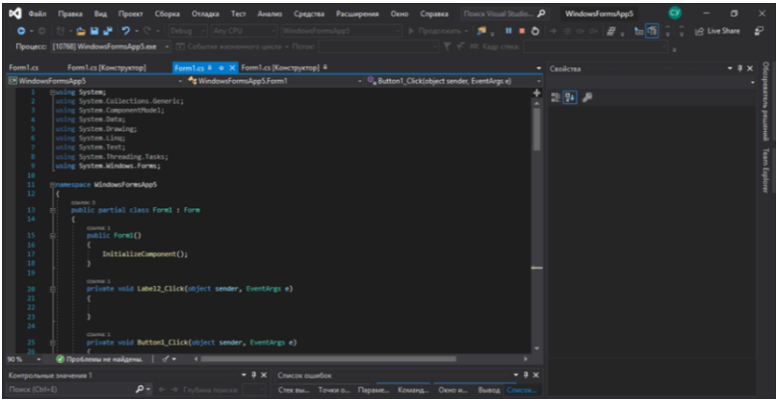


Рис.1. Фрагмент листинга программы

Результаты расчета выдаются в виде окна, в котором указаны основные исходные данные процесса лесозаготовки и обработки лесоматериалов, расчетная мощность пилы для рассматриваемого процесса и рекомендуемые марки пил (одна или несколько). Пример итогового расчета представлен на рис. 2.

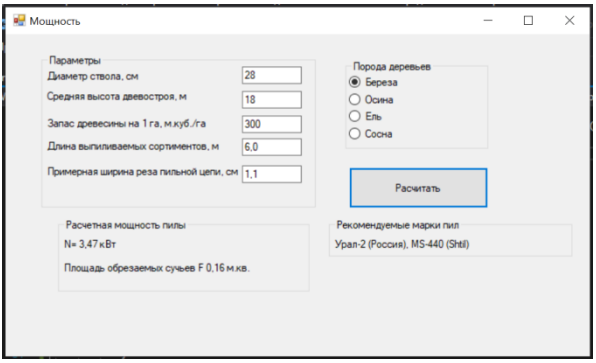


Рис. 2. Фрагмент программы расчета мощности бензиномоторной пилы

Выводы. Использование разработанного приложения для расчета мощности бензиномоторных пил позволяет автоматизировать процесс расчета и подбора марки пилы по мощности двигателя с упрощением процедуры расчета и повышением точности, а также экономией времени. Данное приложение расширено путем введения дополнительного кода расчета производительности подобранной марки пилы при выполнении различного комплекса лесозаготовительных операций и обработки лесоматериалов.

По данному принципу создан код программы расчета и оптимизации подбора многооперационных машин – харвестеров и форвардеров, что позволяет оптимизировать расчет и выбор комплекса машин для выполнения лесозаготовок в зависимости от характеристик древостоя и технологических особенностей производства.

Список литературы

1. Технология и оборудование лесопромышленных производств. Технология и машины лесосечных работ / под ред. В.И. Патякина. – СПб: СПбГЛТУ, 2010. - 330 с.

2. Заикин А.Н. К вопросу о надежности работы бензиномоторной пилы /А.Н. Заикин, Г.Н. Кривченкова // Актуальные проблемы лесного комплекса. 2009. – № 24. – С. 18-20.

3. Волдаев М.Н. Проектирование лесозаготовительных и деревоперерабатывающих производств лесного комплекса / М.Н. Волдаев. – Йошкар-Ола: ПГТУ, 2017. – 92 с.

4. Тарадин Г.С. Уточненный расчет производительности бензиномоторной пилы на валке / Г.С. Тарадин, А.В. Андронов, Е.Г. Хитров, А.В. Чураков // Леса России: политика, промышленность, наука, образование: материалы III международной научно-технической конференции. – СПб.: СПбГЛТУ, 2018. – С. 234-237.

5. Шелепов В.В. Сортиментная заготовка древесины / В.В. Шелепов. − Кострома: КГУ, 2010. − 53 с.

УДК 004.056

Федорова Элина Евгеньевна
направление Информатика и вычислительная техника (магистратура),
гр. ИВТм-21

Научный руководитель: **Васяева Наталья Семёновна**
к.т.н., доцент
ФГБОУ ВО«Поволжский государственный технологический университет», г. Йошкар-Ола

СПЕЦИФИКАЦИЯ АЛГОРИТМА АРБИТРАЖА КОММУТАТОРОВ PCI EXPRESS

Интерфейс PCI Express в настоящее время используется как средство коммуникации в кластерных вычислительных системах, поскольку имеет реализацию не только в качестве внутрисистемной шины, но и в качестве внешней кабельной системы. Использование технологии PCI Express в подобных системах привлекательно для разработчиков, так как она уменьшает стоимость и энергопотребление, улучшает производительность и коэффициент использования кластерных систем, упрощает конструкцию[1].

В архитектуре PCI Express шины, с подсоединенными к ней устройствами, как таковой не существует. Обмен данными между устройствами происходит посредством коммутатора. Следовательно, арбитраж устройств на шине рассматривается как арбитраж между портами коммутатора с учётом специфики, накладываемой протоколом PCI Express [2].

При передаче трафика с нескольких входных портов коммутатора PCI Express на один выходной порт происходит конфликт, который

решается при помощи арбитража, производимого на основе номеров виртуальных каналов и их приоритетов.

Система арбитража PCI Express двухступенчатая. Первая ступень решает задачу обеспечения доступа потокам пакетов с разных входных портов, а вторая ступень распределяет входные потоки с учетом приоритетов. Такая организация является избыточной, что отмечают сами авторы спецификации[2], поскольку на каждый выходной порт число аппаратных очередей должно соответствовать числу входных портов. Затем потоки группируются в 8 выходных очередей, что соответствует числу виртуальных каналов. Но такое большое число оправдано и позволяет равномерно распределять потоки с разных входных портов с учетом принадлежности разным виртуальным каналам.

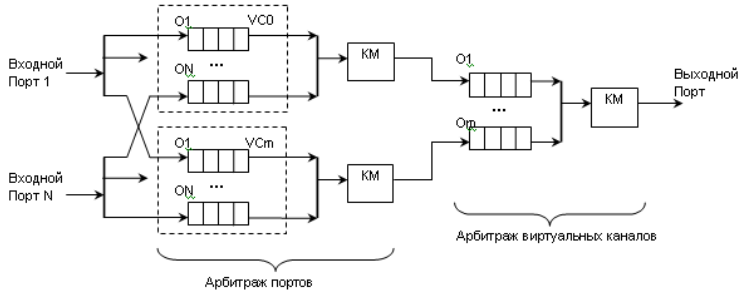


Рис. 1. Структура модели арбитража PCIExpress, где КМ – коммутационная матрица

В PCI Express имеется поддержка дифференцированных по качеству обслуживания (QoS) классов. Арбитр коммутатора PCI Express реализует циклическую и взвешенную циклическую схемы приоритетов, а на этапе арбитража виртуальных каналов также поддерживается статическая смена приоритетов, которая при необходимости может быть применена ко всем виртуальным каналам или только к некоторым[2].

При работе системы с циклической или взвешенной циклической схемой приоритетов может возникнуть ситуация, когда наивысшим приоритетом в определенный момент времени обладает очередь без заявок. Во избежание простоя и серьезного падения пропускной способности коммутатора арбитр должен принимать решение о передаче заявки и просматривать другие очереди быстрее, чем заявка поступает в систему.

