Федеральное государственное бюджетное образовательное учреждение
высшего образования «Московский государственный технический университет
им. Н. Э. Баумана (национальный иследовательский университет)»
Федеральное государственное бюджетное образовательное учреждение
высшего образования «Калужский филиал МГТУ имени Н. Э. Баумана
(национальный иследовательский университет)»

НАУКОЕМКИЕ ТЕХНОЛОГИИ В ПРИБОРО - И МАШИНОСТРОЕНИИ И РАЗВИТИЕ ИННОВАЦИОННОЙ ДЕЯТЕЛЬНОСТИ В ВУЗЕ

Материалы
Всероссийской научно-технической конференции

Том 3

ИЗДАТЕЛЬСТВО МГТУ им. Н. Э. Баумана
Калуга 2016

УДК 378:001.891
ББК 74.58:72
Н34

Н34 **Наукоемкие** технологии в приборо- и машиностроении и развитие инновационной деятельности в вузе: материалы Всероссийской научно-технической конференции, 15 – 17 ноября 2016 г. Т. 3. – Калуга: Издательство МГТУ им. Н. Э. Баумана, 2016. – 256 с.

В сборнике материалов Всероссийской научно-технической конференции представлены результаты научных исследований, выполненных учеными в течение ряда лет. Систематизированы материалы различных научных школ. Результатами научных исследований являются новые методы, вносящие вклад в развитие теории, а также прикладные задачи, воплощенные в конструкции и материалы.

УДК 378:001.891
ББК 74.58:72

СЕКЦИЯ 12.

СОВРЕМЕННЫЕ ТЕХНОЛОГИЧЕСКИЕ ПРОЦЕССЫ И МЕТОДЫ КОНТРОЛЯ В ЭЛЕКТРОНИКЕ И МИКРОЭЛЕКТРОНИКЕ

В.В. Андреев, И.А. Рытиков

АВТОМАТИЗИРОВАННАЯ УСТАНОВКА КОНТРОЛЯ ЭЛЕКТРИЧЕСКИХ ПАРАМЕТРОВ МИКРОСХЕМ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Данная работа посвящена разработке автоматизированной установки контроля электрических параметров микросхем на основе стенда NI PXI EXPRESS, который управляется при помощи заданного алгоритма, написанного в среде LabVIEW.

Создание испытательных режимов и проведение измерения электрических параметров микросхем осуществляется с использованием модулей NI PXI-4132 и NI PXI-4110. Модуль NI PXI-4132 представляет собой высокоточный измеритель/источник питания. Внешний вид модуля NI PXI-4132 показан на рис. 1. Основные параметры NI PXI-4132 приведены в таблице 1 и показаны на рис. 2.

Рис.1. Внешний вид высокоточного измерителя/источника питания NI PXI-4132

Таблица 1. Основные параметры модуля NI PXI-4132 (диапазоны источника и измерителя)

DC Диапазоны напряжения (CAT I)	DC Токи источника и измерителя
±10 В ±100 В	10 мкА 100 мкА 1 мА 10 мА 100 мА

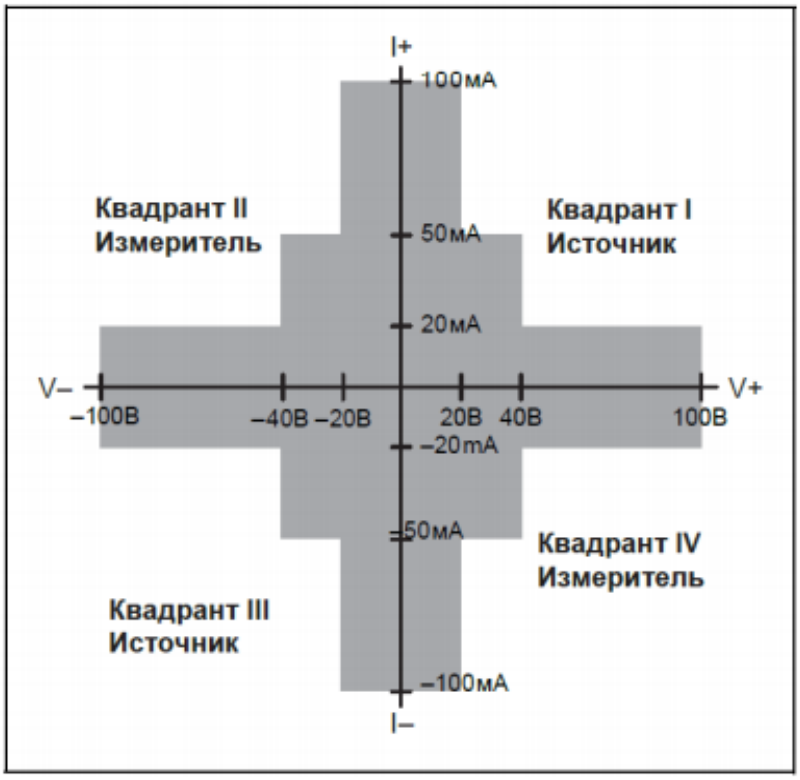


Рис. 2. NI PXI-4132 Секторная диаграмма характеристик

На рис. 3 представлена схема измерения напряжения микросхемы при заданном значении постоянного тока с использованием модуля NI PXI EXPRESS – 4132, выполненной в программе LabVIEW.

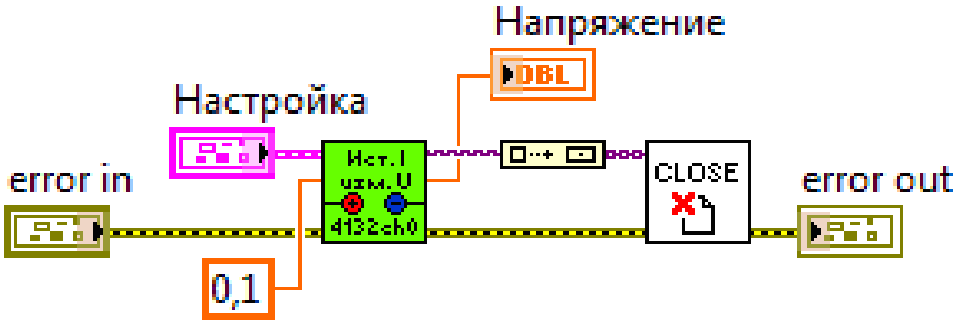


Рис. 3. Схема измерения напряжения при заданном значении постоянного тока, реализованная с использованием модуля NI PXI EXPRESS – 4132

Модуль NI PXI-4110 представляет собой трехканальный программируемый источник питания постоянного тока. Внешний вид модуля NI PXI-4110 показан на рис. 4. Основные параметры NI PXI-4132 приведены в таблице 2.

Рис.4. Внешний вид высокоточного измерителя/источника питания NI PXI-4110

Таблица 2. Основные параметры модуля NI PXI-4110

Канал	Диапазон напряжения (постоянный ток)	Развязка*	Диапазон силы тока (вход/выход)			
			Внешний блок питания		Источник питания	
			Диапазон 20 мА	Диапазон 1А	Диапазон 20 мА	Диапазон 1 А
Канал 0	От 0 В до +6 В	нет	нет	1 А (6 Вт)	нет	1 А (6 Вт)
Канал 1	От 0 В до +20 В	60 В постоянного тока, CAT I	20 мА	1 А (20 Вт)	20 мА	100 мА†
Канал 2	От 0 В до -20 В	60 В постоянного тока, CAT I	20 мА	1 А (20 Вт)	20 мА	100 мА†
* Каналы 1 и 2 изолированы, но не друг от друга † Выходная мощность каналов 1 и 2 не должна превышать 3 Вт в сумме						

На рис. 5 представлена схема измерения напряжения при заданном значении постоянного тока, реализованная с использованием модуля NI PXI EXPRESS – 4110, выполненной в программе LabVIEW.

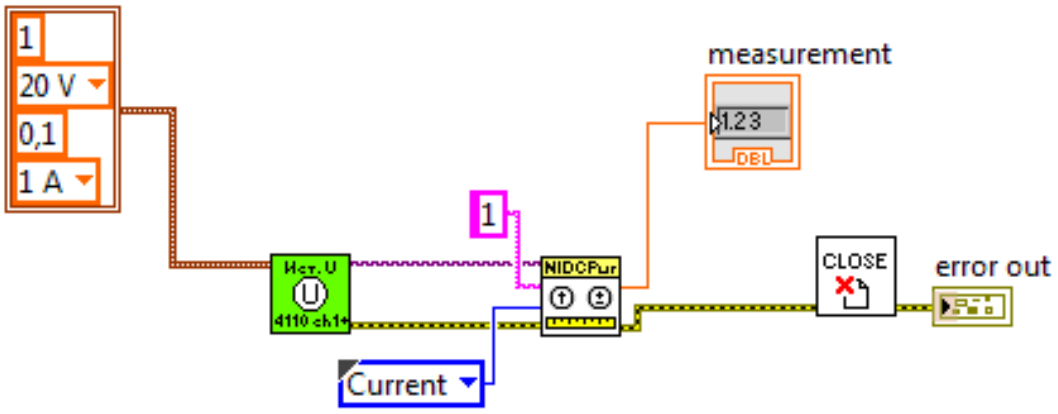


Рис. 5. Схема измерения напряжения при заданном значении постоянного тока, реализованная с использованием модуля NI PXI EXPRESS – 4110

Таким образом, была разработана автоматизированная установка для контроля электрических параметров микросхем на основе стенда NI PXI EXPRESS, которая управляется при помощи заданного алгоритма, написанного в среде LabVIEW.

ЛИТЕРАТУРА

[1] Андреев В.В., Барышев В.Г., Столяров А.А. Инжекционные методы исследования и контроля структур металл-диэлектрик-полупроводник: Монография. // М.: Издательство МГТУ им. Н.Э. Баумана, 2004. – 256 с.

[2] Andreev V.V., Bondarenko G.G., Maslovsky V.M., Stolyarov A.A. Multilevel current stress technique for investigation thin oxide layers of MOS structures // IOP Conf. Series: Materials Science and Engineering. 41 (2012) 012017.

[3] National Instruments. – LabVIEW. Издание октябрь 2009. - 432с.

Андреев Владимир Викторович – д-р техн. наук, профессор КФ МГТУ им. Н.Э. Баумана. E-mail: andreev@bmstu-kaluga.ru

Рытиков Илья Алексеевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: doktorwww@gmail.com

В.Е. Драч, П.А. Максимов

ГЕНЕРАТОР ШУМА

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Тенденция развития современных технологий характеризуется постоянным повышением значения информации. Учитывая стоимость информации в наши дни, технологии и способы её защиты будут постоянно развиваться. Одним из самых действенных способов защиты информации от утечки из линии связи является использование генераторов шума. Такие генераторы позволяют защитить от утечки работающие радиоэлектронные устройства: телефоны, компьютеры и т.д. и способны подавить любой информационный сигнал, который попадает в сферу их действия [3].

В настоящее время для передачи информации используют в основном КВ, УКВ, радиорелейные, тропосферные и космические каналы связи, а также кабельные и волоконно-оптические линии связи [1].

Цель работы - произвести моделирование генератора шума, в котором в качестве источника шума используется стабилитрон.

Генератор шума создаёт спектр помех в заданном диапазоне частот и далее, во время передачи информации, этот спектр подается в линию. Требуется подобрать такую частоту маскирующего сигнала, чтобы после прохождения усилителя его уровень был достаточным для подавления полезного сигнала, но при этом не ухудшал качество связи. После зашумления на выходе получаем смешанный сигнал.

Существуют разные варианты генерации шумового сигнала. Например, его можно сгенерировать на микропроцессоре, разделив звуковой диапазон и смешав сигналы с определенной дискретностью, но самым простым вариантом является использование в качестве источника шума резистора или стабилитрона [2]. Генератор шума на стабилитроне состоит из параметрического стабилизатора. Шум снимается со стабилитрона и передается на операционный усилитель с определенной частотой среза. Выделенный таким образом белый шум далее передается на УЗЧ.

В качестве основного инструмента для моделирования в данной работе используется NI MustiSim 10.1 т.к. он обладает следующими преимуществами: большое количество моделей электронных устройств и более 2000 компонентов мировых производителей, интуитивно понятный интерфейс, кроме традиционного анализа SPICE, Multisim позволят пользователям подключать к схеме виртуальные приборы, высокая точность и глубина анализа.

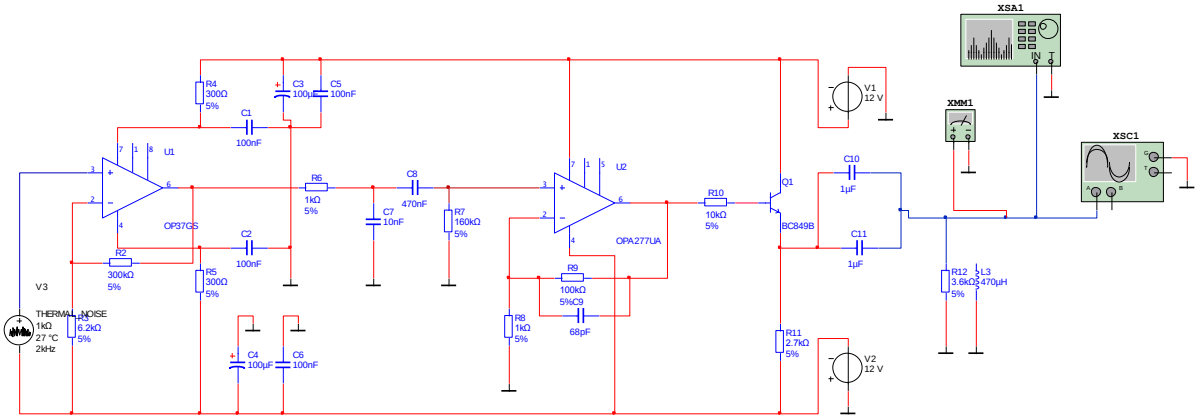


Рис.1 Схема электрическая принципиальная

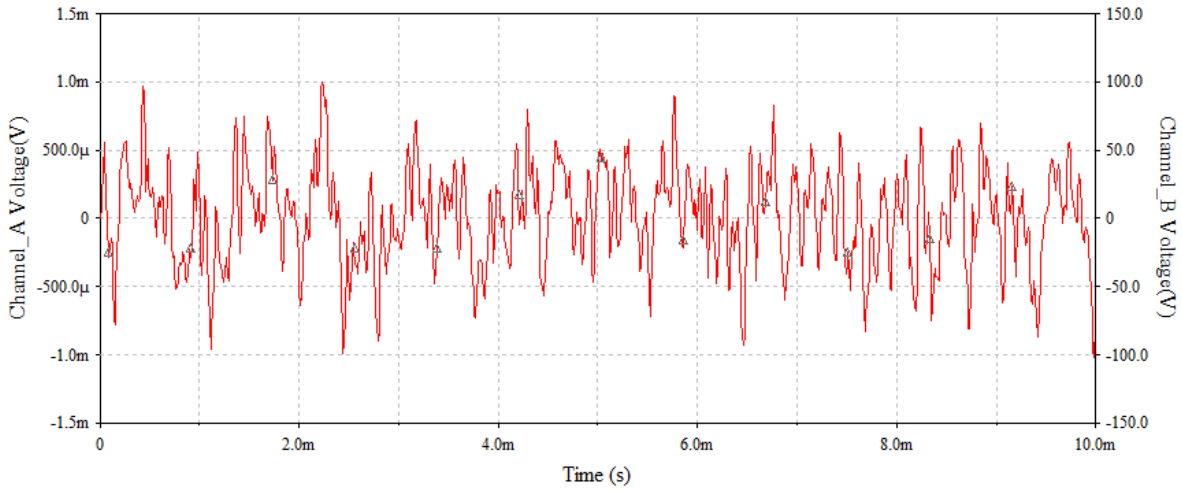


Рис.2 Результат моделирования

Усиление отдельных гармоник в спектре шумового сигнала может привести к утечке информации, т.к. такие гармоники представляют собой несущие частоты с модулированным наложением полезного сигнала. Для того, чтобы убедится, что в нашем сигнале отсутствуют отдельно усиленные гармоники, был проведен спектральный анализ при помощи виртуального прибора Spectrum Analyzer.

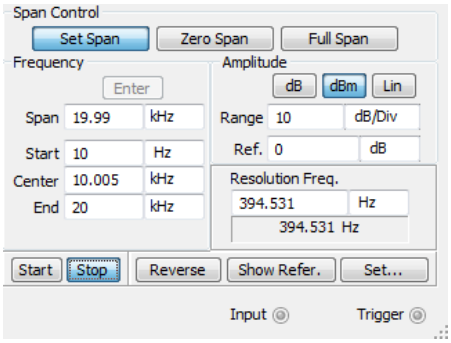


Рис. 3 Окно настроек *Spectrum Analyzer* с заданными параметрами

Чтобы убедиться в равномерности спектрального состава в широкой полосе за рабочим диапазоном 20Гц-10кГц, в настройках анализатора был задан диапазон от 10Гц до 20Кгц.

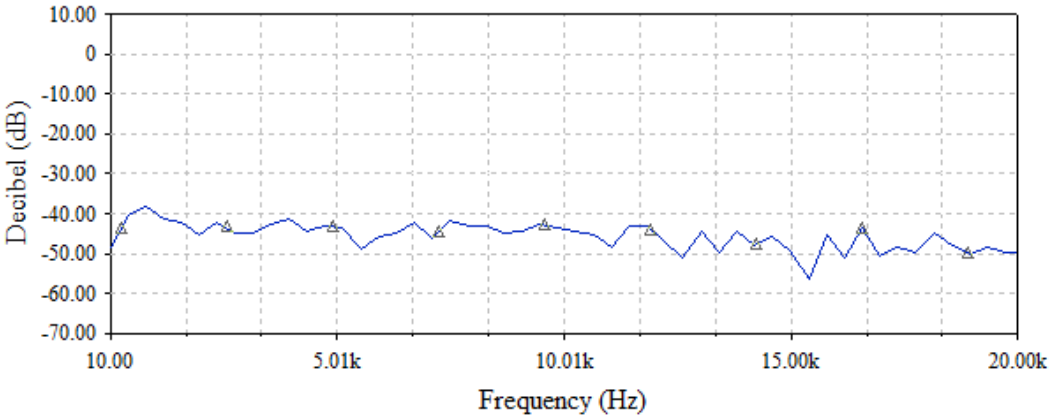


Рис.3 Результаты спектрального анализа

В результате проделанной работы была создана виртуальная схема генератора шума в симуляторе MultiSim 10.1, успешно промоделирована и в итоге получена временная диаграмма выходного сигнала, а также был получен спектр шумового сигнала, из которого видно, что ярко выраженные гармоники отсутствуют и представленный генератор шума сможет обеспечить защиту информации от утечек.

Литература

[1] Кирьянов. Б.Ф. К проблеме защиты информации в каналах связи // Современные проблемы науки и образования –2012. – №6. – С.24

[2] Зеленский А.В. Основы конструирования электронных средств. Учеб. пособие Ч.2. - Самара: гос.аэрокосм. ун-та,2008. - 76 с.

[3] Тетерич Н. М. Генераторы шума и измерение шумовых характеристик. Библиотека по радиоэлектронике, вып. 12. - М.: Энергия, 2009. - 154 с.

Драч Владимир Евгеньевич – канд. техн. наук, доцент кафедры "Конструирование и производство электронной аппаратуры" КФ МГТУ им. Н.Э. Баумана. E-mail: drach@kaluga.org

Максимов Павел Андреевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: failbt@yandex.ru

С.А. Лоскутов, Д.В. Хачев

ЗАВИСИМОСТЬ ЕМКОСТИ КЕРАМИЧЕСКИХ ЧИП-КОНДЕНСАТОРОВ ОТ ПРИЛОЖЕННОГО НАПРЯЖЕНИЯ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Многослойные керамические чип-конденсаторы (MLCC) представляют собой наиболее быстро растущий рынок по сравнению с остальными типами конденсаторов. MLCC используются во всех областях электроники: потребительской, автомобильной, военной, медицинской, промышленной и др. Каждое приложение предъявляет свои требования к компонентам. Только зная все особенности применения, хранения и монтажа, можно сделать правильный и обоснованный выбор конденсатора.

Многослойные керамические чип-конденсаторы играют решающую роль в технологии поверхностного монтажа с момента их появления. Они имеют ценные особенности, которые обеспечивают их широкое распространение [1]. Среди таких особенностей можно отметить: высокую удельную емкость, широкий диапазон номинальных емкостей, широкий диапазон рабочих напряжений, стандартный набор типоразмеров.

Цель данной работы – произвести исследования зависимости емкости керамических чип-конденсаторов от приложенного напряжения.

Большое влияние на параметры конденсаторов оказывают множество факторов. Одним из основных является тип используемого диэлектрика. В MLCC используются неорганические твердые диэлектрики [3,4]. По типу используемого диэлектрика керамические конденсаторы можно поделить на два класса:

Класс 1 (Class 1) – конденсаторы с высокостабильным диэлектриком, имеющим высокую добротность, линейную температурную зависимость (диэлектрическая проницаемость ε_r меняется от 6 до 550). Примером таких конденсаторов являются NPO. Они применяются во времязадающих цепях и фильтрах, где основными требованиями являются низкие потери, высокая стабильность емкости и других параметров.

Класс 2 (Class 2) – конденсаторы с более высоким уровнем потерь и нелинейной зависимостью ε_r. Примером могут быть X7R, X5R и Y5V MLCC. Они используются как разделительные и блокировочные конденсаторы.

Чип-конденсаторы 2 класса используют в качестве диэлектрика $BaTiO_3$, который является ферромагнетиком и имеет доменную структуру. Внутри домена все электрические диполи полярного диэлектрика сориентированы одинаково. Но направления поляризации соседних доменов могут отличаться. При приложении внешнего напряжения происходит ориен-

тация доменов по приложенному полю. В результате диэлектрическая проницаемость изменяется. Однако зависимость является нелинейной (рис.1). Для конденсаторов 1 класса эффект смещения при постоянном токе практически полностью отсутствует.

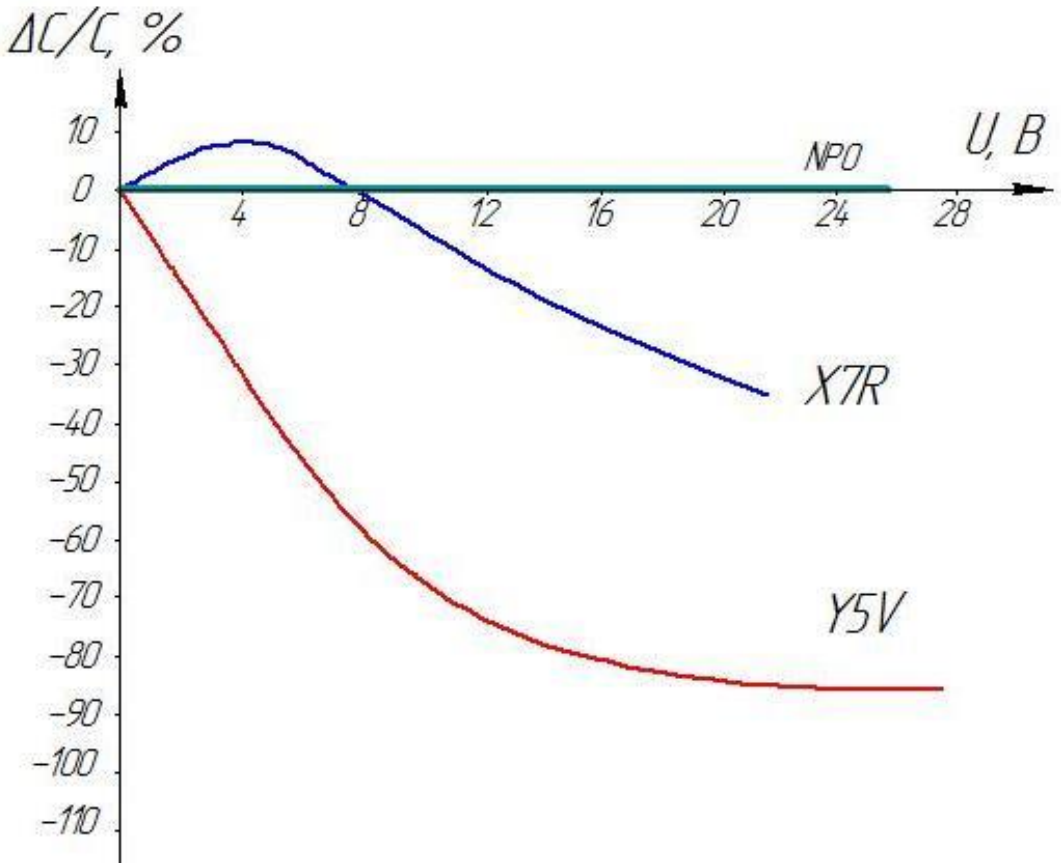


Рис.1. Зависимость емкости конденсаторов фирмы YAGEO (NPO, X7R, Y5V) от приложенного напряжения

Работа чип-конденсатора в рамках рабочих диапазонов напряжений и температур является обязательным условием долгой жизни конденсатора. При несоблюдении этого условия конденсатор может выходить из строя, например, при пробое.

В процессе работы стоит задача исследовать зависимость ёмкости некоторых типов керамических чип-конденсаторов от приложенного напряжения. Чтобы более точно определить характер этой зависимости, потребуется собрать простейший стенд (рис.2), где будет измеряться ёмкость двух последовательно включённых конденсаторов: Cx - исследуемого и Co - вспомогательного.

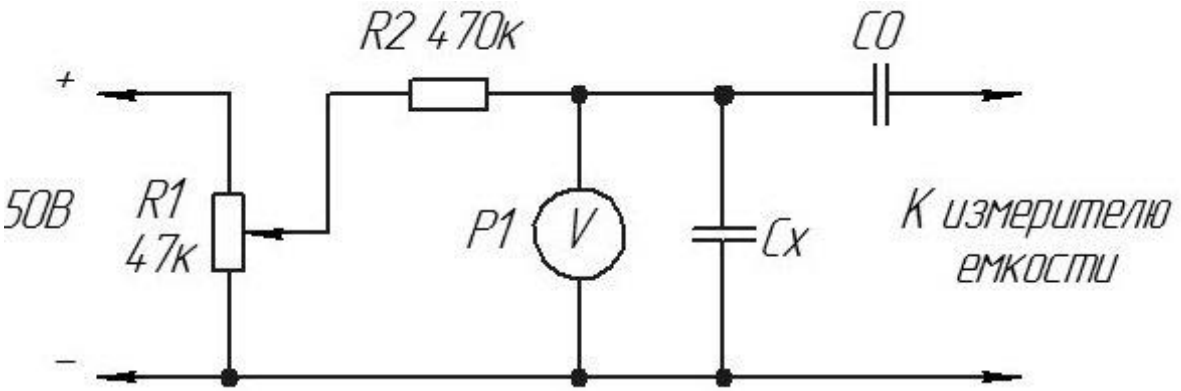


Рис.2.Схема электрическая принципиальная стенда

Таким образом было проверено несколько импортных керамических конденсаторов – Yageo NPO, X7R и Y5V различной ёмкости с разными группами ТКЕ. Результат оказался неожиданным. Ёмкость некоторых конденсаторов при увеличении напряжения от 0 до 30 В уменьшалась в 2-2,5 раза. При напряжении 10 В их ёмкость уже составляла лишь 30...35 % от номинала. Подобное можно объяснить только очень низким качеством применённого диэлектрика. Конечно, далеко не все импортные конденсаторы имеют такие параметры, но проведённый эксперимент говорит о том, что нужно быть готовым к любым сюрпризам, преподносимым нам иностранными производителями.

Литература

[1] MLCC Application Manual. YAGEO 2005 http://www.compel.ru/wordpress/wp-content/uploads/2014/01/MLCC-Application-Manual.-YAGEO-2005.pdf

[2] Петров К.С. Радиоматериалы, радиокомпоненты и электроника. – Спб.: Питер, 2003. – с.432-445.

[3] Surface-Mount Ceramic Multilayer Capacitors. Introduction. V.11. Yageo 2010 http://www.yageo.com/exep/pages/download/literatures/UPY-C_INT_11.pdf

[4] Safety Datasheet. No.R-11-525-001. Yageo, 2013 http://www.compel.ru/wordpress/wp-content/uploads/2014/01/SAFETY-DATA-SHEET.-No.R-11-525-001.-YAGEO-2013.pdf

[5] Казарновский Д.М. Сегнетокерамические конденсаторы. – М.: ГосЭнергоИздат, 2006. – с.185-192.

Лоскутов Сергей Александрович – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: SergeL-75@yandex.ru

Хачев Дмитрий Валерьевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: khachev@yandex.ru

А.В. Иванов, В.В. Кузнецов

МОДЕЛИРОВАНИЕ ВОЗДЕЙСТВИЯ ЭСР НА КМОП ИМС

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

При разработке аппаратуры, работающей в заданной электромагнитной обстановке трудно оценить поведение элементной базы и устройств в целом при воздействии дестабилизирующих факторов. Для этого нужно проводить натурные испытания опытных образцов. Но экономически намного целесообразней проводить моделирование таких воздействий, как ЭСР, и уже на этапе проектирования аппаратуры вводить необходимые внешние средства защиты. Применяемые внешние меры защиты интегральных схем (ИС) от ЭСР полностью не исключают возможности повреждения схем. Поэтому при обязательном применении мер внешней (коллективной) защиты, основным средством защиты ИС от ЭСР является встроенная защита, то есть применение защитных схем, выполненных на кристалле ИС в едином технологическом процессе. В КМОП-микросхемах, наиболее подверженных действию ЭСР, применяются встроенные диодные элементы защиты или элементы защиты из МОП- транзисторов.

Основные элементы защиты от ЭСР. Основными элементами защиты от ЭСР являются следующие [1]:

1. n-МОП транзистор с толстым подзатворным окислом (Thick Field Oxide, TFO);
2. n-МОП транзистор с заземлённым затвором (Grounded Gate NMOS Transistor, GGNMOST);
3. кремниевый управляемый диод (Silicon-Controlled Rectifier, SCR);
4. устройство, основанное на эффекте смыкания областей пространственного заряда (Punchthrough-Induced Protection Element, PIPE);
5. диод Зенера (Zener diode).

GGNMOST представляет собой обычный n-МОП транзистор с тонким подзатворным окислом. Исток и затвор подключены к земле. Принцип действия такого элемента был объяснён в предыдущем случае, главное отличие от элемента TFO заключается только в толщине подзатворного диэлектрика. Можно лишь ещё раз подчеркнуть, что для правильной работы устройства и для обеспечения пропорциональности тока по ширине транзистора необходимо обеспечить $V_{t2} > V_{t1}$. Существуют определенные схемотехнические решения для достижения этих целей [2].

Рассмотрим моделирование одного из базовых встроенных элементов защиты МОП-транзисторе: n-МОП транзистор с заземлённым затвором (Grounded Gate NMOS Transistor, GGNMOST). Модель этого элемента защиты, включенная в модели некоторых микросхем, позволит проводить виртуальные эксперименты по воздействию ЭСР на элементную базу и на аппаратуру, в которой она применяется. На рис. 1 показана структура этого элемента [3].

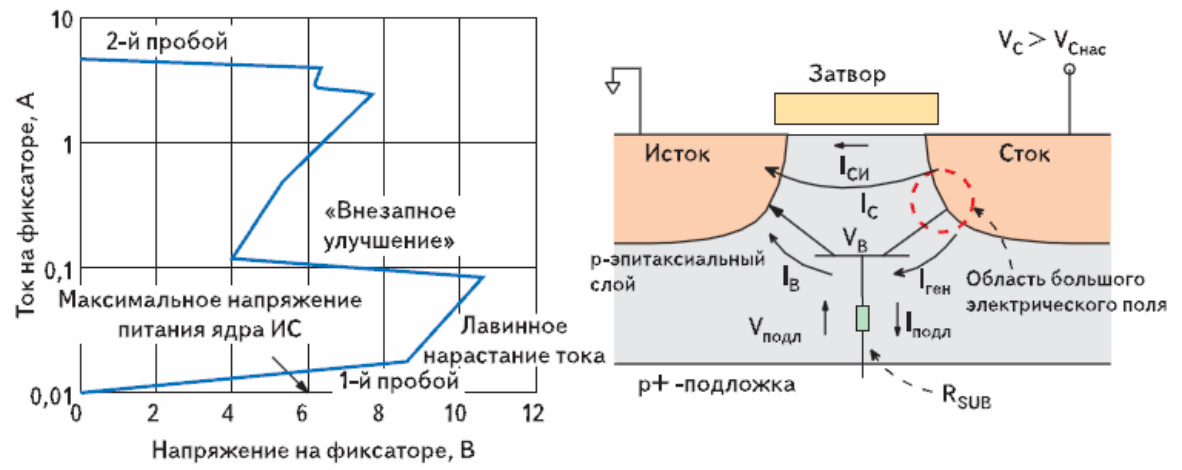


Рис. 1. Латеральный биполярный n-p-n-транзистор в составе элемента GGNMOST и его ВАХ (слева)

Одним из важных аспектов работы n-МОП-транзистора во время ЭСР является время его включения. Оно определяется временем пролета базы t_{be} паразитного биполярного транзистора. При длине канала менее 1 мкм время включения биполярного транзистора составляет менее 250 пс, в то время как время роста ЭСР-стресса по модели HBM и по модели MM составляет более 1 нс. В этом случае время включения паразитного биполярного транзистора можно не принимать во внимание. Паразитный биполярный транзистор может не включится при воздействии электростатического разряда по модели CDM, время роста импульса которого может быть меньше 250 пс.

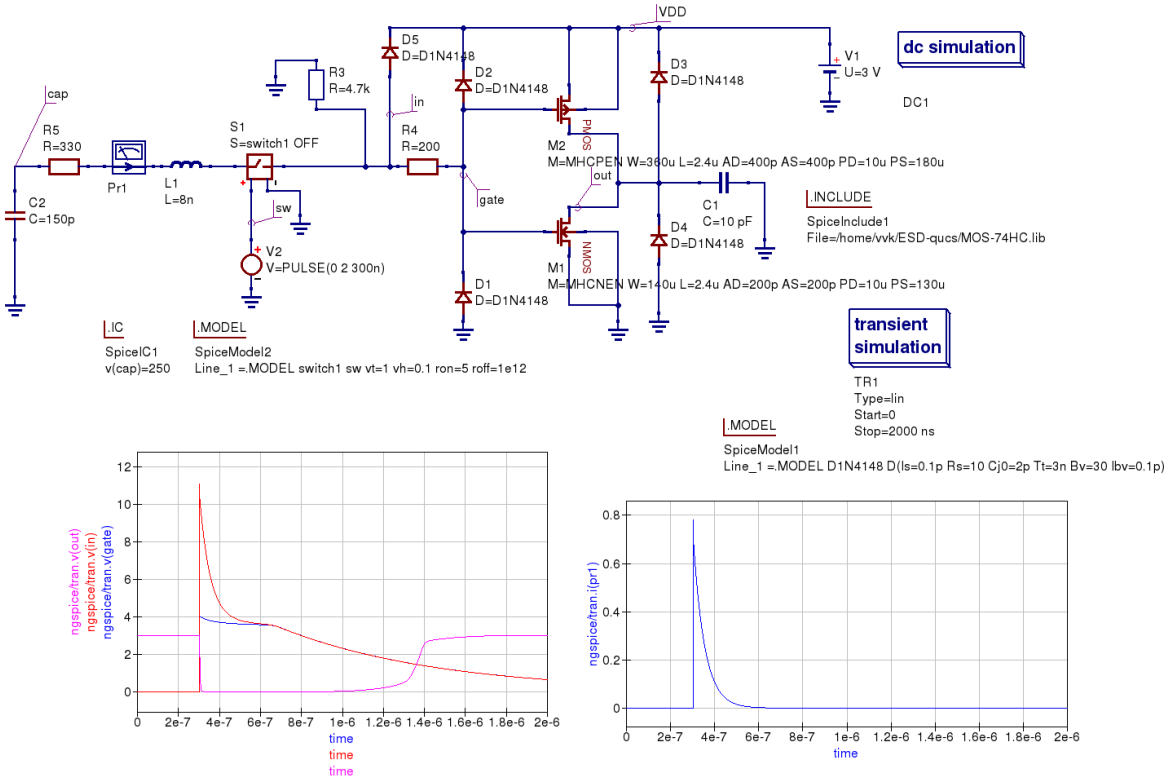


Рис. 2. Моделирование воздействия на КМОП инверетер импульса статического разряда

В настоящее время проводится такое моделирование, которое позволит выявить устойчивость ИМС к ЭСР.

Литература:

[1] Sanjay Dabral, Timothy Maloney. BASIC ESD AND I/O DESIGN. Intel Corporation.

[2] Julian Zhiliang Chen, Ajith Amerasekera, Charvaka Duvvury. Design and Optimization of Gate-Driven NMOS ESD Protection Circuits in Submicron CMOS Processes. IEEE Trans. Electron Devices. Dec. 1998. Vol. 45. P. 2448.

[3] Горлов М., Строгонов А., Адамян А. Воздействие электростатических разрядов на интегральные схемы. − Компоненты и технологии. − 2008. − № 3. − С. 188−192.

Иванов Андрей Витальевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: andrei4600@yandex.ru

Кузнецов Вадим Вадимович – канд. техн. наук, доцент кафедры "Конструирование и производство электронной аппаратуры" КФ МГТУ им. Н.Э. Баумана. E-mail: ra3xdh@gmail.com

С.В. Рыжов, В.В. Андреев

МОДЕЛИРОВАНИЕ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА ИЗГОТОВЛЕНИЯ N-P-N ТРАНЗИСТОРА В СИСТЕМЕ SENTAURUS TCAD

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В данной работе, с использованием модуля Sentausus Process, была получена двумерная модель вертикального n-p-n транзистора микросхемы 1401СА1.

Использование современных программных продуктов при проектировании интегральных микросхем позволяет в значительной мере повысить качество разработки за счет меньшего числа ошибок, корректировок на начальной стадии проекта, ускорить процесс научных исследований и этапа разработки и, за счет этого, снизить финансовые и временные потери.

Одним из наиболее мощных программных продуктов, предназначенных для моделирования технологических процессов является Sentaurus TCAD фирмы Synopsys [1]. Он объединяет лучшие свойства инструментов проектирования от компаний Synopsys и ISE TCAD, Sentaurus позволяет пользователям решать широкий спектр задач: от создания глубоко субмикронной логики, памяти и цифро-аналоговых приборов до сенсоров, оптоэлектроники и высокочастотной техники [2].

SProcess - программа моделирования таких технологических операций как диффузия, ионная имплантация, эпитаксия и т.д. с учетом всех известных физических эффектов и точных моделей физических процессов. Входные данные о порядке и характеристики технологических процессов формируются или в программе Ligament или в виде текстового командного файла [3]. В результате работы Sentaurus Process получаем структуру микроэлектронного устройства.

В данной работе решалась задача моделирования n-p-n транзистора в SProcess. Описание технологии изготовления транзистора было произведено в текстовом командном файле.

Ниже приводятся наиболее используемые команды.

Задание начальной двумерной сетки

В Sprocess ось X направлена вниз, ось Y- слева направо.

Пример задания сетки:

line x loc= 10.0<um> tag=SubBottom

line y loc= 0.0<um> tag=SubLeft

Задание области моделирования

Определяем область моделирования по осям X Y, через теги, заданные при создании сетки.

Пример:

region Silicon xlo=SubTop xhi=SubBottom ylo=SubLeft yhi=SubRight

init concentration=1e+15<cm-3> field=Boron

Здесь используется пластина p-типа с конентрацией Бора 10^{15}

Нанесение фоторезиста

Для создания на поверхности полупропроводниковой пластины слоя фоторезиста необходимо создать маску.

mask name=Base segments= {-1 2 15 40} negative

В данном случае будет создана инвертированная маска, предотвращающее травление от 2 до 15 мкм.

Создаем слой фоторезиста следующей командой:

photo mask=Base thickness=1

Ионная имплантация

Определяем дозу и энергию имплантации

Пример:

implant Boron dose=1e14<cm-2> energy=50<keV>

В данном случае осуществляется имплантация Бором доза 10^{14}, энергия 50 кэВ.

Диффузия

Определяем температуру и время диффузии

Пример:

diffuse temp=1100<C> time=20<min> maxstep=4<min>

Результатом моделирования является получение структуры в транзисторе формате *.trd после формирования областей коллектора (Рис. 1) базы (Рис. 2), эмитера (Рис. 3) и контактных площадок (Рис. 4)

Данные структуры построены при помощи Tecplot.