Список литературы

1. Mallampati K. PCI Express vs. Ethernet – selecting the superior technology for real-time, embedded systems // RTC Magazine. – 2014. – vol. 15, №12, p.28-31

2. PCI Express Base 3.0 Specification [Электронныйресурс] // URL: http://www.pcisig.com/specifications/pciexpress/base3/

3. Иванов, К. В. Программная модель системы арбитража коммутатора PCI Express [Текст]/ К. В. Иванов, А. А. Кошпаев, Н. С. Васяева// Кибернетика и программирование. — 2014. - № 4. - С.66-75. URL: http://e-notabene.ru/kp/article_12758.html

УДК 004.056.55

Фомин Евгений Вячеславович
направление Информационная безопасность (специалитет), гр. БИ-52

Научный руководитель: **Чекулаева Елена Николаевна**,
канд. экон. наук, доцент кафедры Информационная безопасность
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ЦИФРОВАЯ ВАЛЮТА, КАК СРЕДСТВО ПРОВЕДЕНИЯ ВЫСОКОЗАЩИЩЁННЫХ ФИНАНСОВЫХ ОПЕРАЦИЙ

В статье рассматривается мобильный банкинг и цифровая валюта. С точки зрения безопасности и возможности отслеживания всех операций с цифровой валютой, появляется возможность принятия цифровой валюты, как средство для проведения международных финансовых операций. Возможность внедрения цифровой валюты в мобильные приложения банков параллельно с действующей валютой.

Появлениесервисовмобильногобанка приобрело значимый характер в жизни современногообщества. С развитием мобильных технологий, которые направлены на упрощение и ускорение темпа жизни людей, появилась необходимость и в предоставление возможности удалённого управления финансовыми средствами в банковских учреждениях. История развития мобильного банкинга начинается с 1992 г., когда финский банк Merita Nordbanken Group включил в коммерческую эксплуатацию соответствующиесервисы. В 2000-е годы, с ростом пользователей мобильных телефонов, это направление мобильных услуг активно развивается, в большей степени, в традиционно технически продвинутых регионах, таких как: Юго-Восточная Азия, США и в некоторых странах Европы [1].Спрос на такие услуги резко приобрёл

значимый характер, а где появляется спрос - там и рождаётся предложение. Программисты и фирмы, занимающиеся разработкой программногообеспечения для проведения финансовых операций, увидев такую ситуацию на рынке, взялись за решение вопроса. И тем самым развитиесервисов, предоставляющих возможность удалённого управления финансовыми средствами, приобрелостремительный темп.

Через все российскиесервисы мобильного банкинга по итогам 2014 года прошло порядка 15,5 млрд рублей, посчитали предварительнные цифры аналитики J'son & Partners. При этом средняя комиссия при проведении платежасоставила 1,2%. Таким образом, доход всех сервисов мобильного банкинга в России можнооценить в 190 млн рублей [2].

В настоящее время приложения для мобильного банкинга – это"банк в кармане" с урезанным функционалом, адаптированные под небольшие экраны смартфонов и под операционныесистемы, устанавливаемые в мобильных устройствах. Системы мобильного банкингасчитаются инновационными решениями и, содной стороны, противодействуют недружественным проникновениям в банковскиесистемы, а с другой – создают для хакеров новые возможности. Популярные ныне банковские приложения, позволяющие клиентам на расстоянии распоряжаться своими финансами, делать онлайн-переводы, нередкостановятся целью мошенников.

Последние годы ознаменовались большим скачком вперёд в глобальной мировой финансовой системе. То, что кажется незыблемым сейчас, может оказаться через несколько лет вполне реальным. Денежная система была придумана в далёкие времена. Её появлению способствовалосуществование торговли, когда владелец мог обменять свой товар на равный по ценности необходимый ему. С появлением денег рынок перешёл на форму товарногообращения, она базировалась на превращении товара в деньги и наобратном превращении денег в товар. В веке, когда мобильные технологии совершенствуются, а их распространениестало глобальным, люди всё более привыкают к тому, что мобильный телефон можно использовать не только для связи, но и как средствосовершения финансовых операций. Так, например, с помощью мобильного телефона можносовершать денежные переводы, оплачивать счета или делать покупки в интернете. Во многих финансово устойчивых странах мобильный телефон уже интегрирован частично или же полностью с внутренней системой финансового механизма.

В 2008 году трое учёных, а именно жители США и Германии разработали основу, которая и стала началом появления новой криптовалюты. Ими же были поданы заявки на несколько патентов, в самих заявках были заключены теаспекты, которые бы позволили защитить открытие будущей валюты. Чуть позже под псевдонимом Сатоси Накамото ими были опубликованы основныеалгоритмы работы BitCoin, а также код, который работал по принципу нахождения новых единиц валюты и, наконец, первоначальная цепочка переводов[3].

За всё то время виртуальная валюта пережила неодин спад и неодно падение. Стоимость её единицы относительно доллара поднималась и опускалась в несколько тысяч раз. Спустя некоторые время правительства некоторых стран, в том числе и Россия, запретила проведение каких-либоопераций в биткойнах. Основным опасением послужило то, чтоBitCoin может использоваться в незаконной деятельности и участвовать в различного родаспекуляциях.

С увеличением спроса финансовых операций, стал увеличиваться и рост предоставляемых услуг банками. В настоящее время существуют следующие виды дистанционного получения услуг:

Телефонный банкинг (phone banking) – обслуживаниеосуществляется посредством телефона.

Мобильный банкинг (mobile banking) – обслуживаниеосуществляется посредством портативных устройств.

PC-банкинг (e-banking) – обслуживаниеосуществляется посредством персонального компьютера.

Видео-банкинг (video banking) – обслуживаниеосуществляется посредством систем интерактивногообщения с персоналом банка.

Домашний Банкинг (home banking), **Банк-Клиент** – обслуживаниеосуществляется посредством установления стационарной связи между банком и клиентом.

С помощью сервисов мобильного банкингавозможноосуществление двух основныхтиповопераций – получение и передачаинформации и проведениеплатежей.[6] К первому типу операцийможноотнести:проверка денежных средств на банковском счету или банковской карте; просмотр истории операций, совершаемых данным лицевым счётом; SMS-информированиепроведения финансовых операций по банковской карте, получениеинформациидостаткезадолженностипокредиту, просмотркурсоввалют, поискближайшегоотделениябанка и другиеподобныеуслуги. К передаче информации можноотнести внутрибанковскиеоперации ссчетами, оплата услуг, штрафов,

различного рода финансовые переводы между банками и т. д. Функции предоставляемые приложениями мобильного банкинга:

- SMS-уведомления о всех операциях по банковской карте;
- Возможность заблокировать карту при необходимости;
- Управлениесчетами, переводы в другой банк, оплата мобильных услуг, оплата услуг интернет-провайдера, погашение штрафов, оплата ЖКХ, коммерческого телевидения и т.п. (с помощью шаблонов интернет-банка);
- Просмотр детальной информации осчёте;
- Поиск ближайших банкоматов, ближайших отделений плюс просмотр детальной информации по выбранному объекту (адрес, режим работы, возможныесервисы),
- Просмотр актуальных курсов валют и др.

Преимущества и особенности

Главной особенностью сервисов мобильногобанка для современного общества являетсяудобство и экономиявремени, ведьмобильныйтелефонвсегданаходится рядом, азначит, вполненормальноиспользоватьего в качествесредства проведения финансовых операций. Сточкизрениябанка, приложения мобильного банкинга- этоважныймаркетинговыйинструмент для привлеченияклиентов из разных слоёв общества.Основные преимущества использования сервисов мобильного банка:

1. Дистанционное управление финансовыми средствами в банке;
2. Круглосуточный доступ;
3. Упрощение банковских операций;
4. Предоставление полной отчетности;
5. Быстрый анализ расходов и зачислений.

Угроза утечки личной информации возрастает сотсутствием специальных приложений для защиты устройства. Даже простой бесплатный антивирусснижает уровень угрозы. Данные также могут стать достоянием третьих лиц при утере и краже телефона. К основным недостаткам сервисов мобильного банкасостороны клиента можноотнести:

1. Простотаавторизации;
2. Низкая скорость работы приложения;
3. Слишком насыщенный интерфейс;
4. Затруднительный поиск необходимой услуги;
5. Уровень защищённости приложения.