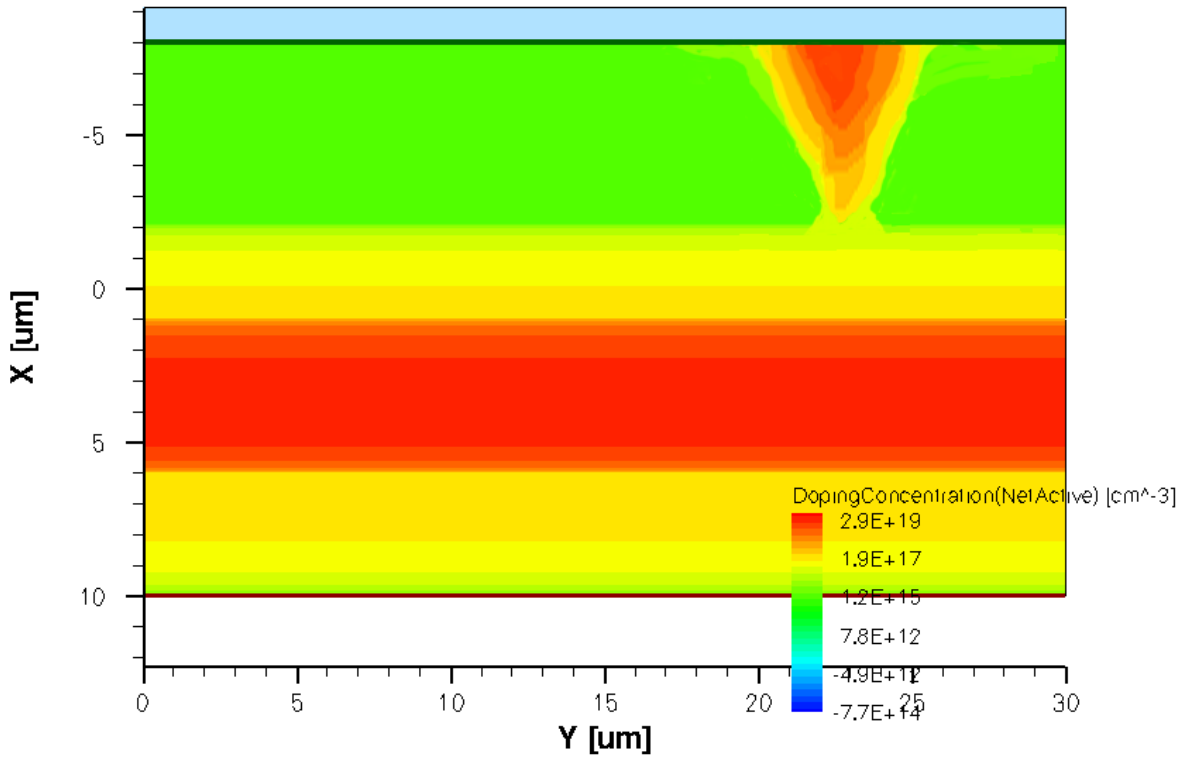


Рис. 1. Структурой транзистора после формирования областей коллектора

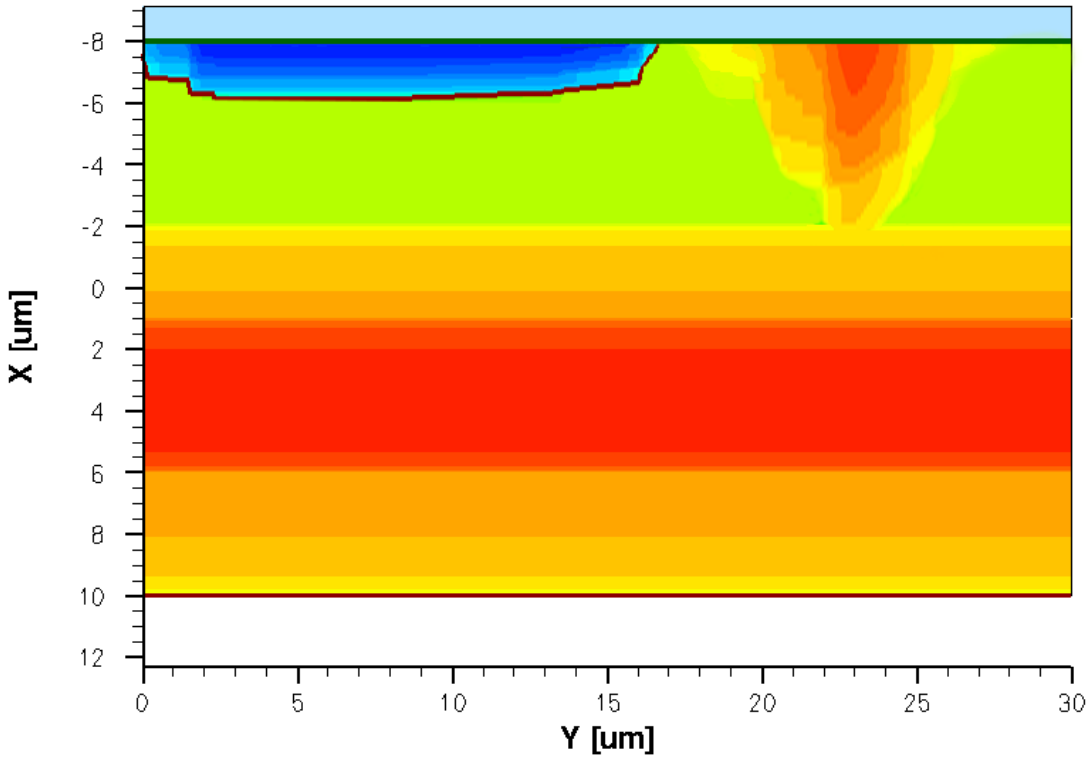


Рис. 2. Структурой транзистора после формирования областей базы

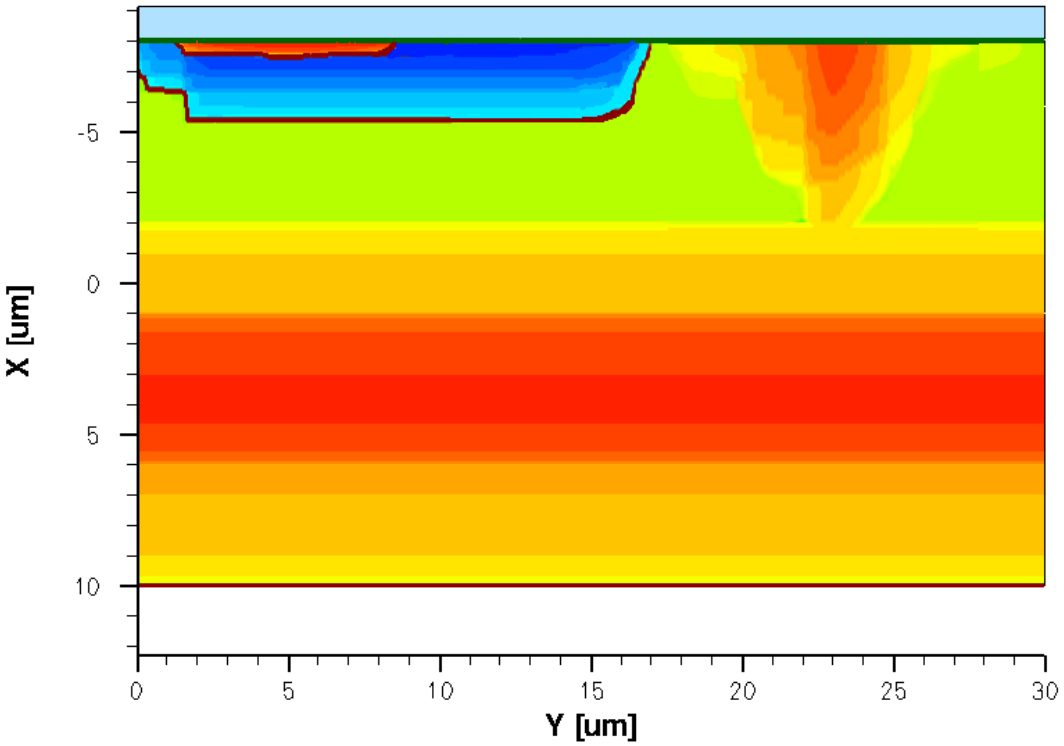


Рис. 3. Структурой транзистора после формирования областей эмиттера

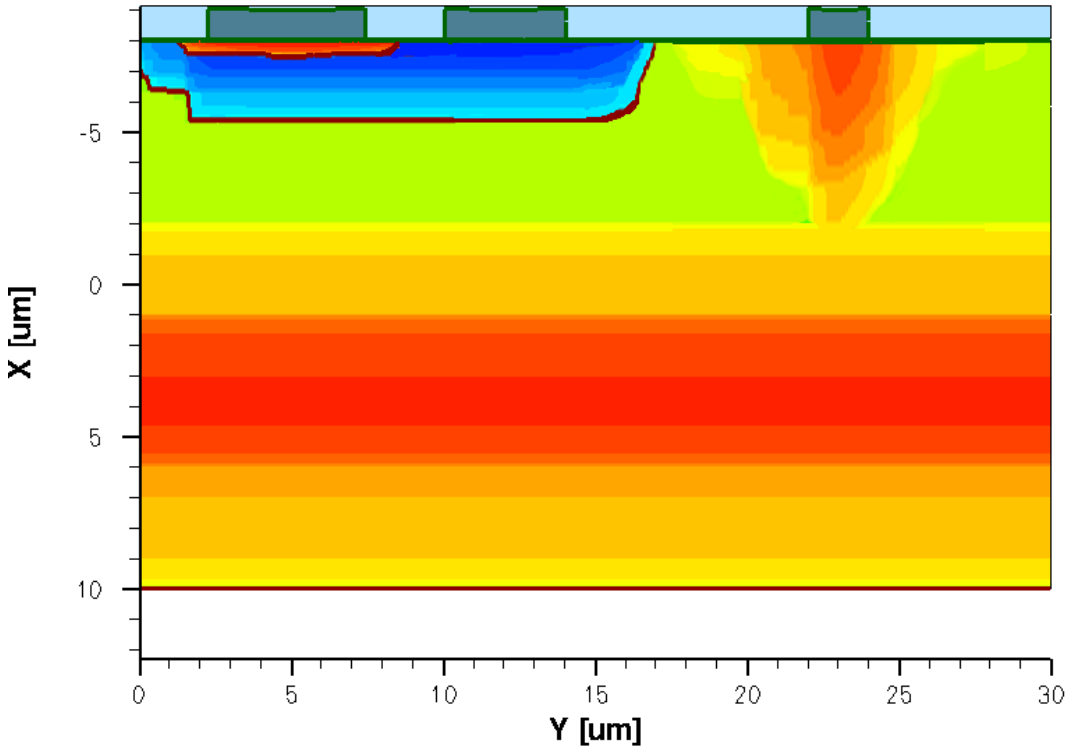


Рис. 4. Структурой транзистора после формирования контактных площадок

В результате выполнения работы была получена двумерная модель вертикального n-p-n транзистора микросхемы 1401СА1. Использование данной модели позволило скорректировать технологический процесс формирования кристалла микросхемы 1401СА1 на предприятии АО «ОКБ Микроэлектроники» (г. Калуга).

Список литературы

[1] Sentaurus TCAD. Datasheet [Электронный ресурс]. URL: http://www.synopsys.com/Tools/silicon/tcad/CapsuleModule/sentaurus_ds.pdf

[2] Зыков А.А., Осипов К.Ю. *Проектирование и технология электронной компонентной бызы. Основы САПР Synopsys TCAD*. Томск: Изд-во ТУСУР, 2012.

[3] Глушко А. А. *Приборно-технологическое моделирование в системе TCAD Sentaurus: методические указания к выполнению лабораторных работ по дисциплине «Автоматизация проектирования электронных средств»*. Москва: Изд-во МГТУ им. Н. Э. Баумана, 2015.

Рыжов Сергей Васильевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: sergey.righov@gmail.com

Андреев Владимир Викторович – д-р техн. наук, профессор КФ МГТУ им. Н.Э. Баумана. E-mail: andreev@bmstu-kaluga.ru

Д.Е. Бородин, В.В. Кузнецов

МОДЕЛИРОВАНИЕ ФОТОПРИЕМНОГО УСТРОЙСТВА ВЫСОТОМЕРА

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Работа любого вида аппаратуры с использованием оптического излучения основана на регистрации этого излучения приемниками оптического излучения, являющимися обязательными элементами структурных схем оптико-электронных устройств. Фотоприемники, в которых на основе конструктивных или схемотехнических решений осуществляется ряд последовательных преобразования сигнала, получили название фотоприемных устройств (ФПУ) [1].

ФПУ высотомера принимает оптическое излучение, преобразует его в электрический сигнал, осуществляет усиление и, при необходимости, преобразование формы, а затем передает сигнал на следующее за ним пороговое устройство.

Объектом исследований является однофазная схема фотоприемного устройства высотомера. Основной проблемой фотоприемного устройства является селекция полезного сигнала. Данную проблему усугубляет наличие синфазных наводок в спектре входного сигнала, вызванных источником импульсного лазерного излучения. В рамках квалификационной работы было разработано схемное решение данной проблемы в виде ФПУ с дифференциальным усилением сигнала. Для более полного обоснования перехода на дифференциальное усиление необходимо произвести моделирование схем с такими входными параметрами, как интенсивность светового потока, падающего на активную площадку фотодиода, и длина волны излучения.

Цель данной работы – создать модель фотодиода с возможностью настройки интенсивности падающего светового потока и его длины волны. На текущем этапе исследований производится обзор научной литературы по данной теме, подбор и тестирование ПО для моделирования объекта. Моделирование обеих схем планируется проводить в симуляторе электронных схем Qucs-S.

Qucs [2-6] – это симулятор электронных схем с открытым кодом. Qucs использует ядро моделирования Qucsator, разработанное с нуля. Это ядро имеет много преимуществ (моделирование S-параметров [6], расширенный постпроцесоор), но также имеет многочисленные баги, связанные с моделированием во временной области (Transient analysis). Для преодоления этого недостатка был разработан набор патчей spice4qucs, позволяющий моделировать схемы при помощи SPICE- совместимых движков (Ngspice или XYCE), и подготовлен специальный выпуск с интегрированным набором патчей: Qucs-0.0.19S (Qucs-S) [6-9].

Формат схемного файла Qucs основан на XML и к нему поставляется документация. Поэтому схема Qucs может быть легко сгенерирована сторонними программами. Это позволяет создавать ПО для синтеза схем, которое является расширением Qucs. Проприетарное ПО как правило использует бинарные форматы.

Библиотека компонентов использует собственный формат, основанный на XML. Но можно импортировать существующие библиотеки компонентов, основанные на SPICE (приводятся в даташитах на электронные компоненты).

Возможности версии Qucs-S [6]:

1. Большинство компонентов Qucs совместимо со SPICE. Поддерживаются подсхемы, библиотечные компоненты. О несовместимых компонентах во время моделирования выдаётся сообщение об ошибке: These components are SPICE-incompatible… Система уравнений (Equations) Qucs частично совместима со SPICE. об ограничениях читать документацию [9].

2. Добавлены виды моделирования совместимые со SPICE: .FOURIER, .NOISE и .DISTORTION Моделирование S-параметров не работает с Qucs-S.

3. Qucs-S позволяет моделировать схемы, недоступные симулятору Qucsator. Прежде всего это силовая электроника, ключевые схемы, схемы на полупроводниковых приборах, работающих с заходом в режим отсечки, и схемы с большим количеством компонентов.

Пример схемы, собранной в данном симуляторе, и её моделирование показаны на рисунках 1 и 2:

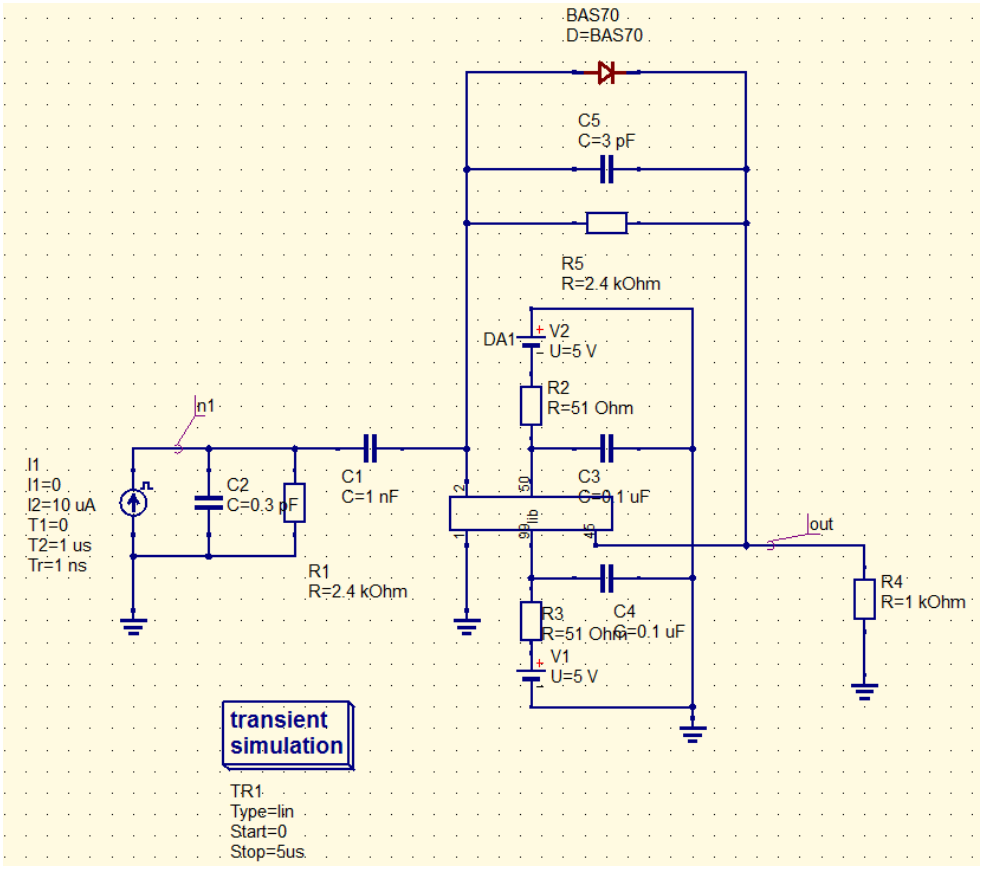


Рис.1. Схема фотоприемного устройства высотомера

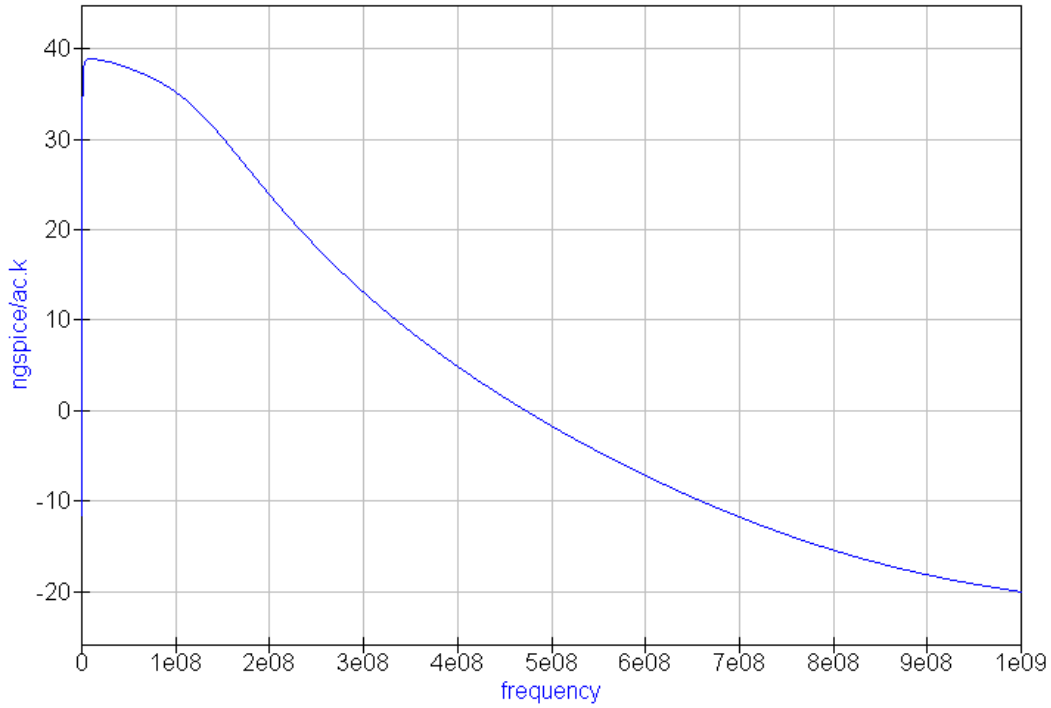


Рис.2. Моделирование АЧХ схемы фотоприемного устройства высотомера, проведенное в Qucs-S

Таким образом Qucs-S является расширенной версией Qucs, которая позволяет применять его не только для анализа высокочастотных схем, но и для решения задач разработки широкого спектра электронных средств, в том числе и рассмотренного выше фотоприемного устройства высотомера. Qucs-S свободно доступен для загрузки [7]. В настоящее время планируется создать SPICE-модели входящих в схемы компонентов, получить результаты таких анализов, как моделирование переходного процесса, моделирование по постоянному и переменному току и построить модель фотодиода на основе подсхем [8].

Список литературы

[1] Аксененко М.Д. Микроэлектронные фотоприемные устройства/ М.Д. Аксененко, М.Л. Бараночников, О.В. Смолин – М.: Энергоатомиздат, 1984. – 208 с.;

[2] Qucs: Quite Universal Circuit Simulator. http://qucs.sourceforge.net.

[3] Brinson M. E., Jahn S. Qucs: A GPL software package for circuit simulation, compact device modelling and circuit macromodelling from DC to RF and beyond // International Journal of Numerical Modelling (IJNM): Electronic Net-works, Devices and Fields. – 2008. – September. – Vol. 22, no. 4. – Pp. 297 – 319.

[4] Кузнецов В.В., Симулятор электронных схем с открытым исходным кодом Qucs: основные возможности и основы моделирования. – Компоненты и технологии. - 2015. - №3. - С.114-120.

[5] Кузнецов В.В. Моделирование высокочастотных схем в частотной области при помощи САПР Qucs. Компоненты и технологии. 2015. № 8 (169). С. 120-127

[6] M. Brinson, R. Crozier, V. Kuznetsov, C. Novak, B. Roucaries, F. Schreuder, and G. B. Torri. Qucs: An introduction to the new simulation and compact device modelling features implemented in release 0.0.19/0.0.19Src2 of the popular GPL circuit simulator. MOS-AK Workshop, Graz. http://www.mosak.org/graz2015/presentations/T_5_Brinson_MOS-AK_Graz_2015.pdf

[7] V. Kuznetsov. Unofficial build with spice4qucs features enabled. release candidate 3. https://github.com/ra3xdh/qucs/releases/tag/0.0.19S-rc3

[8] M. Brinson and V. Kuznetsov, ―Qucs equation-defined and Verilog-A RF device models for harmonic balance circuit simulation,‖ in Mixed Design of Integrated Circuits Systems (MIXDES), 2015 22nd International Conference, June 2015, pp. 192–197.

[9] M. Brinson and V. Kuznetsov. Spice4qucs help documentation. User manual and reference material. https://qucs-help.readthedocs.org/en/spice4qucs/

Бородин Дмитрий Евгеньевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: MisterDmitryBorodin@yandex.ru

Кузнецов Вадим Вадимович – канд. техн. наук, доцент кафедры "Конструирование и производство электронной аппаратуры" КФ МГТУ им. Н.Э. Баумана. E-mail: ra3xdh@gmail.com

В.В. Кузнецов, О.В. Антипенко

ПОГРЕШНОСТИ ИЗГОТОВЛЕНИЯ РЕЗИСТОРОВ В ИМС

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В современной микроэлектронике существует ряд проблем, связанных с несовершенством технологических процессов. Параметры готового устройства могут сильно отличаться от запланированных из-за погрешностей, вносимых на этапе изготовления.

Погрешность изготовления диффузионных резисторов по планарно-эпитаксиальной технологии может достигать 20%. Это связано с множеством факторов, проявляющихся в ходе выполнения технологического процесса. Наиболее существенными из них являются: погрешность изготовления фотошаблона, погрешность при транспонировании, неравномерность нанесения фоторезиста, а также наличие бокового подтрава при внедрении и разгонке примеси. Данные факторы учитывают на этапе проектирования, но несмотря на это величина погрешности может оставаться достаточно большой.

Рассмотрим влияние отклонения номиналов резисторов на работу схемы. В качестве примера рассмотрим схему 1420УД1. Принципиальная электрическая схема данного прибора представлена на Рис.1.

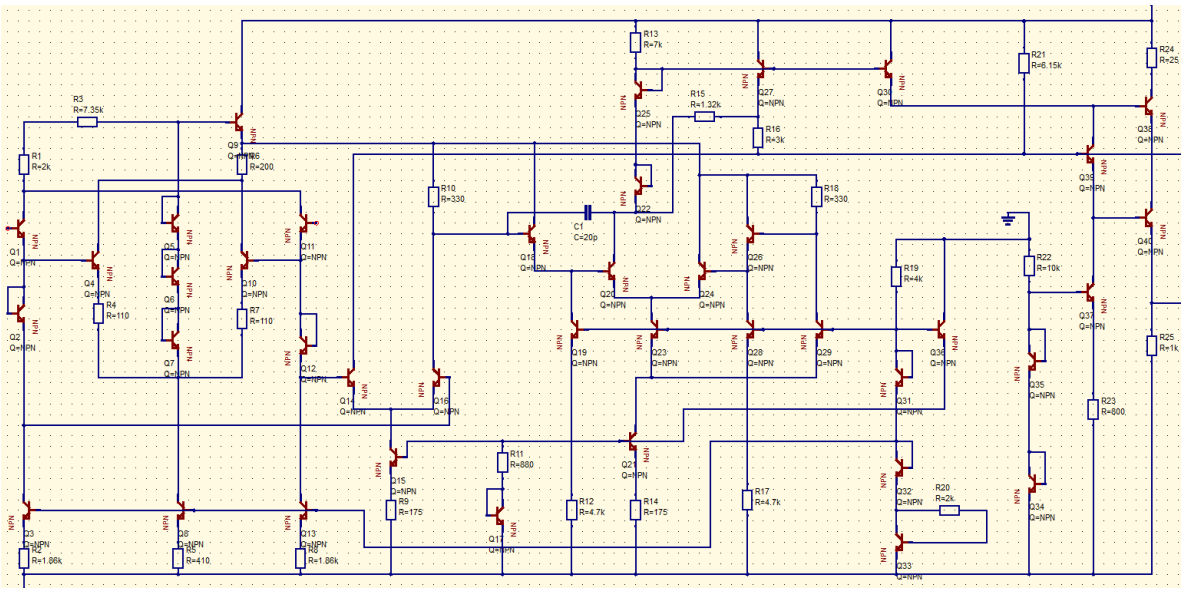


Рис.1 Схема электрическая принципиальная 1420УД1

Данная схема является операционным усилителем с внутренней частотной коррекцией. Основными структурными составляющими являются три усилительных дифференциальных каскада, цепь частотной коррекции, а также источники тока и эммитерные повторители. Отличительной особенностью данной схемы является высокое быстродействие, которое достигается путем использования в схеме транзисторов только n-p-n типа, а также наличию цепи коррекции низких и высоких частот.

Отклонение номиналов резисторов от нормы может внести существенные изменения в работу схемы: уходят рабочие точки транзисторных каскадов, увеличиваются токи потребления, что в свою очередь снижает энергоэффективность схемы, ухудшаются выходные параметры.

Произведем моделирование данной схемы в программе Qucs-s для выявления влияния отклонения номинала резисторов на работу схемы. В качестве примера рассмотрим резистор R14. На Рис. 2 и Рис 3. представлены графики зависимости выходного тока и напряжения от номинала резистора R14.

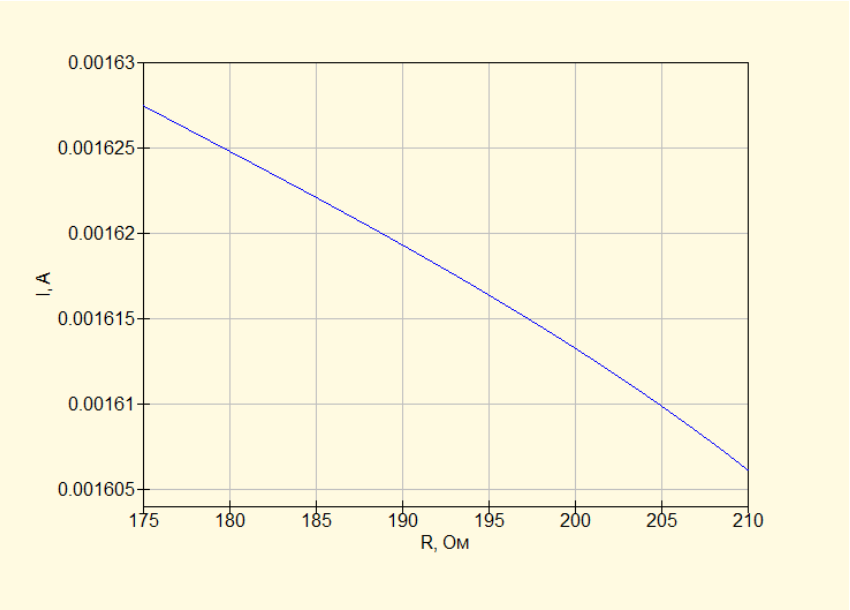


Рис.2 Зависимость выходного тока от номинала резистора R14

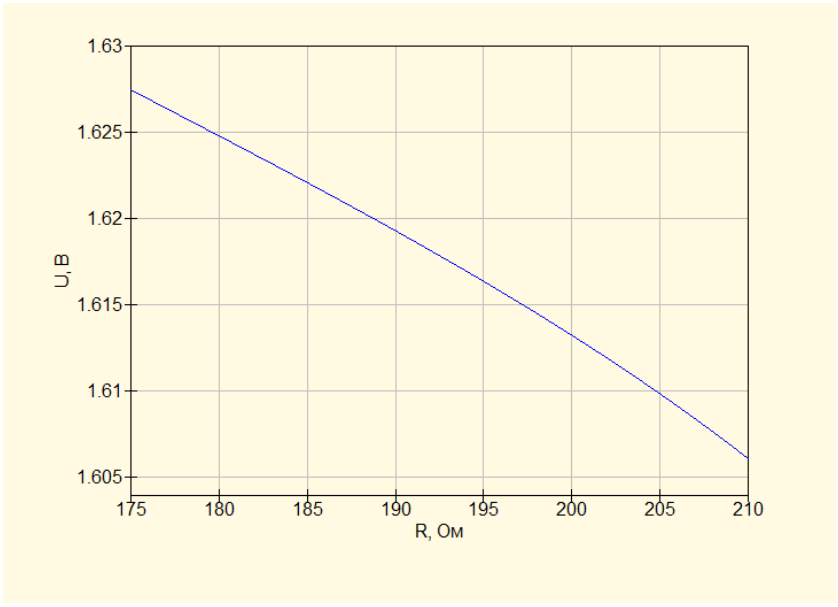


Рис. 3 Зависимость выходного напряжения от номинала резистора R14

Как видно из графиков с увеличением отклонения ухудшаются выходные параметры схемы. Как правило в ходе технологического процесса погрешность накладывается равномерно на всю схему и все элементы в той или иной степени получают отклонение.

Для повышения точности технологических процессов существует несколько методов. Рассмотрим основные.

Метод разделения ошибки. Данный метод основан на замене одного диффузионного резистора на несколько, имеющих параллельное включение. Отклонение при изготовлении каждого резистора остается неизменным, но суммарная ошибка получается меньше за счет ее разделения. Значимым преимуществом данного метода является отсутствие необходимости изменять технологический процесс и оснастку, необходимо лишь внесение изменений в топологию, что незначительно усложняет проектирование. Но данный метод не может обеспечить значительное снижение погрешности, а также его применение затруднено в схемах с высокой плотностью компановки элементов.

Метод пережогов. При этом методе резисторы, точность изготовления которых особенно важна, изготавливаются из нескольких частей, соединенных тонкими дорожками. При пропускании через них тока заданной величины, лишние сегменты отгорают и остаются лишь те, которые формируют резистор необходимого номинала. Преимущества метода: значительное повышение точности по сравнению с обычными диффузионными резисторами. К недостаткам можно отнести усложнение проектирование и требование внесения дополнительных операций по подгонке.

Использование напыленных резисторов. Использование напыленных резисторов в значительной мере повышает точность получения номинала. Так же напыленные резисторы обладают лучшим температурным коэффициентом по сравнению с диффузионными. К ним так же применима лазерная подгонка, что дает возможность получить требуемый номинал с высокой точностью. Данный метод требует применения сложного и дорогостоящего оборудования и в значительной мере усложняет технологический процесс, поэтому его применение оправданно лишь в некоторых случаях, например, для создания приборов специального назначения.

Выбор способа изготовления и метода увеличения точности резисторов является важной задачей в технологии микроэлектроники, так как от этого будет зависеть качество изготавливаемых схем, а также затраты на производство.

Список литературы

[1] Березин А.С., Мочалкина О.Р. Технология и конструирование интегральных микросхем. -М.: Радио и связь, 1983. -232 с.

[2] Курносов А.И. Технология производства полупроводниковых приборов и интегральных микросхем. - М., 1979:-367 с.

Кузнецов Вадим Вадимович – канд. техн. наук, доцент кафедры "Конструирование и производство электронной аппаратуры" КФ МГТУ им. Н.Э. Баумана. E-mail: ra3xdh@gmail.com

Антипенко Олег Викторович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: joe.semper77@gmail.com

С.А. Лоскутов, А.И. Кузенков

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ИМПУЛЬСНЫХ БЛОКОВ ПИТАНИЯ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Импульсные блоки питания (далее ИБП) постепенно вытесняют источники питания непрерывного действия, которые обладает низким КПД и большими габаритами. Современные ИБП имеют высокий КПД (до 98%) при сравнительно малых массо-габаритных показателях, обладают высокой надежностью и небольшой стоимостью. Однако они имеют ограничение по мощности и порождают высокочастотные помехи, которые требуется подавить каким-либо способом. Кроме того, ИБП обладают низкой динамической стабильностью и низкой скоростью реакции на изменение внешних динамических параметров [1].

Цель данной публикации – рассмотреть основные сложности в развитии ИБП.

В настоящее время можно выделить следующие актуальные направления развития ИБП: увеличение КПД и надежности, уменьшение габаритов.

Задача увеличения КПД наиболее актуальная для мощных источников питания. Повышение КПД даже на несколько процентов приводит к снижению выделения тепла силовыми элементами, что приводит к смягчению температурного режима работы и, как следствие, к повышению надежности. Однако в блоках импульсного типа при коммутации силового ключа всегда происходит выделение энергии в окружающую среду. А это, в свою очередь, порождает вопрос теплопередачи и, в конечном счете, влияет на срок службы всего изделия. Но вряд ли в ближайшем будущем следует ждать открытия принципиально нового силового ключевого элемента для ИБП. Если при развитии информационных технологий прогресс при появлении новых, революционных открытий дает порой гигантский скачок в их развитии, то в системах с преобразованием энергии, которая имеет место в импульсных источниках питания, мы можем наблюдать лишь постепенный прогресс. Поэтому увеличение КПД в настоящее время происходит за счет замены силовых тиристоров высокочастотными импульсными преобразователями с ЧИМ-ШИМ управлением, а также за счет совершенствования элементной базы [2].

Повышению надежности способствует работа элементов в слабонагруженном режиме. Оптимальным считается коэффициент нагрузки в интервале 0,5-0,8. Кроме того, современные ИБП разрабатываются с множеством систем защиты от воздействия нештатных ситуаций. Если источник питания обслуживает очень ответственные технологические процессы, применяется резервирование. Это ухудшает массогабаритные показатели, но значительно повышает надежность.

Все чаще начинают использовать ИБП, встроенные в автоматизированные системы и управляемые через контроллер или самим микрокомпьюте-

ром. Применение в качестве устройств управления микропроцессоров (микроконтроллеров) значительно увеличивает функциональные возможности как в части отдельных функций управления и защиты силового ключа, так и измерении и диагностики параметров ИБП. Применение микропроцессоров фактически делает ненужной широкую номенклатуру специализированных микросхем управления для частного применения. В настоящее время для мощных импульсных источников питания от 1 до 10 кВт, а также в сложных системах и источниках бесперебойного питания использование микропроцессоров оправданно, в том числе и с точки зрения снижения удельного показателя стоимости ($/Вт). В то же время очевидно, что широкое внедрение микропроцессоров в ИБП – это одно из направлений бурного развития вычислительных и информационных технологий в последнее время [3].

Но данное применение требует дополнительной защиты линий связи от электрических помех. Для обеспечения надежной передачи сигнала управления используют помехозащищенные интерфейсы, дифференцирование управляющих сигналов. Программное обеспечение системы управления источника должно быть адаптивным к уровню помех и устойчивым к сбоям питания. Наилучшие результаты показывают программы, разработанные на языке низкого, машинного уровня программирования. Они быстро реагируют на происходящие внешние воздействия, не склонны к зависанию, к чему склонны программы, написанные на языках высокого уровня [4].

В процессе работы над озвученной тематикой в процессе обучения в магистратуре планируется глубокий анализ проблем, возникающих при производстве ИБП на предприятии АО «Тайфун», пути их решения и перспективы развития в условиях реального производства.

Список литературы

[1] Лоскутов С.А. Источники электропитания РЭС: рабочий конспект лекций – Калуга, 2008. – 48 с.

[2] Грейвер Е.С. Ключевые стабилизаторы напряжения постоянного тока. – М: Энергия, 2002. – 256 с.

[3] Эраносян С., Ланцов В. Эволюция импульсных источников вторичного электропитания: от прошлого к будущему. Часть 5.1 – М: Силовая электроника, 2009. – № 4.

[4] Зиновьев А.В. Проблемы и тенденции развития мощных вторичных источников питания [Электронный ресурс]. Режим доступа: http://www.power2000.ru/info/article001.html. – Лаборатория силовых источников.

Лоскутов Сергей Александрович – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: SergeL-75@yandex.ru

Кузенков Андрей Игоревич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: kuzya974@yandex.ru

Е.Н. Дрожжова, А.Н. Мозохин

ПРОЕКТИРОВАНИЕ ЦИФРОВОГО УСТРОЙСТВА КОНТРОЛЯ ДВИЖЕНИЯ ТРАНСПОРТНОГО СРЕДСТВА

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

История применения устройства контроля движения транспортного средства началась в Европе в период бурного роста автомобильных грузоперевозок, так как владельцы предприятий хотели контролировать своих сотрудников. Поэтому в автомобили, отправляющиеся в длительные рейсы, были оборудованы устройства, которые были независимы от водителя и могли регистрировать скорость передвижения, пройденное расстояние и время. Первыми производителями таких устройств были часовые фирмы, поэтому в основе был часовой механизм.На сегодняшний день устройство контроля движения транспортного средства, обязательно устанавливать в транспортное средство.

Цифровое устройство обеспечивает определение точного местонахождения и регистрацию: скорости движения; пройденного пути; времени управления ТС; времени нахождения на рабочем месте, времени других работ, времени перерывов в работе и отдыхе; случаев доступа к данным регистрации; перерывов в электропитании длительностью более 100 мс; перерывов в подаче импульсов от датчика движения; вывод на индикатор и распечатку на бумажной ленте информации из энергозависимостей памяти и из карт.

Целью работы является разработка конструкции цифрового устройства контроля движения транспортного средства на базе производства АО «Калужского завода телеграфной аппаратуры (КЗТА)», обеспечивающего контроль непрерывной, некорректируемой регистрации информации о скорости и маршруте движения транспортных средств, и выполнения иных функций.

Цифровое устройство состоит из ТПУ (термопечатающее устройство), индикатора, средства криптографической защиты информации «Блок СКЗИ тахографа», блока управления и модуля навигационного.

В России предъявлены различные требования к оборудованию на транспортные средства, осуществляющие деятельность в России и осуществляющие деятельность за пределами нашей страны (согласно ЕСТР). *Основными отличиями являются:*

1. наличие блока СКЗИ;
2. наличие навигационного модуля ГЛОНАСС/GPS, как дополнительного источника скорости.

На сегодняшний день существует немало моделей таких устройств, и возникает большая конкуренция. На 2016 г. 10 организаций-изготовителей конкурируют между собой, и с каждым годом их становится все больше. Рассмотрим рисунок 1, где приведены параметры некоторых устройств

Параметры	Модель тахографа					
	АТОЛ	Штрих М	VDO Continental	Меркурий ТА 001	Касби	EFAS V2 RUS
Габариты, мм	180x188x58	188x60x175	178x50x150	210x190x60	191x187x58	186x56x181
Масса, кг	1,1	1	1,350	1,2	1,1	1,075
Разрешение дисплея, точек	128x32	160x32	100 x 20	128x64	130 x 32	128 x 21
Мощность, Вт	3-15	6-40	4-10	5-15	5-15	4-20
Диапазон измерения скорости, км/ч	0-250	0-250	0-250	0-220	0-250	0-220
Напряжение питания, В	8-36	8-35	только 24	8,5-30	10-30	8-32
Температура эксплуатации	-40 +70	-20 +70	-25 +70	-20 +85	-40+70	-25+80
Интерфейсы	CAN, USB, K-line	CAN, USB, K-line,Bluetooth	CAN, K-line	CAN, USB	CAN, USB, K-line	CAN, K-line
Кол-во цветов дисплея	10	1	9	1	1	4
Функция выброса карт	есть	нет	есть, с задержкой	нет	нет	нет
Количество клавиш	6	6	4 джостик	6	4	6
Тип разъема антенн	Fakra	SMA	Fakra	SMA	SMA	Fakra
Удаленная выгрузка с карты водителя	ТДО , скоро Wialon	ТДО	есть, ТДО и софт	нет, зависит от протокола	нет	нет
Потеря данных при отключении всех источников питания	Нет	Нет	Да	Нет	Нет	да
Калибровка	калибратор или бесплатное ПО	калибратор или платное ПО	калибратор	калибратор или платное ПО	калибратор или бесплатное ПО	калибратор
Ремонтопригодность	Да	Да	Нет	Да	Да	Нет
Стоимость софта для калибровки, аналитики, чтения карт водителя	Бесплатно	Платно	Платно	платное	бесплатное	—

Рис.1 Сравнение параметров

Рассмотрев данную таблицу, можно сделать вывод о том, что по некоторым параметрам мы уступаем другим устройствам. Ранее мы предложили рассмотреть замену выгрузки данных по USB на выгрузку данных по Bluetooth при помощи микросхемы TI CC2546MODA, что даёт большую универсальность и совместимость с большим количеством устройств по сравнению с исходным USB.

Еще один не мало важный параметр, это удаленная выгрузка с карты водителя, которую необходимо применить для нашего устройства. Удалённая выгрузка работает следующим образом: в устройстве настраивается адрес для сервера мониторинга, на который устройство отправляет как данные о навигации, так и данные, считанные с карт водителей. Данные с карты считываются сразу же как только карта вставляется в устройство и отправляются на сервер. На карту ставится отметка о считывании с текущих даты и времени, которые заданы в устройстве. Для того, чтобы удалённая выгрузка работала, нужно контролировать, чтобы в устройствах всегда были сим-карты с положительным балансом. И, конечно же, она будет работать только на устройствах с GPRS-модулем.

В процессе производства, эксплуатации и хранения устройства могут подвергаться тем или иным механическим воздействиям. В результате воздействия механических нагрузок могут иметь место различные повреждения: нарушение герметичности, обрыв монтажных связей, отслоение пе-

чатных проводников, поломка керамических подложек, временный или окончательный выход из строя разъемных и неразъемных соединений и т.д. Выполним расчет воздействии вибрации на устройство.