Банк России сообщил об увеличении доли граждан РФ, использующих интернет-банкинг или мобильный банкинг, с 31,5% в 2017 году до 45,1%.

Доля тех, кто уже использует интернет-банкинг или мобильный банкинг, выросла в 2018 году до 45,1% (с 31,5% в 2017 году)», — говорится в сообщении регулятора.

Кроме того, с мая 2017 по май 2018 года выросла доля субъектов малого и среднего бизнеса (с 73,6% до 79,6%), использующих дистанционный доступ к банковским счетам, отмечают в Центробанке.

По мнению регулятора, рост использования дистанционных каналов доступа к финансовым услугам фактически компенсирует снижение физической доступности финансовой инфраструктуры. При этом, несмотря на то что данная тенденция сохраняется, темп, с которым происходит снижение количества точек доступа к финансовым услугам, падает. Так, количество действующих подразделений кредитных организаций в 2015 году сократилось на 11,2%, в 2016 году — на 8,7%, в 2017 году — на 3,4%. [5]

Актуальность проблемы безопасности очень высока в настоящее время. В современном обществе человек при выборе банк стал обращать внимание на удобство мобильного приложения. Но, помимоудобства, обращатьвниманиенужно и набезопасностьпрограммногообеспечения. Поэтому при выборебанковскогоприложениясследует учитывать следующие факторы:

1. Системааутентификации (двухфакторнаяаутентификация, одноразовыепароли, смс-вход);
2. Политика безопасности приложения и уровень защиты критически важной информации;
3. Отзывы пользователей приложения;
4. Уровень защиты приложения, личного кабинета;
5. Шифрование транзакций.

Многое будет зависеть и от того, какими станут сами мобильныеустройствав ближайшее время. Появлениемобильных систем развилось до высокого уровня стали, стали появляться телефоны сотносительно крупными сенсорными экранами, возможностью установки сложных приложений, с возможностью совершать массовые небольшие платежи (оплата транспорта или счета в кафе) с помощью бесконтактных чипов (например, NFC). Согласно последним данным, которыми поделился старший вице-президент по мобильным решениями в Google Энди Рубин (Andy Rubin) в своем микроблоге в

сервисеTwitter, сейчасежедневноактивируетсяболее 900 тысячAndroid-устройств [4].

Потенциал развития мобильного банкинга в России огромен. Этому способствует все больший охват регионов высокоскоростным «мобильным» доступом в интернет, да и мобильный телефон стал для всех устройством, без которого уже невозможно вести современный образ жизни.

"Я работаю над новой системой электронных денег, которая полностью одноранговая, без доверенной третьей стороны.

Основныесвойства:

1. Повторные транзакции предотвращаются с помощью одноранговой сети.

2. Нет доверенных сторон.

3. Участники могут быть анонимными.

4. Новые монеты изготовлены по принципу работы Hashcash.

Доказательство работы нового поколения монет также обеспечивает сеть для предотвращения двойных расходов.

Биткойн: электронная кассовая система. Чистая одноранговая версия электронных денег разрешит отправку онлайн-платежей напрямую от одной стороны другой без времени прохождения через финансовое учреждение. Цифровые подписи обеспечивают часть решения, но главное выгода теряется, если доверенная сторона по-прежнему требуется для предотвращения двойных расходов. Мы предлагаем решение дополнительных расходов проблемас использованием одноранговой сети. Сетевые метки времени транзакции путем хеширования их в непрерывную цепочку наоснове хеша. Доказательство работы, формирование записи, которую нельзя изменить без переделывания доказательства работы. Самая длинная цепь не толькослужит, как доказательство последовательности событий, но доказательство того, чтооно пришлоот самого большого пула мощности процессора. Пока четные узлы контролируют наибольшую мощность процессора в сети, они могут генерировать самые длинные цепи и опередить любого злоумышленника. Самасеть требует минимальной структуры. Сообщения транслируются с максимальной отдачей,и узлы могут выходить и присоединяться к сети по желанию, принимая длинную цепочку доказательств работы, как доказательство того, что произошло, покаони ушли.

Полный текст статьи поадресу: http://www.bitcoin.org/bitcoin.pdf

Мы предложили систему электронных транзакций, не полагаясь на доверие. Мы взял обычный каркас монет из цифровых подписей,

который обеспечивает строгий контроль владения, но не является полным без способа предотвращения дополнительных расходов. Чтобы решить это, мы предложил одноранговую сеть, использующую доказательство работы для записи публичной истории транзакций это быстростановится вычислительно непрактичным для атакующего, если четные узлы контролируют большую часть мощности процессора. Сеть надежна в своей неструктурированной простоте. Их не нужно идентифицировать, так как сообщения не направляются в какое-либо конкретное место и должны доставляться только наоснове максимальных вычислительных процессов. Они голосуют с их мощностью процессора, выражая своесогласиес действительными блоками, работая над их расширением и отклоняя недействительные блоки, отказываясь работать с ними. Любые необходимые правила и стимулы могут быть обеспечены спомощьюэтогомеханическогоконсенсуса[7].

Появлениеновых инновационных решений в сфере банков и валют – это всегда риск. Деньги – это риск, поэтому вкладчики всегда на грани некой опасности в этой сфере. Несмотря на все нюансы, криптовалюта продолжает говорить освоей значимости в этом мире. Современноеобщество присматривается к криптовалюте и готовы инвестировать в эту область.Сразу же хотелось бы обратить внимание на все плюсы криптовалюты. Преимущества цифровой валюты:

Безопасность. Невозможно подделать цифровую валюту или взломать единую базу компьютерных кодов. Информационная база фактически хранится на многочисленных компьютерах пользователей, поэтому для ее взлома необходимо получить одновременный доступ ко всем задействованным системам в мире.

Прозрачность. Если взять любую купюру из кошелька, можно ли рассказать обо всех операциях, в которых она участвовала? С цифровой валютой ситуация обратная: каждый пользователь может узнать подробную историю операций с момента появления валюты. Поэтому мнениео том, чтооткрытые виды криптовалют удобно использовать для преступных махинаций, — не более чем выдумка.

Возможность полной анонимности. При обмене криптовалютой необязательно указывать свои паспортные данные или подробную информацию осебе. Это делается исключительно для удобствасамого пользователя и поего желанию. Поэтому ваши данные невозможно похитить или использовать в незаконных корыстных целях, в отличиеот платежей через банковские карты.

Необеспеченность криптовалюты. В отличиеот рублей или долларов цифровая валюта необеспечивается золотым запасом государства или другим видом поддержки. Ее успешность — исключительно интерес пользователей. Чем больше людей участвует в обороте, темтверже и увереннеестановитсякриптовалюта.[8]

Цифровая валютаобладает не только значимыми преимуществами, но и имеет ряд недостатков, которыессвою очередь позволяют задуматься об использование криптовалют. Поэтому при решение использовать данную платежную систему, рекомендуется обратить на ряд следующих недостатков:

1. Чёрный список;
2. Защита;
3. Принципы рынка;
4. Нестабильная ценовая политика;
5. Комиссии сервисов.

Главная причина, которая мешает узаконить любую существующуювиртуальнуювалютузаключается в анонимности этих систем. Из этого фактора следует, что данная система может стать новым совершенным инструментом для проведения трансграничных переводов, совершения нелегальных покупок, обезличивание владельцев "грязных" финансовых средств, также появляется возможность анонимного спонсирования террористических операций и т.д. Именно из-за таких возможностей цифровой валютыполитические структуры с опаской и недоверием относятся к данному виду платежных средств.

Традиционнаяфинансоваясистемаоснованнадовериимеждуучастникамитранзакции, в то время каквиртуальная валюта более технологическипродуманна, что автоматически расширяет её возможности.

В течение последнего десятилетия количество криптовалют стремительно увеличилось.Одни смогли найти свое место под солнцем и успешно работают в какой-тоопределенной сфере, а другие пока что не могут похвастаться такими достижениями. В основном, проблемы разработок заключаются в совместимости, конфиденциальности и безопасности. В ближайшем будущем обществосможет наблюдать:

1. Мультивалютного цифрового кошелька
2. Усилениесредств анонимности и защиты личности
3. Увеличение числа пользователей
4. Упрощённые приложения для использования цифровой валюты
5. Увеличениесферприменениякриптовалют.

Финансоваяпроблемаостра и актуальна в настоящее время. Общество хочет не только не нуждаться в средствах, но и ещё не потерять, то что уже имеют. Поэтому с развитием уровня программирования появляются всё новые и новые возможности проводить финансовыеоперации. Цифровая валюта - этоодни из таких же изобретений современного времени, которое гарантирует анонимность владельца и отсутствие третьих лиц в финансовых сделках. Именно из-за второго яркого плюса, мировая политика и не хочет признавать валюту, как средство мирового платежа. Например: после первоначальной регистрации bitcoin.org с использованием службы регистратора в Японии, которая позволяет анонимно маскировать и размещать домен на IP в Японии приблизительно в течение месяца, IPадрес для bitcoin.org был изменен на немецкого хостинг-провайдера (IP-адрес находился в большом блоке компании, и они предлагали услуги посредничества, так что вполне вероятно, чтосервер был размещен непосредственно на площадкеодного из потенциальных партнеров данной организации).

Проблема безопасности и сохранности финансовых средств остростоит в настоящее время, цифровая валюта предлагает новые методы защиты финансовых средств от вмешательства или непосредственного участия третьих лиц. Изучив вопросы появления, развития, достоинства и недостатки систем работы с финансовыми операциями, не трудноспрогнозировать, что из-за вопросов безопасности появятся системы дистанционного управления финансовыми операциями с цифровыми валютами.

Список литературы

1. https://www.eduherald.ru/ru/article/view?id=16392
2. https://roem.ru/12-03-2015/187614/fintech-mobile-banking-1/
3. http://bubunta.com/kakimi-budut-dengi-budushhego.html
4. https://3dnews.ru/630772
5. https://www.plusworld.ru/daily/digital-banking/dolya-ispolzuyushhih-mobilnyj-i-internet-banking-rossiyan-vyrosla-do-45/
6. https://bankir.ru/publikacii/20110831/mobilnyi-banking-10000394/
7. https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html, https://bitcoin.org/bitcoin.pdf
8. Оригиналстатьи: https://aif.ru/boostbook/kriptovaljuta.html

УДК 004.056

Чемеков Александр Николаевич
направление Информатика и вычислительная техника (магистратура),
гр. ИВТм-21

Научный руководитель: **Моисеев Николай Геннадьевич**
к.т.н., доцент
ФГБОУ ВО«Поволжский государственный технологический университет», г. Йошкар-Ола

РАЗРАБОТКА МЕТОДИКИ ПОСТРОЕНИЯ И СРАВНИТЕЛЬНОГО АНАЛИЗА ОТКАЗОУСТОЙЧИВЫХ СИСТЕМ КОРПОРАТИВНОЙ ТЕЛЕФОННОЙ СВЯЗИ, ПОСТРОЕННЫХ НА БАЗЕ ПРОТОКОЛА IP

В связи с широким распространением систем корпоративной телефонной связи, построенных на базе протокола IP, возникает проблема обеспечения качества телефонной связи, достигаемой, прежде всего за счет ее надежности и отказоустойчивости. Поэтому наряду с потребностью в широкой функциональности корпоративных информационных систем, на передний план выходят требования к максимальной надежности. Это весьма актуально для бизнеса, где сбой системы или ее временной простой оборачиваются порой внушительными финансовыми потерями. В связи с этим, на сегодняшний день задача разработки отказоустойчивой системы IP-телефонии является весьма актуальной. Также весьма актуален вопрос выбора из нескольких вариантов наиболее отказоустойчивой архитектуры. К преимуществам IP-телефонии можно отнести богатый функционал, возможность улучшить взаимодействие сотрудников, сократить издержки на междугороднюю связь и, одновременно, упростить обслуживание системы. Отличием систем IP-телефонии от традиционных коммуникаций, является глубокая интеграция с IP сетью. При проектировании сети IP-телефонии следует учитывать, что сеть должна быть более надежной по сравнению с обычной сетью передачи данных, это обусловлено тем, что традиционные приложения IP-сети (почта, Интернет, передача данных) могут работать и с обрывами связи, но при использовании приложений реального времени такие обрывы связи недопустимы. Для обеспечения безотказной работы компонентов системы IP-телефонии, необходимо обеспечить их резервирование, устранение единой точки отказа, физическое разнесение коммуникаций, интеграцию всей системы для обеспечения функций балансировки нагрузки и переключения компонентов в случае выхода из строя любого

модуля системы. На сегодняшний день не существует абсолютно надежных систем. При проектировании отказоустойчивых систем применяются два подхода. Первый подход – построение системы только из отказоустойчивых компонентов. Второй подход - проектирование отказоустойчивой системы из не отказоустойчивых компонентов, но с применением избыточности. В этом случае система может продолжать свое функционирование, если выйдут из строя один или несколько подкомпонентов системы. Но кроме проблемы проектирования надежной системы, существует и проблема оценки уже спроектированной системы по ряду параметров отказоустойчивости. Одним из таких параметров отказоустойчивости является коэффициент готовности. Коэффициент готовности — вероятность того, что система окажется в работоспособном состоянии в любой произвольный момент времени, исключая планируемые периоды, в течение которых применение системы по назначению не предусматривается. Если есть возможность оценить ряд архитектур по данному параметру отказоустойчивости, это может дать шанс выбора наиболее надежной архитектуры. Существуют два принципиальных подхода к оценке отказоустойчивости систем: аналитический и имитационный.

Аналитический подход основан на математических моделях. К его преимуществам можно отнести: возможность быстрого расчета приближенных математических моделей с оперативным графическим представлением и исследованием результатов моделирования. К недостаткам относится трудность, а иногда и невозможность адекватного учета в модели разнотипных параметров, например, вероятностных и детерминированных. Имитационный подход основан на имитации работы системы и сбора статистики. Преимуществом является возможность получения достоверных оценок для сколь угодно сложных систем с учетом самых различных параметров и факторов. К недостаткам можно отнести сложность организации исследований на основе изменения параметров модели. Необходимо каждый раз перекомпилировать имитационную модель при изменении хоть одного параметра модели. Иногда сложность построения адекватной имитационной модели системы сравнима со сложностью построения аппаратного прототипа системы, так что программная модель теряет всякий смысл. Рассмотрим концептуальную логическую схему отказоустойчивой системы IP-телефонии. Предполагается, что сеть IP-телефонии спроектирована по 3-х уровневой системе и имеет уровень доступа, уровень представления и уровень ядра. Уровень доступа является ближайшим к пользователю и предоставляет ему доступ к

ресурсам сети, чем и объясняется его название. Уровень распределения обеспечивает объединение потоков данных уровня доступа и служит точкой перехода к уровню ядра. Основной задачей уровня ядра является обеспечение наиболее быстрой коммутации между двумя областями распределения. В системе для обеспечения надежности используется резервирование ее основных компонентов: коммутаторов и серверов. Система предназначена для многоэтажного офиса (NЭ.— число этажей), на каждом этаже которого расположены N0 подразделений. Каждое подразделение имеет свой маршрутизатор телефонных звонков (коммутатор нулевого каскада), обозначаемый как К0. Каждый коммутатор нулевого каскада соединен с IP-телефонами сотрудников. Число IP-телефонов обычно примерно равно числу сотрудников в одном подразделении.