Размеры ПП: $axbxh = 170x150x1{,}5$;

Коэффициент перегрузки: $n = 5$;

Материал ПП Стеклотекстолит FR-4-1,5L H035/H035

$\mu = 0{,}22$ - коэффициент Пуассона;

$E = 3{,}02 \cdot 10^5$МПа- модуль упругости второго рода;

1) Определим частоту собственных колебаний при условии равномерно нагружения по поверхности ПП:

$$f_C = \frac{K_B \cdot \alpha}{2\pi a^2} \cdot \sqrt{\frac{Dg}{\gamma h}}, \text{где} K_B = \frac{1}{\sqrt{1 + \frac{m_э}{m_П}}}$$

α - коэффициент, зависящий от способа закрепления ПП, так как закрепление жесткое по всему периметру, то

$$\alpha = 9{,}87(1 + \frac{a^2}{b^2}) = 9{,}87 \cdot (1 + \frac{0{,}17^2}{0{,}15^2}) = 22{,}55$$

$$m_п = 0{,}17 \cdot 0{,}15 \cdot 0{,}0015 \cdot 2050 = 0{,}0784\text{кг}$$

$$m_э = 0{,}3\text{кг}$$

$$K_B = \frac{1}{\sqrt{1 + \frac{0{,}3}{0{,}0784}}} = 0{,}45$$

$$f_c = \frac{0{,}45 \cdot 22{,}55}{2\pi 0{,}17^2} \cdot \sqrt{\frac{60 \cdot 9{,}81}{23000 \cdot 0{,}0015}} = 231\text{Гц}$$

2) Найдем амплитуду колебаний ПП на частоте при заданном коэффициенте перегрузок n.

$$A = \frac{9{,}8 \cdot n}{4 \cdot \pi \cdot f_c^2} = \frac{5 \cdot 9{,}8}{4 \cdot 3{,}14 \cdot 231^2} = 73 \cdot 10^{-6}\text{м} = 73\text{мкм}$$

3) Определим коэффициент динамичности K_D, показывающий во сколько раз амплитуда вынужденных колебаний на частоте f отличается от амплитуды на частоте f_c

$$K_D = \frac{1}{\sqrt{(1 - \frac{f}{f_c})^2 + (\frac{f}{f_c})^2 \cdot \varepsilon^2}} = \frac{1}{\sqrt{(1 - \frac{350}{231})^2 + (\frac{350}{231})^2 \cdot 0{,}06^2}} = 1{,}58$$

$\varepsilon = 0{,}06$ - коэффициент затухания колебаний.

4) Динамический прогиб.

$$S = K_D \cdot A = 115 \cdot 10^{-6}\text{м}$$

5) определим эквивалентную динамическому прогибу равномерно распределенную нагрузку.

$$C_1 = 0{,}0012 + 0{,}4 \cdot lg(\frac{a}{b}) = 0{,}023$$

$$P_D = \frac{S \cdot D}{C_1 \cdot b^4} = \frac{115 \cdot 10^{-6} \cdot 60}{0{,}023 \cdot 0{,}15^4} = 575\text{Па}$$

Максимальный распределенный изгибающий момент, вызванный этой нагрузкой:

$$C_2 = 0{,}0513 + 0{,}108 \cdot lg(\frac{a}{b}) = 0{,}057$$

$$M_{max} = C_2 \cdot P_D \cdot b^2 = 0{,}737H$$

6) Находим максимальное динамическое напряжение изгиба ПП

$$\sigma_{max} = \frac{6 \cdot M_{max}}{h^2 \cdot 10^6} = 1{,}96\text{МПа}$$

7) Проверяем условие вибропрочности: $\sigma_{max} \leq [\sigma]$

$$\sigma = \frac{\sigma - 1}{n_\sigma} = \frac{105}{2} = 52{,}5\text{МПа}$$

$\sigma - 1$- предел выносливости материала ПП, для стеклотекстолита 105 МПа
$n = 1{,}8 \div 2$- допустимый запас прочности для стеклотекстолита.
$1{,}96\text{МПа} \leq 52{,}5\text{МПа}$

Следовательно, условие вибропрочности выполняется.

Проанализировав предложенные варианты усовершенствования данного устройства предлагается, осуществлять удаленную выгрузку с карты водителя что даёт большую универсальность и преимуществом над другими устройствами

Библиографический список

1. Контрольное устройство «ШТРИХ-ТахоRUS» стр. 64

2. Авто-Тахограф URL: http://auto-tahograf.ru/tahograf/sravnit.php. (дата обращения 14.10.2016)

3. CC2564MODx Bluetooth® Host Controller Interface (HCI) Module URL: http://www.ti.com/lit/ds/symlink/cc2564moda.pdf (дата обращения 14.10.2016)

Дрожжова Елена Николаевна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: drozhzhova92@yandex.ru

Мозохин Алексей Николаевич – ст. преп. кафедры "Конструирование и производство электронной аппаратуры" КФ МГТУ им. Н.Э. Баумана. E-mail: mozohin_an@mail.ru

А.Н. Шмаков, В.В. Андреев

РАЗРАБОТКА СИСТЕМЫ УПРАВЛЕНИЯ "INTEGRAL MES 1.0" ДЛЯ РЕГИСТРАЦИИ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ КМДП-ИС

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Данная работа посвящена разработке автоматизированной системы управления предприятием, которое занимается производством интегральных микросхем. Такая система должна поддерживать функции для удобного управления оператором, удобный интерфейс, административную панель редактирования под защитой пароля от несанкционированного доступа.

Для реализации условий потребовалось решить следующие задачи:

1. Проектирование реляционной базы данных таким образом, чтобы включить всю необходимую информацию, о производстве интегральных микросхем.
2. Привязка объёмной реляционной базы данных к клиентскому приложению.
3. Разработка пользовательского интерфейса, включающий в себя весь необходимый функционал для работы технолога.
4. Создание теста с помощью JavaScript на официальном сайте «Integral MES 1.0».
5. Размещение справочной информации на официальном сайте.
6. Создание доступа с помощью пароля в информационную базу и к панели редактирования.
7. Возможность вывода информации на бумажный носитель.
8. Создание системы, которая отслеживает технологические маршруты и потоки партий в режиме «реального времени».

Система управления производством должна быть оперативной, для обычного цеха необходимо принять около 10^2 решений в месяц о сборке изделий и примерно 10^3 решений, связанных с обработкой кремниевых пластин. Оперативность подразумевает, что такая информационная система должна базироваться на современных компьютерно-сетевых технологиях. Сложность задач по разработке заключается в создании "интеллектуальности" системы управления.

В процессе решения задачи по созданию программного обеспечения были детально рассмотрены особенности, необходимые для разработки программного продукта для промышленных предприятий. Эти особенности применяются в решении различных задач, например, система с возможностью "обратная связь", которая автоматически управляется событиями реального времени, но для которой ресурсы памяти и времени ограничены. В технологической части освещены все основные этапы для решения задачи на ЭВМ: тестирование программного продукта и отладка.

Реляционная база данных хранит информацию о технологических операциях кристального и сборочного производства. Тут хранятся данные маршрутных карт, а так же данные постащиков материаллов и заказов.

Основная цель базы данных это сбор инфорации в свою структуру, обрабатывать, устанавливать порядки очереди о технологических операциях. Цель программного модуля обеспечивать защиту от несанкционированного доступа к базе данных, выполнять подключение к базе, расположенной на сервере, или на физическом носителе операционной системы. Автоматизация программного обеспечения упрощает задачи в области управления предприятием, а так же сокращает объем бумажной документации.

Для проектирования структуры такой базы данных потребовалось изучить алгоритм производства интегральных схем на АО «Восход» - КРЛЗ. В результате, были взяты в основу следующие схемы показанные на рис. 1 и 2.

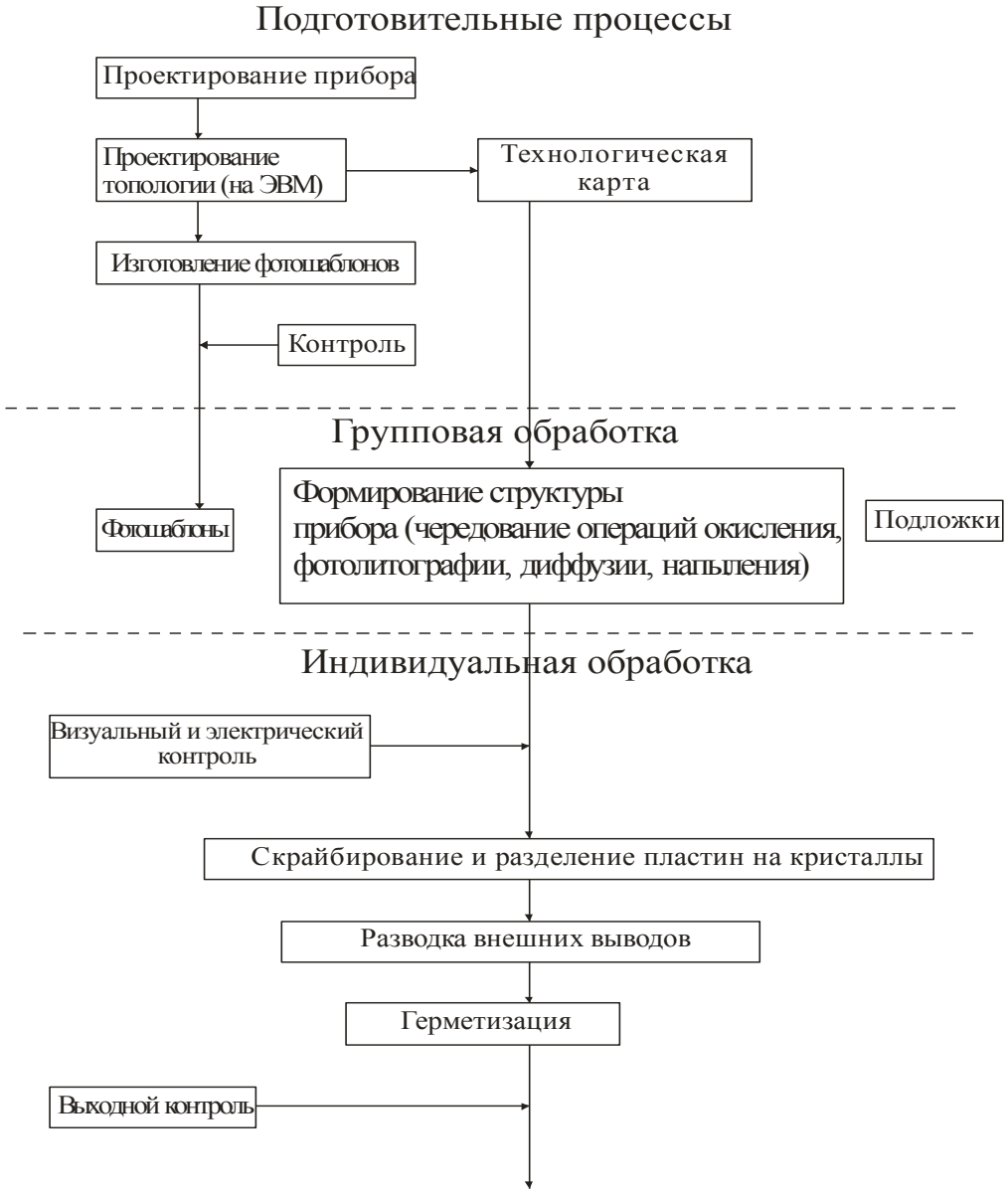


Рис 1. Общая схема технологических процессов

Рис. 2. Общая схема алгоритма производства ИС

Результатом исследования была спроектирована база данных, которая представляет собой структуру, показанную на рис. 3.

Алгоритм работы начинается с запуска приложения. Доступ в информационную базу приложения под защитой пароля, чтобы получить пароль, требутся перейти на сайт по ссылке в виде кнопки. На сайте находится тест по технике безопасности, после его прохождения пользователю будет выдан логин, пароль и пароль от панели редактирования. Первое, что требуется сделать при работе с программой, записать серию микросхемы в таблицу «Изделия», а затем заполнять маршрутный лист этой серии микросхем. На рисунках изображены некоторые возможности программы.

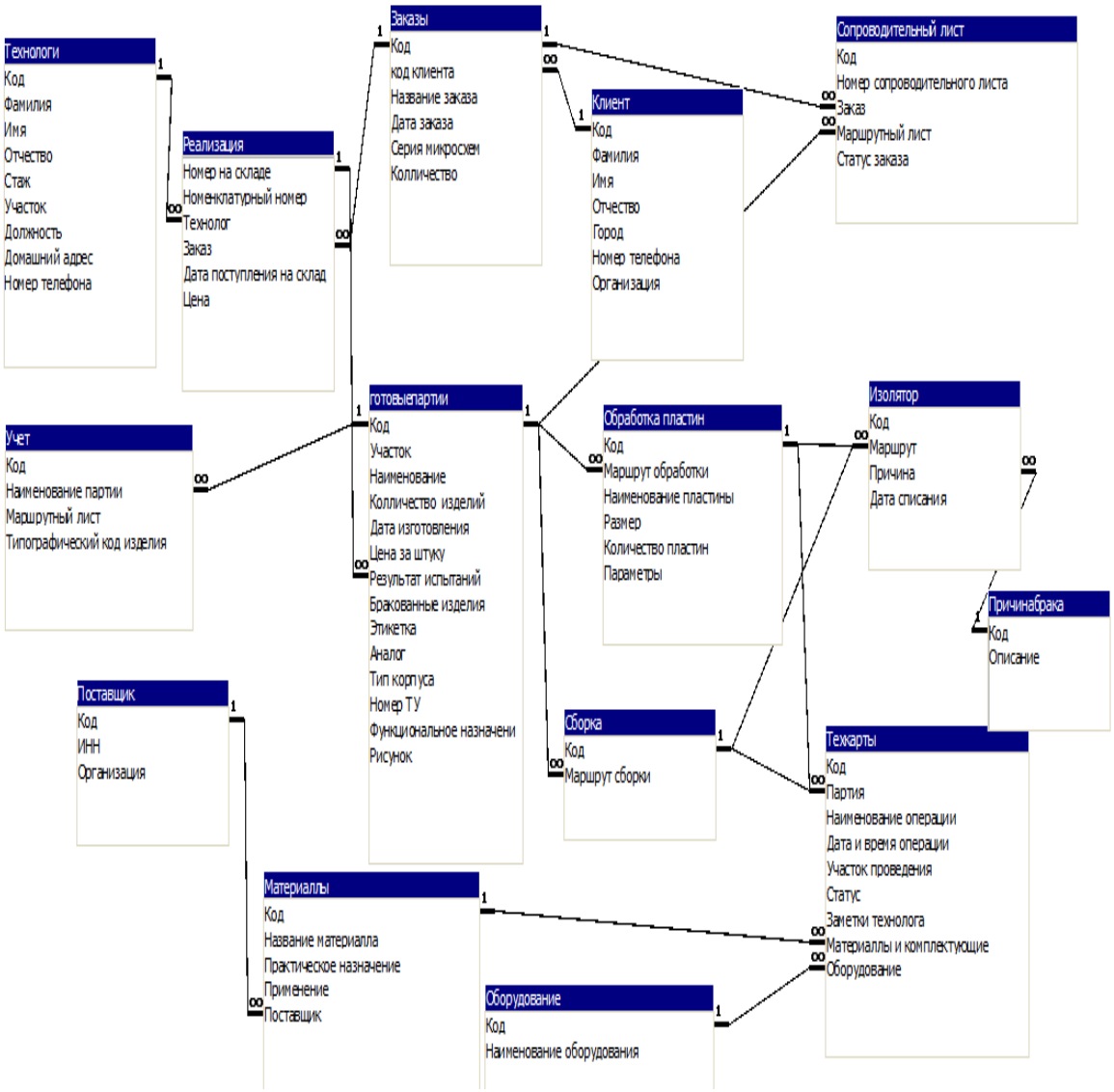


Рис. 3. Структура базы данных

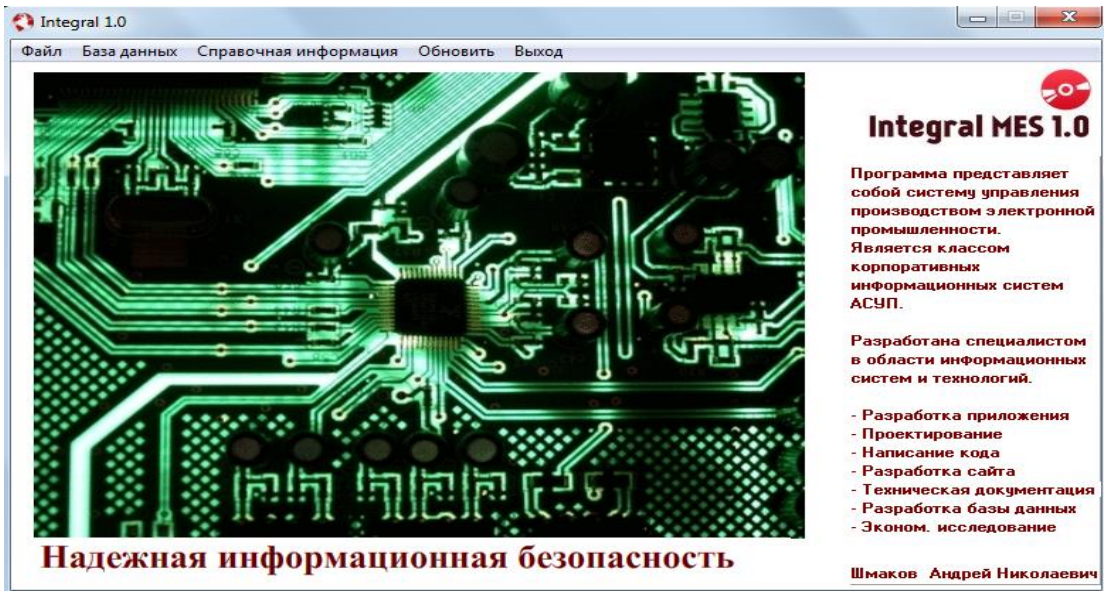


Рис.4. Главное окно программы

В результате проделанных работ были намечены пути для построения системы управления на современных компьютерно-сетевых ресурсах. Было проанализировано настоящее состояние производственного цикла, проанализированы методы по разработке аналогичных информационных систем, а так же разработаны некоторые предложения по проектированию сложной системы управления, которая будет охватывать производство в целом с учетом каждого производственного объекта. В итоге, разработано приложение, которое запускается с файла формата «exe», к приложению разработан офицальный сайт. Можно заметить, что разработка автоматизированных систем для регистрации производства и управления на компьютерно-сетевых ресурсах актуальна для отечественной промышленности. И возможно, разрабатываемая АСУПП может стать образцом для большого класса "интеллектуальных" промышленных автоматизированных информационных систем.

СПИСОК ЛИТЕРАТУРЫ

[1] MES Explained: A High Level Vision for Executives. [Электронный ресурс]. Издание 1997. Режим доступа: http://www.cpdee.ufmg.br

[2] MicrosoftAccses 2010. Функции и установка. Официальный сайт Майкрософт [Электронный ресурс] Режим доступа: http ://www.microsoft.com/

[3] Архангельский А. Язык Pascal и основы программированияв Delphi. – М.: ППП, 2009. – 200 с.

[4] Буч Г. Объектно-ориентированный анализ и проектирование с примерами приложений на C++. - Санта-Клара, Калифорния, 1998 г. – 125 с.

[5] Гайсарян С.С. Объектно-ориентированные технологии проектирования прикладных программных систем. Москва, 2011 г. – 180 с.

[6] Клыков Ю.И. Ситуационное управление большими системами. Санкт-Петербург, 1974 г. – 560 с.

[7] Коед П., Мэйфилд М. Объектные модели: Стратегии, шаблоны и приложения. Берлин,1996 г – 140 с.

[8] Коноли Т., Бегг К., Страчан А. Базы данных: проектирование, реализация и сопровождение. Москва, 2014 г. - 1180 с

[9] Мотев А.А., Уроки MySQL. BHV. Санкт-Петербург, 2013 г – 356 с.

[10] Мэдленд Г.Р. Интегральные схемы Основы проектирования и технологии. Бостон, 1966 г. – 360 с. Перевод К.И. Мартюшова, Москва 1970 г. – 360 с

Шмаков Андрей Николаевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: ArhangelSD@yandex.ru

Андреев Владимир Викторович – д-р техн. наук, профессор КФ МГТУ им. Н.Э. Баумана. E-mail: andreev@bmstu-kaluga.ru

А.А. Корнеев, В.В. Кузнецов

СХЕМОТЕХНИЧЕСКОЕ РЕШЕНИЕ ДЛЯ ПРОВЕРКИ КАБЕЛЕЙ И ИНДУКТИВНЫХ ДАТЧИКОВ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

При схемотехническом проектировании любого устройства не всегда бывает возможной симуляция его схемы. Часто это бывает из-за наличия цифровых интегральных микросхем, отсутствия определенных электронных библиотек с математической моделью компонента, сложности реализованной схемы, наличия компонентов с переменными параметрами.

Цель данной работы: исследование модели стенда проверки кабелей и индуктивных датчиков, а также сравнение анализов до и после внесения корректировок параметров и схемотехнических изменений.

Схема электрическая принципиальная такого устройства представлена на рисунке 1:

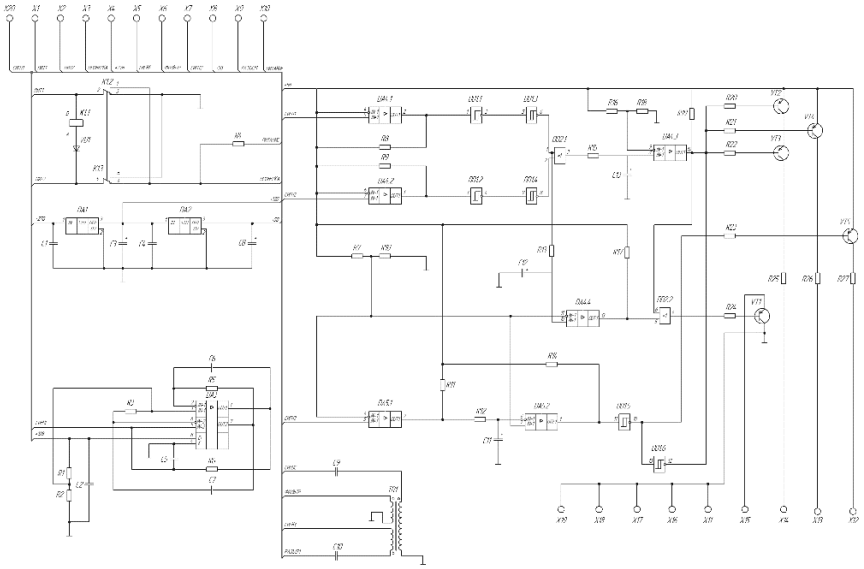


Рис.1. Схема электрическая принципиальная стенда.

Полезный пилообразный сигнал генерируется на операционном усилителе DA3, выступающем в роли генератора эталонного сигнала, далее развязывается на трансформаторе T1 и превращается в синусоидальный, а далее и сравнивается на компараторах. В симуляторе амплитуда такого сигнала равна 5В, но это при идеальных условиях. При подключении жгута, состоящего из 200 жил, такой кабель будет являться набором сопротивлений, а все напряжение полезного сигнала упадет на трансформаторе и на выходной нагрузке. Так же необходимо учитывать собственные шумы микросхем. Такой исход приведет стенд к сбоям в работе и к невозможности тестирования индуктивных датчиков, а также проверяемых кабелей.

Осциллограмма выходных сигналов представлена на рисунке 2, где синий – собственный шум, а красный – полезный сигнал задающего генератора:

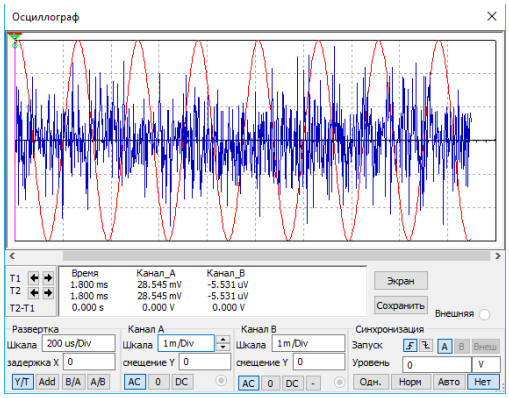


Рис.2. Временные диаграммы шумового и полезного сигналов.

Чтобы полезный сигнал не смешивался с шумами, была поставлена задача усилить данный сигнал при помощи обычного усилителя низкой частоты. В качестве УНЧ была применена микросхема TDA7052.

Данная ИМС является интегральным одноканальным усилителем низкой частоты, мощностью 1Вт, преимущественно применяется в различной переносной аппаратуре с низковольтным питанием. Ток потребления в холостом режиме составляет 7мА…10мА, что позволяет использовать усилитель в мобильных условиях совместно с маломощными источниками сигнала. Диапазон рабочих напряжений микросхемы находится в диапазоне от 4.5В до 18В, в типовом режиме при питании в 6В, мощность усилителя составляет 1Вт. Сборка усилителя ограничивается минимальным количеством компонентов, что предусмотрено типовой схемой включения.

Так как в схеме не имеет смысла регулировка входного напряжения на УНЧ, были подобраны резисторы и конденсаторы так, чтобы на выходе усилителя с нагрузкой получилось ровно 5В.С помощью такого решения шумовой сигнал на фоне полезного стал незначительным, что положительно повлияло на временные диаграммы и работу устройства в целом. Результат моделирования измененной схемы представлен на рисунке 3:

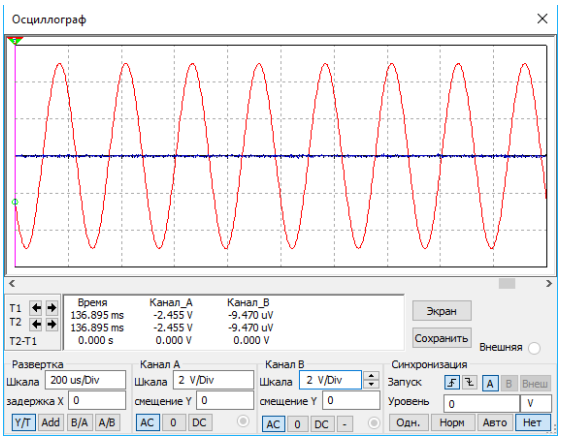


Рис.3. Результат моделирования с применением усилителя низкой частоты.

При дальнейших исследованиях было принято решение подтяжки цепи питания и общей цепи резисторами. Подтягивающий резистор (pull-up-резистор) – резистор, включенный между проводником, по которому распространяется электрический сигнал, и питанием, либо между проводником и землей.

Такой резистор нужен, чтобы гарантировать на логическом входе, с которым соединен проводник, высокий (в первом случае) либо низкий (во втором случае) уровни напряжения. Данное схемотехническое решение привело схему стенда к полной стабильности работы, так же к практически идеальным временным диаграммам выходных напряжений на элементах сравнения. Временные диаграммы до и после текущего изменения для логической 1 и 0 приведены на рисунках 4 и 5 соответственно:

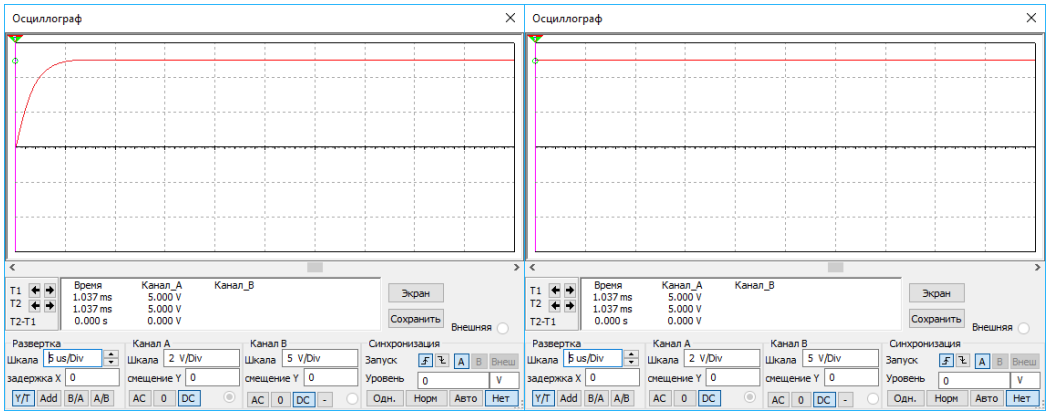


Рис.4. Результат «до» и «после» подтяжки логической единицы.

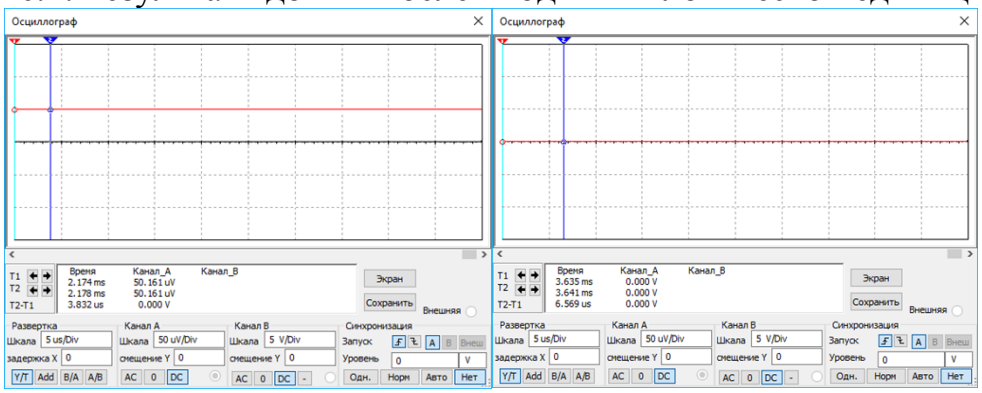


Рис.5. Результат «до» и «после» подтяжки логического нуля.

Схема электрическая принципиальная стенда проверки со всеми внесенными изменениями представлена на рисунке 6:

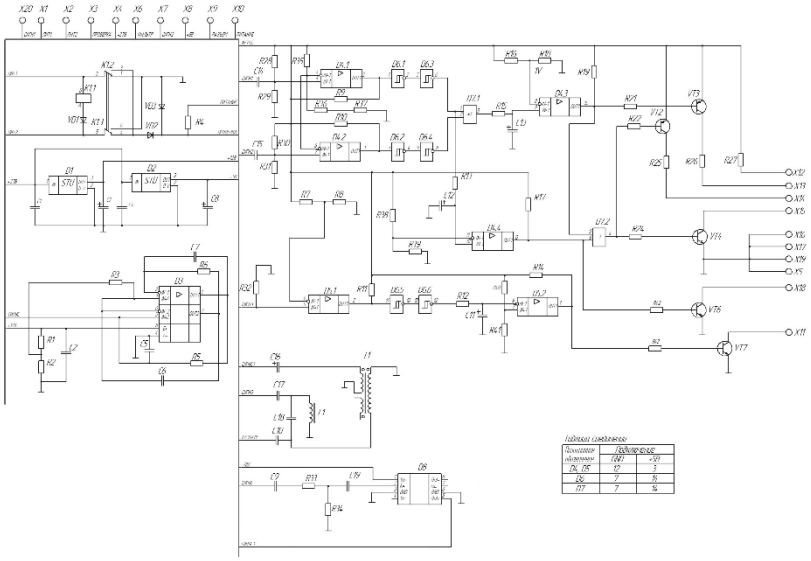


Рис.6. Измененная схема стенда контроля.

В заключении хотелось бы отметить, что данная схема стенда проверки была успешно промоделирована и были получены осциллограммы выходных сигналов генератора с УНЧ, а также компараторов, которые удовлетворяют поставленной задаче в рамках данной научной работы.

Список литературы:

[1] Особенности УНЧ TDA7025 http://radiostorage.net/?area=news/7

[2] Марк Е. Хернитер. Multisim: Современная система компьютерного моделирования и анализа схем электронных устройств. -М.: ДМК Пресс, 2012. - С.114-120.

[3] Антипенский Р.В., Фадин А.Г. Схемотехническое проектирование и моделирование радиоэлектронных устройств. -М.: Техносфера, 2007. – С.89-92.

[4] Красько А. - Схемотехника аналоговых электронных устройств. – ТУСУиР, 2005. –С109-112.

Корнеев Александр Анатольевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: sas825@yandex.ru

Кузнецов Вадим Вадимович – канд. техн. наук, доцент кафедры "Конструирование и производство электронной аппаратуры" КФ МГТУ

А.В. Рытикова, В.В. Андреев

ТЕСТОВЫЕ СТРУКТУРЫ ДЛЯ КОНТРОЛЯ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА В ПРОИЗВОДСТВЕ КМДП ИМС

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Большинство КМОП-технологий в настоящее время следуют стандартным принципам планарной кремниевой микротехнологии [1-3]. Основными элементами интегральных микросхем, изготавливаемых по таким технологиям, являются металл-оксид-полупроводник полевые транзисторы (МОП-транзисторы) с каналом n-типа или p-типа проводимости. Часть микросхемы, изготовленной по КМОП технологии с n- и p-канальными полевыми транзисторами и пять металлических слоев стека показаны на рис. 1.1. Количество металлических слоев может варьироваться от трех до десяти или более.

В настоящее время наблюдается экспоненциальный рост количества элементов на интегральных схемах. Эта тенденция соответствует снижению минимального размера объекта (рис. 1.2) для КМОП технологий [4]. Каждые 2-3 года, продукты нового поколения КМОП-технологии внедряются на рынке. В настоящее время разработка ведется по проектным нормам 22 и 14 нм и ниже.

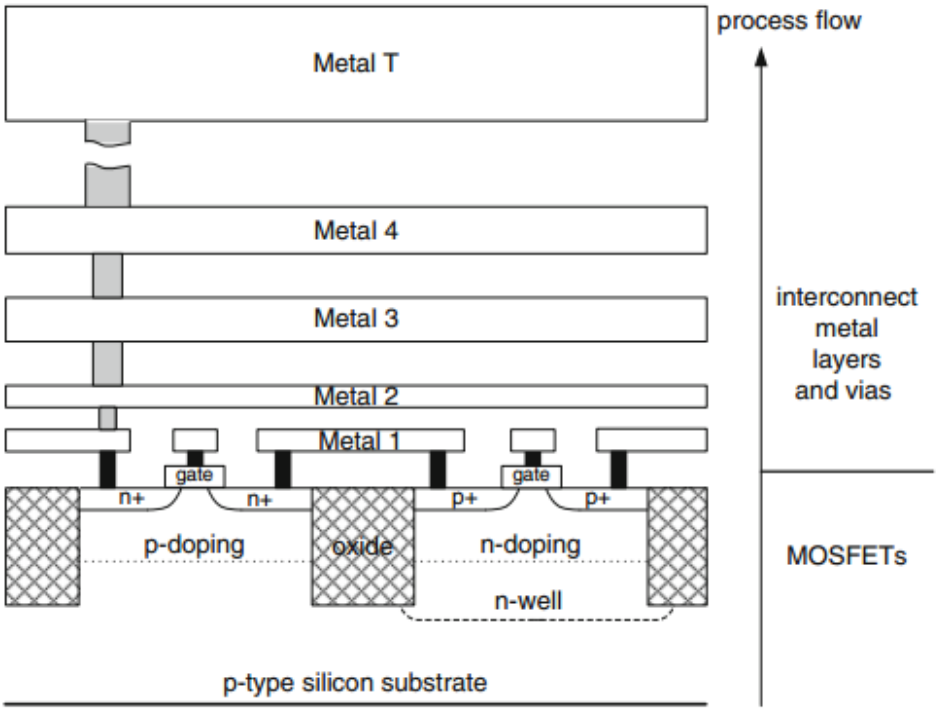


Рис. 1.1 Часть схемы КМОП, схема с пятью металлическими слоями и межуровневая диэлектрическая изоляция

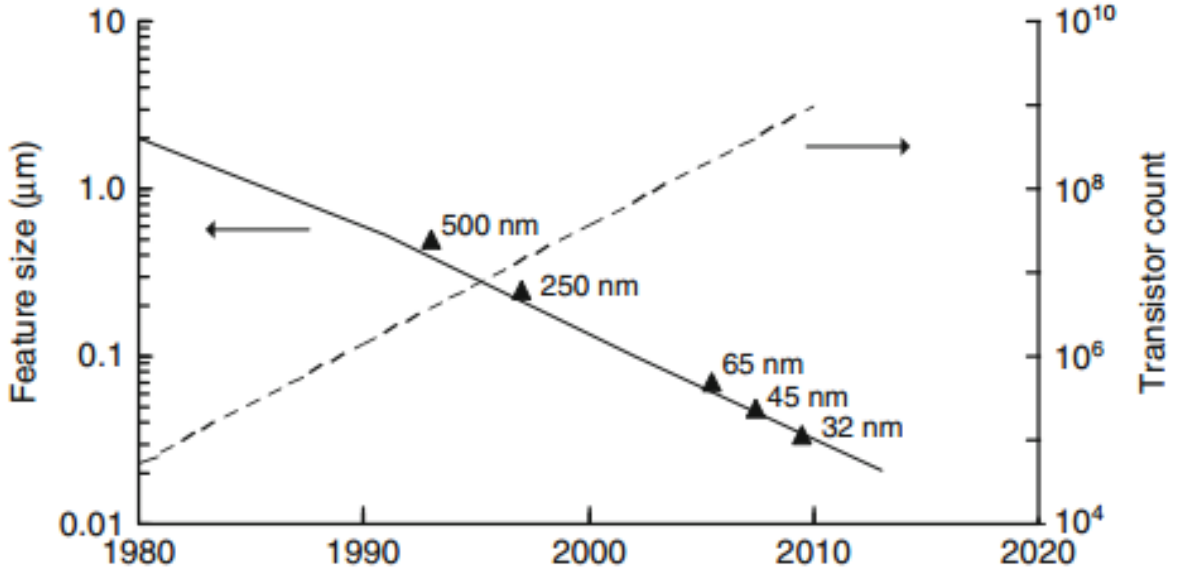


Рис. 1.2 Минимальные размеры и характеристики транзистора на ИС с 1980 года. КМОП-технологий, соответствующие 500, 250, 65, 45 и 32 нм

Тестовые структуры используются в разработке технологических процессов и оптимизации поведения устройства. Характеристика изготовления КМОП микросхемы осуществляется на нескольких различных уровнях процесса интеграции. На более низком уровне осуществляются процессы: ионная имплантация, нанесение рисунка фоторезиста, травление и химико-механического полирования. Такие характеристики включают методы тонкопленочного контроля сопротивления, линии ширины измерения, эллипсометрию и оптическую и электронную микроскопию [5]. На более высоком уровне интеграции, электрических тестовых структур используются элементы КМОП-схемы и функциональной схемы блоков логики и памяти. Они могут быть протестированы после прохождения многих этапов процесса, как показано на рис. 1.3.

МОП-транзистор и простая схема блоков могут быть проверены только после того, как минимум первый металлический слой, M1, будет сформирован. Следовательно, проведение электрических испытаний начинается сразу после получения слоя M1. Время изготовления кристалла до формирования слоя M1 обычно занимает половину или более от общего времени изготовления микросхемы. После получения слоя M1 и проверки электрофизических характеристик тестовых элементов, может быть несколько последующих промежуточных тестов после формирования последующих металлических слоев. Окончательное тестирование проводится на кристалле после формирования всех металлических слоев, когда становится возможной проверка работоспособности интегральной микросхемы в целом.

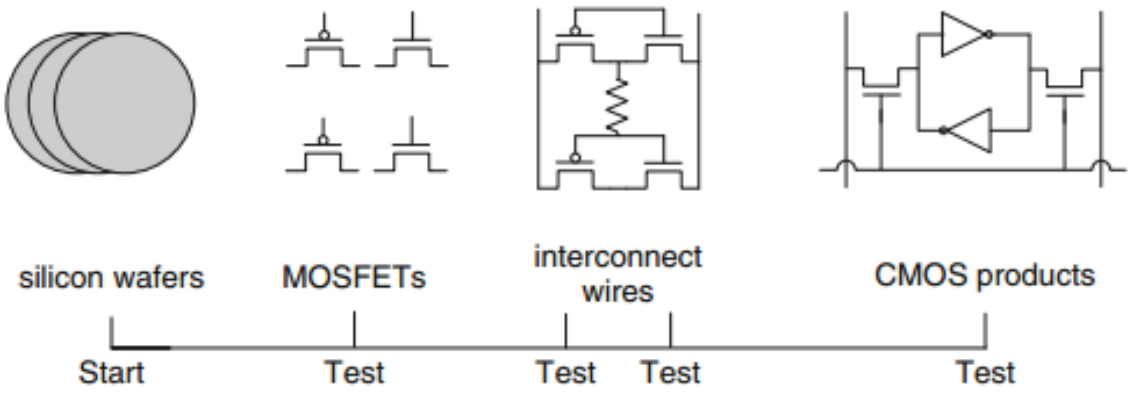


Рис. 1.3 Электрические тестовые испытания проводимые в процессе изготовления КМОП интегральных микросхем

Работа выполнена в рамках государственного задания МГТУ им. Н.Э. Баумана министерства образования и науки РФ (проект № 1117), а также при финансовой поддержке администрации Калужской области (грант № 16-42-400791).

ЛИТЕРАТУРА

[1] *Jaeger R.C.* Introduction to microelectronic fabrication, vol 5, Modular series on solid state devices, 2nd edn. Prentice Hall (2001), Upper Saddle River, NJ

[2] *Андреев В.В., Барышев В.Г., Столяров А.А.* Инжекционные методы исследования и контроля структур металл-диэлектрик-полупроводник – М: Издательство МГТУ им. Н.Э. Баумана. – 2004. – Г.2, п. 2.2 – 42 с.

[3] *Campbell S.A.* The science and engineering of microelectronic fabrication, 2nd edn. Oxford University Press, (2001) Oxford.