Целью диссертационной работы является разработка инженерной методики построения и решение задачи организации отказоустойчивых систем корпоративной телефонной связи на базе IP-телефонии, обладающих высокими качественными и эксплуатационными показателями.

Для достижения поставленной цели в работе сформулированы и решаются следующие задачи:

1. Исследование архитектуры, принципов построения и организации систем корпоративной телефонной связи на базе IP-телефонии, с целью выявления проблем отказоустойчивости и качества функционирования присущих исследуемой системе. Анализ и выбор методов для обеспечения отказоустойчивости систем корпоративной телефонной связи.

2. Создание математических моделей функционирования и методов оценки надежности систем корпоративной телефонной связи, позволяющих учитывать вид и характеристики контроля, время подключения резерва и другие параметры. Создание имитационных моделей, для проверки достоверности аналитических результатов.

3. Исследование особенностей процесса обслуживания вызовов в системах корпоративной телефонной связи на базе IP-телефонии. Создание моделей, позволяющих оценить качество

4. функционирования систем корпоративной телефонной связи с учетом возможных отказов оборудования.

5. Разработка инженерной методики проектирования отказоустойчивых

6. систем корпоративной телефонной связи на базе IP-телефонии, обладающих высокими качественными и эксплуатационными показателями.

Методы исследования. Исследования проводились с использованием математического аппарата марковских и полумарковских процессов, математической статистики, теории надежности, теории восстановления, теории массового обслуживания. Также при решении поставленных в диссертационной работе задач использовались методы статического моделирования случайных процессов на ЭВМ.

Научная новизна. Новизну представляют следующие научные результаты:

1. Исследованы архитектура, принципы построения и организации систем корпоративной телефонной связи на базе IP-телефонии. Выявлено, что наиболее критичными с точки зрения отказоустойчивости являются серверы системы распределения вызовов (СРВ), модуль IP-телефонии и шлюз IP-телефонии. Впервые определены и адаптированы для систем корпоративной телефонной связи методы, которые следует использовать для повышения надежности систем корпоративной телефонной связи на базе IP-телефонии и их подсистем. В число данных методов входят кластерный подход с различными режимами использования резерва, общий резерв для однотипных компонентов (в основном серверов), а также комбинированные подходы.

2. Показана применимость известных математических моделей и методов, а также созданы новые модели и методы для оценки характеристик надежности систем корпоративной телефонной связи. Предложенные модели позволяют учесть параметры непрерывного (аппаратного) и/или периодического (программного) контроля, время подключения резерва. В отличие от большинства существующих, модели позволяют учитывать не экспоненциальный характер распределения периода тестового контроля, а также времени подключения резерва, что более близко к характеристикам реальных систем. Созданы соответствующие имитационные модели, подтвердившие правильность аналитических результатов.

3. Предложены модели, позволяющие оценить качество функционирования систем корпоративной телефонной связи с учетом возможных отказов оборудования. Использование предлагаемых моделей позволяет учесть различную интенсивность поступления, различное число мест в системе для вызовов со стороны телефонной

сети общего пользования (ТфОП), IP-телефонии и другие особенности обслуживания вызовов в системах корпоративной телефонной связи на базе IP-телефонии.

Впервые разработана и представлена в виде алгоритма инженерная методика проектирования отказоустойчивых систем корпоративной телефонной связи на базе IP-телефонии, обладающих высокими качественными и эксплуатационными показателями.

Научные положения, выносимые на защиту:

1. Наиболее критичными с точки зрения отказоустойчивости подсистемами систем корпоративной телефонной связи являются серверы СРВ, модуль IP-телефонии и шлюз IP-телефонии. В число методов, которые следует использовать для повышения надежности систем корпоративной телефонной связи на базе IP-телефонии и их подсистем, входят кластерный подход с различными режимами использования резерва, общий резерв для однотипных компонентов (в основном серверов), а также комбинированные подходы.

2. Математические модели и методы для оценки характеристик надежности систем корпоративной телефонной связи, спроектированных с применением различных методов повышения отказоустойчивости. Предлагаемые модели позволяют учесть параметры непрерывного (аппаратного) и/или периодического (программного) контроля, время подключения резерва.

3. Модели, позволяющие оценить качество функционирования систем корпоративной телефонной связи с учетом возможных отказов оборудования. Использование предлагаемых моделей позволяет учесть различную интенсивность поступления в контакт-центр, различное число мест в системе для вызовов приходящих со стороны ТфОП, IP-телефонии и другие особенности обслуживания вызовов в системах корпоративной телефонной связи на базе IP-телефонии.

4. Инженерная методика проектирования отказоустойчивых систем корпоративной телефонной связи на базе IP-телефонии, обладающих высокими качественными и эксплуатационными показателями.

Практическая значимость работы заключается в том, что предложен ряд моделей и методов, которые позволяют обеспечить отказоустойчивость, оценить качество функционирования систем корпоративной телефонной связи на базе IP-телефонии. Данные модели и методы, как отдельно, так и в сочетании с другими моделями и методами, могут применяться для обеспечения надежности и оценки качества функционирования систем корпоративной телефонной связи как на стадии их проектирования, так и для анализа характеристик

разработанных систем. Разработана и предложена инженерная методика, позволяющая проектировать контакт-центры, обладающие высокими качественными и эксплуатационными показателями. Созданные модели и научную основу принципов организации отказоустойчивых систем корпоративной телефонной связи можно использовать при дальнейших исследованиях. В частности можно собирать статистику отказов различных систем корпоративной телефонной связи и производить дальнейшие исследования на отказоустойчивость. Также представляет интерес исследование работоспособности систем корпоративной телефонной связи при критическом возрастании нагрузки, например, в результате какого-либо чрезвычайного происшествия, затронувшего большое число граждан и т.п.

Достоверность результатов исследования подтверждается корректным использованием математического аппарата, результатами экспериментальных исследований на программных моделях и результатами испытаний реальной системы, при создании которой использовались предложенные модели и методики.

УДК 004.056

Чернова Анастасия Юрьевна
направление Информатика и вычислительная техника (бакалавриат),
гр. ИВТ-11-16

Научный руководитель **Галанина Наталия Андреевна**,
д-р техн. наук, профессор кафедры математического и аппаратного обеспечения информационных систем
ФГБОУ ВО «Чувашский государственный университет»,
г. Чебоксары

ИСПОЛЬЗОВАНИЕ ОБЛАЧНЫХ ВЫЧИСЛИТЕЛЬНЫХ РЕСУРСОВ ДЛЯ САПР

Цель работы – рассмотрение вопросов использования облачных вычислительных ресурсов для САПР в настоящее время и перспектив их дальнейшего развития.

Актуальность темы. В настоящее время на рынке IT-продуктов появляется все больше прикладных программных систем, ориентированных на использование облачных технологий. Тенденция переноса в облако проектирующих подсистем САПР наблюдается при необходимости привлечения значительных вычислительных ресурсов и

для сокращения количества дорогостоящих лицензий на программное обеспечение.

Основная часть. Система автоматизированного проектирования (САПР) – сложный комплекс средств, предназначенный для автоматизации проектирования.

Техническое обеспечение (ТО) – совокупность связанных и взаимодействующих технических средств, обеспечивающих работу САПР. ТО САПР включает устройства вычислений и организационной техники, средства передачи данных, измерительную технику, устройства подготовки данных и организации архивов. В настоящее время большинство практически действующих САПР строятся на базе локальных вычислительных сетей.

Учитывая организации российских предприятий, не трудно предположить, что большую популярность достигнут частные облака для размещения в них САПР. Недоверие к внешним серверам, задачи безопасности и надежности пока что будут превосходить при утверждении решений. САПР в облаке, в первую очередь, позволяет сэкономить на "железе", поскольку это дает использовать всю мощь обработки данных, а не только для рабочего или личного персонального компьютера.

Очень осторожно следует относиться к так называемым «дешевым альтернативам» ПО САПР. Рабочие места сотрудников, которые непосредственно проектируют или вносят изменения, целесообразно оборудовать полноценными лицензиями.

*Использование вычислительных САПР по моделям **SaaS** и **Autodesk***

SaaS – одна из форм облачных вычислений, модель обслуживания, при которой подписчикам предоставляется готовое прикладное программное обеспечение.

Отличительной чертой SaaS является возможность оплачивать работу в САПР только за то время, которое специалист реально в системе нуждается. Это позволяет не приобретать постоянные лицензии для временных групп или внештатных сотрудников.

Autodesk – облачное и интерактивное ПО САПР. Оно предлагает своим клиентам доступ к большому количеству работающих в "облаках" модулей через программу подписки, которая включает в себя ряд дополнительных сервисов: предоставление новых версий, гибкое лицензирование, возможность использовать лицензионную копию ПО на домашнем компьютере, а также предоставление права пользоваться дополнительными модулями, часть из которых используют «облачные» технологии.

Облачные вычислительные ресурсы находятся в России, а не за рубежом. Вся облачная система безопасно защищена, и компания за это несет полную ответственность. Доступ к приложениям выполняется по защищенным каналам. Имеется контроль физического доступа, постоянно выполняется резервное копирование, а также резервное копирование по требованию.

Заключение. Предприятия, которые лишь время от времени сталкиваются с задачами, требующими серьезных вычислительных мощностей, могут не вложиться в покупку и обслуживания суперкомпьютеров, а выполнять необходимые задачи в облачной САПР. Рынок облачных сервисов и неограниченных вычислений будет однозначно расти. Скоро, работая с привычной САПР-программой от Autodesk, пользователи вообще не будут ощущать, какие задачи решаются на их компьютере, а какие передаются для реализации в "облако".

Список литературы

1. Малюх В.Н. Введение в современные САПР/ В.Н.Малюх. М.: ДМК Пресс, 2010. – 192 с.
2. https://www.pointcad.ru/novosti/obzor-sistem-avtomatizirovannogo-proektirovaniya
3. https://www.osp.ru/os/2011/02/13007702/
4. https://softline.ru/about/blog/sapr-v-oblake.-oblachnyie-vyichislitelnyie-resursyi-softline-dlya-vashih-proektov
5. https://cloud.softline.ru/
6. http://e-notabene.ru/kp/article_18612.html
7. https://www.itweek.ru/industrial/article/detail.php?ID=144835

УДК 521.3, 618.5.015

Четвертакова Юлия Сергеевна
направление Математическое обеспечение и администрирование информационных систем (магистратура), гр. ПМИМ-91

Научный руководитель: **Черникова О.С.**
К.т.н., доцент каф. теоретической и прикладной информатики
ФГБОУ ВО «Новосибирский государственный технический университет», г. Новосибирск

ПРОГРАММНЫЙ КОМПЛЕКС ПРОГНОЗИРОВАНИЯ ОРБИТАЛЬНОГО ДВИЖЕНИЯ СПУТНИКА НА ОСНОВЕ МЕТОДОВ ПАРАМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ

Введение

В настоящее время для определения пространственных координат объектов широко используются Спутниковые Системы Навигации

(СНС), в частности, Система Глобального Позиционированияи ГЛОНАСС – Глобальная Навигационная Спутниковая Система.

Несмотря на интенсивное развитие космической геодезии в последние десятилетия остается актуальной задача повышения точности и надёжности координатно-временных определений на основе применения СНС.

Качество эфемеридно-временного обеспечениядля ГЛОНАСС технологий в значительной мере зависит от степени адекватности применяемых математических моделей, описывающих движение орбитальной группировки навигационных спутников (НС). При формировании таких моделей проблемным остается учет возмущений от радиационного давления на спутник солнечного излучения. Данная работа посвящена разработке программного обеспечения, позволяющего решить задачу прогнозирования траектории спутника путем оценки параметров в модели радиационного давления на спутник солнечного излучения на основе применения современных математических методов.

Описание разработанного программного обеспечения

Движение космического аппарата (КА) в инерциальной системе координат (ИСК) в гравитационном поле Земли можно описать следующей нелинейной непрерывно-дискретной моделью в пространстве состояний [1]:

$$\frac{d}{dt}\begin{pmatrix} r(t) \\ \dot{r}\ t \end{pmatrix} = f(r(t), \dot{r}(t) \qquad w(t), \quad t \in [t_0, t_N], \tag{1}$$

$$s(t_{k+1}) = r(t_{k+1}) + v(t_{k+1}), \quad k = 0,1,..,N-1. \tag{2}$$

Здесь $r(t)$ –вектор координат КА в ИСК; $f(\cdot)$ – нелинейная вектор-функция, учитывающая влияние на траекторию движения КА радиационного давления (РД) солнечного излучения, несферичностигеопотенциала Земли, гравитационного воздействия Луны, Солнца и других планет; θ - вектор неизвестных параметров модели РД; $s(t_{k+1})$ – вектор измерения; $w(t)$ и $v(t_{k+1})$ – взаимно некоррелированные гауссовские векторы шумов системы и измерения соответственно с нулевыми математическими ожиданиями и ковариационными матрицами

$$\mathrm{E}\left[w(t)w^T(\tau) \right] = Q(t)\delta(t-\tau), \ \mathrm{E}\left[v(t_{k+1})v^T(t_{i+1}) \right] = R(t_{k+1})\delta_{ki}.$$

Относительно функции $f(\cdot)$ в правой части уравнения состояния (1) заметим, что в настоящее время можно с незначительной погрешностью учесть несферичностьгеопотенциала и гравитационное влияние Луны, Солнца и других планет (см., например, [2]). Иначе обстоит дело с моделированием воздействия сил РД. Воспользуемся следующей моделью РД в объектоцентрической системе координат (ОСК) из [3]:

$$f_{RD} = \Lambda \cdot d \cdot r_{OS}^{-2} \cdot \left[x_{RP} \cdot (\theta_1 + \theta_2 \cos\kappa + \theta_3 \sin\kappa) + y_{RP} \cdot (\theta_4 + \theta_5 \cos\kappa + \theta_6 \sin\kappa) + \right.$$
$$\left. + \; z_{RP} \cdot (\theta_7 + \theta_8 \cos\kappa + \theta_9 \sin\kappa) \right]. \quad (3)$$

Данная модель применяется в центрах обработки международной службы International GNSS Service. Здесь Λ – фактор затмения; d – фактор, зависящий от формы НС, его массы, отражательной и поглощательной способности материалов его поверхности; r_{OS} – расстояние между спутником и Солнцем; x_{RP}, y_{RP}, z_{RP} - координаты НС в ОСК; κ – аргумент широты НС.

Сотрудниками кафедры теоретической и прикладной математики Новосибирского государственного технического университета совместно с коллективом государственной службы времени, частоты и определения параметров вращения Земли (Сибирский государственный научно-исследовательский институт метрологии) ведется разработка программного комплекса SATTELITE_ORBIT, позволяющего строить прогноз траектории движения навигационного спутника на определенный промежуток времени[4].