[4] *Bohr M.* The new era of scaling in an SoC world. International solid-state circuit conference (ISSCC) proceedings, 2009:23–28

[5] *Schroder D.K.* Semiconductor material and device characterization, 3rd edn. Wiley, 2006. Hoboken, NJ

Рытикова Александра Владимировна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: sandramair555@gmail.com

Андреев Владимир Викторович – д-р техн. наук, профессор КФ МГТУ им. Н.Э. Баумана. E-mail: andreev@bmstu-kaluga.ru

С.А. Лоскутов, В.Э. Толоконников

УВЕЛИЧЕНИЕ КАНАЛОВ СБОРА ДАННЫХ УСТРОЙСТВА КОММУТАЦИИ.

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Любая деятельность человека так или иначе связана с информацией. Мы получаем ее в различной форме, однако с развитием технологий все большие объемы информации представлены в виде *электрических* сигналов. Для работы с данными сигналами необходимы различные технические устройства.

Развитие технических устройств передачи и обработки информации идет опережающими темпами. Представленный блок относится к этому классу устройств, соответственно тема является актуальной.

В данной статье рассмотрим структуру (рис.1) и принцип работы блока коммутатора дискретных сигналов (далее по тексту - БКДС).

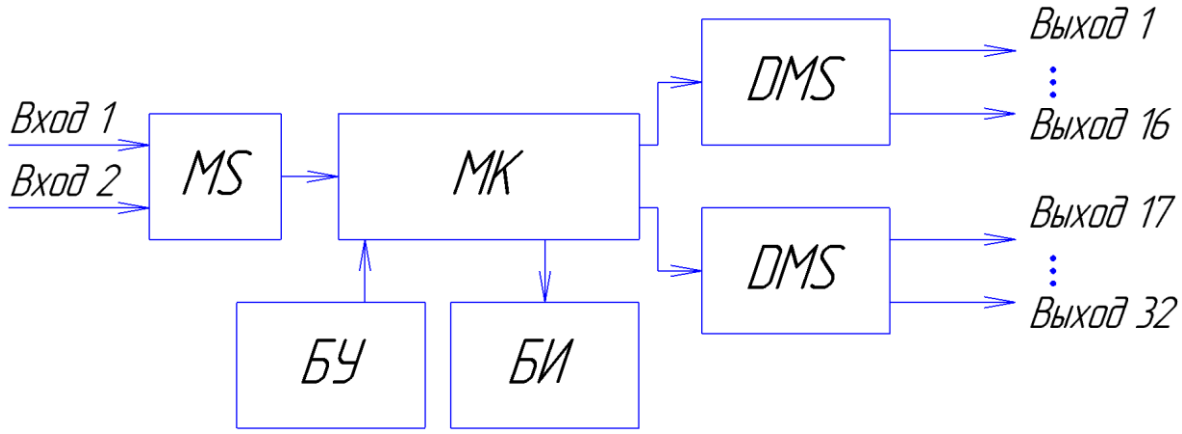


Рис.1. Структурная схема БКДС:
MS – мультиплексор, DMS – демультиплексор, БИ – блок индикации,
БУ – блок управления, МК – микроконтроллер.

Элементы MS и DMS выполняют коммутацию одного из входных сигналов на один или несколько выходных каналов Выход1-Выход32. Процесс коммутации осуществляется посредством микроконтроллера.

Устройство ввода позволяет пользователю управлять процессом коммутации, а именно, выбирать входные и выходные каналы. Блок индикации отображает состояние системы.

Блок БКДС осуществляет объединение информации, поступающей от блока сбора дискретных данных (БСДД) по двухпроводным физическим линиям (до тридцати двух линий) и передачу её по одной двухпроводной физической линии типа «витая пара» на блок сопряжения с персональным компьютером головного комплекса обработки данных.

Анализ работы устройства приведен в статье Ерёмина В.В. «Аналоговый коммутатор КА-4-16» [1].

В связи с увеличением количества датчиков, а, следовательно, и каналов приёмо-передачи информации, возникла потребность в модернизации устройства.

Для решения поставленной задачи мною было выбрано каскадное соединение блоков БКДС.

Рассмотрим основные преимущества и недостатки такого подключения.

Технические плюсы:

- возможность сведения информации на удаленном объекте в одну информационную линию вместо необходимости использовать несколько информационных линий к каждому блоку БСДД. Это позволяет сократить длину кабеля связи и каналообразующей аппаратуры
- возможность использования различного интерфейса передачи данных. Например, часть пути информация идет по линии RS-485, потом через блок БКДС переводится в интерфейс V.22bis и проходит дальше. Это может понадобиться при использовании различной каналообразующей аппаратуры. Такая аппаратура позволяет делать «прозрачное удлинение» какого-либо интерфейса, например, через Ethernet.
- возможность построения более длинной линии, т.к. БКДС выступает в роли приемо-передатчика. Сигнал по линии затухает, БКДС принимает его и передает дальше с большей амплитудой сигнала.
- с экономической точки зрения, введение такой функции улучшит привлекательность комплекса для части заказчиков. Соответственно можно ожидать увеличение продаж.

Технические минусы:

- пинг, т.е. задержка распространения пакета данных, соединения увеличивается. Т.к. пакет данных полностью принимается, а уже потом передается дальше.
- увеличение количества оборудования снижает надежность системы в целом.

Электронные ресурсы

[1] Ерёмин В.В., Меркулов С.В. Аналоговый коммутатор КА-4-16. URL: http://lib.tpu.ru/fulltext/c/2011/C01/V01/092.pdf (дата обращения 15.10.2016).

Лоскутов Сергей Александрович – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: SergeL-75@yandex.ru

Толоконников Вадим Эдуардович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: vadimtv1994@gmail.com

В.В. Андреев, В.С. Кулагин

ЭКСПЕРИМЕНТАЛЬНАЯ АВТОМАТИЗИРОВАННАЯ УСТАНОВКА КОНТРОЛЯ ПАРАМЕТРОВ МДП-СТРУКТУР

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Данная работа посвящена разработке экспериментальной автоматизированной установки контроля параметров тестовых МДП-структур с использованием прецизионного источника питания постоянного тока NI PXI-4132, который управляется с помощью алгоритма, написанного в среде LabVIEW.

Используемый в данной работе модуль – NI PXI-4132 – является как источником постоянного тока и напряжения, так и измерителем этих параметров. В таблице 1 приведены основные параметры прибора.

Таблица 1. Основные параметры NI PXI-4132

Подаваемый ток	0,2 мкА - 100 мА
Предельное напряжение	100 В
Максимальная точность измерения напряжения	10 мкВ
Подаваемое напряжения	0 - 100 В
Предельный ток	100 мА
Максимальная точность измерения тока	10 пА

Для исследования параметров МДП-структур необходимо спроектировать коммутатор, обеспечивающий связь между исследуемой МДП-структурой и измерительным модулем, а также написать программу-алгоритм в среде LabVIEW.

На рисунке 1 представлена схема электрическая принципиальная измерения параметров МДП-структуры в режиме управляемого токового воздействия [1]. На рисунке 2 представлена блок-диаграмма виртуального прибора LabVIEW для измерения параметров МДП-структуры в режиме управляемого воздействия током. Показания снимаются с помощью модуля NI PXI-4132. Приведенный алгоритм последовательно устанавливает значение тока, подаваемого на МДП-стркутуру, и измеряет падение напряжения на испытываемом образце (всего 5 итераций).

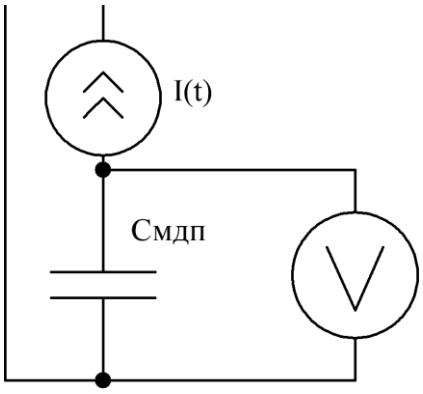


Рис. 1. Схема измерения параметров МДП-структуры в режиме управляемого токового воздействия

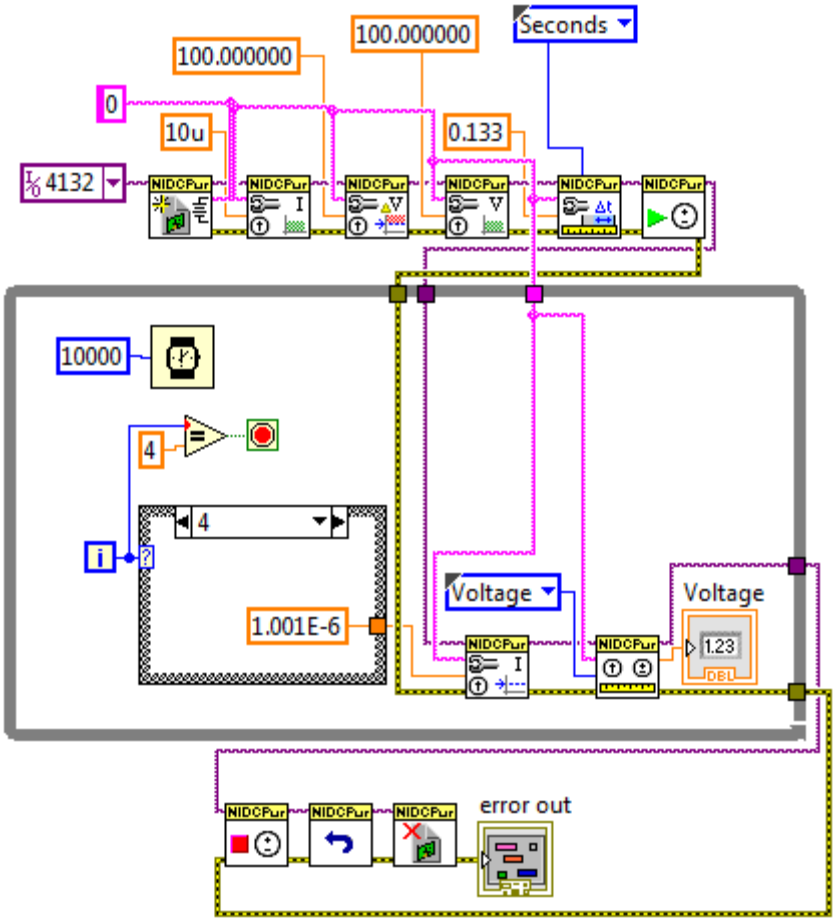


Рис. 2. Блок-диаграмма виртуального прибора LabVIEW для измерения напряжения МДП-структуры

На рисунке 3 представлена схема электрическая принципиальная измерения параметров МДП-структуры в режиме воздействия управляемым напряжением [1]. На рисунке 4 представлена блок-диаграмма виртуального прибора LabVIEW для измерения тока МДП-структуры. Показания снимаются с помощью модуля NI PXI-4132. Приведенный алгоритм последовательно устанавливает значение напряжения, подаваемого на МДП-стркутуру, и измеряет ток на испытываемом образце (всего 5 итераций).

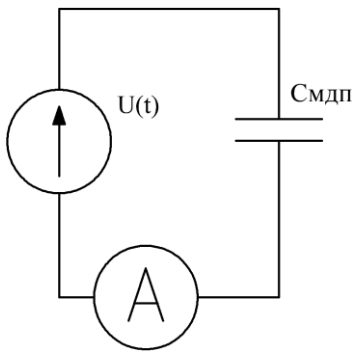


Рис. 3. Схема измерения параметров МДП-структуры в режиме воздействия управляемым напряжением

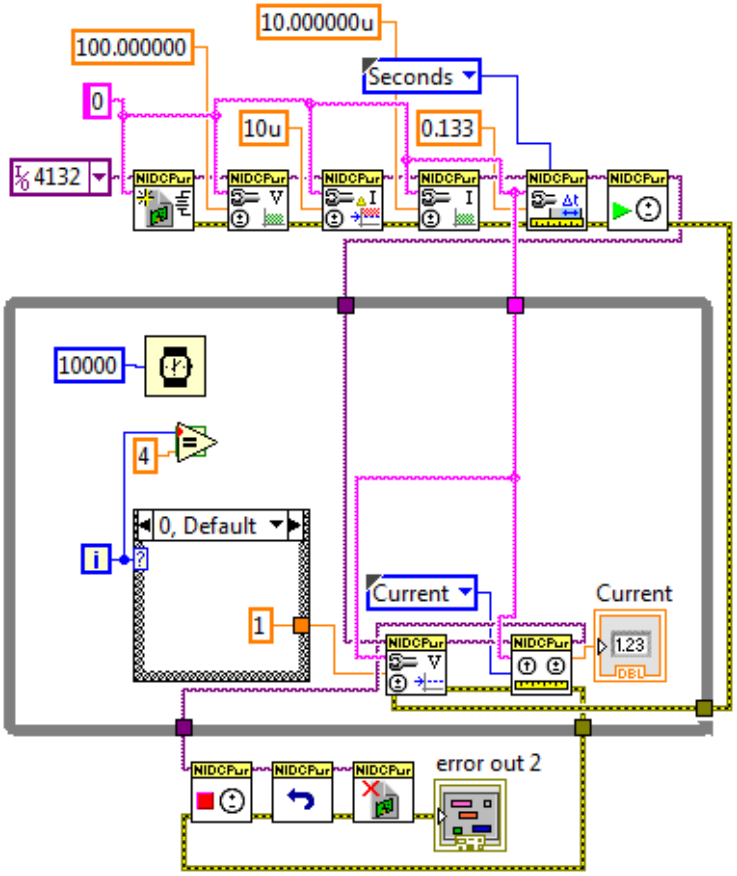


Рис. 4. Блок-диаграмма виртуального прибора LabVIEW для измерения тока МДП-структуры

Таким образом, разработана экспериментальная автоматизированная установка контроля параметров МДП-структур на основе прецизионного источника питания постоянного тока NI PXI-4132, работающего в среде LabVIEW. Разработанная установка позволяет контролировать параметры МДП-структур как в режиме управляемого токового воздействия, так и в режиме воздействия управляемым напряжением.

ЛИТЕРАТУРА

[1] Андреев В.В., Барышев В.Г., Столяров А.А. Инжекционные методы исследования и контроля структур металл-диэлектрик-полупроводник: Монография. // М.: Издательство МГТУ им. Н.Э. Баумана, 2004. – 256 с.

Андреев Владимир Викторович – д-р техн. наук, профессор КФ МГТУ им. Н.Э. Баумана. E-mail: andreev@bmstu-kaluga.ru

Кулагин Владислав Сергеевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: kulagin.vladislav@mail.ru

СЕКЦИЯ 13.

ЗАЩИТА ИНФОРМАЦИИ

И.Л. Луговский, Е.Е. Коваль, А.О. Волкова, М.К. Савкин

RFID АНАЛИЗ ВОЗМОЖНОСТЕЙ ТЕХНОЛОГИИ И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

История развития технологии радиочастотного идентификации начинается в начале 30-ых XX века, когда шотландским физиком сэром Робертом Александром Ватсоном-Ваттом был изобретен первый радар, который позволял узнавать воздушную обстановку на десятки миль. Но технология распознавания была несовершенна (зачастую за самолеты принимались и большие стаи птиц), поэтому нельзя было точно сказать, чей самолет приближается, свой или врага. Первый шаг к определению принадлежности сделали немцы, которые при в хождении в зону действия своего радара совершали «бочку». При этом изменялись параметры отраженного луча, что могло и служило сигналом о подлете своих самолетов. Английские инженеры под руководством Ватсона-Ватта разработали первую активную систему распознавания, которую впоследствии назвали «система свой-чужой». Передатчик на самолете, принимая специальный сигнал от наземной станции наведения, посылал ответ с указанием принадлежности. Так сформировались 2 основных подхода к радиочастотной идентификации – пассивный, где система построена на посылке сигнала и приеме его эха, и активный, где в метку встраивается отдельный передатчик. Развитием данных систем в 60-е годы стала разработка противокражных меток. В этих устройствах задействован всего 1 бит, который указывает на приобретение товара. Но наиболее активным местом стало использование технологии RFID для логистики. Изначально еще в 70-ые годы RFID метки ставились на тару для ядерных материалов, а впоследствии и на автомобили, которые подъезжая к барьеру уже передавали на КПП всю информацию о грузе, данные на водителя и т.д. Впоследствии эту систему коммерциализировали, и она стала использоваться в грузоперевозках на дорогах и мостах во всем мире. Одним из направлений использования RFID технологий стало отслеживание домашних животных (по законам Австралии все домашние животные должны иметь метку и паспорт) и учет крупного рогатого скота (отслеживание прививок); многие товары с помощью меток защищаются от подделок (лекарства и т.д.).

Физические основы RFID. Общий принцип работы любой RFID-системы прост. Основные компоненты системы – это считыватель, идентификатор (карта, метка, брелок, тег). Считыватель излучает в окружающее пространство электромагнитную энергию. Идентификатор принимает сигнал от считывателя и формирует ответный сигнал, который принимается антенной считывателя и обрабатывается. (рис. 1).

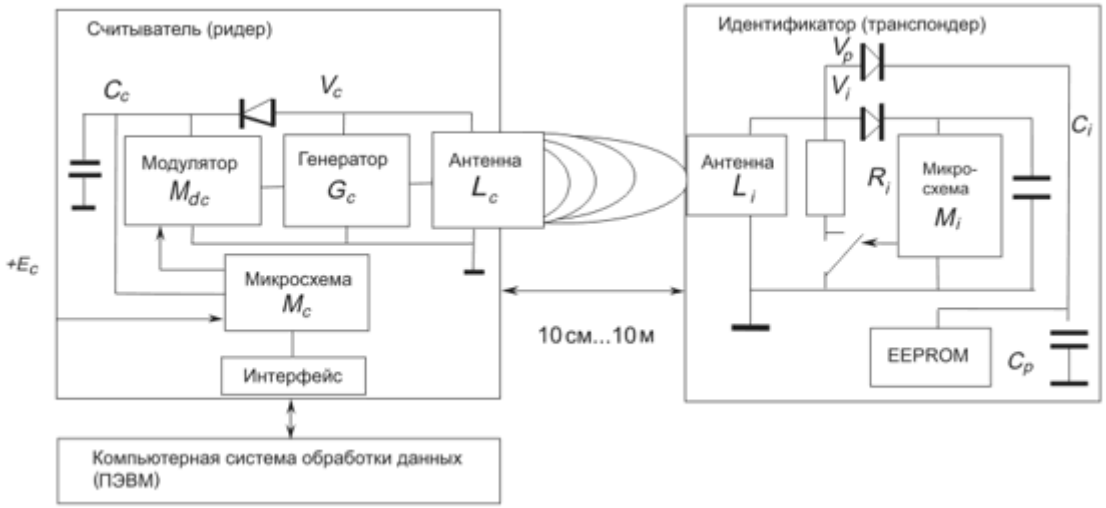


Рис. 1. Принцип работы RFID-системы (1)

Идентификаторы бывают активными или пассивными. Активные работают от присоединенной или встроенной батареи, они требуют меньшей мощности считывателя и, как правило, имеют большую дальность чтения. Пассивная метка функционирует без источника питания, получая энергию из сигнала считывателя. Пассивные метки меньше и легче активных, менее дороги, имеют фактически неограниченный срок службы. В пассивной системе излучение считывателя постоянно во времени (не модулировано) и служит только источником питания для идентификатора. Получив требуемый уровень энергии, идентификатор включается и модулирует излучение считывателя своим кодом, который считывателем и принимается. Активные и пассивные теги могут быть:

- только для чтения;
- с чтением-записью;
- однократно записываемыми, данные в которые могут быть занесены пользователем.

Частотные диапазоны и стандарты

В технологии RFID есть два ключевых определения:

- Proximity (карты и брелки) – идентификаторы малой дальности, как правило, около 10 см. Используются в системах доступа, транспортных приложениях;
- Vicinity – идентификаторы средней дальности (около полутора метров); Используются для идентификации товаров и продукции.

С точки зрения рабочих частот основными являются низкочастотный диапазон (125 или 134 кГц), среднечастотный (13,56 МГц) и высокочастотный (800 МГц … 2,45 ГГц).

Особенности стандартов приведены в табл. 1.

Таблица 1. Общие характеристики RFID-технологии (2)

Стандарт	Частота	Приложения
ISO 14223 ISO 11784/11785	125 (135) кГц	для идентификации животных (в том числе, домашнего скота)
ISO 14443 ISO 15693 ISO 10373	13,56 МГц	смарт-карты
ISO 18000	800 … 2,45 ГГц	метки с увеличенной дальностью

Высокочастотные (850-950 МГц и 2,4-5 ГГц), системы используются там, где требуются большое расстояние и высокая скорость чтения, например, при контроле железнодорожных вагонов, автомобилей, в системах сбора отходов.

Системы промежуточной частоты (10-15 МГц) – используются там, где должны быть переданы большие массивы данных.

Низкочастотные (100-500 кГц). Используются там, где допустимо небольшое расстояние между объектом и считывателем. Обычное расстояние считывания составляет 0,5 м, а для тегов, встроенных в маленькие объекты, дальность чтения, как правило, равна примерно 0,1 м. Большая антенна считывателя может в какой-то мере компенсировать такую дальность действия небольшого тега, но излучение высоковольтных линий, моторов, компьютеров, ламп и т.п. мешает ее работе. Большинство систем управления доступом, бесконтактные карты управления складами и производством используют низкую частоту.

RFID: Перспективы развития. До недавнего времени популяризацию RFID-чипов тормозила их громоздкость и, главное, дороговизна. Компания Hitachi, разработала так называемый mu-chip, имеющий размеры менее четверти квадратного миллиметра и способный обмениваться данными на расстоянии в четверть метра. Малый радиус действия и необходимость подключения внешней антенны ограничивают применение этого продукта торговлей и сферой услуг. Так же японская компания FEC Inc. Разработала RFID-чип Manathir площадью в половину квадратного миллиметра и ценой в 10 центов, пригодного для слежки и за товарами, и за людьми. Радиус его действия не называется, но, очевидно, составляет несколько метров.

Безопасность RFID. Технология RFID, не смотря на свои плюсы, имеет и уязвимости с точки зрения безопасности. Различные протоколы и стандарты призваны сократить риски кражи данных, но сам механизм передачи – открытый эфир – не позволяет этого сделать. Системы, основанные на индивидуальном отклике чипа, так же уязвимы к дублированию посылаемых данных.

Так, например, группа экспертов по безопасности THC/vonJeek представила эмулятор для ePassport. Этот эмулятор позволяет создать резервную копию электронного паспорта. Используя этот инструмент, хакерам

удалось обойти систему безопасности терминалов и создать поддельный паспорт, который успешно прошел таможню.

Интересным выглядит сообщение о появлении устройства Contactless Infusion X5 от хакерской группировки The CC Buddies. Согласно заявлению хакеров, изобретенный скиммер способен считывать информацию со скоростью 15 бесконтактных карт в секунду. X5 является современным RFID-устройством для считывания информации с бесконтактных банковских карт. Считываемые данные хранятся в зашифрованном виде на внутреннем хранилище устройства. В комплект входит набор из 20 пустых пластиковых карт, USB-кабель и драйвер для работы с устройством. В технических характеристиках указано, что устройство способно работать без подзарядки в течение 10 часов, способно считывать информацию с карты любого банка на расстоянии до 8 сантиметров со скоростью 1024Кбит/с.

Считывание данных даже с низкочастотных меток возможно и удаленно, на расстоянии порядка 3-5 метров, что позволяет считать данные с носителя и скопировать их. Далее полученный код записывается в чистый носитель, и злоумышленник получает полный дубликат оригинального ключа. Для этих целей может использоваться как портативные копирайт (ручное устройство по считыванию/записи карт), так и промышленно выпускаемые принтеры, которые помимо записи информации, позволяют напечатать на карте текст или изображение для обеспечения подлинности. Что может привести к проникновению на территорию ограниченного доступа посторонних людей.

Выходы из сложившейся ситуации

Готовые защитные корпусы и бумажники, блокирующие RFID-сигналы.

Такие компании, как, например, Identity Stronghold продают различные аксессуары, которые могут защитить карты от электронных краж. В настоящее время правительство США требует, чтобы все государственные служащие пользовались подобными защитными корпусами для идентификационных карт.

Одноразовый код

Для предотвращения копирования меток RFID и NFC можно использовать криптографию. Одноразовый код или код, непрерывно изменяющийся после каждого сканирования, можно использовать для того, чтобы помешать перехватчикам записывать операции для последующего воспроизведения. Даже если мошенникам удастся украсть одноразовый код, они не смогут им воспользоваться.

Для более сложных устройств также можно использовать аутентификацию методом «запрос-ответ» в тех случаях, когда метка взаимодействует с ридером. При таком типе аутентификации ридер выдает метке запрос, а метка в свою очередь отвечает секретным цифровым кодом, который может быть основан на симметричной или двухключевой криптографии. При

использовании этого протокола информация не передается по небезопасному каналу связи между ридером и меткой.

Технология переключения кредитных карт.

Ученые Инженерной школы Свенсона Питтсбургского университета (Pittsburgh Swanson School of Engineering) разработали метод предотвращения мошенничества с RFID с помощью использования технологии включения и выключения карты при контакте с ее определенным участком при сканировании. Профессор Марлин Микл (Marlin Mickle), доктор технических наук и исполнительный директор Научно-инновационного центра по RFID-технологиями (RFID Center for Excellence) в Школе Свенсона, заявил, что новая технология «позволяет блокировать кредитные карты на основе RFID или NFC, когда они лежат в кармане или на столе, и предотвращает их считывание мошенниками с использованием портативных сканеров». Карту невозможно считать, пока кто-либо не включит ее. Новая разработка включает антенну и электросхему, контакты которой можно разомкнуть простым переключением, как, например, при выключении освещения дома или в офисе. Кредитная карта на основе RFID или NFC блокируется, если она остается в кармане или лежит на какой-либо поверхности, и мошенники не могут считать ее с помощью портативных сканеров. «Это весьма простое и недорогое решение, которое можно использовать в процессе изготовления кредитных карт на основе RFID и NFC. Мы подали заявку на патент и надеемся на скорое внедрение этой технологии после одобрения патента».

Список литературы

[1] *Финкенцеллер*. RFID-технологии. – Додэка XXI –2010. – 57 с.
[2] *Финкенцеллер*. RFID-технологии. – Додэка XXI –2010. – 165 с.
[3] *Финкенцеллер*. RFID-технологии. – Додэка XXI –2010. – 302 с.

Луговский Иван Леонидович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: ivalug@rambler.ru

Коваль Евгений Евгеневич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: ivalug@rambler.ru

Волкова Анастасия Олеговна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: ivalug@rambler.ru

Савкин Михаил Константинович – ассистент кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: savkinmk@gmail.com

Е.А. Коваленко, А.Б. Лачихина

АЛГОРИТМЫ ВОССТАНОВЛЕНИЯ МАТРИЧНЫХ ДАННЫХ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В настоящее время многие стратегические решения в сфере экономического и социального регулирования, базируются на результатах массовых социологических исследований, основанных на массовых опросах или переписях. В качестве примеров подобных исследований можно назвать Всероссийскую сельскохозяйственная перепись, объектами которой являлись сельскохозяйственные структуры всех форм собственности, Российский мониторинг экономики и здоровья, Опрос население по проблемам занятости. Одной из важнейших проблем любого социологического опроса или переписи является достоверность данных, полученных в ходе проведения того или иного исследования. Основным недостатком, характерным для большинства массовых исследований является большое количество частичных пропусков в данных.

Существует несколько причин, по которым возникают пропуски данных. Одной из них является некорректная работа исследователя. Например, неграмотно составленная им анкета, не достаточно подготовленные интервьюеры, а также обилие сенситивных вопросов в анкете. Сенситивными могут считаться любые вопросы, направленные на получение сведений, которые люди обычно предпочитают утаивать. Ответы на личностные или деликатные вопросы чаще бывают неискренними и соответственно ведут к не связанным с выборкой систематическим ошибкам в данных. [4]

Но даже если со стороны исследователя ошибок в организации и проведении этапов предварительной подготовки и непосредственного сбора информации допущено не было, то недостающие данные могут возникнуть по вине респондента в следствие не ответа на тот или иной поставленный вопрос. Причинами для этого могут быть:

- психологические факторы;
- некомпетентность респондента в теме исследования;
- неконтактность респондента;
- нежелание отвечать.

Можно выделить 3 степени состояния данных, полученных в результате исследования:

1. Для первой характерно, что отобранный респондент ответит на абсолютно все вопросы, иначе говоря, мы получим абсолютно полное наблюдение (full response).
2. Для второй - что респондент совсем откажется участвовать в опросе, то есть наблюдение вообще не будет получено (unit –

nonresponse), что приведёт к возникновению проблемы недостижимости объекта.

3. Но, на самом деле, чаще всего имеет место третья, промежуточная ситуация – респондент отвечает только на некоторые вопросы, другие же по тем или иным причинам остаются без ответа. В этом случае мы имеем дело с неполным наблюдением или отдельными пропусками (item/partial nonresponse).

Отдельные пропуски могут быть двух видов: реальные и артефактные. Реальные пропуски возникают, если, несмотря на все усилия, включающие в себя методики стимулирования ответа, а также различные формы вопроса, от респондента не удалось получить ответа на поставленный вопрос. Артефактные, или искусственные пропуски возникают после удаления из массива нереалистичных, заведомо ложных значений, нарушающих логику последовательности ответов, которые приходится удалять самому исследователю на этапе чистки массива

В большинстве ситуаций на практике довольно сложно детерминировать конкретные причины, по которым респонденты не ответили на поставленные вопросы, не рассматривая при этом случаи, когда отсутствия ответов провоцируются искусственно. Существует связь между причиной пропуска и, так называемой, степенью его случайности, а также между степенью случайности пропуска и выбором соответствующего способа борьбы с пропусками. [3]

Выделяются следующие типы пропусков, в зависимости от их случайного или систематического характера:

1. Полностью случайные пропуски (missing completely at random – MCAR). Вероятность возникновения пропуска в ответе на какой-либо вопрос анкеты не зависит ни от истинного ответа, который мог бы быть получен, ни от ответов на другие вопросы. Например, если отобрать из массива респондентов, полностью случайно не ответивших на вопрос, то есть отобрать анкеты с полностью случайными пропусками, то они составят простую случайную выборку из всех опрошенных, не зависящую от наблюдаемых или ненаблюдаемых ответов. Такая независимость исключает систематические различия между людьми, ответившими и не ответившими на вопрос.
2. Неслучайные, систематические пропуски (not missing at random – NMAR). Эти пропуски возникают, если вероятность ответа на вопрос зависит от смысла самого вопроса. Например, респондент может отказаться отвечать на вопрос по личным причинам, которые могут быть обусловлены боязнью общественного порицания или нежеланием разглашать какую-либо информацию о себе. Вместе с тем неслучайные пропуски могут быть обусловлены ошибками в формулировке вопроса.

3. Случайные пропуски (missing at random – MAR). Эти пропуски отличаются от полностью неслучайных тем, что они обусловлены известными значениями других переменных, но не связаны с переменной, значение которой пропущено. Например, в анкете необходимо указать свой возраст. В этом случае неуказание своего возраста будет случайным, если его вероятность зависит от пола респондента, но не зависит от его истинного возраста.

Проблему наличия пропусков в данных массовых социологических исследований нельзя недооценивать. Наличие пропусков в данных чревато различными негативными последствиями, которые в большинстве случаев влияют на качество всего исследования. Среди них можно назвать следующие:

- сокращение общего размера доступной для анализа выборки;
- потеря в качестве результатов из-за снижения валидности статистических выводов, то есть обоснованности и пригодности результатов исследования;
- в некоторых случаях − возникновение в данных систематической ошибки измерения;
- ограничения в применении некоторых видов анализа.

Процесс заполнения пропусков после этапа сбора данных называют ремонтом выборки. Существует три основных подхода к работе с пропусками: исключение неполных наблюдений, взвешивание данных и импутирование.

1. Исключение неполных наблюдений. При этом подходе наблюдения, для которых отсутствуют значения хотя бы одного признака, исключаются из анализа. Такой метод может быть применим только если малая часть объектов выборки имеет пропущенные значения. Преимуществом данного подхода является простота реализации. Также, надо отметить, что, не пытаясь восстановить отсутствующие данные каким-либо способом, нельзя в значительной степени повлиять на анализ выборки. Но при этом нужно учесть, что это справедливо только для полностью случайных и случайных пропусков в данных. Недостатком подхода является то, что при его применении теряется информация по признакам, не содержащим пропущенных значений, поскольку наблюдение удаляется целиком.
2. Взвешивание данных. Суть этого подхода заключается в том, что исследователь сначала удаляет все неполные наблюдения, а затем использует оставшиеся данные во взвешенном виде, то есть неполные анкеты заменяются другими, взятыми из имеющихся полностью заполненных. При этом подходе структура выборочной совокупности по переменной, в значениях которой были пропуски, смещается в сторону той структуры, которая имеет место для пол-

ных наблюдений относительно это же переменной, что является недостатком данного метода.

3. Импутирование. Является более прогрессивным и активно развивающимся подходом, в отличие от двух предыдущих. Его смысл заключается в восстановлении пропущенных данных. Существует множество способов заполнения пропусков, после применения которых массив данных обрабатывается, не принимая во внимание различия между изначально полными наблюдениями и наблюдениями, в которых были пропуски. Недостаток этого метода заключается в возникновения в результате его применения смещений в структуре массива относительно реальной ситуации. Однако заполнение пропусков позволяет получить массив полных данных и реализовывать на нем методы анализа данных, требующие их абсолютной полноты, что является преимуществом импутирования. [1]

На данный момент разработано уже большое количество разнообразных алгоритмов заполнения пропущенных данных. Проблема выбора подходящего алгоритма заключается в том, что эффективность каждого из них в конкретных исследовательских ситуациях можно оценить только экспериментально. Для этого необходимо сравнить результаты, полученные после заполнения определенным способом искусственно внесённых в массив пропусков, с результатами, полученными на массиве полных данных до внесения в него искусственных пропусков. [2]

Список источников

[1] Luengo J., Garcia S., Herrera F. On the choice of the best imputation methods for missing values considering three groups of classification methods

[2] Злоба Е., Яцкив И. Статистические методы восстановления пропущенных данных

[3] Литтл Р.Дж.А., Рубин Д.Б. Статистический анализ данных с пропусками

[4] Лачихина А.Б., Твердова С.М. Поддержание целостности информации в базах данных корпоративных информационных систем. // Вопросы радиоэлектроники. – 2014. – серия ОТ, выпуск 4. с. 137-146.

Коваленко Елизавета Александровна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: www.yoursmile@yandex.ru

Лачихина Анастасия Борисовна – канд. техн. наук, доцент кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: anastasialach73@gmail.com

П.А. Чувак, О.Ю. Жарова

АЛГОРИТМЫ РАСПОЗНОВАНИЯ ЛИЧНОСТИ ПО ФОТО

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Идентифицировать личность человека по изображению лица является одной из самых популярных технологий. Она востребована в области систем безопасности, где её применение включает контроль доступа на охраняемые объекты, поиск человека в архиве системы видеонаблюдения, подтверждение личности по биометрическому паспорту и многое другое.

Несмотря на большое разнообразие представленных алгоритмов, можно выделить общую структуру процесса распознавания лиц:

Рис. 1. Общий процесс обработки изображения лица при распознавании

На первом этапе производится детектирование и локализация лица на изображении. На этапе распознавания производится выравнивание изображения лица (геометрическое и яркостное), вычисление признаков и непосредственно распознавание – сравнение вычисленных признаков с заложенными в базу данных эталонами. Основным отличием всех представленных алгоритмов будет вычисление признаков и сравнение их совокупностей между собой.

Нейронные сети. Нейронные сети способны классифицировать полученное изображение в соответствии с предварительным обучением сети. Обучаются нейронные сети на наборе обучающих примеров. В процессе обучения происходит извлечение ключевых признаков, определение их важности и построение взаимосвязей между ними. Наилучшие результаты в области распознавания лиц показала сверочная нейронная сеть, обеспечивающая частичную устойчивость к смене ракурса, изменения масштаба, смещениям, поворотам и прочим искажениям изображения. Минусом данного метода является проблема с обучением сети. Добавление нового эталона в базу требует полного переобучения сети, что является достаточно длительной процедурой.

Метод гибкого сравнения на графах. В основе метода лежит эластичное сравнение графов, описывающих изображение лиц. Лица на изображении представлены в виде графов с взвешенными вершинами и ребрами. На этапе распознавания эталонный граф остается неизменным, в то время как другой деформируется с целью подгонки к эталонному.

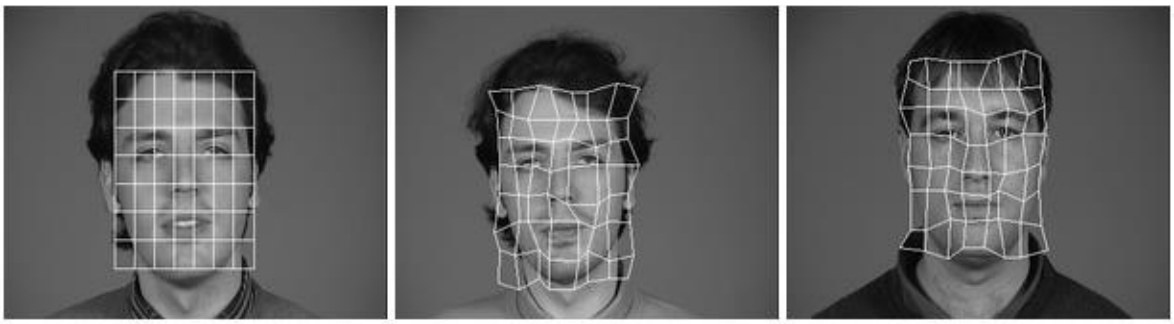


Рис. 2. Пример деформации графа в виде регулярной решетки

Далее в вершинах графа вычисляются значения признаков. Обычно для этих целей используют фильтры Габора. Ребра графа взвешиваются расстояниями между смежными вершинами, после чего происходит деформация графа и выбор такой его позиции, при котором разница между значениями признаков в вершине эталонного графа будет минимальна. Данный метод предназначен для слежения за лицом в реальном времени. И минусам данного метода можно отнести линейную зависимость между скоростью работы и размером базы данных лиц и низкую технологичность при запоминании новых эталонов.

Скрытые Марковские модели. Модели являются одним из статистических методов распознавания личности. Скрытые Марковские модели используют статистические свойства сигналов и учитывают их пространственные характеристики. Модель состоит из множества скрытых и наблюдаемых состояний, матрицы переходных состояний и начальной вероятности состояний. Каждому соответствует своя Марковская модель. При распознании личности проверяются сгенерированные для базы данных Марковские модели и происходит поиск максимальной наблюдаемой вероятности того, что последовательность наблюдений для объекта сгенерирована соответствующей моделью. К минусам данного метода можно отнести необходимость подбора параметров модели для каждой базы данных, к тому же данный алгоритм максимизирует отклик на свою модель, но не минимизирует отклик на другие модели.

Метод главных компонент. Применение данного метода для идентификации личности имеют следующий вид. Сначала весь обучающий набор лиц преобразуется в одну общую матрицу данных, где каждая строка представляет собой один экземпляр изображения лица, разложенного в строку.

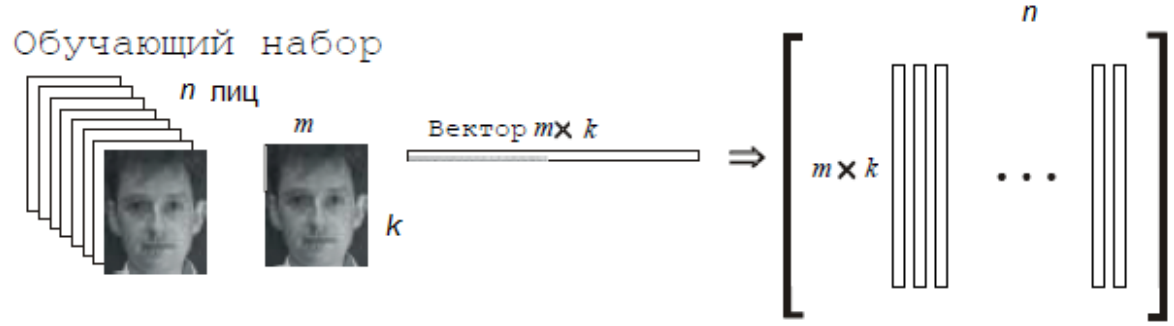


Рис. 3. Преобразования обучающего набора лиц в одну общую матрицу X

Входные векторы представляют собой отцентрированные и приведённые к оному масштабу изображения лиц. Вычисляются собственные векторы, называемые собственными лицами. С помощью вычисленных ранее матриц входное изображение разлагается на набор линейных коэффициентов, называемых главными компонентами. Для изображения лица вычисляют его главные компоненты. Процесс распознавания заключается в сравнении главных компонент неизвестного изображения с компонентами всех остальных изображений в базе данных. Метод главных компонент на данный момент является одним из самых продуманных и коммерчески успешных методов. К минусам данного метода можно отнести падение эффективности метода при значительных изменениях освещенности пространства на изображении или изменение выражения лица.

Активные модели внешнего вида (Active Appearance Models, AAM). AAM - это статистические модели изображений, которые путем разного рода деформаций могут быть подогнаны под реальное изображение. Первоначально активные модели внешнего вида применялись для оценки параметров изображений лиц. Активная модель внешнего вида содержит два типа параметров: параметры, связанные с формой (параметры формы), и параметры, связанные со статистической моделью пикселей изображения или текстурой (параметры внешнего вида). Перед использованием модель должна быть обучена на множестве заранее размеченных изображений. Разметка изображений производится вручную. Каждая метка имеет свой номер и определяет характерную точку, которую должна будет находить модель во время адаптации к новому изображению.

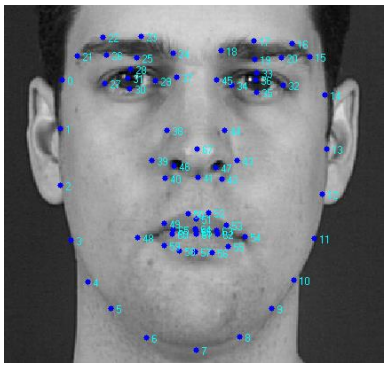


Рис. 4. Пример разметки изображения лица из 68 точек, образующих форму AAM

Несмотря на то, что в идеальных условиях различающая способность всех вышеперечисленных методов колеблется от 50% до 97% процесс распознания испытывает ряд серьезных проблем. К основным проблемам можно отнести изменчивость визуальных образов, связанную с изменениями освещенности и ракурсов наблюдения, и возникновение неоднозначности, связанной с проектированием трехмерных объектов на плоские изображения.