Разработанный программный продукт реализованв рамках программной системыMatlab.Работа с программным обеспечение начинается с главного меню (см.рис.1):

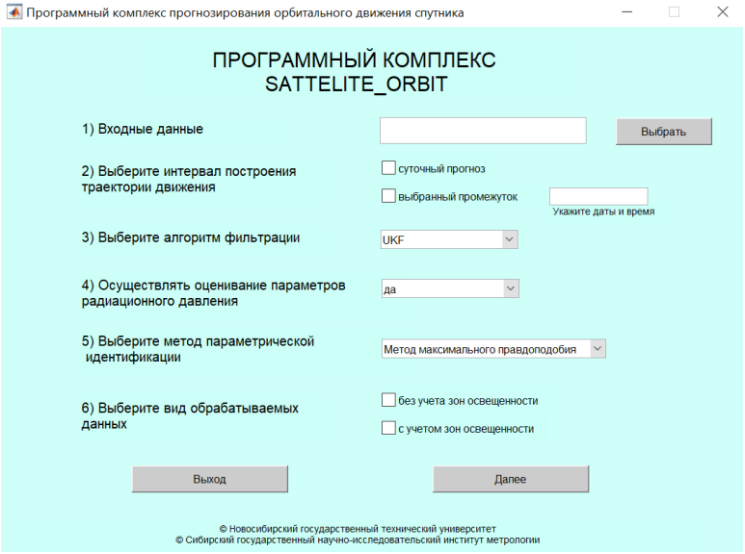


Рис. 1 – Окно 1 графического интерфейса пользователя

На рис. 1 представлено окно 1 графического интерфейса пользователя, которое позволяет выбрать:

1) входной файл, содержащий координаты навигационного спутника (например, в качестве исходных данных могут использоваться срочные эфемериды, представленные в формате *.sp3);
2) интервал построения временной траектории (суточный или выбранный промежуток, который можно задать самостоятельно в предложенном окне);
3) алгоритм фильтрации (сигма-точечныйфильтрКалмана (UKF), квадратно-корневойсигма-точечныйфильтрКалмана (SRUKF) илиадаптивныйсигма-точечныйфильтрКалмана (AUKF));
4) метод параметрического оценивания (метод максимального правдоподобия, рекуррентное оценивание, метод наименьших квадратов), в случаеесли необходимо оценивать параметры РД;
5) вид обрабатываемых данных (с учетом освещенности или без).

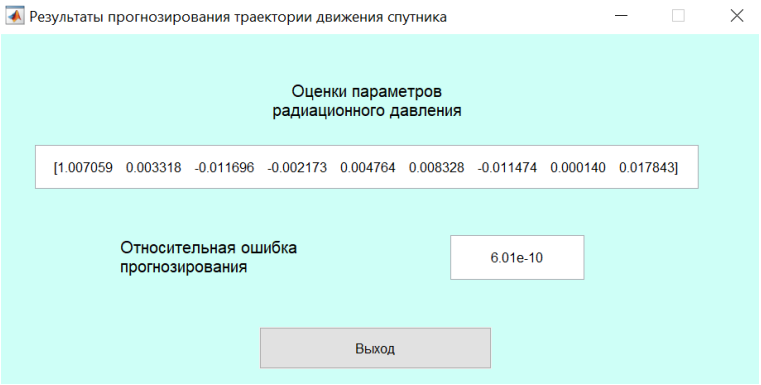


Рис. 2 – Окно 2 графического интерфейса пользователя

На рис. 2 пользователю предоставляется информация о полученныхоценках параметров радиационного давления и относительной ошибке прогнозирования траектории (полученные координаты НС записываются в выходной файл). К тому же имеется возможность увидеть графическую интерпретацию результатов, а также, при возможности, сравнение прогноза с траекторией движения.

Список литературы

1. Дубошин Г.Н. Небесная механика. Методы теории движения искусственных небесных тел / Г.Н.Дубошин– М.: Наука, 1983.–352 с.

2. Бордовицына Т.В. Теория движения искусственных спутников Земли. Аналитические и численные методы : учеб. пособие / Т.В. Бордовицына, В.А.Авдюшев– Томск : Изд-во Том. ун-та, 2007.– 178 с.

3. Kouba J. A Guide to using international GNSS Service (IGS) Products. – Ottawa, 2009. – 34 p.

4. Толстиков А. С. Повышение качества решения задачи эфемеридного обеспечения на основе современных методов параметрической идентификации / А. С. Толстиков, В. М. Чубич, О. С. Черникова // Решетневские чтения : материалы 22 междунар. науч.-практ. конф., посвящ. памяти генер. конструктора ракетно-косм. систем акад. М. Ф. Решетнева, Красноярск, 12–16 нояб. 2018 г.: в 2 ч. – Красноярск, 2018. – Ч. 1. – С. 177–178.

УДК 651.93

Шестакова Анастасия Сергеевна
направление Информационная безопасность автоматизированных систем (магистратура), гр. ИБм-21

Научный руководитель: **Сидоркина Ирина Геннадьевна**
д.т.н., профессор, декан Факультета информатики и вычислительной техники
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

ИССЛЕДОВАНИЕ И СРАВНЕНИЕ МЕТОДОВ СТЕГАНОГРАФИИ НА ОСНОВЕ СИСТЕМНОГО АНАЛИЗА

Исследования и разработки в области стеганографии становятся все более популярными в современном информационном обществе. Стеганография позволяет передавать секретную информацию через открытые каналы, скрывая сам факт ее передачи.

1. Обеспечивающая система (X) – реализация и сравнение методов стеганографии для сокрытия больших объемов данных в изображения графических форматов.

Обеспечение деятельности исследования и сравнения методов стеганографии осуществляется путем реализации следующих задач:

- выявить понятие и классификацию стегосистем;
- обозначить основные направления стеганографии;
- описать стеганографию с точки зрения обеспечивающей, целевой системы и системы в операционном окружении;
- описать стеганографию при помощи модели «гамбургера»;
- описать жизненный цикл для разрабатываемой системы (Рис.1).

2. Целевая система (S). Реализация и сравнение методов стеганографии для сокрытия больших объемов данных в изображения графических форматов. Включает в себя обобщение и систематизирование основных методов и положений цифровой стеганографии, с указанием видов атак на нее.

3. Система в операционном окружении (R).При построении стегосистемы должны учитываться следующие положения:

- противник имеет полное представление о стеганографической системе и деталях ее реализации. Единственной информацией, которая остается неизвестной потенциальному противнику, является ключ, с помощью которого только его держатель может установить факт присутствия и содержание скрытого сообщения;

- если противник каким-то образом узнает о факте существования скрытого сообщения, это не должно позволить ему извлечь подобные сообщения в других данных до тех пор, пока ключ хранится в тайне;

- потенциальный противник должен быть лишен каких-либо технических и иных преимуществ в распознавании или раскрытии содержания тайных сообщений.

Рис.1.Жизненный цикл стегосистемы, описанной с помощью системного анализа.

Система представляет собой единство функции, конструкции и других групп описаний (Рис.2). Модель «гамбургера» описывает иерархию архитектурнойдекомпозиции, т.едля каждой заданной

функции элемента на любом уровне конструктивной иерархии есть возможность иметь альтернативные технические решения.

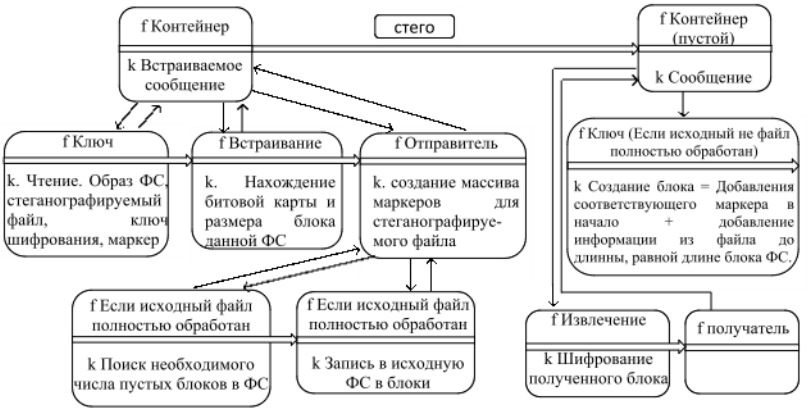


Рис.2. Модель «гамбургера» стегосистемы, описанная с помощью системного анализа.

Список литературы

1. [Электронный ресурс]. - Режим доступа: https://habr.com/ru/post/253045/ (дата обращения: 26.09.2019).

2. Голубев Е.А., Емельянов Г.В. Стеганография как одно из направлений обеспечения информационной безопасности // Технологии информационного общества, Спецвыпуск T-Comm, 2009. - с. 185- 186.