У всех методов идентификации личности примерно одинаковый процент распознавания, но из-за определённых сложностей в архитектуре методов они имеют разный круг применения. Так скрытые Марковские модели из-за низкой минимизации отклика на другие модели походят только в обучающих целях. Метод гибкого сравнения на графах из-за линейной зависимости скорости работы от размера базы данных подойдет для создания приложений для предприятий с малым штатом сотрудников. Метод главных компонент подойдет для распознавания личности в местах со стабильным окружающим фоном и освещением. Нейронные сети подойдут большим корпорациям из-за дороговизны в реализации.

Список литературы

[1] Анализ существующих походов к распознаванию лиц [Электронный ресурс]. URL: http://habrahabr.ru/company/synesis/blog/238129/

[2] Методы распознавания человека по изображению лица. Достоинства и недостатки, сравнение [Электронный ресурс]. URL: http://house-control.org.ua/article/3289/metody-raspoznavaniya-cheloveka-po-izobrajeniyu-lica--dostoinstva-i-nedostatki-sravnenie/

[3] Активные модели внешнего вида [Электронный ресурс]. URL: https://habrahabr.ru/post/155759/&post=5385365_18497/

Чувак Павел Андреевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: chuvak-pascha@ya.ru

Жарова Ольга Юрьевна – ассистент кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: ouzharova@yandex.ru

О.С. Клочко, И.С. Силкина

АНАЛИЗ МЕТОДОВ ОБФУСКАЦИИ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Проблема защиты программного обеспечения от обратной разработки всегда была актуальна и повсеместна. В современном мире методами анализа программного обеспечения для его последующей обратной разработки является динамический и статический анализы.

Статический анализ исследования обычно связан с изучением файлов программного продукта. В качестве исходных данных для статического анализа может быть использован код программы, а также это может быть различная метаинформация или сопровождающая программное обеспечение документация.

Динамический анализ предполагает исследование программы во время работы. При этом подходе изучаются обращения программы к памяти, потоки данных, которыми обмениваются процессы программы в ходе её работы.

Популярным методом защиты от статического и динамического анализа является обфускация программ.

Обфускация (от лат. obfuscare – затенять, затемнять; и англ. obfuscate – делать неочевидным, запутанным, сбивать с толку) или запутывание кода – приведение исходного текста или исполняемого кода программы к виду, сохраняющему её функциональность, но затрудняющему анализ, понимание алгоритмов работы и модификацию при декомпиляциях. [1]

Задача обфускации программ заключается в разработке таких преобразований, которые сохраняют функциональные характеристики программ, но при этом делают невозможным или чрезвычайно трудоемким извлечение из открытого текста программы ключевой информации об устройстве содержащихся в ней алгоритмов и структур данных. Именно сочетание этих двух противоположных качеств – общедоступного кода программы (синтаксиса) и защищенного ее содержания (семантики) – открывает обфускирующим преобразованиям программ широкие возможности применения в криптографии и компьютерной безопасности. [2]

Принято выделять следующие уровни процесса обфускации:

- низший уровень – механизм обфускации осуществляется над ассемблерным кодом программы, или непосредственно над двоичным файлом программы, хранящим машинный код.
- высший уровень – механизм обфускации осуществляется над исходным кодом программы, написанном на языке высокого уровня.

Большое количество методов и алгоритмов обфускации могут найти применение для реализации защиты программного кода с помощью меха-

низма обфускации на обоих уровнях – и на низшем, и на высшем. Однако в отдельных случаях подвергать обфускации весь программный код нецелесообразно (например, причиной может послужить значительное снижение времени выполнения программы), во избежание подобных инцидентов стоит осуществлять обфускацию отдельных, наиболее важных участков программного кода.

К обфускации программ предъявляются три главных требования:

- сохранение функциональности программы;
- полиномиальное замедление;
- требование стойкости.

Существуют различные способы преобразования программ, следовательно, данный процесс подразделяется по видам (способам) такого преобразования.

1. Лексическая обфускация. Наиболее простая, заключается в изменении исходного кода программы для приведения его к нечитабельному виду. Включает в себя: удаление комментариев или изменение их на дезинформирующие; удаление отступов и пробелов; замена имён идентификаторов (имён переменных, функций, процедур и т. д.) на длинные наборы символов, сложных для визуального восприятия; изменение расположения блоков программы.

2. Обфускация данных. Данный тип обфускации связан с изменением структур данных. Является более сложной, чем лексическая, однако наиболее используемой. Этот вид обфускации делится на 3 группы:

- Обфускация хранения. Заключается в трансформации хранилищ данных, а также самих типов данных (например, создание и использование необычных типов данных, изменение представления существующих и т. д.);
- Обфускация соединения. Один из важных этапов в процессе реверсивной инженерии программ, основан на изучении структур данных. Поэтому важно постараться в процессе обфускации усложнить представление используемых программой структур данных. Например, при использовании обфускации соединения это достигается благодаря соединению независимых данных или разделению зависимых;
- Обфускация переупорядочивания. Заключается в изменении последовательности объявления переменных, внутреннего расположения хранилищ данных, а также переупорядочивании методов, массивов, определенных полей в структурах и т. д.

3. Превентивная обфускация. Данный вид обфускации предназначен для предотвращения успешного применения деобфускаторов к коду программного продукта. Нацелен на использование недостатков часто используемых программных средств деобфускации. [3]

Интенсивное развитие информатизации и глобальное проникновение информационных технологий в нашу жизнь ставят перед нами все новые задачи по обеспечению информационной безопасности для повышения стойкости к автоматическим средствам защиты и организации более высокого быстродействия защищенной программы. [4] Современный опыт решения проблем показывает, что для достижения наибольшего эффекта при организации информационной безопасности необходимо верно выбрать инструменты и методы защиты программного кода. Механизм обфускации является одним из самых популярных и часто используемых инструментов защиты информации на сегодняшний день, поэтому следует подробно рассмотреть и проанализировать существующие методы обфускации, чтобы выбрать наиболее подходящий в каждом отдельном случае.

Список литературы

[1] Обфускация (программное обеспечение) // Википедия. [2016–2016]. Дата обновления: 05.09.2016. URL: http://ru.wikipedia.org/?oldid=80636250 (дата обращения: 17.09.2016).

[2] Варновский Н. П., Захаров В. А., Кузюрин Н. Н., Шокуров А. В. Современные методы обфускации программ: сравнительный анализ и классификация. *Известия Южного федерального университета. Технические науки*, 2007, Т.1, №1, С.93.

[3] Никольская К.Ю., Хлестов А.Д. Обфускация и методы защиты программных продуктов. *Вестник УрФО. Безопасность в информационной сфере,* 2015, №2(16), С.8-9.

[4] Щелкунов Д.А. *Разработка методик защиты программ от анализа и модификации на основе запутывания кода и данных*. Дис. ... к.т.н. Москва, 2009, с 10-15

Клочко Ольга Сергеевна – ассистент кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: klochkoolgakaluga@gmail.com

Силкина Ирина Семеновна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: www.irina.net@yandex.ru

В.Л. Бухман, О.С. Клочко

АНАЛИЗ УГРОЗ И СРЕДСТВ ЗАЩИТЫ БАНКОВСКИХ СИСТЕМ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Банки играют ключевую роль в экономической системе современного общества. Однако их деятельность всегда была связана с определенными рисками атак со стороны злоумышленников. Ранее, все банковские операции проводились только с использованием бумажных денежных средств, поэтому банкам угрожала только опасность, связанная с физическим хищением денег. С течением времени происходило техническое развитие, что также затронуло и сферу банков. В настоящее время каждый банк оборудован множеством различных технических средств, хранящих или обрабатывающих конфиденциальную информацию. К конфиденциальной информации в первую очередь относятся персональные данные о клиентах, о их вкладах и о всех операциях. Это частично решило проблему с физической кражей денег, однако появились и другие более опасные угрозы. Анализируя банковскую систему можно выделить ряд основных угроз безопасности [1]:

1. Угроза несанкционированного доступа – получение доступа к информации лицами, не имеющими права на нее;
2. Умышленное или случайное искажение банковской информации;
3. Умышленное или случайное уничтожение банковской информации.

Угроза несанкционированного доступа. На сегодняшний день этот вид угроз является самым распространенным и может привести к большим финансовым потерям. Получение конфиденциальной информации может осуществляться различными способами: физический доступ к местам обработки и хранения информации, несанкционированный доступ сотрудников банка, получение доступа к резервным копиям.

К физическим способам получения информации чаще всего относят установка специального оборудования для электромагнитного съема информации, хищение физических носителей информации либо злоумышленниками, либо сотрудниками банка и даже примитивное вооруженное нападение с целью хищения информации или денег.

Несанкционированный доступ сотрудниками является наиболее вероятным и простым способом получения информации. Нередко сотрудники банка обладают высоким уровнем доступа. Данными сотрудниками являются администраторы. Однако эта привилегия может использоваться не только для выполнения служебных обязанностей, но и для более простого хищения информации. Кроме того, не только умышленные действия могут нанести ущерб. Простое несоблюдение правил безопасности информации

сотрудниками также может повлечь за собой серьезные проблемы. К таким нарушениям относится копирование информации с целью работы дома.

Практически во всех банках предусмотрено резервное копирование данных. Это является полезным инструментом во многих случаев, начиная от ошибочных действий сотрудника при работе с базой данных, заканчивая отключением питания здания и потери некоторых данных. Однако данная опция может нести огромную угрозу. Чаще всего резервные копии хранятся в отдельном помещении. В ряде случаях доступ к этому помещению менее защищен, что является ошибкой. Хоть и информация хранящиеся на данных носителях не является актуальной, она все равно представляет большую ценность.

Умышленное или случайное искажение банковской информации. Искажение информации чаще всего является следствием некомпетентностью сотрудников. Работники банка могут допустить ошибку при работе с информацией или при вводе данных и просто не заметить этого. Тем не менее, не стоит перекладывать вину только на них. Существуют ситуации, когда искажение информации тоже может стать целью злоумышленников. К способам искажения информации относятся ввод неверных данных, специальное вредоносное аппаратное или программное оборудование, подделка документов.

Умышленное или случайное уничтожение банковской информации. Причинной возникновения данного вида угроз являются не только программные сбои и другие события, не зависящие от человека, но и специальные компьютерные вирусы, нацеленные на уничтожение конфиденциальных данных. Троянские кони – один из видов вредоносного программного обеспечения, скрывающиеся под видом полезного приложения, но наносят вред операционной системе и базам данных и в некоторых случаях способны копировать и передавать злоумышленнику пользовательскую информацию. Также к компьютерным вирусам относятся компьютерные черви. Особенностью червей является их самовоспроизведение на компьютерах или через компьютерные сети. Так как каждая воспроизведенная копия также имеет возможность создавать червей, то заражение компьютера происходить очень быстро. Существует множество различных компьютерных червей, большая часть из которых направлена на разрушение [2].

Средства защиты. В большинстве случаях банки уделяют внимание физической защите. Это уменьшает риск получения доступа физическим путем, в то же время сервера с базами данных имеют такую же ценность, что и сейфы в банках, поэтому нужно использовать различные виды средств защиты [3].

Средства защиты делятся на четыре вида: программные, технические (аппаратные), аппаратно-программные и организационные средства. Программные включают в себя программы для идентификации, шифрование информации, контроля доступа, тестирование системы, удаление времен-

ных файлов. Под аппаратными или техническими подразумеваются средства, решающие проблемы защиты информации на уровне оборудования: защита от прослушивания, предотвращают физическое проникновения, защита утечки информации, маскировка данных. Смешанные аппаратно-программные средства защиты объединяют в себе свойства предыдущих видов. Организационные средства защиты информации сочетают организационно технические (прокладка кабельной системы и др.) и организационно правовые средства (правила работы, установленные руководством) [4].

При выборе средств защиты аппаратные и аппаратно-программные системы превосходят программные по характеристикам. Это обосновывается тем, что эти системы в большинстве случаях специализированы, т.е. выполняют строго определенные функции. Специализированные системы имеют преимущество в том, что гарантируют высокую надежность, независимость от субъективных факторов и высокую устойчивость к модификации. Кроме того, еще одно преимущество этих систем – физическая и логическая изоляция важных блоков. При всех положительных свойствах аппаратной и аппаратно-программных систем нужно еще учитывать экономическую составляющую и гибкость системы. Чаще всего, по причине экономии, банки используют программные средства, т.к. стоимость специализированных аппаратных модулей достаточно высока. При использовании программных средств защиты информации гарантируется гибкость, надежность, простота установки и достаточный уровень защиты. Также эти системы имеют преимущество в возможности изменения в сторону усложнения или упрощения, в зависимости от необходимой защиты. Однако эти системы ограничены в функциональности сети, высокая чувствительность к изменениям и зависимость от типов аппаратных средств.

Таким образом, проанализировав структуру банковских систем можно выделить основные средства защиты информации [5]:

- Надежное специализированное программное обеспечение;
- Антивирусное программное обеспечение;
- Физическая защита для защиты от механических повреждений, хищения;
- Программы специального шифрования информации [6];
- Аутентификация пользователей – проверка подлинности пользовательской информации;
- Тщательный обор и контроль персонала, имеющего доступ к данным;
- Резервное копирование информации и надежная защита носителей;
- Разграничение прав и привилегий пользователей на доступ к информации;
- Тестирование операционных систем;
- Контроль подключаемых внешних носителей информации.

В результате изучения данной темы можно сделать следующий вывод: обеспечение информационной безопасности является важнейшей задачей каждого банка. Для достижения данной цели необходимо учитывать недостатки различных систем. Кроме того, нужно принимать во внимание, что не все банки могут позволить себе наилучшие компоненты защиты. Но в таком случае, всегда существуют аналоги, гарантирующие достаточную защиту конфиденциальной информации.

Список литературы

[1] Информационный ресурс Объединенный Кредитный Банк https://oaookb.ru/articles/sposoby-zashchity-bankovskoy-informacii

[2] Информационный ресурс Лаборатория Касперсого http://www.kaspersky.ru/internet-security-center/threats/viruses-worms

[3] Федеральный закон РФ "О персональных данных", N 152-ФЗ от 27.07.2006.

[4] Информационный ресурс ИНТУИТ Национальный открытый университет

[5] Информационный ресурс Журнал Хакер https://xakep.ru/2001/04/03/12274/
www.intuit.ru/studies/higher_education/3406/courses/57/lecture/1688

[6] ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

Бухман Владислав Леонидович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: vladislav.buhman@outlook.com

Клочко Ольга Сергеевна – ассистент кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: klochkoolgakaluga@gmail.com

В.А. Шавернев, К.А. Празян

ВИРУС-ШИФРОВАЛЬЩИК

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Введение. Компьютерный вирус был назван по аналогии с биологическими вирусами за сходный механизм распространения. По-видимому, впервые слово «вирус» по отношению к программе было употреблено Грегори Бенфордом (Gregory Benford) в фантастическом рассказе «Человек в шрамах», опубликованном в журнале Venture в мае 1970 года.

Компью́терный ви́рус – вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи [1].

Как правило, целью вируса является нарушение работы программно-аппаратных комплексов: удаление файлов, приведение в негодность структур размещения данных, блокирование работы пользователей или же приведение в негодность аппаратных комплексов компьютера. Сами по себе вирусы как компьютерная угроза сегодня никого не удивляют. Но если раньше они воздействовали на систему в целом, вызывая сбои в ее работоспособности, сегодня, с появлением такой разновидности, как вирус-шифровальщик, действия проникающей угрозы касаются больше пользовательских данных. Он представляет собой, быть может, даже большую угрозу, чем деструктивные для Windows исполняемые приложения или шпионские апплеты.

Основная часть.Вирусы-шифровщики впервые появились в 2004 году, они использовали достаточно простые методы шифрования, а порой шифрование попросту не было и злоумышленники, лишь только запугивали своих жертв, заставляя последних выплачивать им деньги. Основное распространение получили так называемые вирусы вымогатели-шифровальщики под названием Ransom.Gpcode, Ransom.CryFile и др. (это целая группа вирусов Ransom), заражение которым участились в последнее время. При попадании на компьютер данный вирус шифрует все файлы (Microsoft Word “doc”, Microsoft Excel “xls”, картинки и фотографии “jpg, jpeg, png, gif”, файлы базы данных 1С Бухгалтерии, видео файлы “avi, mkv, mov”, аудио файлы “mp3, wav”). На сегодняшний день большинство вирусов-шифровальщиков имеют алгоритм шифрования RSA1024 + AES256 и расшифровать их без закрытой части ключа, известной только злоумышленнику, невозможно.

Заражение чаще всего происходит через вложение электронного письма. В заголовке письма учитывается специфика интересов и род занятий конкретного пользователя, то есть через сеть интернет злоумышленник

может узнать, чем занимается конкретный адресат, и, чтобы письмо было открыто наверняка, в теме используются ключевые слова. Например, на адрес компании housebuild@yandex.ru, которая занимается строительством домов в тему сообщения может быть добавлена ключевая фраза «Предложение по застройке». Такое письмо будет открыто и вирус начнет свое дело. К письму обязательно прикрепляется вложение в виде файла с расширением: .rar. При скачивании и открытии такого архива происходит запуск, приложения такого же формата, что и вложенный в архиве. При этом многие, как платные популярные, так и бесплатные антивирусные программы, к сожалению, пропускают данный вирус. Об этом свидетельствуют посетители форумов антивирусных компаний. В тот же момент запускался шифровальщик, работу которого можно увидеть по достаточно интенсивному обращению к жесткому диску компьютера. В это время программа сканирует жесткий диск на наличие файлов интересующих форматов и шифровать их таким образом, что спустя некоторое время эти файлы перестают запускаться, а пользователь остается без данных, сохраненных на локальном диске. В тоже время на рабочем столе появляется текстовый файл с инструкцией решения проблемы с помощью перечисления денег на указанный кошелек. Проблема заключается в том, что, когда компьютер уже будет заражен, тогда только антивирус может отреагировать, а может отреагировать и через 1 или 3 дня.

Приведем примеры ответов известных антивирусных компаний:

Ответ **лаборатории Касперского**:

Файлы зашифрованы Trojan-Ransom.Win32.Shade. Для шифрования он использует криптографически стойкий алгоритм, поэтому расшифровка данных, к сожалению, не представляется возможной. Если нет заранее созданных резервный копий пострадавших файлов, можно попробовать воспользоваться встроенным в Windows механизмом «предыдущие версии файлов»: windows.microsoft.com/ru-ru/windows/previous-versions-files-faq [2].

Ответ **лаборатории Drweb**:

Никаких способов расшифровать такое на данный момент не известно. Ведутся исследования. Прогноз, к сожалению, плохой: никаких даже путей для разработки декриптора не видно. Если мы когда-нибудь всё-же получим какую-либо практически полезную для расшифровки вашей информации, мы вам сообщим. Какие действия необходимо произвести чтобы данного заражения не происходило? К сожалению, в мире не существует антивирусов, способных обеспечить 100% зашиту информации от воздействия вредоносных программ, и в частности «энкодеров». Это если говорить об антивирусах. Но задача обеспечения информационной безопасности не может быть решена одними только антивирусными средствами. Как минимум, помимо всего прочего, должно быть организовано резервное копирование данных. Бэкап, выполняемый в соответствии с хорошей практикой резервного копирования: в каждый момент времени должны

существовать минимум две (последняя и предпоследняя) резервных копии; бэкап нельзя хранить в той системе, для которой он создан; и т.д. по учебнику. Общая рекомендация: обратитесь с заявлением в территориальное управление «К» МВД РФ; по факту несанкционированного доступа к компьютеру, распространения вредоносных программ и вымогательства [3].

Авторы, разрабатывающие вредоносное программное обеспечение, все чаще применяют анонимную сеть Tor для сокрытия реального расположения их командно-контрольных серверов.

The Tor Hidden Service - это протокол, который позволяет пользователям устанавливать собственные сервисы, как правило, это веб-сервисы, однако обратиться к ним можно только через саму сеть Tor и через хосты, заканчивающиеся на псевдо-доменное разрешение: .onion. Данный протокол был создан с целью сокрытия реального IP-адреса посредством скрытого сервиса, который явно закрывает IP-адреса клиентов и серверов, работающих друг с другом. Сам трафик между Tor-клиентом и скрытым сервисом Tor маршрутизируется случайным образом через сеть шлюзов, которые выбираются в различных вариантах, причем шлюзами могут быть и обычные компьютеры в сети. Таким образом, установить местоположение сервера на практике почти невозможно.

Заключение. Проблема вирусов на сегодняшний день актуальна. Люди создают их быстрее, чем антивирусные программы. Исследовав вирус-шифровальщик можно убедиться, что развитие вирусов не стоит на месте, они становятся умнее и борьба с ними требует не только больших материальных затрат, но и хороших специалистов.

Список литературы

[1] Косарёв В.П. – «Компьютерные сети и системы» М. 2000 г.

[2] https://forum.kaspersky.com/index.php?showforum=7

[3] http://forum.drweb.com/

Шавернев Виктор Алесандрович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: vladislav. barus625@gmail.com

Празян Константин Арменович – ассистент кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: prazyan.konstantin@gmail.com

О.Ю. Жарова, И.С. Хлыстов

ГЕНЕТИЧЕСКИЕ АЛГОРИТМЫ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Оптимизационная задача – задача, в которой необходимо найти решение, в некотором смысле наилучшее или оптимальное из множества альтернатив. Наилучшего решения во всех смыслах быть не может. Оно может быть признано оптимальным на основе критерия (меры оценки исследуемого явления) или целевой функции [2].

Генетический алгоритм - это эвристический алгоритм поиска, используемый для решения задач оптимизации и моделирования путём случайного подбора, комбинирования и вариации искомых параметров с использованием механизмов, аналогичных естественному отбору в природе. Является разновидностью эволюционных вычислений, с помощью которых решаются оптимизационные задачи с использованием методов естественной эволюции, таких как наследование, мутации, отбор и кроссинговер [2].

Задача формализуется таким образом, чтобы её решение могло быть закодировано в виде вектора генов, где каждый ген может быть битом, числом или неким другим объектом.

Этапы генетического алгоритма [4]:

1. Создание начальной популяции.

Нужно случайным образом создать начальную популяцию, даже если она окажется совершенно неконкурентоспособной. Итогом первого шага является популяция H, состоящая из N особей.

2. Отбор (селекция).

На этапе отбора нужно из всей популяции выбрать определённую её долю, которая останется «в живых» на этом этапе эволюции. Вероятность выживания особи h должна зависеть от значения функции приспособленности $Fitness(h)$. Сама доля выживших s обычно является параметром генетического алгоритма, и её просто задают заранее. По итогам отбора из N особей популяции H должны остаться sN особей, которые войдут в итоговую популяцию H'. Остальные особи погибают.

3. Размножение (скрещивание или кроссинговер).

Размножение в генетических алгоритмах обычно половое – чтобы произвести потомка, нужны несколько родителей, обычно два. Размножение в разных алгоритмах определяется по-разному и зависит от представления данных. Главное требование к размножению – чтобы потомок или потомки имели возможность унаследовать черты обоих родителей, «смешав» их каким-либо способом. Для размножения обычно выбираются особи из всей популяции H.

4. Мутирование.

К мутациям относится все то же самое, что и к размножению: есть некоторая доля мутантов m, являющаяся параметром генетического алгоритма, и на шаге мутаций нужно выбрать mN особей, а затем изменить их в соответствии с заранее определёнными операциями мутации.

Этот набор действий с пункта 2 до пункта 4 повторяется несколько циклов (поколений), пока не будет выполнен критерий остановки алгоритма.

Критерии остановки алгоритма:

1. Нахождение глобального или оптимального решения.
2. Исчерпание числа поколений, отпущенных на эволюцию.
3. Исчерпание времени, отпущенного на эволюцию.

Генетическое программирование – это методика машинного обучения, прототипом которой является биологическая эволюция. В общем случае всё начинается с большого набора программ (популяция), сгенерированных случайным образом или написанных вручную, о которых известно, что это достаточно хорошие решения. Затем эти программы конкурируют между собой в попытке решить некоторую поставленную пользователем задачу. По завершении состязания составляется ранжированный список программ – от наилучшей к наихудшей [1].

Программы, которые необходимо тестировать, подвергать мутациям и скрещиванию, сначала преобразуют в дерево разбора. Каждый узел представляет либо операцию над дочерними узлами, либо является листовым, например, параметром или константой (Рис. 1) [3].

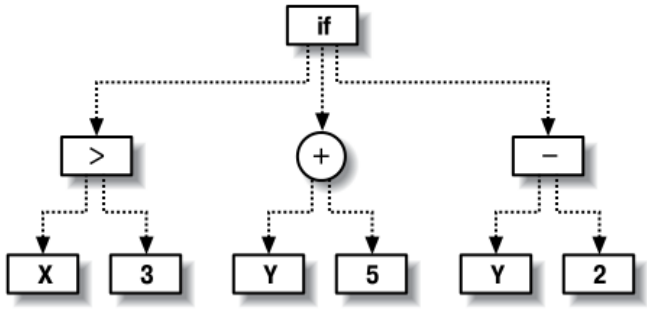


Рис. 1. Программа, представленная в виде дерева разбора

Этапы генетического программирования:

1. Создание начальной популяции.

Программы для генетического программирования можно создавать и вручную, но обычно начальная популяция состоит из случайно сгенерированных программ. Это упрощает запуск процесса, поскольку отпадает необходимость проектировать несколько программ, которые почти решают задачу. Кроме того, таким образом в начальную популяцию вносится разнообразие, тогда как разные программы для решения одной задачи, написанные одним программистом, скорее всего, были бы похожи и, хотя дава-

ли бы почти правильный ответ, идеальное решение могло бы выглядеть совершенно иначе.

2. Отбор (селекция).

На каждом этапе качество программ вычисляется с помощью функции выживаемости (fitness function). Так как размер популяции не изменяется, программы, оказавшиеся плохими, удаляются из популяции, освобождая место для новых. Создается новая популяция, которая называется «следующим поколением», и весь процесс повторяется. Поскольку сохраняются и изменяются самые лучшие программы, то есть надежда, что с каждым поколением они будут совершенствоваться. Новые поколения создаются до тех пор, пока не будет выполнено условие завершения.

3. Размножение (скрещивание или кроссинговер).

Две успешные программы комбинируются с целью получения новой. Обычно это делается путем замены какой-то ветви одной программы ветвью другой (Рис. 2) [3].

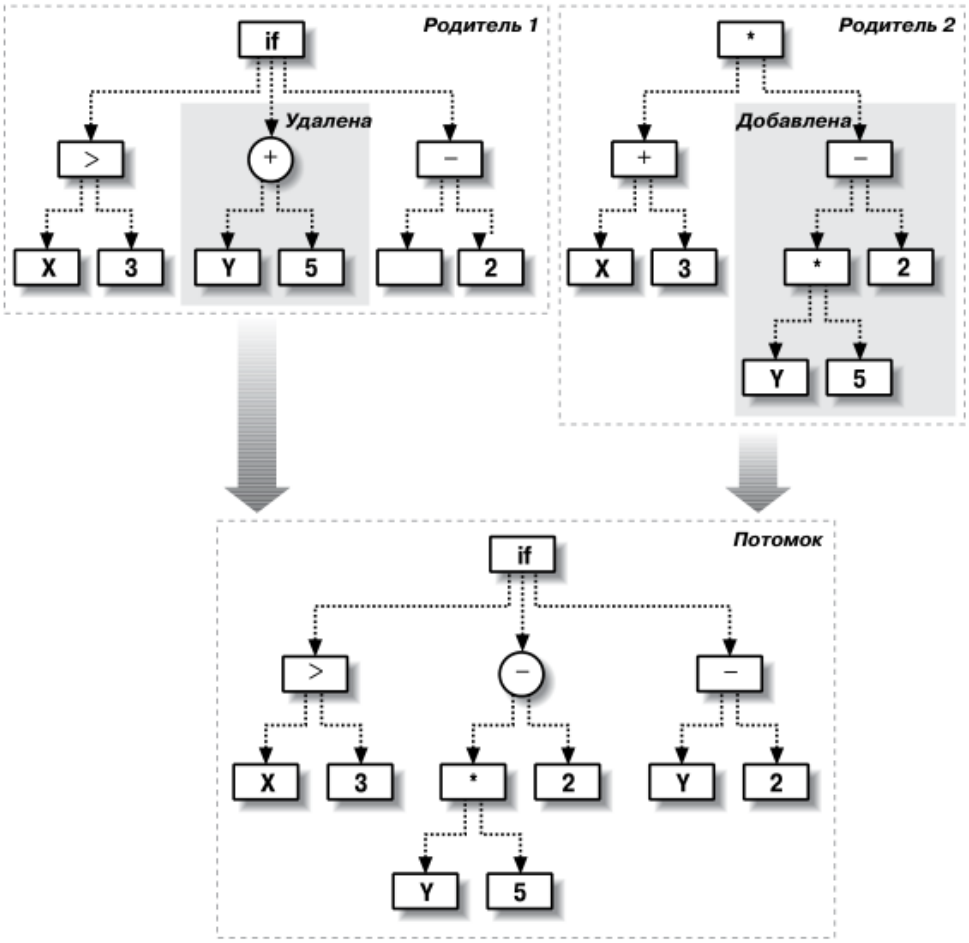


Рис. 2. Скрещивание программ

4. Мутирование.

Мутация заключается в небольшом изменении одной программы. Изменить древовидную программу можно разными способами.

4.1. Изменив функцию в каком-то узле или одну из ветвей. Если для новой функции требуется другое количество дочерних узлов, то либо какие-то ветви удаляются, либо добавляются новые (Рис. 3) [3].

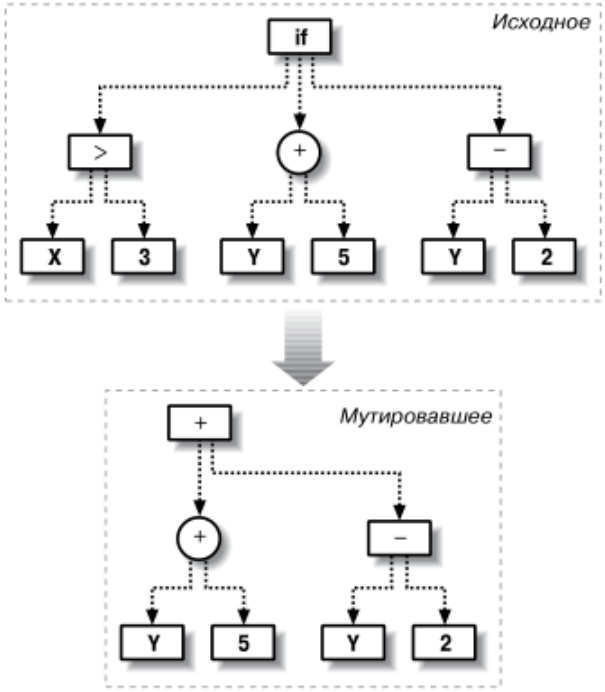


Рис. 3. Мутация узла

4.2. Замена какого-то поддерева целиком (Рис. 4) [3].

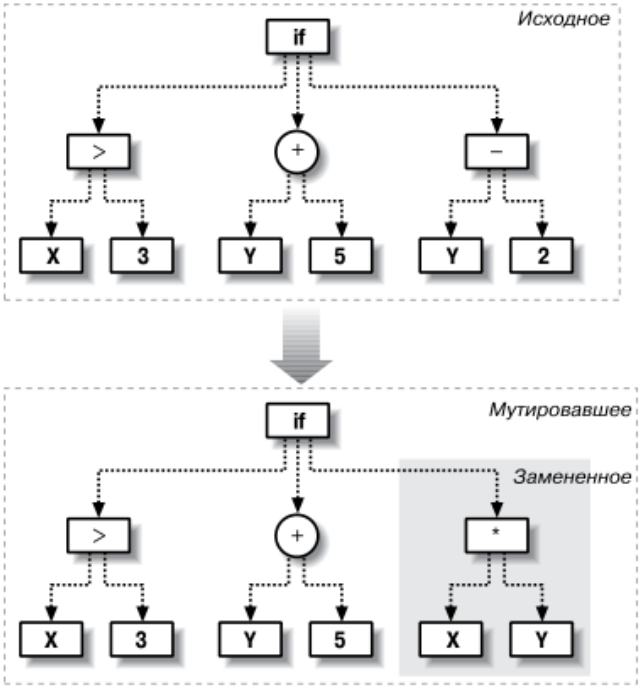


Рис. 4. Мутация поддерева

Генетические алгоритмы применяются для решения следующих задач [5]:

1. Оптимизация функций.
2. Оптимизация запросов в базах данных.
3. Разнообразные задачи на графах (задача коммивояжера, раскраска, нахождение паросочетаний).
4. Настройка и обучение искусственной нейронной сети.
5. Задачи компоновки.
6. Составление расписаний.
7. Игровые стратегии.
8. Теория приближений.
9. Искусственная жизнь.
10. Биоинформатика (фолдинг белков).
11. Синтез конечных автоматов.
12. Настройка ПИД регуляторов.

Основные недостатки генетических алгоритмов:

1. Генетические алгоритмы плохо масштабируемы под сложность решаемой проблемы. Это значит, что число элементов, подверженных мутации очень велико, если велик размер области поиска решений.

2. Во многих задачах генетические алгоритмы имеют тенденцию сходиться к локальному оптимуму или даже к спорным точкам, вместо глобального оптимума для данной задачи. Это значит, что они «не знают», каким образом пожертвовать кратковременной высокой пригодностью для достижения долгосрочной пригодности.

Список литературы

[1] Гладков Л.А., Курейчик В.В., Куречик В.М. Генетические алгоритмы / Под ред. В.М. Курейчика. – М.: ФИЗМАТЛИТ, 2006. – 320 с.

[2] Скобцов Ю.О. Основы эволюционных вычислений / Донецк: ДонНТУ, 2008. – 326 с.

[3] Сегаран Т. Программируем коллективный разум / СПб: Символ-Плюс, 2008. -368 с.

[4] Курейчик В.В, Курейчик В.М, Родзин С.И. Теория эволюционных вычислений. - М.: ФИЗМАТЛИТ, 2012. - 260 с.

[5] Семенкина М.Е. Самоадаптивные эволюционные алгоритмы проектирования информационных технологий интеллектуального анализа данных // Искусственный интеллект и принятие решений. – 2013. – С. 13-23.

Жарова Ольга Юрьевна – ассистент кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: ouzharova@yandex.ru

Хлыстов Игорь Сергеевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: KListov888Ig@yandex.ru

А.Ю. Макарова

ЗАЩИТА ОТ ФИШИНГА

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Целью данной работы является исследование различных алгоритмов защиты от фишинга и их реализации в веб-браузерах.

Фишинг – это вид интернет-мошенничества, представляющий собой угрозу информационной безопасности. Он осуществляется при помощи методов социальной инженерии для того, чтобы обманным путем получать личную и конфиденциальную информацию пользователей Интернета. В рамках обеспечения информационной безопасности основной задачей является обнаружение и профилактика фишинговых атак, поскольку злоумышленники реализуют эти атаки таким образом, что они способны обойти существующие средства защиты от фишинга. Атака заключается в том, что злоумышленник создает поддельную веб-страницу путем копирования или внесения небольших изменений в законную веб-страницу таким образом, что пользователь Интернета не сможет найти никаких отличий между ними. Один из эффективных методов защиты от фишинговых атак заключается в интеграции средств безопасности в веб-браузер, который может предупреждать пользователя всякий раз, когда он обращается к фишинговому сайту. Как правило, веб-браузеры обеспечивают безопасность системы от фишинговых атак при помощи методов, основанных на списке. Такие методы содержат либо черный список, либо белый список, либо сочетание обоих списков. Эти методы сопоставляют предоставленный домен с доменами из черного или белого списков, чтобы принять решение о принадлежности сайта к фишинговым.

Некоторые из основных типов фишинговых атак:

- Фишинговая атака на неизвестные уязвимости: неустраненные уязвимости несомненно являются брешью в средствах защиты от фишинговой атаки. Уязвимости используются хакерами до тех пор, пока они не станут известны и производители ПО не устранят их.
- Фишинговые атаки, использующие встроенные объекты: существующая веб-страница выгружается для создания фишинговой, которая внешне похожа на подлинную. Злоумышленники перекрывают адресную строку, используя изображение или скрипт, которые заставляют пользователей считать, что они попадают на нужный вебсайт.
- Атака на систему имен доменов DNS: отравление кэша DNS эксплуатирует уязвимости системы имен доменов. В этой атаке злоумышленники направляют интернет-трафик от легитимного вебсайта к поддельному веб-сайту.

- Фишинговые атаки, использующие зависимость от языка: в основе большинства методов защиты от фишинга лежит алгоритм, включающий в себя ключевые слова, часто встречаемые на поддельных сайтах. Если эти методы обнаруживают ключевые слова, написанные на английском языке, то они не смогут обнаружить написанные на других языках, например, китайском, японском и т.д.

Методы на основе черного списка содержат подозрительные доменные имена и IP-адреса. Черные списки регулярно обновляются; однако, большинство методов на основе черного списка не эффективны в борьбе с атаками на неизвестные уязвимости. Интерфейс безопасного просмотра в браузере Google Chrome использует такой список. При попытке посещения сайта, подозреваемого в фишинге или распространении вредоносного ПО, браузер показывает предупреждение.

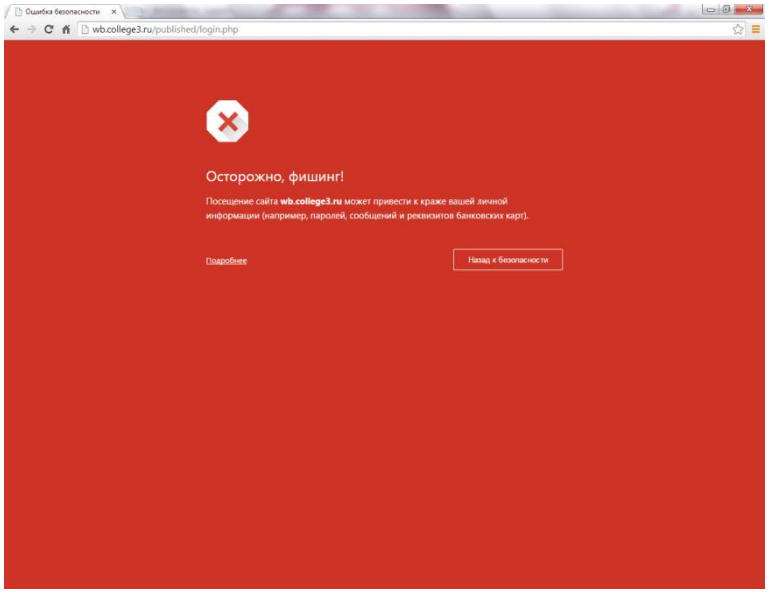


Рис. 1. Предупреждение о фишиге в браузере Google Chrome

Принцип ее работы состоит в следующем. В браузер загружается список с информацией о сайтах, которые могут содержать вредоносное ПО или подозреваются в фишинге. Этот список не содержит полные адреса URL каждого подозрительного сайта. Вместо этого каждый URL хэшируется (изменяется таким образом, что его нельзя прочесть) и разделяется на фрагменты. Только часть каждого хэшируемого URL включается в список в браузере. При работе в Интернете браузер создает хэшированные версии посещаемых URL и проверяет их в соответствии со списком. Если адрес посещаемого сайта соответствует хэшированному фрагменту URL в списке, браузер свяжется с серверами Google и запросит полный список (а не только фрагменты) хэшированных URL подозрительных страниц. Затем компьютер определит, является ли сайт подозрительным, и выведет соответствующее предупреждение.

Защита от фишинга в браузере Internet Explorer 11.

Начиная с Internet Explorer 8 в состав Internet Explorer входит фильтр SmartScreen -- набор технологий, предназначенный для защиты пользователей от возможных интернет-угроз, в том числе угроз социальной инженерии. Базируется SmartScreen на технологии фишингового фильтра и предназначен для защиты пользователей от известных вредоносных веб-узлов. Кроме того, данный фильтр включает защиту от ClickJacking, технологии, применяемой для перехвата клавиш, искажения веб-страниц и т.д. По умолчанию он включен.

Фильтр SmartScreen в Internet Explorer 11 использует сразу несколько технологий. В первую очередь происходит сравнение адреса посещаемого сайта со списком известных мошеннических и вредоносных сайтов. Если сайт найден в этом списке, больше проверок не производится. В противном случае он анализируется на предмет наличия признаков, характерных для мошеннических сайтов. Также возможна отправка адреса того сайта, куда пользователь собирается зайти, онлайн-службе Microsoft, которая ищет его в списке фишинговых и вредоносных сайтов. Причем доступ к онлайн-службе производится асинхронно по SSL-соединению, так что это не сказывается на скорости загрузки страниц. Однако обращение к данной службе пользователь может запретить.

Чтобы уменьшить сетевой трафик, на клиентском компьютере хранится зашифрованный DAT-файл со списком тысяч наиболее посещаемых узлов; все включенные в этот список не подвергаются проверке фильтром SmartScreen.

Для защиты от фишинга и эксплойтов фильтр SmartScreen исследует строку URL целиком, а не подмножество адресов URL, на которые заходил пользователь, а значит, службе URS могут быть переданы личные сведения, поскольку иногда они находятся в самой строке URL.

Список литературы

[1] Мостовой Д.Ю. Современные технологии борьбы с вирусами. – СПб.: БХВ-Петербург, 2006. – 120 с.

[2] Крис Касперски «Секретное оружие социальной инженерии»: Компания АйТи. – СПб.: BHV, 2005. – 495с.

[3] ru.wikipedia.org

[4] osp.ru

Макарова Анастасия Юрьевна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: nastyamakarova1794@yandex.ru

Е.А. Заломлёнкова

ЗАЩИТНЫЕ МЕХАНИЗМЫ СУБД

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В современном мире ни одна компания не может обойтись без использования баз данных. Встроенные защитные механизмы СУБД играют важную роль в обеспечение информационной безопасности корпоративных информационных систем. В течение долгих лет более 80% рынка СУБД контролируется тремя компаниями производителями: IBM, Oracle и Microsoft.

Задача настоящего исследования состояла в определении наиболее подходящей СУБД для защиты большого объема информации. Объектами исследования были выбраны СУБД Oracle и Microsoft SQL Server.

OracleDatabase – объектно-реляционная система управления базами данных компании Oracle. [1] Oracle поддерживает самые большие базы данных размером до сотен гигабайт, а также большое число пользователей, одновременно выполняющих разнообразные приложения, которые оперируют одними и теми же данными. Данная система оптимизации одновременного доступа позволяет СУБД выполнять за секунду больше транзакций в расчете на одного пользователя, чем любая другая база данных. СУБД Oracle обладает уникальными качествами переносимости, а также предоставляет открытую платформу для разработки переносимых приложений клиент/сервер. [2]

Microsoft SQL Server™ –это система анализа и управления реляционными базами данных в решениях электронной коммерции, производственных отраслей и хранилищ данных.SQL Server является масштабируемой базой данных, так как она может хранить значительные объемы данных и поддерживать работу многих пользователей, осуществляющих одновременный доступ к базе данных. Данная СУБД функционирует только в среде Windows. Также SQL Server имеет целый набор специальных мастеров и средств автоматической настройки параметров конфигурации. [3].

Было проведено исследование защитных механизмов выбранных систем управления базами данных для дальнейшего их анализа. Были рассмотрены такие аспекты обеспечения информационной безопасности баз данных как:

- обеспечение целостности базы данных;
- шифрование;
- резервное копирование;
- архивация;
- аутентификация;
- аудит;
- дополнительные возможности.

Результаты исследования сведены в таблицу 1.

Таблица 1. Результаты исследования

Параметры сравнения		**OracleDatabase**	**MS SQL Server**
Обеспечение целостности базы данных	На уровне типа данных	+	+
	На уровне ключей	+	+
	На уровне триггеров	+	+
	Дополнения		*Использование ограничения CHECK*
Шифрование	Прозрачное шифрование данных	+	+
	Место хранения ключа шифрования	Вне базы данных[4]	В загрузочной записи базы данных
	Дополнения		*Использование сертификатов для цифровой подписи*
Резервное копирование	Резервное копирование	+	+
	Дополнения	*Выбор вида: холодное резервное копирование / резервное горячее копирование*	*Выбор модели восстановления: простая / полная модель*
Режим архивирования		+	-
	Дополнения	*Возможность автоматического архивирования*	
Аудит	Опция Аудит	+	-
	Дополнения	Возможна генерация аудиторских отчетов	
Аутенификация	Аутенификация	+	+
	Дополнения		Поддержка политики управления паролями
Дополнительные возможности		– «Умное сжатие» – Data Guard FarSync – Application Continuity – DataRedaction	– *WindowsUpdate* – *Конфигурация области атаки* – DeclarativeManage-mentFramework [5]

Для устранения уязвимых мест разработано множество механизмов, которые реализуются в самих системах управления базами данных. При исследовании защитных механизмов СУБД Oracle иMicrosoft SQL Server отразились их сходства и различия в функциональном наборе. Было выявлено, что СУБД Oracle предоставляет более широкий спектр возможностей для защиты информации, однако немаловажное значение имеет правильная настройка данных параметров.

Список литературы

[1] Основные характеристики СУБД Oracle. // URL: http://bourabai.ru/dbt/servers/Oracle.htm

[2] Лачихина А.Б., Мазин А.В. Методика рациональной настройки баз данных на примере системы "Аналитик". // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия: Приборостроение. – 2010. – № 4. – С. 91-103.

[3] Лачихина А.Б., Петраков А.А. Вопросы обеспечения безопасности данных в корпоративных информационных системах. // Вопросы радиоэлектроники. - 2016. - № 2. –С. 29-31.

[4] Абдулхассан Ф. Х. Прозрачное шифрование данных (TDE) // Молодой ученый. – 2014. – №8. – С. 122-125.

[5] Обзор механизмов защиты SQL Server 2008 для администраторов баз данных. // URL: http://studydoc.ru/doc/3775629/obzor-mehanizmov-zashhity-sql-server-2008-dlya

Заломлёнкова Екатерина Александровна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: shadowkzal@gmail.com

Я.А. Фотина, К.А. Празян

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СРЕДЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

За последние несколько лет концепция облачных вычислений стала популярной в сфере информационных технологий. В настоящее время она рассматривается в качестве альтернативы традиционной модели обработки информации. С помощью систем облачных вычислений становится возможной реализация удаленной обработки информации, благодаря которой достигаются высокие показатели отказоустойчивости и доступности информационной инфраструктуры. Однако кроме положительных тенденций развития облачных технологий есть много связанных с ними проблем, так как инфраструктура облачных вычислений еще не полностью исследована с точки зрения информационной безопасности.

Под облачными вычислениями (cloud computing) понимается технология обработки данных, согласно которой программы запускаются и выдают результаты работы в окно стандартного веб-браузера на локальном ПК, при этом все необходимые для работы приложения и их данные находятся на удаленном сервере в Интернете. Другими словами, облачные вычисления – это программно-аппаратное обеспечение, доступное пользователю через Интернет (или локальную сеть) в виде сервиса, позволяющего использовать удобный веб-интерфейс для удаленного доступа к выделенным ресурсам (вычислительным ресурсам, программам и данным).

По сравнению с традиционными информационными системами, системы облачных вычислений обладают рядом характерных особенностей, которые необходимо учитывать при анализе защищенности данных систем. К ним относятся:

- Портал самообслуживания – инструмент, с помощью которого пользователь может заказать для себя заранее предопределенный сервис с уточнением деталей конфигурации, изменить параметры заказанного сервиса или отказаться от него.
- Каталог сервисов –правила, согласно которым средства автоматизации будут конфигурировать данный сервис на реальном оборудовании и программном обеспечении.
- Оркестратор – механизм, выполняющий последовательность операций, определенных в шаблоне для каждого сервиса.
- Система тарификации и выставления счетов – механизм, определяющий объем потребленных пользователем ресурсов и соотнесение с пользователем соответствующих финансовых затрат.

В концепции облачных вычислений ресурсы общего пользования предоставляются аналогично распределению электроэнергии по проводам. Компьютеры, осуществляющие облачные вычисления («вычислительное облако»), и компьютер пользователя настроены на совместную работу, при этом различные приложения используют общую вычислительную мощность так, как будто выполняются на одиночной системе.

Облачная обработка данных включает в себя идею «все как услуга» с помощью Интернета и виртуализации. Виртуализация данных – процесс представления их пользователю посредством интерфейса, скрывающего все технические аспекты хранения данных (способ, структуры, язык доступа, местоположение). Виртуализация заключается в абстрагировании данных от конкретной формы их хранения, сбора ресурсов в общий пул и их дальнейшем распределении между пользователя ми. В свою очередь, виртуальная машина - это программное обеспечение, которое устанавливается на систему пользователя и с помощью которого можно работать в другой операционной системе. [1]

Модель облачных вычислений состоит из внешней и внутренней частей, связь которых осуществляется через Интернет. Посредством внешней части, которая состоит из пользовательского компьютера и приложений, используемых для доступа к облаку, пользователь взаимодействует с системой. Внутренней частью является само облако. Это различные приложения, компьютеры, серверы и хранилища данных, создающие облако сервисов.

Существует несколько моделей развертывания облака:

1. Частное облако – инфраструктура, предназначенная для использования одной организацией, включающей несколько потребителей.
2. Публичное облако – инфраструктура, предназначенная для свободного использования широкой публикой. Оно может находиться в собственности, управлении и эксплуатации коммерческих, научных и правительственных организаций.
3. Гибридное облако – сочетание частного и публичного облаков, связанных между собой стандартизованными или частными технологиями передачи данных и приложений.

Интернет-услуги облачных вычислений, известные как облачные сервисы, подразделяются на три уровня:

1. Уровень инфраструктуры – основа облака. Он состоит из физических активов - серверов, сетевых устройств, дисков и т.д.
2. Платформа – промежуточный уровень, предоставляющий доступ к операционным системам и соответствующим сервисам. Она дает способ развертывания приложений в облаке при помощи языков программирования и инструментальных средств, поддерживаемых поставщиком.

3. Уровень приложений – верхний уровень, который обычно и изображают в виде облака. Приложения, выполняющиеся в нем, предоставляются пользователям по требованию. [2]

Рассмотрев основные положения облачных вычислений, можно выделить достоинства их использования в сфере информационных технологий.

- Доступность и отказоустойчивость заключается в возможности использования облачных сервисов всеми пользователями из любой точки, где есть Интернет, с любого компьютера, где есть браузер.
- Экономичность и эффективность заключается в учете и оплате только фактически потребленных ресурсов строго по факту их использования.
- Простота - не требуется покупка и настройка программ и оборудования, их обновление.
- Гибкость и масштабируемость заключается в неограниченности вычислительных ресурсов (память, процессор, диски), при этом ресурсы выделяются и освобождаются по мере надобности.

Главным недостатком облачных вычислений является необходимость постоянного соединения с сетью. Если нет доступа в сеть - нет работы, программ, документов. Многие «облачные» программы требуют хорошего Интернет-соединения с большой пропускной способностью. Соответственно, программы могут работать медленнее, чем на локальном компьютере.

Как уже было сказано, технология облачных вычислений имеет ряд проблем, связанных с обеспечением безопасности находящихся в облаке данных, поскольку гарантий того, что все ресурсы облака посчитаны и в нем нет неконтролируемых виртуальных машин, не запущено лишних процессов и не нарушена взаимная конфигурация элементов облака, нет. Рассмотрим различные виды угроз.

- Серверы облачных вычислений используют те же операционные системы и веб-приложения, что и локальные виртуальные и физические сервера. Следовательно, для облачных систем высока угроза удаленного взлома или заражения вредоносным кодом. Уязвимости и ошибки в настройках могут бесконтрольно распространяться и часто проявляются после произвольного промежутка времени. Кроме того, факторы риска и угрозы безопасности с трудом поддаются оценке, особенно количественной, по причине недостаточной прозрачности операций, протекающих в облаке.
- Ещё одной угрозой является угроза целостности данных. Данные могут быть необратимым образом раскрыты нежелательным лицам, так как их копии удерживаются в системе еще долгое время после того, как прекратилось использование сервиса. Взломщики могут воспользоваться разнообразными лазейками из-за того, что одной

технологией одновременно пользуются различные клиенты (так при плохой архитектуре системы может происходить утечка счетов, чтение массивов информации и получение неавторизованного доступа к данным других клиентов облака).

- Опасности заражения подвергается также выключенная виртуальная машина. На выключенной виртуальной машине абсолютно невозможно запустить защитное программное обеспечение.
- Гипервизор является одним из ключевых элементов виртуальной системы. Основной его функцией является разделение ресурсов между виртуальными машинами. Атака на гипервизор может привести к тому, что одна виртуальная машина сможет получить доступ к памяти и ресурсам другой. Также она сможет перехватывать сетевой трафик, отбирать физические ресурсы и даже вытеснить виртуальную машину с сервера.

При использовании облачных вычислений периметр сети размывается или исчезает. Это приводит к тому, что защита менее защищенной части сети определяет общий уровень защищенности.

Основываясь на анализе возможных угроз в облачных вычислениях, предложен возможный программно-аппаратный комплексный защиты безопасности облачных вычислений, включающий следующие решения:

- Шифрование – основной метод, используемый для обеспечения безопасности данных в облаке. Провайдер, предоставляющий доступ к данным, должен шифровать информацию клиента и безвозвратно удалять ее в случае необходимости. Недостаток этого метода заключается в том, что шифрование требует больших вычислительных мощностей и значительно влияет на производительность систем управления базами данных (СУБД). Есть несколько подходов к шифрованию, каждый имеет свои недостатки: одни лучше обеспечивают безопасность, а другие сосредоточены на производительности.
- Разделение данных - методы, которые служат в качестве альтернативы шифрования. Идея состоит в том, чтобы разделить данные на несколько хостов, которые не могут взаимодействовать друг с другом, и только владелец, который может получить доступ к каждому из хостов, может воссоздать из них исходные данные. Этот способ очень быстр, но он требует, по крайней мере, двух отдельных, но однородных поставщиков услуг.
- Аутентификации – защита паролем. Зашифрованные данные при передаче должны быть доступны только после аутентификации. Данные не получится прочитать или сделать изменения даже в случае доступа через ненадежные узлы.

- Изоляция пользователей - использование индивидуальной виртуальной машины и виртуальной сети. Часто провайдеры изолируют данные пользователей друг от друга за счет изменения данных кода в единой программной среде. Данный подход имеет риски, связанные с опасностью найти дыру в нестандартном коде, позволяющему получить доступ к данным. В случае возможной ошибки в коде пользователь может получить данные другого.

Таким образом, облачные вычисления являются перспективной отраслью информационных технологий. На данный момент идет активная разработка и совершенствование системы облачных вычислений. Но речь идет именно о разработке, а не об использовании, поскольку существуют проблемы, связанные с защитой информации, находящейся в среде облачных вычислений. И хотя уже определены пути решения данной проблемы, многие аспекты защиты информации облачных вычислений до конца не изучены.

Литература:

[1] Клементьев И.П. Устинов В.А. - Введение в Облачные вычисления – 2009, - с. 5-30.

[2] Риз Дж. – Облачные вычисления – 2011, с. 10-34.

Фотина Яна Александровна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: fotina_yana@mail.ru

Празян Константин Арменович – ассистент кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: prazyan.konstantin@gmail.com

Д.У. Белетова, А.Н. Молчанов, А.В. Паньковец

ИСПОЛЬЗОВАНИЕ СТАНДАРТА IEEE 802.1X ДЛЯ ЗАЩИТЫ ОТ НСД

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В настоящее время пользователей беспроводной сети становится всё больше. Связано это с удобством использования Wi-Fi сети, ведь для подключения пользователям необязательно иметь физический доступ к сетевому устройству, а достаточно быть в радиусе действия данной сети.

Этот аспект является привлекательным и для злоумышленников. При недостаточной защите беспроводной сети имеется возможность получить несанкционированный доступ к ресурсам диска пользователей Wi-Fi, осуществлять перехват трафика для извлечения конфиденциальной информации, модифицировать проходящие в сети данные, внедрять поддельные точки доступа, рассылать спам от имени данной сети и т.п. Поэтому в данной статье будет рассматриваться стандарт IEEE 802.1X для контроля доступа к беспроводной сети и основанные на нем технологии WPA и WPA2, их характеристики.

Стандарт сетевой аутентификации 802.1x («Протокол управления доступом к сети на основании портов») был разработан 13 декабря 2004 года группой IEEE (Institute of Electrical and Electronic Engineers – Институт инженеров по электротехнике и электронике). Изначально данный стандарт применялся для контролируемого доступа к проводным сетям, но в современное время он может использоваться и в беспроводных локальных сетях. Данный стандарт осуществляет аутентификацию и авторизацию устройств, запрашивающих доступ к ресурсам, устраняя недостатки стандарта 802.11 в WEP (Wired Equivalent Privacy), где подобных проверок не производится.

В стандарте IEEE 802.1x предполагаются три основных элемента (рис.1):

- ♦ суппликант (supplicant), то есть устройство (например, ПК), запрашивающее доступ к сети;
- ♦ сервер аутентификации (authentication server), выполняющий установку подлинности предъявленных данных. Обычно используется RADIUS-сервер;
- ♦ аутентификатор (authenticator), осуществляющий процесс аутентификации перед предоставлением доступа. Он располагается между суппликантом и сервером аутентификации.

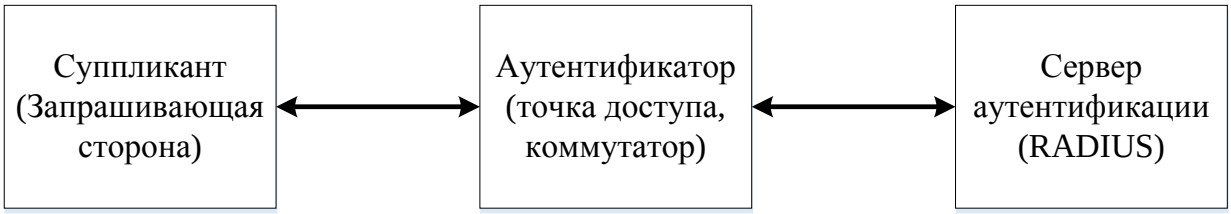


Рис.1. Составляющие 802.1x

Аутентификация по стандарту 802.1x в общем случае происходит следующим образом:

1) Запрашивающая сторона отправляет запрос в точку доступа. Точка доступа запрашивает идентификационную информацию.
2) Суппликант посылает пакет с идентификационной информацией, которая далее пересылается в сервер аутентификации.
3) Сервер аутентификации отправляет пакет подтверждения в точку доступа.
4) Точка доступа переводит порт клиента в авторизованное состояние, после чего возможна отправка данных [1].

Стандарт 802.1x включает:

- EAP (Extensible Authentication Protocol – расширенные протокол аутентификации)
- TLS (Transport Layer Security - протокол транспортного уровня)
- RADIUS (Remote Access Dial-in User Service – служба удаленной аутентификации пользователей коммутируемого доступа).

EAP описывает обмен данными между клиентом и сервером аутентификации. Протокол передачи EAP-сообщений в стандарте 802.1x называется EAPOL (EAP encapsulation over LAN). Функционирует протокол следующим образом:

1. Аутентификатор посылает запрос на аутентификацию (EAP-Request/Identity) суппликанту, как только один из его портов переходит в активное состояние (link active). При повторном подсоединении клиентской станции, прошедшей ранее аутентификацию, процесс аутентификации потребуется пройти снова.
2. Суппликант посылает сообщение/ответ (EAP Response/Identity) аутентификатору, которое затем передается им на сервер аутентификации (RADIUS) [2].
3. Сервер аутентификации отправляет ответ-запрос (challenge) аутентификатору, который переупаковывает его из IP-транспорта в EAPOL и затем отправляет его суппликанту. В EAP поддерживается как аутентификация клиентской стороны, так и взаимная аутентификация клиента и сервера, но только последний вариант считается приемлемым для использования в беспроводных сетях [2].

4. Суппликант отвечает на запрос по выбранному алгоритму и передает его аутентификатору, которое отправляет его серверу аутентификации.
5. Если суппликант отправляет верный ответ на запрос, сервер аутентификации передает пакет подтверждения в аутентификатор.
6. Аутентификатор переводит порт суппликанта в авторизованное состояние, после чего возможна неограниченная передача данных.

Стоит отметить, что после прохождения аутентификации, пользователю высылается сеансовый ключ в зашифрованном виде. Шифрование производится согласно алгоритму RC4. По завершению времени действия данного ключа пользователю высылается новый сеансовый ключ. Протокол защиты транспортного уровня TLS обеспечивает целостность и шифрование передаваемых данных между сервером и клиентом, их взаимную аутентификацию, предотвращая перехват и подмену сообщений. По умолчанию ключ составляет 128 бит [3].

RADIUS-сервер решает задачи учета времени пребывания пользователей в сети и расчета стоимости услуг, работает по протоколу AAA (Authorization, Authentication and Accounting – авторизация, аутентификация и ведение учетных записей), выполняет следующие функции:

- ♦ Создание и хранение учётных записей пользователей (абонентов);
- ♦ Управление учётной записью пользователя (абонента) из персонального интерфейса;
- ♦ Создание карточек доступа (логин/PIN-код) для предоставления услуг, с некоторым лимитом действия;
- ♦ Ручная и автоматическая блокировка учётной записи абонента по достижению заданного критерия или лимита;
- ♦ Сбор и анализ статистической информации о сессиях пользователя и всей обслуживаемой системы;
- ♦ Создание отчётов по различным статистическим параметрам;
- ♦ Создание, печать и отправка счетов к оплате;
- ♦ Аутентификация всех запросов в RADIUS-сервер из обслуживаемой системы.

Стандарт 802.1x в чистом виде сейчас не используется, а используется в качестве дополнительного средства обеспечения информационной безопасности WLAN (Wireless Local Area Network – беспроводная локальная сеть). Рассмотрим стандарты WPA и WPA2, использующие протокол проверки подлинности 802.1x.

WPA и WPA2 (Wi-Fi Protected Access) - это программы сертификации устройств беспроводной связи. Данные технологии схожи в архитектуре системы безопасности с улучшенными механизмами аутентификации

пользователей и протоколами распространения и обновления ключей [4]. Но есть и отличия.

WPA реализует аутентификацию по стандарту 802.1x, обмен ключами, использует протокол целостности временного ключа TKIP (Temporal Key Integrity Protocol) и протокол EAP. В задачи TKIP входит расширение ключа от 40 до 128 бит, управление ключами, которые автоматически генерируются и пересылаются сервером аутентификации, создание нового ключа для каждого пакета данных. Используемый алгоритм шифрования - RC4, но работает только с динамическими ключами (в отличие от WEP, главной проблемой которого являлось использование слишком похожих ключей для разных пакетов данных). WPA2 для шифрования данных использует алгоритм AES. Для подтверждения целостности пакетов WPA использует криптографическую контрольную сумму (MIC). MIC позволяет защитить передаваемые данные от несанкционированного изменения содержимого пакета.

WPA = 802.1X + EAP + TKIP + MIC – формула определения WPA от организации Wi-Fi Alliance.

В основе WPA2 лежит IEEE 802.11i. IEEE 802.11i – это стандарт, направленный на повышение безопасности корпоративных беспроводных сетей. Для аутентификации 802.11i использует стандарт 802.1x вместе с RADIUS и технологию TKIP.

WPA работает в двух режимах: PSK (Pre-Shared Key) и Enterprise (корпоративный). При использовании первого варианта аутентификация производится путем введения единого пароля при подключении, а в WPA-Enterprise имеется множество ключей, хранящиеся на отдельном сервере RADIUS. Для поддержки WLAN стандарта WPA, достаточно обновить их ПО, в отличие от WPA2 на основе 802.11i, где для совместимости потребуется новое оборудование с поддержкой AES.

Таким образом стандарт контроля доступа IEEE 802.1x является достаточно надежным механизмом для защиты от несанкционированного доступа, даже спустя десятилетие после своего создания. Технология WPA2 на основе данного стандарта с использованием алгоритма AES для шифрования данных обеспечит более высокий уровень защищенности беспроводной сети по сравнению с WPA, использующий RC4 с динамическими ключами. Но WPA проще в установке, которое сводится к обновлению ПО на сетевом устройстве, нежели WPA2, которому потребуется оборудование с поддержкой стандарта 802.11i. Однако, стоит отметить, что одного протокола защиты недостаточно – следует также уделять внимание корректному построению, настройке и администрированию сети.

СПИСОК ЛИТЕРАТУРЫ

[1] [Электронный ресурс] Обзор возможностей защиты. Руководство пользователя сетевого адаптера Intel® PRO/Wireless 3945ABG. URL: ftp://ftp.physik.hu-berlin.de/pub/driver/netz/intel-centrino/WLAN_Generic_SW_2200BG_2915ABG_3945ABG_V10.1.0.3_TIC_107948/Docs/RUS/security.htm#wpa (дата обращения 10.10.2016)

[2] [Электронный ресурс] Сетевая аутентификация на практике. URL: http://citforum.ru/nets/articles/authentication/ (дата обращения 10.10.2016)

[3] [Электронный ресурс] Технология защиты Wi-Fi сетей. Стандарт IEEE 802.1x. URL: http://confonline.susu.ru/index.php?option=com_content&view=article&id=95:--wi-fi--c-ieee-80211x&catid=16:-2----&Itemid=18 (дата обращения 10.10.2016)

[4] [Электронный ресурс] Защита беспроводных сетей. URL: http://ypn.ru/370/wireless-networking-securin/ (дата обращения 10.10.2016)

Белетова Дженнет Умалатовна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: zhennet.beletova@mail.ru

Молчанов Алексей Николаевич – ст. преп. кафедры «Информационная безопасность автоматизированных систем» КФ МГТУ им. Н.Э. Баумана. E-mail: alexeymolchanov@outlook.com

Паньковец Александр Валерьевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: pankovets.a.v@gmail.com

Я.А. Бланк, А.С. Макаров

ИСПОЛЬЗОВАНИЕ ЭКСПЕРТНЫХ СИСТЕМ ДЛЯ КОНТРОЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Информация всегда играла чрезвычайно важную роль в жизни человека. Она стала одним из важнейших стратегических, управленческих ресурсов, наряду с материальными, человеческими и финансовыми ресурсами. Именно поэтому на сегодняшний день крайне актуальным стал вопрос обеспечения информационной безопасности. Основными целями информационной безопасности является сохранения целостности, доступности и конфиденциальности информации. Уровень информационной безопасности можно значительно повысить благодаря применению экспертных систем.

Экспертные системы – это направление исследований в области искусственного интеллекта по созданию вычислительных систем, умеющих принимать решения, схожие с решениями экспертов в заданной узкоспециализированной предметной области. Экспертная система имеет следующую структуру:

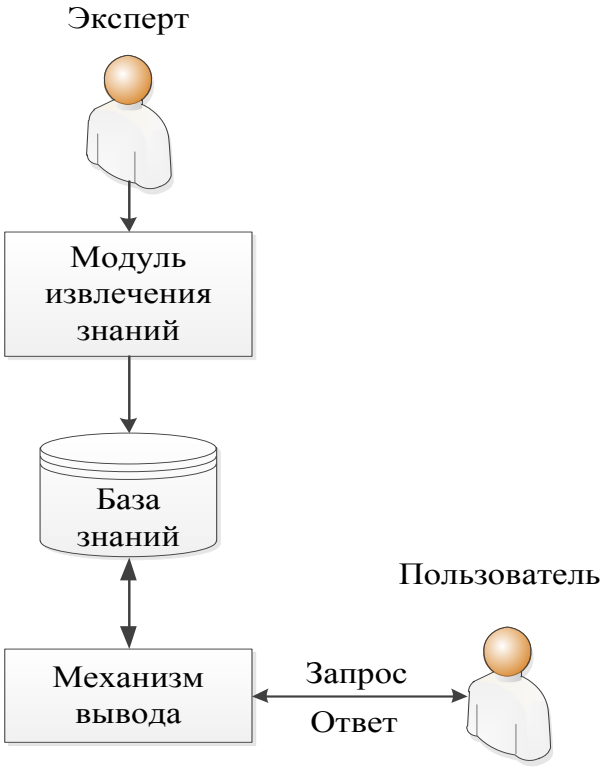


Рис.1. – Экспертная система

Эксперт наполняет базу знаний данными и правилами о конкретной предметной области. База знаний – сердце экспертной системы. В рамках обеспечения информационной безопасности в базу знаний должны включаться описания угроз безопасности, задач защиты, концепции политики безопасности, требования, предъявляемые к безопасности. В результате экспертная система может самостоятельно отвечать на вопросы пользователя, связанные с ее предметной областью. Модуль извлечения знаний структурирует и представляет экспертные знания в виде, пригодном для системы. Механизм вывода осуществляет обработку данных по заложенным в базе знаний правилам, чтобы ответить на запрос пользователя. Помимо этого, механизм вывода дополняет и изменяет базу знаний.

Одним из лучших способов оценки, достижения и поддержания информационной безопасности является аудит информационной безопасности. [1] Аудит информационной безопасности – это системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности системы в соответствии с определенными критериями и показателями безопасности и предоставление результатов в виде рекомендаций [2]. Это крайне сложный, многоступенчатый и дорогой процесс. Для качественной оценки необходимо несколько высококвалифицированных экспертов. Не каждое предприятие, нуждающиеся в защите своей информации, обладает такими ресурсами. Решением в данной ситуации могут быть экспертные системы. Использование экспертных систем для аудита безопасности актуально по следующим причинам:

1. количество квалифицированных специалистов в области информационной безопасности систем крайне мало, а услуги их дороги. Создание 1 качественной экспертной систем для анализа безопасности и ее дальнейшее тиражирование сможет решить проблему;
2. создание экспертной системы предотвратит потерю знаний специалистов, которые могут уволиться, выйти на пенсию и пр.;
3. улучшение качества работы. В создании экспертной системы принимают участие несколько специалистов, что положительно сказывается на качестве работы готовой системы;
4. отсутствие человеческого фактора. Существует множество факторов, которые могут повлиять на работу специалиста, тем самым ухудшив ее качество (например, эмоциональное потрясение, стресс и др.). Экспертная система работает беспристрастно, тем самым уменьшая возможность возникновения ошибки;
5. экономия времени. Должен пройти продолжительный период, чтобы человек приобрел необходимые навыки в сфере информационной безопасности и стал экспертом. Помимо этого, сам процесс аудита, проводимого человеком, требует большого количества временных ресурсов.

Несмотря на все преимущества применения экспертных систем для аудита информационной безопасности, на сегодняшний день они не так широко распространены. Это может быть вызвано следующим:

1. несмотря на то, что тиражирование готовой экспертной системы, которую смогут использовать несколько организаций, уменьшает стоимость системы, ее разработка все равно остается крайне дорогостоящим предприятием;
2. отсутствие человеческого фактора. Выше этот фактор отмечался как преимущество оценки экспертной системы перед человеком. Но в тоже время это и ее недостаток. Система способна действовать только по правилам, заложенным в базу знаний экспертом. В этом экспертная система проигрывает человеку, который способен действовать нестандартно, творчески и креативно.

Для обеспечения информационной безопасности необходим комплексный подход, включающий такие механизмы как антивирусные и криптографические средства, межсетевые экраны и пр. Экспертные системы, способные проводить аудит информационной безопасности системы занимают в этом списке не последнее место. Однако в силу финансовых, материальных и временных затрат на данный момент экспертные системы не имеют широкого распространения. В ближайшее время работу человека нельзя будет заменить искусственным интеллектом. Но возможно через несколько десятилетий экспертные системы займут заслуженное место среди механизмов, используемых для обеспечения информационной безопасности.

Список литературы

[1].K. Kozhakhmet, G. Bortsova, A. Inoue, L. Atymtayeva Expert System for Security Audit Using Fuzzy Logic, Midwest Artificial Intelligence and Cognitive Science Conference 2012, Cincinnati, USA, Apr 21-22, 2012.

[2]. Сердюк В. Аудит информационной безопасности – основа эффективной защиты предприятия. BYTE/Россия, 2006, №4(92), стр. 32-35

Бланк Яна Андреевна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: yanablank10@gmail.com

Макаров Антон Сергеевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: makarov.bas@gmail.com

Е.А. Колодкина, М.К. Савкин

ИССЛЕДОВАНИЕ СОВРЕМЕННЫХ ВИДОВ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Вредоносное ПО – программное обеспечение, которое разрабатывается для получения несанкционированного доступа к вычислительным ресурсам ЭВМ, а также данным, которые на ней хранятся. Такие программы предназначены для нанесения ущерба владельцу информации или ЭВМ путем копирования, искажения, удаления или подмены информации.

Киберпространство стало неотъемлемой частью повседневной жизни. Наблюдается рост объема, масштаба и стоимости киберпреступлений. За последнее время эти показатели достигли небывалого уровня. Каждую минуту можно наблюдать около полумиллиона попыток нападения, которые происходят в киберпространстве [1].

Тенденции развития информационных технологий в повседневной и корпоративной жизни влияет на спецификацию и направленность применения вредоносного программного обеспечения. Цель данной работы – рассмотреть современные направления применения вредоносного ПО, их виды и тенденции развития.

Программы-вымогатели. Программы-вымогатели (ransomware) – это вредоносные программы, которые заражают компьютерные системы, ограничивая доступ пользователей к зараженной системе. Злоумышленники пытаются вымогать деньги у жертв, отображая на экране предупреждения. Как правило, эти предупреждения сообщают, что система пользователя была заблокирована или что файлы пользователя были зашифрованы. Пользователю сообщают, что, если выкуп не будет выплачен, доступ не будет восстановлен. Размер требуемого выкупа для индивидуального пользователя широко варьируется, но чаще всего составляет $200–$400 долларов и оплачивается в виртуальной валюте, такой как bitcoin [2].

Согласно отчету Check Point Software Technologies Threat Index, в августе число видов активного вымогательского ПО выросло на 12%, в то время как число обнаруженных попыток атак с использованием ransomware выросло на 30%. По мнению специалистов Check Point, рост числа вымогательского ПО – следствие относительной легкости внедрения, а также того, что некоторые компании просто платят мошенникам, чтобы получить критические данные. В результате такие атаки становятся прибыльным и привлекательным направлением для киберпреступников.

За период 2015–2016 годов наибольшую активность показали четыре шифровальщика: это TeslaCrypt (почти половина атак), CTB Locker, Scatter и Cryakl.

В начале 2016 года появилась первая программа-вымогатель, работающая на JavaScript, получившая имя Ransom32. Использование JavaScript делает данный вымогатель кроссплатформенным, т.е. он может использо-

ваться для Windows, Linux и OS X. Ключевой особенностью Ransom32 является модель распространения SaaS (Software as a service).

Банковские зловредные ПО. В данном разделе будет рассмотрено несколько разновидностей ПО, крадущих данные банковских карт:

1) Троянец Skimer для банкоматов

Вместо традиционного подхода – приладить к банкомату фальшивое устройство, читающее карты, злоумышленники берут под контроль сразу весь банкомат. Сначала они устанавливают на банкомате троянец Skimer – либо имея физический доступ к банкомату, либо взломав внутреннюю сеть банка. Троянец заражает ядро банкомата – часть устройства, ответственную за взаимодействие с банковской инфраструктурой в целом, обработку карт и выдачу денег. В отличие от традиционной кражи данных банковских карт с помощью скиммеров, в этом случае нет никаких физических признаков того, что банкомат заражен, и злоумышленники могут спокойно считывать данные карт, вставляемых в банкомат (включая номера банковских счетов и PIN-коды пользователей), или напрямую красть наличные из банкомата [3].

2) Троянец QAKBOT

Это мульти-компонентная угроза, целью которой являются банковские данные, информация о привычных действиях пользователя и другая конфиденциальная информация. Ключевой проблемой при борьбе с троянами такого типа, как QAKBOT, является их непрерывная эволюция и возникновение всё новых модификаций [4].

3) Мобильные банковские троянцы

Мобильные банковские троянцы – одни из самых опасных видов: эти приложения воруют деньги с банковских счетов пользователей смартфонов (и планшетов).

Мобильное вредоносное ПО. Мобильные вредоносные программы продолжают эволюционировать в сторону монетизации – создатели вредоносного кода разрабатывают его для того, чтобы получать деньги от своих жертв.

По данным отчета «Лаборатории Касперского» в рейтинге обнаруженных во втором квартале 2016 года детектируемых объектов для мобильных устройств лидируют программы типа RiskTool – легальные приложения, которые потенциально опасны для пользователей. Их доля за квартал значительно выросла – с 31,6% до 45,1%, то есть практически в 1,5 раза.

Второе место в рейтинге заняли потенциально нежелательные рекламные приложения (AdWare). Их доля снизилась по сравнению с первым кварталом 2016 года на 1,4 п.п. и составила 14,2%.

В 1,7 раза упала доля Trojan-SMS – с 18,5% до 10,8%. В результате в этом рейтинге Trojan-SMS сместились со второго на третье место. Большая часть обнаруженных файлов типа Trojan-SMS является зловредами Trojan-SMS.AndroidOS.Agent.qu и Trojan-SMS.AndroidOS.Agent.f, на каждого приходится примерно по 30% от общего количества вредоносных файлов.

Практически так же упала доля Trojan-Dropper – с 14,5% в первом квартале до 9,2% во втором. Лидером среди этого типа программ стал Trojan-Dropper.AndroidOS.Agent.v – было обнаружено более 50 000 установочных пакетов, относящихся к этому троянцу [3].

Количество вирусных атак в мире растёт со скоростью плюс 3% в месяц, атак на веб-сервисы – 2,5%, краж денежных средств с различных устройств или электронных кошельков – не менее 3,5%. В России, по данным Сбербанка, потери от киберугроз составили 550-600 млрд руб. в 2015 году. Эта цифра примерно в 2 раза превышает ущерб от всех других экономических преступлений. В июне 2016 года эксперты сообщили о вероятности роста потерь от киберугроз во всем мире до $2 трлн к 2018 году.

Неуклонный рост киберпреступности остается реальной и серьезной угрозой для безопасности. Продолжает расти количество атак, используемых для кражи информации и денег. Пользователи сталкиваются с кражей их регистрационных данных или аккаунтов, причем во многих случаях они не были атакованы напрямую. Вместо этого их информация была обнаружена в базах данных, которые были украдены из взломанных сетей различных компаний.

Атаки шифровальщиков стали достаточно сложными. В ближайшие месяцы можно ожидать рост подобных атак. Эту тенденцию поддерживает рост численности мошенников, возможность высокого заработка от незаконной деятельности, а также появление новых инструментов для совершения киберпреступлений в таких сферах, как мобильное вредоносное ПО и мошенничество, направленное против банкоматов.

Для защиты от вредоносного ПО необходимо следовать основным правилам поведения в сети. К ним относятся использование антивирусной защиты, осторожность по отношению ко всей поступающей на компьютер информации (не открывать подозрительные вложения и ссылки). Также следует обращать достаточно внимания на информацию от антивирусных компаний и от экспертов по компьютерной безопасности.

Компании должны обязательно применять политику безопасности и использовать методы защиты от вредоносных программ на основе контроля доступа к файлам. Поддержание систем в актуальном состоянии также существенно снижает вероятность успешной атаки. Регулярное тестирование на проникновение и проверка конфигураций (своими силами или с помощью внешних организаций) позволят выявить ошибки в конфигурациях, до того, как злоумышленники воспользуются ими.

Список литературы

[1] http://www.cnbc.com/2015/12/28/biggest-cybersecurity-threats-in-2016.html

[2] https://www.us-cert.gov/ncas/alerts/TA16-091A

[3] Развитие информационных угроз во втором квартале 2016 года. https://securelist.ru/analysis/malware-quarterly/29062/it-threat-evolution-in-q2-2016-statistics/

[4] https://www.anti-malware.ru/news/2016-09-22/21018

Колодкина Екатерина Александровна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: rina11ri11@gmail.com

Савкин Михаил Константинович – ассистент кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: savkinmk@gmail.com

А.В. Левков, А.Н. Молчанов

К ВОПРОСУ О ПЕРЕХОДЕ НА НОВЫЙ СТАНДАРТ ШИФРОВАНИЯ ГОСТ 34.12-2015

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В Российской Федерации начали действовать новые национальные криптографические стандарты: ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры» и ГОСТ Р 34.13-2015 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров», разработанные Центром защиты информации и специальной связи ФСБ России с участием Открытого акционерного общества «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС» [1]).

Блочный шифр является важным криптографическим механизмом, который может использоваться как самостоятельный криптографический алгоритм, так и входить в состав других криптографических алгоритмов и протоколов для защиты данных, передаваемых по сетям засекреченной связи или в информационно-телекоммуникационной сети «Интернет».

Учитывая, что алгоритм криптографического преобразования ГОСТ 28147-89 хорошо зарекомендовал себя в программной и аппаратной реализации и по своим свойствам он не накладывает ограничения на степень конфиденциальности защищаемой информации, признано целесообразным включить в новый криптографический стандарт ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры» описание этого шифра с размером блока 64 бит с зафиксированными блоками нелинейной подстановки (шифр «Магма»). Фиксация блоков нелинейной подстановки сделает алгоритм, описанный в стандарте, более унифицированным и поможет исключить использование «слабых» блоков нелинейной подстановки.

При условии, что в ГОСТ Р 34.12-2015 используется шифр идентичный шифру «Магма» ГОСТ 28147-89, процесс перехода на новый стандарт шифрования является менее затратным. Но для остальных алгоритмов шифрования придется полностью перерабатывать алгоритмы криптографического преобразования.

В стандарт также включен новый блочный шифр (шифр «Кузнечик») типа «подстановочно-перестановочная сеть» с размером блока 128 бит. Данный тип шифров является хорошо изученным и относительно простым с точки зрения криптографического анализа и обоснования требуемых свойств. Ожидается, что блочный шифр с длиной блока 128 бит будет устойчив ко всем известным на сегодняшний день атакам на блочные шифры.

Режимы работы n-битного блочного шифра (режим простой замены, режим гаммирования, режим гаммирования с обратной связью по выходу, режим гаммирования с обратной связью по шифртексту, режим простой замены с зацеплением и режим выработки иммитовставки) выведены в отдельный национальный стандарт ГОСТ Р 34.13-2015 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров», что соответствует принятой международной практике.

Как уже говорилось, вторым шифром, включенным в стандарт, является опубликованный в 2013 г. российскими специалистами криптографический алгоритм «Кузнечик» с длиной входного блока, равной 128 битам, и 256-битовым ключом.

Так же, как и AES, алгоритм "Кузнечик" основан на использовании SP-сети, однако при его разработке удалось реализовать ряд синтезных решений, которые позволяют исключить выявленные за последние годы недостатки алгоритма AES.

Как мы уже отмечали ранее, использование MDS-матриц необходимо для обеспечения "быстрого" перемешивания входного вектора. С криптографической точки зрения было бы хорошо использовать большую MDS-матрицу для всего блока входных данных, однако хранить в памяти матрицу большого размера невыгодно с точки зрения эксплуатационных характеристик. В «Кузнечике» при синтезе MDS-преобразования использовался подход, предложенный отечественным ученым-алгебраистом Александром Нечаевым и заключающийся в генерации матрицы с помощью линейного регистра сдвига. Такой подход позволяет в некоторых случаях существенно экономить объем требуемой для реализации алгоритма памяти и получить матрицу для всего 128-битного блока, обрабатываемого алгоритмом, в отличие от алгоритма AES, для которого такие матрицы действуют только на 32-битных подблоках. Подход, используемый в «Кузнечике», предпочтительнее, поскольку позволил в 1,5 раза сократить число итераций по сравнению с AES и обеспечить большую защиту от атак по побочным каналам, за счет блочности линейного преобразования AES при его реализации на платформе CUDA возможно практическое восстановление ключа с использованием Timing-атаки. Для алгоритма "Кузнечик" такая атака не применима.