3. Стеганография [Электронный ресурс]. - Режим доступа: https://tplit.wikispaces.com/ (дата обращения: 26.09.2019).

4. ЦВЗ [Электронный ресурс]. - Режим доступа: https://ru.wikipedia.org/wiki/Цифровой водянойзнак. (дата обращения: 26.09.2019).

5. А.Г. Коробейников, С.С. Кувшинов, С.Ю. Блинов, А.В. Лейман, И.М. Кутузов Цифровые водяные знаки в графических файлах // Научнотехнический вестник информационных технологий, механики и оптики, № 1, 2013.- с. 152-157.

6. Оков И.Н., Ковалев Р.М. Электронные водяные знаки как средство аутентификации передаваемых сообщений // Защита информации. Конфидент. 2001. № 3, с.80-85.

7. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография Теория и практика - К: МК-Пресс, 2006. – 288с.

8. Генне О.В. Основные положения стеганографии // Журнал "Защита информации. Конфидент", 2000. - №3.

9. Рябко Б. Я., Фионов А. Н. Основы современной криптографии и стеганографии. - 2-е изд. - М.: Горячая линия - Телеком, 2013. - 232 с.

10. Грибунин В. Г., Костюков В. Е., Мартынов А. П., Николаев Д. Б., Фомченко В. Н. «Стеганографические системы. Критерии и методическое

обеспечение»: Учебн.-метод. пособие / Под ред. д-ра техн. наук В. Г. Грибунина. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2016. - 324 с.

УДК 004.422

Яровиков Константин Владимирович
направление Информатика и вычислительная техника (магистратура),
гр. ИВТм– 21

Научный руководитель: **Савинов Александр Николаевич**
К.т.н., доцент каф.ИВС
ФГБОУ ВО «Поволжский государственный технологический университет», г. Йошкар-Ола

СИСТЕМА ШИФРОВАНИЯ МОБИЛЬНОГО ГОЛОСОВОГО ТРАФИКА

Аннотация. Рассматривается актуальность и проблемы мобильной связи с точки зрения информационной безопасности. Разрабатывается система шифрования и дешифрования голосового трафика по средствам мобильных сетей с использованиемалгоритма шифрования «в реальном времени» и передача зашифрованной информации без помощи сторонних сервисов и сети интернет.

Ключевые слова:
мобильная связь, система шифрования

Безопасность информации – одна из первостепенных задач в современном мире. Защита конфиденциальных данных, коммерческой тайны и другой информации для узкого круга лиц от шпионажа или корыстных действий злоумышленников является одним из главных вопросов любой организации. И если обеспечением сохранности данных внутри самой организации занимаются специалисты по информационной безопасности, то с мобильными устройствами дела обстоят сложнее. Особенно уязвимы телефонные переговоры с личных устройств.

В настоящее время используется, как минимум, 3 способа взлома для прослушивания телефона: установка вредоносного программного обеспечения, взлом на уровне оператора и дистанционное прослушивание. При первом способе пользователь сам способен обеспечить должный уровень безопасности, а в остальных – от абонента ничего не зависит.

Взлом на уровне оператора происходит или через подключение к сигнальной сети SS7 и злоумышленник может просто подключиться к

разговору по принципу конференц-связи или взлом фемтосоты оператора для перехвата разговора (более дорогой в реализации вариант – установка своей фемтосоты, имитирующей фемтосоту оператора).

Дистанционное прослушивание с развитием информационных технологий становится одним из самых дешевых, малозаметных и несложных способов. В сети GSM существует защита голосового трафика 64-битным шифрованием A5, но, фактически, шифрование 54-битное (первые 10 бит всегда нулевые), однако, в 2010 году был показан метод взлома с помощью радужных таблиц (мобильные операторы используют A5 шифрование до сих пор). То есть, для перехвата и расшифровки любой информации потребуется мощный ноутбук со специальным ПО, 1,7 ГБ радужных таблиц и модернизированный мобильный телефон.

В связи с тем, что существующее шифрование GSM было скомпрометировано и безопасность телефонных переговоров под большим вопросом, на рынке появляются новые способы защиты: от «криптофонов» до специального ПО. В большинстве случаев, мобильный телефон – это не только средство связи, но и необходимое в повседневной жизни устройство, поэтому «криптофоны» не имеют такого распространения, как смартфоны. А для защиты смартфона необходимо специализированное ПО, способное обеспечить тайну переговоров.

Программные продукты, существующие на рынке хоть и обеспечивают необходимую защиту, но способны работать только через сеть интернет (Wi-Fi, 3G/4G), что не всегда возможно использовать. К тому же ряд продуктов получает данные о местоположении абонента, что, для обеспечения конфиденциальности переговоров, излишне.

Для универсальности использования и улучшения уровня защиты указанных выше продуктов, необходимо отказаться от использования определения местоположения, сети интернет, привязки к SIM-карте и двухфакторной авторизации (клонирование SIM-карты и перехват SMS также могут использоваться при хакерских атаках).

В связи с вышесказанным актуальным является разработка системы шифрования и дешифрования голосового трафика по средствам мобильных сетей.

В настоящий момент ведётся разработка системы сохранения конфиденциальности переговоров, которая включает в себя:

1. Алгоритм шифрования AES с 256-битным ключом. На сегодняшний день не существует никакой реальной атаки на AES;

2. Процедуру генерации открытого и закрытого ключей, связанную с IMEI мобильного аппарата и номера телефона владельца;

3. Алгоритм приема и передачи зашифрованных сообщений;

4. Пользовательский интерфейс для ОС Android, который позволяет пользователю выбирать режимы «конфиденциально» или «открытая связь».

Разрабатываемая система дает необходимую защиту при телефонном разговоре и является стойкой ко взлому при дистанционном прослушивании. Разработанный метод шифрования является адекватным и способен работать в реальном времени независимо от сторонних факторов.

Список литературы

1.Бабаш А. В. «Криптографические методы защиты информации: учебник для вузов» - М : КноРус, 2016.

2. Баричев С. Г., Гончаров В. В., Серов Р. Е. «Основы современной криптографии» 3-е изд. - М.: Диалог-МИФИ, 2011.

3. Гаранин М.В., Журавлев В.И., Кунегин С.В. «Системы и сети передачи информации: Учеб. пособие для вузов» - М.: Радио и связь, 2001.

4. Данилов В. И. «Сети и стандарты мобильной связи: учебное пособие» - СПбГУТ, 2015.

5. Darwin I.F. «Android Cookbook» - O'Reilly, 2011.

6. https://msdn.microsoft.com

СОДЕРЖАНИЕ

Научное издание

ИНЖЕНЕРНЫЕ КАДРЫ – БУДУЩЕЕ ИННОВАЦИОННОЙ ЭКОНОМИКИ РОССИИ

Материалы V Всероссийской
студенческой конференции

Йошкар-Ола, 5-8 ноября 2019 г.

Часть 4

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ – ОСНОВА СТРАТЕГИЧЕСКОГО ПРОРЫВА В СОВРЕМЕННОЙ ПРОМЫШЛЕННОСТИ

Излагается в авторской редакции
Техническая подготовка материалов *А.Н. Савинов*

Материалы конференции опубликованы за счет средств гранта Всероссийского конкурса молодежных проектов среди образовательных организаций высшего образования, проводимого Федеральным агентством по делам молодежи (Росмолодежь)

Подписано в печать 02.12.2019. Формат 60×84 $^{1}/_{16}$.
Бумага офсетная. Печать офсетная.
Усл. печ. л. 7,3. Тираж 110 экз. Заказ № 6102.

Поволжский государственный технологический университет
424000 Йошкар-Ола, пл. Ленина, 3

Отпечатано в типографии ООО «Вертола»
424030 Республика Марий Эл, г. Йошкар-Ола, ул. Мира, 21