В качестве нелинейного преобразования была выбрана подстановка, использованная в хеш-функции ГОСТ 28147-89. Как показали 3 года интенсивных исследований отечественными и зарубежными специалистами, ее характеристики позволяют эффективно обеспечивать защиту от современных методов криптоанализа. При этом последние исследования специалистов университета Люксембурга позволили получить эффективную низкоресурсную реализацию данной подстановки[2].

Алгоритм развертки ключа основан на схеме Фейстеля и использует в качестве функции усложнения итерационное преобразование алгоритма

"Кузнечик". При таком подходе итерационные ключи шифрования имеют сложные нелинейные связи, что затрудняет применение атак со связанными ключами и метода биклик.

Стоит сказать, что алгоритм «Кузнечик» хотя и не имеет такой богатой истории, как алгоритм ГОСТ 28147–89, но его криптографические свойства уже подтверждены рядом научно-исследовательских работ зарубежных специалистов в области криптографии.

Если говорить о быстродействии программной реализации алгоритма «Кузнечик», то результаты работ позволили получить скорость порядка 135 Мбайт/с на одном ядре процессора 3.3 HGz и порядка 558 Мбайт/с на графическом процессоре[2].

ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ

Прежде чем применять новые стандарты шифрования, необходимо понять, как с минимальными затратами осуществить переход на них со старых стандартов, в частности при замене программного обеспечения. Представители ФСБ уже заявили, что с лета 2016 года года они перестанут принимать на сертификацию средства шифрования, в которых «Кузнечик» не реализован [3].

Это должно стимулировать эволюцию и замещение прежних наборов алгоритмов.

Таким образом, все производители, решившие поддерживать новые стандарты, будут вынуждены изменить криптографический слой своих программных продуктов. То есть необходимо реализовать алгоритмы стандарта ГОСТ 34.12-2015 с длиной ключа 256 бит («Кузнечик»), поскольку остальные алгоритмы, называемые «Магма», не изменились. Заказчикам же потребуется лишь обновить уже существующие средства и системы шифрования до актуальных версий». Так же, нужно еще стимулировать клиентов на приоритетное использование «Кузнечика». Пока на этом не акцентируют внимания, но очевидно, что изменение документов по использованию СКЗИ (Средства контроля защищенности информации) будет следующим шагом в их утверждении.

Чтобы новые алгоритмы получили признание, они должны быть не только более устойчивыми ко взлому, но и более производительными и хорошо распараллеливаться.

Следует отметить, что для «Стрибога» уже имеются некоторые оценки производительности, позволяющие выявить особенности алгоритма. В частности, в системах с достаточным ресурсом памяти «Стрибог» работает примерно в два раза быстрее по сравнению с реализацией на «Магме», но при ограничении по памяти (например, при выполнении кода в графических ускорителях) старая реализации хеш-функции выигрывает. Вполне возможно, что аналогичные результаты будут получены и для блочных шифров: для ограниченных по ресурсам применений будут оптимальны

старые алгоритмы «Магмы», а для полноценных вычислительных систем – новый «Кузнечик».

Следующим логичным шагом стала бы отмена действия старого ГОСТ 28147-89. Однако пока регулирующие органы не торопятся идти на жесткие меры.

Подводя итоги, можно сделать вывод, что вновь разрабатываемые СКЗИ, будут поддерживать ГОСТ Р 34.12-2015, а для действующих СКЗИ пока нет смысла переходить на новый ГОСТ. Срок отмены старого ГОСТа еще обсуждается в техническом комитете ТК-26. Эксперты полагают, что будет установлен длительный переходный период на новый стандарт шифрования. Но если вспомнить, что «Магма» входит в состав нового ГОСТа, а по сути представляет собой переопределение прежнего алгоритма шифрования, то формально перестанет действовать только старый ГОСТ, а алгоритмы из него будут легитимизированы ГОСТ Р 34.12-2015. Однако их применение, скорее всего, будет ограничено определенными классами СКЗИ.

Библиографический список

[1] http://www.infotecs.ru/press/news/15/14508/ ИнфоТеКС (ОАО «Информационные Технологии и Коммуникационные Системы») – ведущий производитель программных и программно- аппаратных VPN-решений и средств криптографической защиты информации.

[2] http://www.itsec.ru/articles2/crypto/gost-r-chego-ozhidat-ot-novogo-standarta ГОСТ Р 34.12–2015: чего ожидать от нового стандарта?

[3] http://www.osp.ru/lan/2016/06/13049759 Обновление ГОСТов на шифрование

[3] Зуев Е.С., Сорокина И.И., Астахов М.В. К вопросу расчета на прочность металло-композитного фланцевого соединения // Электронный журнал: наука, техника и образование. - 2016. - №1/2016. – [Электронный ресурс]. – Режим доступа: URL: http://nto-journal.ru/uploads/articles/8cb0dd5e83ef55edc5600f312168e7e7.pdf (дата обращения 14.10.2016)

Левков Андрей Вадимович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: furianes357@yandex.ru

Молчанов Алексей Николаевич – ст. преп. кафедры «Информационная безопасность автоматизированных систем» КФ МГТУ им. Н.Э. Баумана. E-mail: alexeymolchanov@outlook.com

К.А. Евраскина, А.А. Нефедов, О.Ю. Жарова

КЕЙЛОГГЕР

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Целью данной работы является исследование программного перехватчика событий, его основных функций, возможностей, методов его реализации и способов защиты.

Кейлоггер – программное обеспечение или аппаратное устройство, регистрирующее различные действия пользователя – нажатия клавиш на клавиатуре компьютера, движения и нажатия клавиш мыши и т. д.

Программные кейлоггеры осуществляют контроль над действиями пользователя, фиксируют нажатия клавиш, мыши, сообщения различных программ. Реализуются путем установки hook- перехватчика в фильтр сообщений Windows. После извлечение сообщения из фильтра и передаче его оконной процедуре злоумышленника оно может быть преобразовано в Unicode и далее передано в очередь, или же может быть модифицировано и также передано в очередь.

Аппаратные кейлоггеры осуществляют контроль над действиями пользователя, фиксируя нажатия клавиш. Реализуются путем установки в полости клавиатуры небольшой платы, установки считывающего устройства в разрез кабеля клавиатуры или считывания с кабеля бесконтактным методом.

Перехват нажатий клавиш может использоваться обычными программами и часто применяется для вызова функций программы из другого приложения с помощью "горячих клавиш" или, например, для переключения неправильной раскладки клавиатуры.

Большинство существующих на данный момент кейлоггеров считаются "легальными" и свободно продаются, так как разработчики декларируют множество причин для использования кейлоггеров, например:

- для службы безопасности организации: отслеживание фактов нецелевого использования персональных компьютеров, их использования в нерабочее время;
- для службы безопасности организации: отслеживание фактов набора на клавиатуре критичных слов и словосочетаний, которые составляют коммерческую тайну организации, и разглашение которых может привести к материальному или иному ущербу для организации;
- для различных служб безопасности: проведение анализа и расследования инцидентов, связанных с использование персональных компьютеров; другие причины.
- Восстановление информации в случае утери

- Определить случаи набора на клавиатуре критичных слов и словосочетаний, передача которых третьим лицам приведет к материальному ущербу;
- Исследование компьютерных инцидентов
- Выявить попытку подбора пароля
- Перехват чужой информации

Любой легальный кейлоггер может использоваться во вредоносных целях, и в последнее время именно кража информации пользователей различных систем онлайновых платежей стала главным применением кейлоггеров.

Кроме того, многие кейлоггеры прячут себя в системе, что значительно облегчает их использование в преступных целях.

Методы защиты от кейлогеров:

- Использование антишпионских/антивирусных программ
- Использование программ шифрующие вводимы данные с клавиатуры
- Эвристические анализаторы
- Внутренняя и внешняя диагностика компьютерных систем
- Пользование виртуальными клавиатурами

В отличие от других типов вредоносного программного обеспечения, для системы кейлоггер абсолютно безопасен. Однако он может быть чрезвычайно опасным для пользователя: с помощью кейлоггера можно перехватить пароли и другую конфиденциальную информацию, вводимую пользователем с помощью клавиатуры. В результате злоумышленник узнает коды и номера счетов в электронных платежных системах, пароли к учетным записям в online-играх, адреса, логины, пароли к системам электронной почты и так далее.

Использование кейлоггеров позволяет осуществлять экономический и политический шпионаж, получать доступ к сведениям, составляющим не только коммерческую, но и государственную тайну, а также компрометировать системы безопасности, используемые коммерческими и государственными структурами (например, с помощью кражи закрытых ключей в криптографических системах).

В последние годы отмечается значительный рост числа различных вредоносных программ, использующих функции кейлоггеров. От столкновения с кибер-преступниками не застрахован ни один пользователь сети Интернет, в какой бы точке земного шара он ни проживал и в какой бы организации ни работал.

В настоящий момент в антивирусных базах "Лаборатории Касперского" присутствует информация более чем о 300 семейств специализированных кейлоггеров.

Способы распространения кейлоггеров:

- Присоединение к электронному письму;

- При запуске файла из каталога, находящегося в общем доступе в peer-to-peer сети;
- С помощью скрипта на веб-страницах, который использует особенности интернет-браузеров, позволяющие программам запускаться автоматически при заходе пользователя на данные страницы;
- С помощью ранее установленной вредоносной программы, которая умеет скачивать и устанавливать в систему себе подобные аналоги

Отмечается тенденция добавления в программные кейлоггеры rootkit-технологий, назначение которых – скрыть файлы кейлоггера так, чтобы они не были видны ни пользователю, ни антивирусному сканеру;

Обнаружить факт шпионажа с помощью кейлоггеров можно только с использованием специализированных средств защиты;

Сегодня существует универсальная и надежная методика, позволяющая обойти аппаратный клавиатурный шпион, – это использование экранной клавиатуры. Следует отметить, что большинство современных антикейлоггеров специально для этих целей содержат собственную встроенную экранную клавиатуру.

Поиск аппаратных кейлоггеров непременно следует включить в должностные обязанности сотрудников службы информационной безопасности. Также необходимо иметь в виду, что вероятность установки аппаратного кейлоггера прямо пропорциональна ценности информации, вводимой на рабочем месте.

Таким образом, были рассмотрены программные и аппаратные кейлоггеры, способы их реализации, распространения и методы защиты. В результате было установлено, что в настоящее время отмечается значительный рост вредоносных программ на основе кейлоггеров, в ввиду их простой реализации.

Список литературы:

[1] *Зайцев О.* Rootkits, Spyware/ADWARE, Keyloggers & Backdoors. Обнаружение и защита. – СПб.: БХВ-Петербург, 2006. – 304 с.

[2] *Петцольд Ч.* Программирование для Windows 95. – СПб.: BHV, 1997. – 495с.

[3] ru.wikipedia.org

[4] habrahabr.ru

Евраскина Кира Александровна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: evraskinakira@yandex.ru

Нефедов Андрей Андреевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: nefedov1000@yandex.ru

Жарова Ольга Юрьевна – ассистент кафедры «Информационная безопасность автоматизированных систем» КФ МГТУ им. Н.Э. Баумана. E-mail: ouzharova@yandex.ru

Г.А. Бушина, В.В. Драган, М.К. Савкин

КРАТКИЙ ОБЗОР КЛАССОВ-КОЛЛЕКЦИЙ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В языке C# существует множество новых возможностей, наиболее значительной из них является концепция обобщенных типов, которые также называются дженериками. Их использование позволяет создавать классы, интерфейсы, которые могут работать с различными типами данных. Многие алгоритмы логически реализуются одинаково, независимо от того, к каким типам данных они будут применяться. С помощью обобщенных типов можно записать реализацию нужного алгоритма только один раз независимо от конкретного типа данных и затем применить его к любым типам данных без каких-либо трудностей.

Основополагающим понятием обобщенных типов является класс, поскольку большинство методов и задач построено на его основе. В свою очередь класс является основой языка C#, так как он определяет характер объекта. Кроме того, класс является основой объектно-ориентированного программирования.

Класс – это шаблон, который определяет форму объекта. Спецификация класса используется для создания объекта, который является его экземпляром. Важно понимать, что класс – это логическая абстракция и в памяти не существует его физического представления до тех пор, пока не создан объект этого класса. Он может содержать только код или только данные, большинство реальных классов содержат и то и другое.

Главное преимущество коллекций заключается в том, что они стандартизируют обработку групп объектов в программе. Все коллекции разработаны на основе набора четко определенных интерфейсов.

В среде .NET Framework поддерживаются несколько типов коллекции: необобщенные, специальные, с поразрядной организацией, обобщенные.

Основополагающим для всех коллекций является понятия перечислителя, который обеспечивает стандартный способ поочередного доступа к элементам коллекции.

Более подробно мы рассмотрим обобщенные коллекции. Обобщенные коллекции обеспечивают обобщенную реализацию нескольких стандартных структур данных, включая связные списки, стеки, очереди и словари. Такие коллекции являются типизированными в силу их обобщенного характера. Это означает, что в обобщенной коллекции могут храниться только такие элементы данных, которые совместимы по типу с данной коллекцией. Благодаря этому исключаются случайные несовпадения типов. Обобщенные коллекции объявлены в пространстве имен System.Collections.Generic.

Основными классами обобщенных коллекций являются:

- *Dictionary<TKey, Tvalue>*,
  Позволяет хранить пары “ключ-значение” в коллекции как в словаре. Значения доступны в словаре по соответствующим ключам. Главное свойство словарей – быстрый поиск по ключу. Ключ трансформируется в хеш. Тип, используемый в качестве ключа словаря, должен переопределять методы GetHashCode() и Equals(). Все ключи в этой коллекции должны быть уникальными, причем ключ не должен изменяться, пока он включен в словарь. В то же время значения не обязательно должны быть уникальными. При добавлении в словарь необходимо указать два параметра: ключ и значение, а удаление происходит только по ключу. Словари имеют динамический характер, расширяясь по мере необходимости.
- *List<T>*,
  Реализуется обобщенный динамический массив. Класс предоставляет возможность доступа к произвольному элементу по индексу за постоянное время (так как это массив), обеспечивает минимум накладных расходов при хранении такого списка. Вставка в конец списка происходит за постоянное время, если новое количество элементов не превышает вместимость списка. Если места нет, то необходимо создать массив в два раза больше исходного, в него будут помещены все элементы из старого массива плюс новый элемент. В итоге получаем, что при добавлении элемента при необходимости расширения массива, время линейно зависит от длины массива. Недостаток класса проявляется при вставке/удалении элемента, когда происходит перезапись всех элементов. При удалении элементов вместимость массива не уменьшается.
- *LinkedList<T>*,
  Создается коллекция в виде обобщенного двунаправленного списка. За постоянное время может выполнять вставку/удаление элементов в списке (именно вставку и удаление, поиск позиции вставки и удаления сюда не входит). Доступ к произвольному элементу осуществляется за линейное время (но доступ к первому и последнему элементу списка всегда осуществляется за константное время – ссылки постоянно хранятся на первый и последний, так что добавление элемента в конец списка вовсе не значит, что придется перебирать весь список в поисках последнего элемента). LinkedList предпочтительно применять, когда происходит активная работа (вставка/удаление) с серединой списка или в случаях, когда необходимо гарантированное время добавления элемента в список.
- *Stack<T>*
  Является обобщенным эквивалентом класса необобщенной коллекции Stack, в котором поддерживается стек в виде списка, действу-

ющего по принципу “первым вошел - последним вышел”. Коллекция класса Stack<T> имеет динамический характер, расширяясь по мере необходимости, чтобы вместить все элементы, которые должны в ней храниться.

- *Queue<T>*.
  Является обобщенным эквивалентом класса необобщенной коллекции Queue. В нём поддерживается очередь в виде списка, действующего по принципу “первым пришел – первым вышел”. Это означает, что первым из очереди извлекается элемент, помещенный в нее первым. Очереди часто встречаются в реальной жизни. Многим из нас нередко приходилось стоять в очередях к кассе в банке, магазине или столовой. В программировании очереди применяются для хранения таких элементов, как процессы, выполняющиеся в данный момент в системе, списки приостановленных транзакций в базе данных или пакеты данных, полученные по интернету. Также, как и Stack<T>, имеет динамический характер, расширяясь по мере необходимости, чтобы вместить все элементы, которые должны храниться в ней.
- *HashSet<T>*.
  Позволяет проводить высокопроизводительные операции над множествами. В этой коллекции реализуется множество, все элементы которого являются уникальными, а порядок расположения элементов во множестве особого значения не имеет. В этом классе определяется набор операций с множествами. Обход коллекции происходит с помощью цикла foreach и возвращает никак не упорядоченные результаты. Коллекция такого типа имеет динамический характер и расширяется по мере необходимости, чтобы вместить все элементы, которые должны в ней храниться.

Список литературы:

[1] Герберт Шилдт, C# 4.0: полное руководство. – М.: ООО “И.Д.Вильямс”, 2016. – 1056с.

[2] Иен Гриффитс, Программирование на C# 5.0. – М.: Эксмо, 2014. – 1136с.

[3] C# и .NET. Руководство по C# – Часть 2. URL:http://professorweb.ru/my/csharp/charp_theory/level1/index1.php

Бушина Галина Александровна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: foxylinas@yandex.ru

Драган Валерия Владимировна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: leraspanda@yandex.ru

Савкин Михаил Константинович – ассистент кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: savkinmk@gmail.com

Е.И. Алкина, О.С. Клочко

КРИПТОГРАФИЯ В НАШИ ДНИ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Каждому поколению и каждому из нас когда-либо приходится скрывать информацию от посторонних. На протяжении долгого времени людям приходилось изобретать средства шифрования и тайнописи. Позже появлялись целые шифровальные системы, которые долгое время верой и правдой служили правителям и властям, обеспечивая конфиденциальность их переписок.

В настоящее время искусство шифрования превратилось в науку – криптография. Сегодня любой желающий может защитить свои секреты от посторонних глаз, при этом с каждым днём появляются всё новые методы рассекречивания конфиденциальной информации. На поле информационной войны сохраняется баланс, тем самым придавая толчок, как для развития способов шифрования, так и для злоумышленников.

Существует два основных способа защиты информации[1]. Во-первых, можно попытаться скрыть сам факт существования секрета: нет секрета – нет и желающих его узнать. Второй способ – полная противоположность первого. Мы не скрываем факт существования секретной информации, и не ограничиваем доступ для посторонних лиц, но информация хранится в зашифрованном виде, который доступен только для «посвященных». Второй способ защиты информации и есть криптография. Шифрование происходит с помощью определенного алгоритма, и чтобы прочитать информацию необходимо ее расшифровать. Шифрование и дешифрование происходит при использовании некой ключевой информации, которой обладают только те, кому разрешен доступ к секретным данным. Например, вы написали коллеге записку: «Подготовь документы». Данная записка может быть увидена любым сотрудником, но вашу просьбу сможет понять лишь тот, кто обладает информацией о документах, т.е. вы и тот коллега, которому предназначалось послание. В действительности существует множество «хитрых» шифров, но в настоящее время, благодаря вычислительным средствам, в криптографии используются такие алгоритмы, которые до этого считались слишком трудоемкими.

Существует две области использования криптографии: защита данных во время их передачи и защита данных во время их хранения[2].

Во время передачи информации предполагается существование двух сторон: передающей и принимающей. При этом информация шифруется на передающем узле, а дешифруется на принимающем, при этом злоумышленник не может расшифровать информацию, так как не обладает «ключом». При этом способе самым уязвимом местом является распределение

ключей легальным пользователям. Существует два способа распределения ключей: симметричные и асимметричные.

Симметричные алгоритмы[3] предполагают, что данные будут зашифровываться и дешифровываться одним ключом, то есть у обеих сторон одинаковый «ключ». «Ключ» может быть как физическим (пластиковая карточка, пин-код и т.п.), так и передаваться в зашифрованном виде (предполагается, что пользователи уже владеют некой ключевой информацией). Также проблема распределения легальности заключается в том, что необходимо часто менять «ключи» для повышения стойкости против взлома, что делает систему неликвидной по отношению цена/качество. Поэтому на практике обычно используются комбинированные модели: пользователям физически доставляются долговременные ключи, а на них передаются сеансовые и уже на их основе шифруется секретная информация.

Асимметричные алгоритмы[4] появились сравнительно недавно, привнеся новое дыхание криптографии. Такой алгоритм состоит из двух частей: ключа для шифрования и ключа для дешифровки, при этом, зная ключ шифрования, практически невозможно вычислить ключ дешифровки. Недостатки существуют у любых алгоритмов, в асимметричных алгоритмах главным недостатком служит наличие лазейки для злоумышленников, которая состоит в возможности подмены легального открытого ключа, после чего он получает возможность читать перехваченные шифрованные сообщения. И вторым недостатком является низкая производительность и высокие требования к вычислительным ресурсам, что является критичным при постоянных увеличениях скорости передачи данных.

Защита данных во время хранения связана с возможностью несанкционированного доступа к компьютерам или к внешним носителям информации. При защите во время хранения нет необходимости в распределении легальностей, обычно, шифрование и дешифрование производит один и тот же человек. Поэтому для защиты данных во время хранения используют асимметричные алгоритмы.

Остался нераскрытым главный вопрос: как и где применяется данная наука практически. Главным критерием для реализации криптосхем является возможность создания эффективных и недорогих программ или устройств. Возможно, мы не замечаем, но такие программы или устройства находятся повсюду, например, для монтировки во внешние накопители или шифрования сетевого трафика, также в виде самостоятельных устройств: всевозможные электронные ключи, USB-брелоки, «магнитные таблетки», пластиковые электронные карты. Именно криптосхемы защищают наши хранимые файлы и сообщения электронной почты. Криптографические функции закладываются даже во многие операционные системы, файловые менеджеры, серьезные офисные пакеты (текстовые редакторы, электронные таблицы и т.д.). Возможно, многие и не замечают, но, благодаря криптосхемам наши конфиденциальные данные всегда защищены.

Список литературы

[1] http://school-collection.edu.ru/catalog/res/28399747-3cbc-6ad7-b265-807b7918559a/view/

[2] https://habrahabr.ru/hub/crypto/

[3] С.К.Варлатая, М.В.Шаханова «Криптографические методы и средства обеспечения ИБ» учебно-методический комплекс ДВФУ, 2015

[4] http://citforum.ru/security/cryptography/crypto_1.shtml

Алкина Елизавета Игоревна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: alkina.liza@yandex.ru

Клочко Ольга Сергеевна – ассистент кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: klochkoolgakaluga@gmail.com

М.О. Швачкина, О.С. Клочко

МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ КАК СРЕДСТВО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СИСТЕМЫ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В настоящее время использование Интернета как средства передачи конфиденциальной информации приводит к необходимости создания системы защиты данных. Межсетевое экранирование является одним из средств защиты информационных систем[1].

Межсетевой экран (firewall) представляет собой комплексное устройство, состоящее из системы предотвращения атак IPS, VPN, системы противодействия шпионскому ПО, антивируса для шлюза, URL – фильтрации и системы защиты от спама.

Межсетевой экран выполняет проверку и фильтрацию сетевых пакетов на различных уровнях сетевой модели OSI, а именно:

- На сетевом уровне осуществляется проверка адресов отправителя и получателя пакетов, номеров портов транспортного уровня, а также происходит фильтрация на основе правил, определенных администратором;
- На сеансовом уровне реализуется процедура отслеживания сеансов приложений, которая исключает передачу пакетов, нарушающих спецификации сетевых протоколов передачи данных TCP/IP, которые могут использоваться злоумышленниками.
- На уровне приложений осуществляется анализ данных пакета, что позволяет блокировать передачу информации, представляющей угрозу.

С использованием механизма NAT (Network Address Translation - функция трансляции сетевых адресов) межсетевой экран имеет возможность скрывать IP –адреса защищаемой системы. Это реализуется путем замены действительного IP -адреса отправителя на виртуальный с последующей передачей измененного пакета данных получателю. При получении ответных пакетов, межсетевой экран реализует обратную замену IP –адреса [2].

Несмотря на то, что межсетевое экранирование является средством обеспечения безопасности системы, существуют способы обхода его защитных механизмов, поэтому межсетевой экран можно отнести к одному из слабых мест инфраструктуры.

К способам обхода межсетевого экрана относятся:

1) Уязвимости при настройке межсетевого экрана.

Управление межсетевым экраном осуществляется людьми, а людям свойственно ошибаться. Злоумышленникам необходимо найти уязвимость в настройках межсетевого экрана для совершения атаки.

Существует множество ситуаций, когда администраторам отдела защиты информации требуется разрешить доступ к запрещенным серверам на некоторое время и им приходится выполнить распоряжение, изменяя

настройки межсетевого экрана и образуя, тем самым, уязвимости, которыми может воспользоваться злоумышленник.

2) Обход средств защиты.

Администраторам необходимо знать точное количество модемов, установленных в сети, и цель их использования, так как многие нарушения информационной безопасности осуществляются со стороны внутренних пользователей.

Существуют случаи обнаружения неизвестных модемов сети после анализа защищенности с помощью системы Internet Scanner, которые использовались сотрудниками фирмы для организации удаленной работы с каталогами или для получения доступа в Интернет, минуя средства защиты межсетевого экранирования.

Межсетевой экран не в состоянии обеспечивать защиту системы, если трафик, который использует уязвимости в защите, не просматривается средствами межсетевого экранирования

3) Туннели.

Защита трафика средствами межсетевого экранирования осуществляется чаще всего на основе разрешения или запрета использования конкретного протокола [3]

Злоумышленники осуществляют свою преступную деятельность в рамках разрешенного протокола.

Например, если межсетевой экран использует протокол SMTP, то через сообщения электронной почты, которые содержат вредоносные вложения, в систему могут проникнуть макровирусы и черви.

Существует атака, использующая механизм туннелированния - Loki. Данный инструмент использует протокол ICMP и позволяет злоумышленнику организовать связь с другой системой по скрытым каналам, записывая данные сразу после заголовка ICMP.

4) Использование доверенных сетей.

Высокий уровень безопасности при организации VPN-соединений с помощью межсетевых экранов с функциями VPN достигается исключительно в отсутствии связи между оппонентами по незащищенным каналам [4].

Если злоумышленнику удается получить доступ к доверительным сетям или узлам, то он может осуществлять несанкционированные действия, которые нанесут большой вред системе по причине ограниченных требований безопасности к доверенным узлам и сетям, в отличие от других узлов.

5) Межсетевой экран - как цель атаки.

После вывода из строя межсетевого экрана, злоумышленник может получить полный доступ к системе. Некорректная обработка TCP-пакетов с установленным флагом ECE в межсетевом экране IPFW может привести к таким последствиям.

В межсетевом экране BorderWare Firewall Server 6.1.2. была использована уязвимость, связанная с посылкой широковещательных запросов ICMP Echo Request по сети [5].

6) Использование уникального элемента.

Согласно модели разграничения доступа к информации, права на доступ к объекту предоставляются субъекту после предъявления и проверки уникального элемента.

Флаг заголовка или адрес пакета являются уникальными элементами сетевого уровня. Если злоумышленник предоставит такой элемент межсетевому экрану, то ему будут присвоены права субъекта - владельца секретного элемента.

Получить информацию о секретном элементе можно с помощью анализаторов протоколов при передаче по сети или путем подбора средствами специальных программ (L0phtCrack, LC4, LC+4, Crack).

Межсетевые экраны являются механизмом обеспечения безопасности системы и способны противостоять многим угрозам. Однако межсетевой экран не в состоянии организовать полную защиту системы и решить все проблемы безопасности сети. Существует множество уязвимых мест межсетевого экранирования, а также угрозы, от которых нельзя защитить систему.

Федеральная служба по техническому и экспортному контролю России (ФСТЭК) опубликовала информационное сообщение об утверждении новых требований к межсетевым экранам, в которых выделяется пять классов межсетевых экранов от «А» до «Д». Эти требования вступят в силу с 1 декабря 2016 г. [6].

Список литературы

[1] О.С. Клочко, А.В. Мазин «Анализ методов противодействия угрозам и атакам на вычислительные системы» // Наукоемкие технологии в приборо- и машиностроении и развитие инновационной деятельности в вузе: материалы Всероссийской научно-технической конференции, 25–27 ноября 2014 г. Т. 3. - М.: Издательство МГТУ им. Н. Э. Баумана, 2014. - 332 с.

[2] Бирюков А.А. «Информационная безопасность: защита и нападение» Москва: ДМК Пресс, 2013. - 474 с.

[3] Бабин С. А. Б12 «Инструментарий хакера». – СПб.: БХВ-Петербург, 2014. – 240 с.: ил. – (Глазами хакера)

[4] «Программные межсетевые экраны: огненная стена или соломенная ширма? Часть1» http://www.securitylab.ru/analytics/240197.php

[5] Поколодина Е.В., Шарипова Т.Л. «Межсетевые экраны как выжный аспект безопасности информационной системы организации» http://elibrary.ru/item.asp?id=25200224

[6] Приказ ФСТЭК России об утверждении требований к межсетевым экранам от 28 апреля 2016 г. № 240/24/1986

Швачкина Мария Олеговна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: m444767087@yandex.ru

Клочко Ольга Сергеевна – ассистент кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: klochkoolgakaluga@gmail.com

И.И. Золотин, О.Ю. Жарова

МЕЖСЕТЕВЫЕ ЭКРАНЫ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В данной научной работе исследуется одно из самых актуальных средств защиты информации - межсетевые экраны. Цель работы - рассмотреть виды, принципы функционирования, классификацию межсетевых экранов, а также их роль в обеспечении информационной безопасности не только персональных ЭВМ, но и для локальных сетей организаций и предприятий.

Межсетевой экран (брандмауэр, firewall) – комплекс аппаратных и\или программных средств, осуществляющий фильтрацию сетевого трафика согласно заданным правилам[3]. В брандмауэре может быть реализована экспертная система, которая, анализируя трафик, диагностирует события, представляющие угрозу безопасности внутренней сети, и извещает об этом администратора. Экспертная система в состоянии автоматически ужесточать условия фильтрации и изменять конфигурацию. Среди задач, которые решают межсетевые экраны, основной является защита сетей или отдельных хостов от несанкционированного доступа (рисунок 1), с использованием уязвимых мест в протоколах сетевой модели OSI или в программном обеспечении, установленном на компьютере[2].

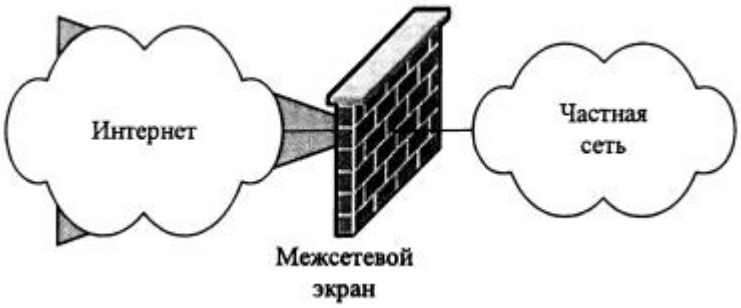


Рисунок 1. Схема применения межсетевого экрана

Первые устройства, выполняющие функцию фильтрации сетевого трафика, появились в конце 1980-х, когда Интернет был новшеством и не использовался в глобальных масштабах. Этими устройствами были маршрутизаторы, инспектирующие трафик на основании данных, содержащихся в заголовках протоколов сетевого уровня. Впоследствии, с развитием сетевых технологий, данные устройства получили возможность выполнять фильтрацию трафика, используя данные протоколов более высокого, транспортного уровня. Именно маршрутизаторы можно считать первой программно-аппаратной реализацией межсетевого экрана.

Первые программные реализации межсетевого экрана появились существенно позже и были гораздо моложе, чем антивирус. Например, проект Netfilter/iptables (один из первых программных межсетевых экранов, встроенный в ядро Linux с версии 2.4) был основан в 1998 году. Такое позднее появление вполне объяснимо, так как долгое время антивирус решал проблему защиты персональных компьютеров от вредоносных программ. Однако, в конце 1990-х, вирусы стали активно использовать отсутствие межсетевых экранов на компьютерах, что привело к повышению интереса пользователей к данному классу устройств.

Технологические возможности межсетевых экранов с начала 1990-х годов существенно улучшились. Сначала были разработаны простые пакетные фильтры, которые постепенно развивались в более сложные межсетевые экраны, способные анализировать информацию на нескольких сетевых уровнях (рисунок 2).

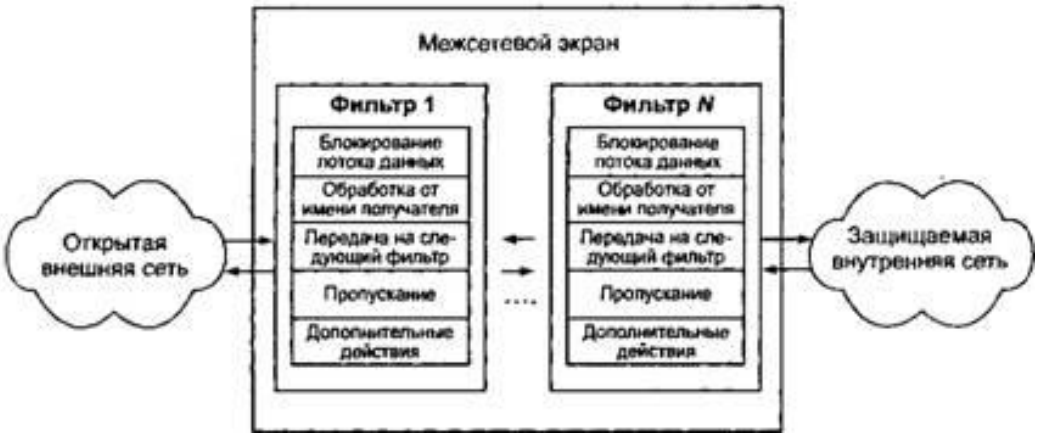


Рисунок 2. Структура межсетевого экрана

До сих пор не существует единой и общепризнанной классификации межсетевых экранов. Их можно классифицировать, например, по следующим признакам[1]:

По функционированию на уровнях модели OSI:

- пакетный фильтр (экранирующий маршрутизатор – screening router);
- шлюз сеансового уровня (экранирующий транспорт);
- прикладной шлюз(application gateway);
- шлюз экспертного уровня (stateful inspection firewall).

По используемой технологии:

- контроль состояния протокола (stateful inspection);
- на основе модулей посредников (proxy).

По исполнению:

- аппаратно-программный;
- программный.

По схеме подключения:

- схема единой защиты сети;
- схема с защищаемым закрытым и не защищаемым открытым сегментами сети;
- схема с раздельной защитой закрытого и открытого сегментов сети.

Дополнительно межсетевой экран может выполнять следующие функции:

- идентификация и аутентификация пользователей (рисунок 3). Прежде чем пользователю будет предоставлено право использования какого-либо сервиса, необходимо убедиться, что он действительно тот, за кого себя выдаёт. Данная процедура может осуществляться с использованием постоянных и одноразовых паролей, цифровых сертификатов, выдаваемых удостоверяющими центрами. Как правило, большинство межсетевых экранов поддерживаю несколько различных схем аутентификации, позволяя администратору сетевой безопасности выбрать наиболее приемлемую.

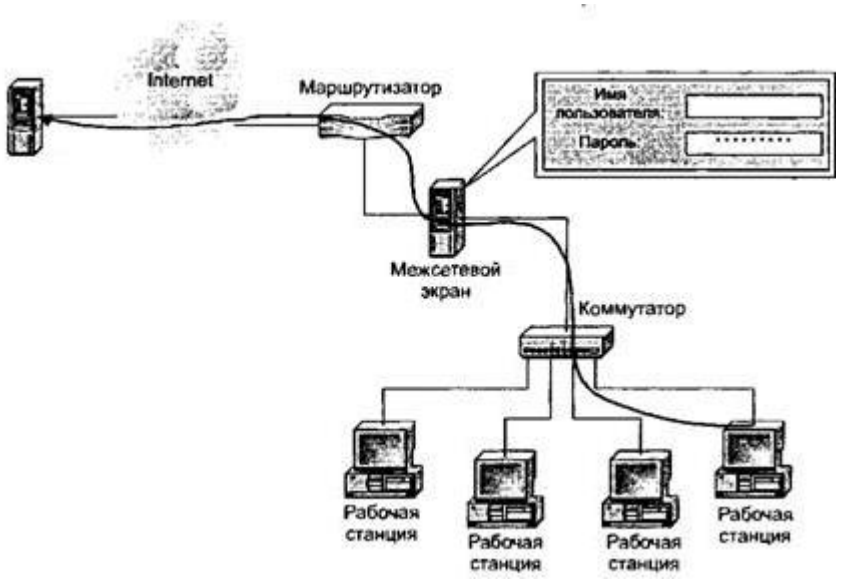


Рисунок 3. Схема аутентификации пользователя с использованием межсетевого экрана

- трансляция сетевых адресов (рисунок 4). Для реализации атак злоумышленнику необходимо знать сетевой адрес атакуемого компьютера. Для сокрытия адресов внутри сети и её топологии, межсетевые экраны выполняют трансляцию внутренних сетевых адресов. Для всех исходящих пакетов выполняется автоматическое преобразование IP-адресов компьютеров-отправителей в один IP-адрес, используемый межсетевым экраном. Кроме выполнения защитных функций, данный механизм позволяет иметь внутри сети собственную систему адресации, что эффективно решает проблему расширения адресного пространства внутренней сети и дефицита адресов внешней сети.

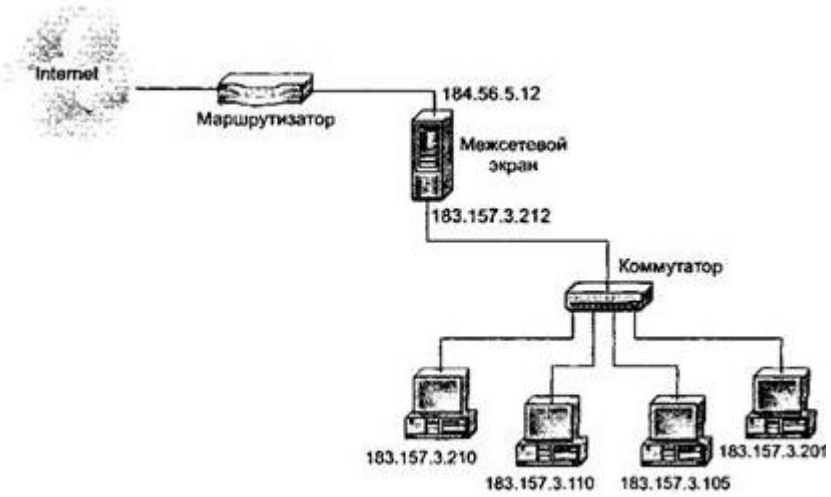


Рисунок 4. Трансляция сетевых адресов

- администрирование, регистрация событий и генерация отчётов. Важными функциями межсетевых экранов являются регистрация событий, реагирование на них, анализ зарегистрированной информации и составление отчётов. К таким действиям относятся не только пропуск или блокирование сетевых пакетов, но и изменение правил доступа и конфигурации. Регистрация позволяет обращаться к журналам для расследования инцидентов безопасности. При выполнении атаки или зондирования межсетевого экрана злоумышленником, система может выдать сигнал администратору и детальную информацию о событии в реальном времени.

В результате проведённого исследования было установлено, что межсетевые экраны являются одним из наиболее эффективных и актуальных специализированных средств защиты информации. Несмотря на то, что для обеспечения информационной безопасности необходим комплексный подход, включающий в себя множество элементов, как аппаратных, так и программных, межсетевой экран в состоянии противодействовать подавляющему большинству внешних сетевых угроз.

Список литературы

[1] Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. – ИНФРА-М, 2011. – 416 с.

[2] Лебедь С. В. Межсетевое экранирование. Теория и практика защиты внешнего периметра. – МГТУ им. Н. Э. Баумана, 2002. – 306 с.

[3] ru.wikipedia.org

Золотин Иван Игоревич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: xdfgd2014@yandex.ru

Жарова Ольга Юрьевна – ассистент кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: ouzharova@yandex.ru

Т.С. Белова, О.С. Клочко

МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДАННЫХ ОТ СНИФФЕРОВ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В настоящее время неотъемлемой частью нашей жизни является использование интернета, который выполняет важные функции во всех сферах жизнедеятельности людей. В большинстве случаев люди предпочитают использовать бесплатный интернет (сеть WiFi), так как это позволяет сэкономить деньги, требуемые на покупку личного роутера. Но в погоне за экономией люди забывают об опасностях, которые несут незащищенные сети, таких как перехват личных данных и паролей, хранимых на персональных устройствах. В большинстве случаев кража через сеть WiFi осуществляется за счет использования злоумышленником анализаторов пакетов (снифферов). Целью данной статьи является изучение принципа работы анализатора пакетов и обзор основных методов защиты данных от них.

Сниффер или анализатор пакетов – это программа, используемая злоумышленниками для перехвата, интерпретирования, сохранения пакетов, передаваемых по сети, и их последующего анализа. Первоначально разработанные для решения проблем в сети, данные программы с 1990 года получили широкое распространение среди хакеров, которые применяли их для захвата логина и пароля пользователя. В большинстве случаев конфиденциальные данные пользователей передаются в ряде сетевых протоколов незашифрованными или слабозашифрованными, что повышает легкость их перехвата и минимизирует возможность хакеров быть обнаруженными. Сниффер может анализировать только ту информацию, которая проходит через его сетевую карту. Поэтому злоумышленнику для совершения перехвата необходимо создать свою собственную сеть (название обычно совпадает с названием популярного заведения), к которой впоследствии подключится жертва. После подключения все пакеты личных данных жервы следуют через устройство злоумышленника, что предоставляет ему возможность перехватить их и, проанализировав, заполучить логины и пароли.

Рассматривая принцип работы программных снифферов (Рис.1), предназначенных для сетей Ethernet, необходимо отметить особенность, что они работают на уровне сетевого адаптера NIC (Network Interface Card) и имеют возможность тайным образом перехватывать весь траффик. Снифферы могут уклоняться от средств фильтрации, применяемых для интерпретации данных драйверами Ethernet и стеком TCP/IP, и затем овладевают всем, что проходит по проводам. Также они сохраняют кадры в двоичном формате и

затем декодируют их для извлечения информации более высокого уровня, которая замаскирована внутри. Для перехватывания всех пакетов, проходящих через сниффер, ему необходим «беспорядочный режим», который может быть автоматически включен при запуске пакетного анализатора или координироваться им вручную при помощи определенных настроек. Декодер пакетов сниффера расшифровывает всю перехваченную информацию и затем распределяет ее по уровням иерархии для последующего анализа. [1]

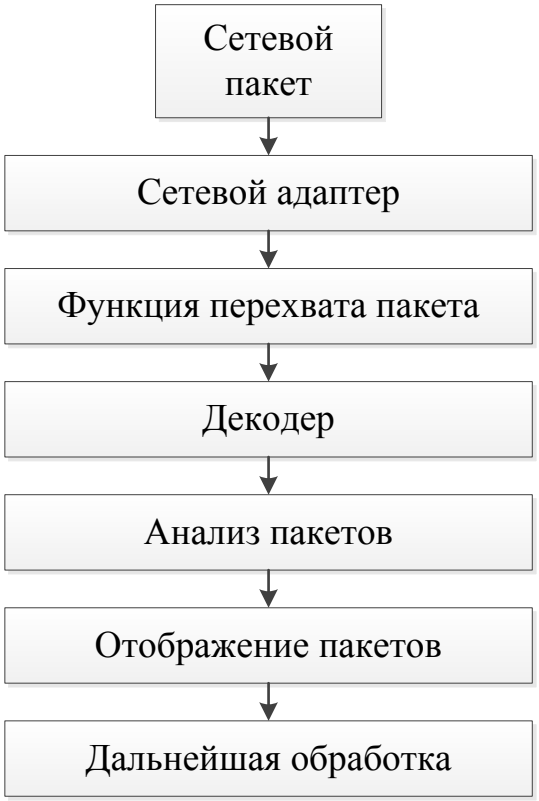


Рис. 1. Схема принципа работа сниффера

Способы перехвата сетевых пакетов:

- «прослушивание» сетевого интерфейса, разделяемое на активное и пассивное. Пассивное прослушивание – перевод сетевой платы в неразборчивый режим и перехват проходящего через устройство злоумышленника трафика. Активное прослушивание – использование специализированных средств для принудительного перевода трафика на злоумышленника (даже из другого сегмента сети);
- принудительное подключение сниффера в разрыв канала с целью прохождения через него сетевого трафика жертвы;
- побочные электромагнитные излучения – генерируемые смециальными устройствами злоумышленника;
- организация перехвата путем атаки на канальном или на сетевом уровне. В этом случае, первоначально, трафик жертвы переориентируется на сниффер, поступая затем к самой жертве. [2]

В настоящее время наибольшую известность получили следующие снифферы:

1. Ngrep. Данный анализатор может выделять те данные из перехваченного трафика, которые соответствуют регулярным выражениям (подобно утилите grep). Для работы данного анализатора необходимо вводить команды в командную строку. Ngep может быть скомпилирован и перенесен на различные платформы. Он работает во многих UNIX-подобных операционных системах, таких как Linux и Solaris, AIX и BSD, Microsoft.
2. *Tcpdump. Данный анализатор пакетов является утилитой Unix. Он позволяет прослушивать и анализировать сетевой трафик, который проходит через устройство с данной программой. Управление данным снифферо*м *происходит через командную строку. Сниффер работает* на большинстве Unix-подобных операционных системах: Linux и Solaris, BSD и OS X, HP-UX и AIX, Windows
3. Wireshark. Данный анализатор пакетов позволяет перехватывать сетевой трафик и отображать его в детальном виде. Он имеет графический пользовательский интерфейс и может свободно перемещаться по всем перехваченным данным. Главными особенностями данного сниффера являются автоматическая сортировка пакетов на заранее определенные для данного протокола поля и система фильтров, отображающая только интересующие данные. Сниффер работает на большинстве Unix-подобных операционных систем: Linux и OS X, BSD и Solaris, Microsoft.

Обеспечения безопасности данных, подверженных угрозе перехвата данных с помощью сниффера, осуществляется при использовании следующих методов:

1) Использование безопасного соединения HTTPS. HTTPS является расширением протокола HTTP, которое поддерживает шифрование. Информация отправленная через данный протокол получает защиту через криптографические механизмы SSL (secure sockets layer – уровень защищённых сокетов) и SSH (Secure Shell – «безопасная оболочка»), что обеспечивает защиту от злоумышленных нападений, осуществляемых через вторжения снифферов в сетевое соединение.
2) Аутентификация. Она подразумевает однократный пароль, который генерируется по случайному принципу. Если с использованием сниффера злоумышленник перехватит данный пароль, то полученная информация будет бесполезной, так как в данный момент времени момент пароль уже будет использован и выведен из употребления.
3) Криптография. Данный механизм позволяет сделать канал связи криптографически защищенным, а значит злоумышленник перехватит не конфиденциальную информацию, а зашифрованный текст.

Основными криптографическими протоколами сетевого управления являются протоколы SSH и SSL.

4) Антиснифферы. Это аппаратные или программные средства, осуществляющие обнаружение снифферов, действующих в пользовательской сети. (Табл.1) Их основными задачами являются измерение времени реагирования хостов и выявление «лишнего» трафика.

Таблица 1. Наиболее распространенные виды антиснифферов

Название	Описание
AntiSniff	Данный продукт, выпущенный группой разработчиков Lopht, позволяет выявлять чужеродные программы в сети, которые собирают и анализируют данные пользователя. Особенностью данной программы является возможность сканирования как одной машины, так и нескольких.
PromiScan	Программа, позволяющая сканировать локальную сеть на узлы (сетевые карты), которые работают в «беспорядочном» режиме. При обнаружении снифферов своевременно предупреждает об этом.

5) Коммутирующая инфраструктура. Используется для разделения сети на сегменты и последующего экранирования локального трафика внутри сегмента. Данный механизм не позволяет передавать данные за пределы данного сегмента, за исключением тех, которые адресованы другим сегментам данного компьютера. [3]

Таким образом, чтобы обезопасить свою конфиденциальную информацию от перехвата сниффером необходимо применять предназначенные для защиты данных программные продукты, либо быть предельно внимательными к подключаемой сети.

Список литературы

[1] Информационный ресурс КомпьютерПресс http://compress.ru/Article.aspx?id=16244

[2] Информационный ресурс Кафедра Интеллектуальных Информационных Технологий ИнФО УрФУ http://lecturesnet.readthedocs.io/net/sniff.html

[3] *Советов*, Б. Я. Информационные технологии: Учеб. для вузов/ 3-е изд., стер. – М.: Высш. шк., 2006

Белова Татьяна Сергеевна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: tanya.belova19@yandex.ru

Клочко Ольга Сергеевна – ассистент кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: klochkoolgakaluga@gmail.com

И.А. Мальцев, М.К. Савкин

ОБЗОР СВЁРТОЧНЫХ НЕЙРОННЫХ СЕТЕЙ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Свёрточная нейронная сеть (англ. *convolutional neural network, CNN*) – специальная архитектура искусственных нейронных сетей, предложенная Яном Лекуном и нацеленная на эффективное распознавание изображений, входит в состав технологий глубинного обучения (англ. *deep learning*). Использует некоторые особенности зрительной коры, в которой были открыты так называемые простые клетки, реагирующие на прямые линии под разными углами, и сложные клетки, реакция которых связана с активацией определённого набора простых клеток. Таким образом, идея свёрточных нейронных сетей заключается в чередовании свёрточных слоев (англ. *convolution layers*) и субдискретизирующих слоев (англ. *subsampling layers*, слоёв подвыборки). Структура сети – однонаправленная (без обратных связей), принципиально многослойная. Для обучения используются стандартные методы, чаще всего метод обратного распространения ошибки. Функция активации нейронов (передаточная функция) – любая, по выбору исследователя.

Название архитектура сети получила из-за наличия операции свёртки, суть которой в том, что каждый фрагмент изображения умножается на матрицу (ядро) свёртки поэлементно, а результат суммируется и записывается в аналогичную позицию выходного изображения.

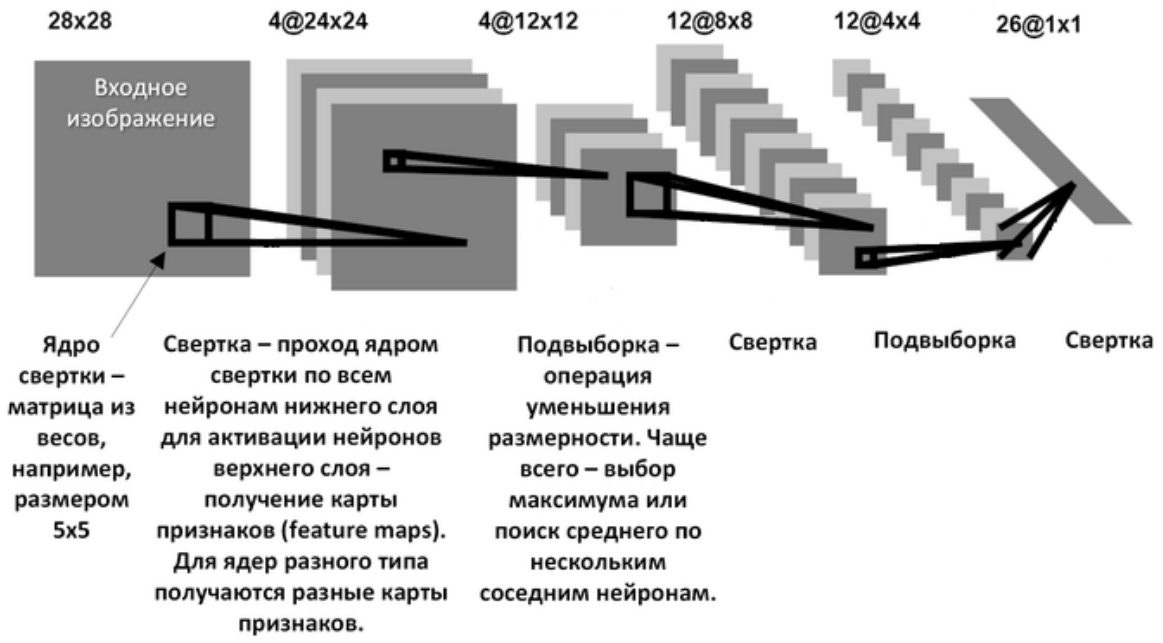


Рис. 1. Архитектура свёрточной нейронной сети

Архитектура и принцип работы. В обычном перцептроне, который представляет собой полносвязную нейронную сеть, каждый нейрон связан со всеми нейронами предыдущего слоя, причем каждая связь имеет свой персональный весовой коэффициент. В свёрточной нейронной сети в операции свёртки используется лишь ограниченная матрица весов небольшого размера, которую «двигают» по всему обрабатываемому слою (в самом начале – непосредственно по входному изображению), формируя после каждого сдвига сигнал активации для нейрона следующего слоя с аналогичной позицией.

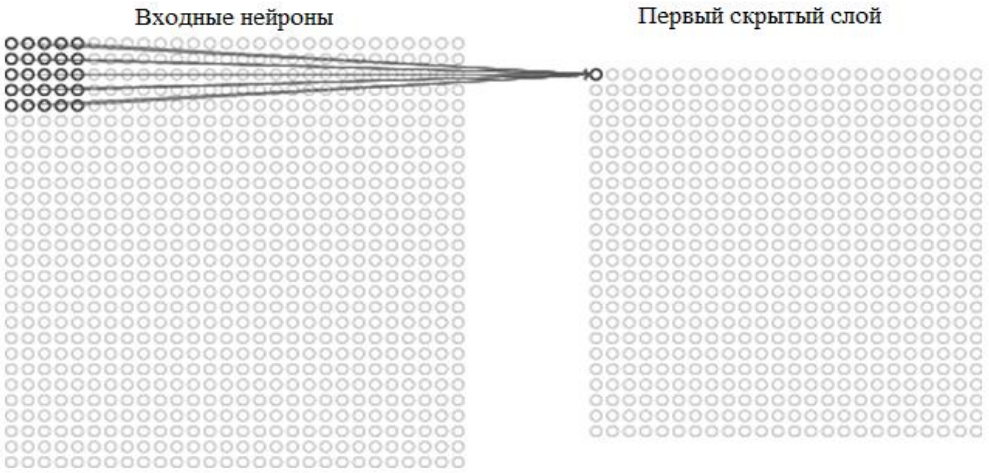


Рис. 2. Свёртка исходного изображения

Для различных нейронов выходного слоя используются общие веса - матрица весов, которую также называют набором весов или *ядром свёртки*. Она построена таким образом, что графически кодирует какой-либо один признак, например, наличие наклонной линии под определенным углом.

0	0	0	0	0	30	0
0	0	0	0	30	0	0
0	0	0	30	0	0	0
0	0	0	30	0	0	0
0	0	0	30	0	0	0
0	0	0	30	0	0	0
0	0	0	0	0	0	0

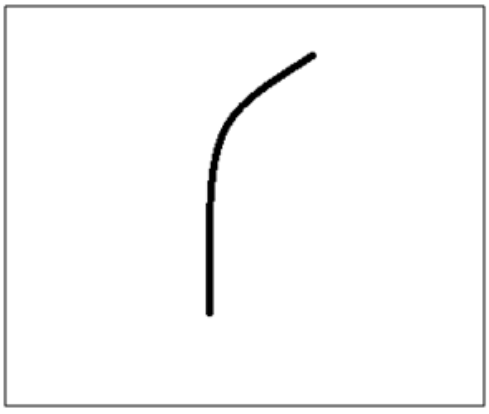


Рис. 3. Ядро свёртки

Тогда следующий слой, получившийся в результате операции свёртки такой матрицей весов, показывает наличие данной наклонной линии в обрабатываемом слое и её координаты, формируя так называемую карту признаков (англ. *feature map*).

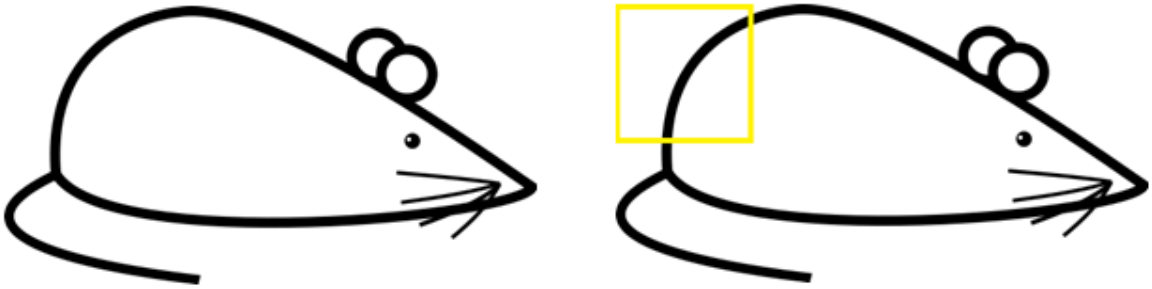


Рис. 4. Исходное изображение

0	0	0	0	0	0	30
0	0	0	0	50	50	50
0	0	0	20	50	0	0
0	0	0	50	50	0	0
0	0	0	50	50	0	0
0	0	0	50	50	0	0
0	0	0	50	50	0	0

Элемент входного изображения

*

0	0	0	0	0	30	0
0	0	0	0	30	0	0
0	0	0	30	0	0	0
0	0	0	30	0	0	0
0	0	0	30	0	0	0
0	0	0	30	0	0	0
0	0	0	0	0	0	0

Ядро свёртки

Произведение и сумма = (50*30)+(50*30)+(50*30)+(20*30)+(50*30) = 6600

Рис. 5. Признак, указанный в ядре свёртки, найден

0	0	0	0	0	0	0
0	40	0	0	0	0	0
40	0	40	0	0	0	0
40	20	0	0	0	0	0
0	50	0	0	0	0	0
0	0	50	0	0	0	0
25	25	0	50	0	0	0

Элемент входного изображения

*

0	0	0	0	0	30	0
0	0	0	0	30	0	0
0	0	0	30	0	0	0
0	0	0	30	0	0	0
0	0	0	30	0	0	0
0	0	0	30	0	0	0
0	0	0	0	0	0	0

Ядро свёртки

Произведение и сумма = 0

Рис. 6. Признак, указанный в ядре свёртки, не найден

Естественно, в свёрточной нейронной сети набор весов не один, а целая гамма, кодирующая всевозможные линии и дуги под разными углами. При этом такие ядра свертки не закладываются исследователем заранее, а формируются самостоятельно путём обучения сети классическим методом распространения ошибки. Проход каждым набором весов формирует свой собственный экземпляр карты признаков, делая нейронную сеть многомерной (много независимых карт признаков на одном слое). Также следует отметить, что при переборе слоя матрицей весов её передвигают обычно не на полный шаг (размер этой матрицы), а на небольшое расстояние. Так, например, при размерности матрицы весов 5×5 её сдвигают на один или два нейрона (пикселя) вместо пяти, чтобы не «перешагнуть» искомый признак.

Операция субдискретизации (англ. *subsampling*, англ. *pooling*, также переводимая как «операция подвыборки» или операция объединения), выполняет уменьшение размерности сформированных карт признаков. В данной архитектуре сети считается, что информация о факте наличия искомого признака важнее точного знания его координат, поэтому из нескольких соседних нейронов карты признаков выбирается максимальный и принимается за один нейрон карты признаков уменьшенной размерности. Также иногда применяют операцию нахождения среднего между соседними нейронами. За счёт данной операции, помимо ускорения дальнейших вычислений, сеть становится более инвариантной к масштабу входного изображения. Таким образом, повторяя друг за другом несколько слоёв свёртки и субдискретизации, строят свёрточную нейронную сеть. Чередование слоёв позволяет составлять карты признаков из карт признаков, что на практике означает способность распознавания сложных иерархий признаков. Обычно после прохождения нескольких слоев карта признаков вырождается в вектор или даже скаляр, но таких карт признаков становится сотни. На выходе сети часто дополнительно устанавливают несколько слоев полносвязной нейронной сети (перцептрон), на вход которой подаются оконечные карты признаков. Если на первом слое ядро свёртки проходит только по одному исходному изображению, то на внутренних слоях одно и то же ядро проходит параллельно по всем картам признаков этого слоя, а результат свертки суммируется, формируя (после прохождения функции активации) одну карту признаков следующего слоя, соответствующую этому ядру свертки.

Наиболее простым и популярным способом обучения является метод обучения с учителем (на маркированных данных) – метод обратного распространения ошибки и его модификации.

Применение сверточных нейронных сетей. За несколько лет в задачах классификации изображений свёрточные нейросети добились точности, сравнимой с точностью, достигаемой человеческим мозгом; можно сказать, что на данный момент они существенно превосходят человеческий

мозг. Когда вам нужно распознавать изображение, принадлежащее нескольким тысячам классов, человеческий мозг обычно не может удержать названия этих тысяч классов в памяти, а свёрточная нейросеть может помнить все эти классы. Из года в год прогресс достигается во многом за счет того, что нейросеть становится все глубже и глубже, то есть содержит все больше и больше слоев. И если первая большая нейросеть из группы Торонто содержала чуть более десятка слоев, то в 2016 году самая глубокая нейросеть, которая выигрывала в нескольких соревнованиях, содержит больше 150 слоев.

Кроме того, выяснилось, что любую задачу, связанную с распознаванием образов в компьютерном зрении, свёрточные нейросети могут решать более успешно, чем предшествующие методы. Это касается не только задачи классификации, но и задачи обнаружения небольших объектов на фото или видео, задачи распознавания лиц, задачи определения положения, позы человека на фотографии – во всех таких задачах свёрточные нейросети стали добиваться результатов, которые раньше были невозможны. Более того, выяснилось, что свёрточные нейросети могут очень успешно применяться в обратной задаче, когда вам нужно не обработать, а синтезировать изображение или обработать его каким-то специальным образом, например, стилизовать его, как в нашумевших приложениях вроде *Prisma*.

Список литературы

[1] *Yann LeCun, J. S. Denker, S. Solla, R. E. Howard and L. D. Jackel: Optimal Brain Damage, in Touretzky, David (Eds), Advances in Neural Information Processing Systems 2 (NIPS*89), Morgan Kaufman, Denver, CO, 1990*

[2] https://habrahabr.ru/post/309508/

[3] https://ru.wikipedia.org/wiki/Сверточная_нейронная_сеть

[4] https://postnauka.ru/video/66872

Мальцев Игорь Алексеевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: igor.astralwork@yandex.ru

Савкин Михаил Константинович – ассистент кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: savkinmk@gmail.com

В.О. Нестеров, А.Н. Молчанов

ОБЗОР ТЕХНОЛОГИИ ЕДИНОЙ ТОЧКИ АВТОРИЗАЦИИ (SINGLE SIGN-ON)

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Авторизация – это предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий. [1]

Существуют различные подходы(механизмы) к решению вопросов авторизации в информационных системах, одним из которых является single sign-on.

Single sign-on - это механизм единого входа в систему или в приложение, принцип работы которого состоит в распознавании любого интерфейса процесса аутентификации и автоматического заполнения формы ввода пароля для каждого корпоративного приложения. Другими словами, решения на основе SSO осуществляют аутентификацию во все приложения вместо пользователя, при этом исключают необходимость запоминания множества паролей и сокращают время доступа к приложениям. Ключевыми особенностями таких решений являются быстрая реакция на действия пользователя и отсутствие внесения каких-либо сценариев или изменений в существующие процессы аутентификации приложений. [2]

Большинство современных и успешных организаций используют множество корпоративных приложений в своей повседневной деятельности. Это различные почтовые, CRM и ERP системы, корпоративные порталы, бухгалтерские и Интернет приложения, базы данных и службы каталогов. Для разграничения доступа к данным и предоставления соответствующих прав и возможностей каждое приложение требует **аутентификации пользователей** перед началом работы. При этом корпоративная политика безопасности устанавливает ряд требований к системе аутентификации, например, допустимое время входа в приложение, формат имени пользователя, политика использования паролей. Многообразие приложений в сочетании с применением политики аутентификации приводит к следующим проблемам:

- Пользователю необходимо запоминать множество сложных паролей для входа в различные приложения. Пароли периодически меняются, что вынуждает пользователей записывать их на видном месте. Часто пользователи пытаются использовать один пароль одновременно для доступа к корпоративным и личным приложениям.
- Сотрудникам ИТ и Help Desk подразделений необходимо управлять системой аутентификации приложений, следить за сложностью па-

ролей, сроком их действия, проводить операции по восстановлению и отвечать на вопросы пользователей. По статистике, наиболее частое обращение пользователей в техническую поддержку связано с забытыми паролями и невозможностью входа в приложение.

- При увольнении, приеме на работу или смене должности сотрудника обслуживающим подразделениям необходимо отслеживать порядок доступа к каждому приложению и вовремя активировать/удалять/изменять пароли.

Чем больше организация использует приложений, требующих аутентификации, тем сильнее проявляются эти проблемы.

Возможности SSO. Надежность единой прозрачной аутентификации в корпоративные ресурсы основана на первоначальном входе в систему, поэтому для безопасного доступа необходимо использовать механизмы строгой аутентификации пользователей. При этом решения по строгой аутентификации, например, One Time Password и USB токены, биометрические считыватели и смарт-карты могут применяться одновременно для Single Sign On доступа, входа в приложение или операционную систему и удаленного VPN подключения. Это позволяет комбинировать и связывать различные модули аутентификации в единую корпоративную систему аутентификации пользователей.

Некоторые SSO решения позволяют совмещать физический доступ в помещение с логическим входом в операционную систему или приложение. Например, сотрудник покинул здание, приложив карту доступа к датчику «выход» - его учетная запись автоматически заблокировалась; в корпоративную сеть пытается авторизоваться учетная запись сотрудника, еще не пришедшего на рабочее место - авторизация не будет успешной, но в журналах будет сделана соответствующая запись о такой попытке. В результате организации могут использовать общую политику доступа на основе местонахождения пользователя, роли и/или статуса сотрудника - включая мгновенный запрет входа в корпоративную сеть на основе аннулирования карточки физического доступа в здание организации. Дальнейшее развитие интеграции систем доступа отражается в совместном использовании web-камер, которые позволяют в режиме реального времени следить за наличием пользователя на рабочем месте; при его отсутствии учетная запись блокируется автоматически. [3]

Для снижения звонков в службу поддержки решение SSO позволяет пользователям управлять своими паролями в случае их утери или смены. Пользователю выдается список вопросов, характерный для данной должности, на которые он раньше ответил. После правильного ответа на вопросы пользователю предоставляется возможность сменить пароль.

С ростом необходимости соответствия стандартам и для упрощения аудита по процедурам аутентификации каждое SSO решение должно иметь компонент отчетности. В централизованном журнале ведется запись всех

событий, связанных с пользователями - пользовательский профиль, смена пароля, запуск/окончание сессии, удачные/неудачные попытки аутентификации и т.д.

Технология Single Sign On - это эффективное решение по управлению доступом пользователей к корпоративным приложениям. За счет однократной прозрачной аутентификации SSO позволяет получить доступ к клиент-серверным, Windows, Java и Web приложениям, упрощает управление учетными записями сотрудников и позволяет соответствовать политикам безопасности и требованиям регуляторов.

Достоинства и недостатки Single Sign On.

Достоинства:

- Приложение может не хранить аутентификационную информацию – все хранится на стороне провайдера. Если приложение взломают, атакующий не получит аутентификационную информацию (в зависимости от приложения – это могут быть пароли, хеши паролей, зашифрованные пароли).
- У пользователя одна и та же учетная запись для доступа к нескольким приложениям, если они используют один и тот же SSO-провайдер. Теоретически это должно заставить пользователя выбрать более стойкий единый пароль.
- Если пользователь был аутентифицирован при доступе к одному из приложений, то при доступе к другому приложению повторный ввод имени пользователя и пароля не потребуется. [4]

Недостатки:

- Атакующему нужно узнать только один пароль, чтобы получить доступ сразу к нескольким приложениям от имени пользователя.
- Необходимо доверять SSO-провайдеру, который представляет собой «черный ящик». Как правило, владелец приложения ничего не знает о безопасности SSO-провайдера: каким образом хранится аутентификационная информация, кто имеет к ней доступ, какие действия предпринимает SSO-провайдер для обеспечения безопасности.
- SSO-провайдер – это точка отказа. Если по каким-то причинам он недоступен, это приведет к неработоспособности приложения.
- Код на стороне приложения, отвечающий за SSO, – это дополнительный источник уязвимостей. [4]

Выводы. Единая система авторизации является хорошим концептом для обеспечения единого безопасного доступа к приложениям, увеличения производительности труда сотрудников поддерживающих подразделений и снижения нагрузки на пользователей. При этом если система будет построена не корректно или с ошибками, то потери данных будут более пагубными, чем при использовании классических методов авторизации.

При выборе данной системы авторизации необходимо учитывать тот факт, что при потере единых авторизационных данных теряются ключи сразу от всех ресурсов, привязанных к этим данным. С другой стороны, имея множество авторизационных данных тяжелее обеспечить их безопасность и сложнее отследить потерю авторизационных данных от одного из ресурсов.

Список литературы

[1] Олифер В. Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. - П.Питер - 2016. - С. 992.

[2] Шаньгин В.Ф. Защита информации в компьютерных сетях. - М.ДМК - 2012. - С. 589

[3] Аутентификация пользователей на основе технологии SSO// «Совит». Обзорные статьи по информационной безопасности – 2016 - [Электронный ресурс]. – Режим доступа: URL: http://www.sovit.net/articles/technologies/single_sign_on1/ (дата обращения 5.10.2016)

[4] Егоров М. Небезопасная аутентификация. Ищем баги в приложениях с Single Sign-On на базе SAML// Электронный журнал: Хакер. - 2016. - №213/2016. – [Электронный ресурс]. – Режим доступа: URL: https://xakep.ru/2016/02/09/hacking-single-sign-on/ (дата обращения 5.10.2016)

Нестеров Владислав Олегович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: v-neste@yandex.ru

Молчанов Алексей Николаевич – ст. преп. кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: alexeymolchanov@yandex.ru

Я.А. Кадурин, М.К. Савкин

ОБЩЕЯЗЫКОВАЯ ИСПОЛНЯЮЩАЯ СРЕДА

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Общеязыковая исполняющая среда. «Общеязыковая исполняющая среда» (англ. «Common Language Runtime», CLR) – составная часть .NET Framework. Система, обеспечивающая переносимость программ между различными архитектурами компьютеров, возможность написания программных модулей на различных языках программирования, а также отвечающая за безопасность использования ресурсов компьютера. Данная система весьма упрощает работу программистов при написании различного ПО, так как автоматически отслеживает все аспекты программирования, связанные с архитектурной совместимостью программ и корректного использования ресурсов системы.

Промежуточный язык Microsoft. «Промежуточный язык Microsoft» (англ. «Microsoft Intermediate Language», MSIL, или просто IL) – специальный псевдокод, представляющий собой набор переносимых инструкций, не зависящих от типа процессора. В результате компиляции программы, написанной на языке, который поддерживается CLR, на выходе получается не исполняемый код, а файл, содержащий IL-код. При необходимости получить исполняемый файл программы, CLR-система, основываясь на особенностях процессора и системы в целом, должна перевести промежуточный файл в исполняемый файл непосредственно во время работы программы.

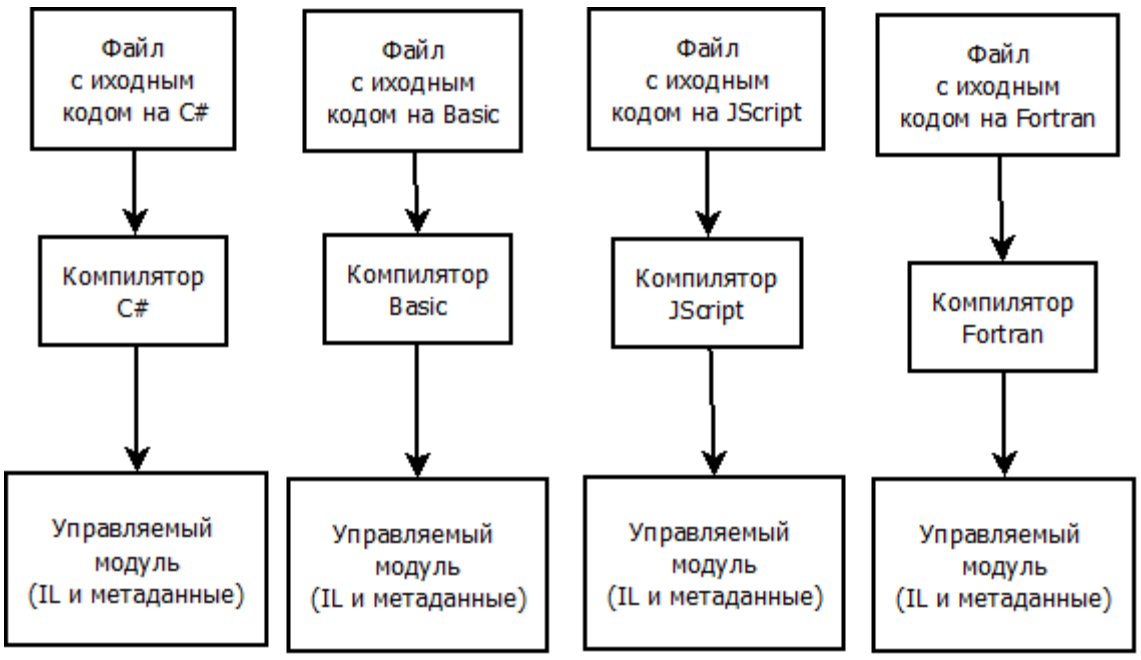


Рис. 1. Трансляция исходных файлов в IL

Все языки, поддерживаемые CLR-системой, транслируются в IL-файлы, которые затем транслируются в исполняемые. Таким образом, в CLR не возникнет никаких конфликтов, если одна часть программы будет написана, к примеру, на C#, а другая на Visual Basic. Благодаря MSIL в CLR организована поддержка многоязыкового программирования.

JIT-компиляция. Перевод IL-кода осуществляется с помощью JIT-компиляции (англ. JIT – «Just-in-Time» – рус. «к нужному моменту»). JIT-компилятор транслирует промежуточный код в машинные команды непосредственно перед выполнением этой команды. Данный вид компиляции увеличивает скорость трансляции кода за счет увеличения используемой памяти. При запуске программы, главная функция, когда вызывается некоторый метод, передает управление JIT-компилятору. Затем JIT-компилятор обращается к описанию вызываемого метода и получает его IL-код. После JIT-компилятор выделяет блок памяти, транслирует IL-код в машинный код, записывает его в выделенный ранее блок, меняет точку входа метода на данный блок памяти и передает машинному коду в данном блоке управление. JIT-компилятору достаточно единожды преобразовать IL-код метода в машинный код. Если же в программе снова будет вызываться уже скомпилированный метод, то весь процесс компиляции будет проигнорирован, а управление сразу же будет передано машинному коду, хранящимся в памяти.

Общеязыковая спецификация. С появлением .NET Framework многие компании начали настраивать различные языки программирования, чтобы они могли работать в среде CLR. Однако, это было затруднительно, так как языки программирования имеют множество различных аспектов, конфликтующих с принципами работы CLR, например, парадигмы программирования, способы сообщений о наличии ошибок в работе программы или чувствительность к регистру. Чтобы программисты могли настроить язык программирования под .NET, Microsoft создала «общеязыковую спецификацию» (англ. «Common Language Specification», CLS), которая описывает минимальный набор требований к языку, чтобы он мог быть управляем CLR-системой. Например, т.к. CLR использует исключения для уведомления пользователя о наличии непредвиденной ситуации, и ее обработки, то и язык, который настраивается под CLR, должен использовать исключения. CLS не ограничивает программиста в определении возможностей настраиваемого им языка, а лишь подсказывает, что необходимо реализовать в первую очередь для корректной и эффективной работы языка в CLR.

Безопасный и небезопасный код. Любой код, написанный на языке под управлением CLR, является по умолчанию безопасным. В безопасном коде CLR не позволяет использовать указатели и адресную арифметику, а сборщик мусора очищает выделенную память при ненадобности. В итоге все сомнительные операции, описанные в IL, CLR предотвращает. Такой

подход весьма хорош с точки зрения безопасности. Однако, для получения прямого доступа к низкоуровневым функциям или написания критически важных алгоритмов, требующих максимальной производительности, такой подход не годится. Поэтому CLR позволяет писать небезопасный код, который не будет подвергаться проверке средой. В C# для обозначения небезопасного участка кода используется ключевое слово unsafe. При написании небезопасного кода, программист должен полностью отслеживать правильность его работы, так как возможны возникновения ошибок, которые в безопасном коде среда выполнения могла бы предотвратить. Немаловажным аспектом также является перемещение объектов сборщиком мусора для лучшей организации памяти. При использовании указателей на объект в небезопасном коде может образоваться так называемый висячий указатель, если объект, на который он указывал, был перемещен в другой участок памяти. Для предотвращения подобных действий в C# существует ключевое слово fixed, которое указывает сборщику мусора, что данный объект нельзя перемещать из одного блока памяти в другой. Небезопасный код – очень мощный инструмент, однако его использование крайне нежелательно, ведь он может создать брешь в безопасности кода и разрушить уже существующие структуры данных. Поэтому для использования этого инструмента не только нужно помечать расположение небезопасного участка кода, но и производить компиляцию с параметром /unsafe. В противном случае, CLR запретит компиляцию данного кода.

Список литературы

[1] Рихтер Дж. CLR via C#. Программирование на платформе Microsoft .NET Framework 2.0 на языке C# – СПб.: Питер, 2008. – 656 с.

[2] Шилдт Г. Полный справочник по C# – М.: ООО “И.Д. Вильямс”, 2004. – 752 с.

[3] Троелсен Э. Язык программирования C# 5.0 и платформа .NET 4.5 М.: ООО “И.Д. Вильямс”, 2013. – 1312 с.

Кадурин Ярослав Алексеевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: mr.cadurin@yandex.ru

Савкин Михаил Константинович – ассистент кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: savkinmk@gmail.com

А.А. Празян, К.А. Празян

ОСНОВНЫЕ ПОЛОЖЕНИЯ МЕТОДОВ ПРИМЕНЕНИЯ ЭЭГ В КАЧЕСТВЕ НЕЙРОИНТЕРФЕЙСА

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В работе рассматривается возможность использования РМА в качестве интерфейса управления программным обеспечением. Приводится классификация волн, получаемых с электроэнцефалографа, а также предлагаются варианты использования волн для кодирования-декодирования информации, получаемой из головного мозга человека.

Ключевые слова: *РМА, ЭЭГ, нейроинтерфейс, кодирование волн.*

В настоящее время с развитием вычислительной техники становится возможным использование самого человека в качестве интерфейса управления программным обеспечением. Основной сложностью становится выбор параметров, по которым можно однозначно определить, какие действия требуется выполнить программе. Сегодня существует большое количество реализаций голосового управления. Писатели-фантасты предложили использование головного мозга человека в качестве интерфейса. Остается выбрать параметры, по которым можно определить “направление мышления” человека.

Одними из таких параметров могут служить **РМА** – ритмы мозговой активности. Природа РМА идентична практически для всех млекопитающих, а интенсивность волн зависит от количества нервных клеток, находящихся рядом (для человека - это головной мозг).

Головной мозг человека можно «грубо» разделить на три составляющие:

1. Глиальные клетки, которые обладают способностью делиться и размножаться в течение всей жизни. Они имеют ответвления, но не имеют аксонов и дендритов. В последних исследованиях выяснилось, что некоторые глиальные клетки могут действовать как усилители, наподобие транзисторов. Их назначение - поддержка нервных связей и обеспечение функционирования нервной сети, объединяющей различные области коры головного мозга.

2. Нейроны - нервные клетки мозга. Они образуют серое вещество, представляющее собой внешний 2-хмиллиметровый слой мозга. Нейроны состоят из тела клетки, аксона и одного или более дендритов. Функция нейронов – создавать и проводить нервные импульсы.

3. Дендриты образованы благодаря процессам в протоплазме нейронов и передают импульсы к телу клетки нейрона. Обычно задействованы несколько сотен дендритов. Они формируют связи, которые называются «синапсы», с другими нейронами. В результате, дендриты представляют собой систему «проводов» мозга. Они формируются мыслительными процессами, воздействием окружающей среды, обучением и жизненным опытом.

Самому обычному нейрону нужна примерно одна микросекунда, чтобы ответить на раздражитель. Это происходит постоянно. Естественно,

один нейрон не создаст разряд достаточной «силы», но их количество велико. При раздражении миллионы нейронов начинают работать в унисон, создавая при этом электрические разряды, которые, в свою очередь, создают ритм. Этот ритм получил название «мозговая волна».

Ритмы мозговых волн поддаются изучению посредством ЭЭГ (электроэнцефалографии) - метода исследования РМА, с помощью энцефалографа. Суть его работы: создание графического изображения электрического процесса, происходящего в головном мозге, с помощью электродов, размещенных на лобной, височной, волосистой части головы. В среднем электроэнцефалограмма записывает информацию с частотой 5-10 сигналов в минуту. Пример электроэнцефалограммы представлен на рис. 1.

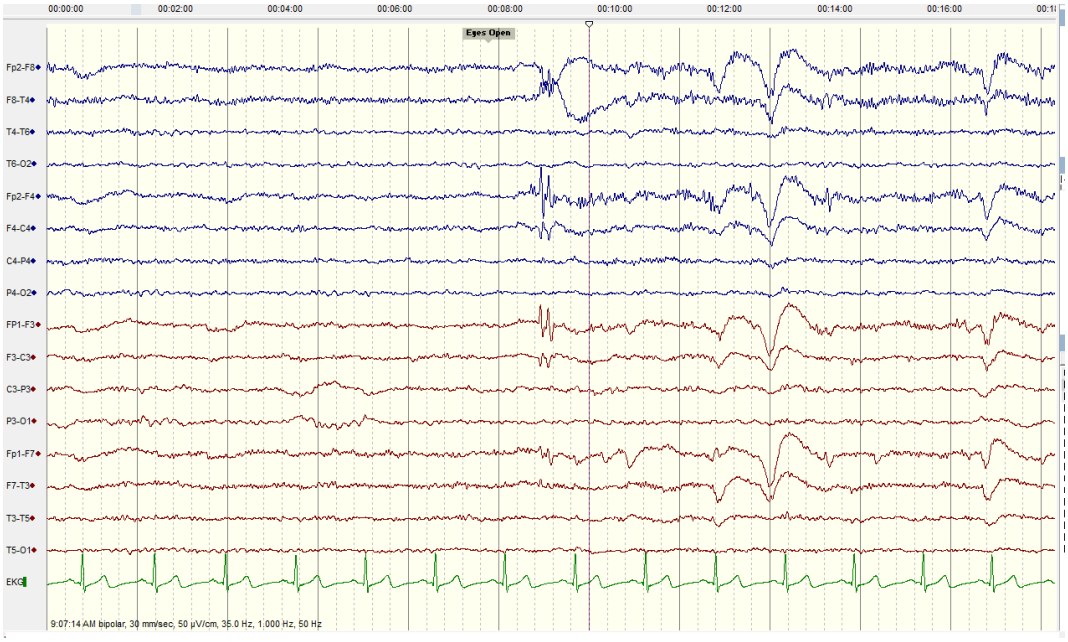


Рис 1. Пример электроэнцефалограммы

Выделяют различные ритмы, главным критерием при этом является частота и амплитуда, α-ритм, β-ритм, γ-ритм, δ-ритм, θ-ритм, κ-ритм, λ-ритм, μ-ритм, σ-ритм, τ-ритм.

Альфа-ритм – частота колебания от 8 до 13 Гц. Амплитуда 5-100 мкВ. Наибольшая амплитуда наблюдается при закрытых глазах и затемненном помещении, то есть при минимальных раздражениях зрительного рецептора. Этот “ритм” регистрируется у людей в расслабленном состоянии, но не во сне. При открытии глаз наблюдается депрессия альфа-ритма.

Бета-ритм - частота колебания от 14 до 40 Гц. Амплитуда до 20 мкВ. Такие волны наблюдаются при открытых глазах, при тщательном наблюдении за объектом, при сосредоточении на какой - либо проблеме. А также может повлиять резкое стрессовое воздействие.

Гамма-ритм - частота выше 30 Гц, амплитуда не превышает 15 мкВ. Проявляются при сходных условиях с бета - волнами, только при максимальном сосредоточении на решении, к примеру, математической задачи.

Дельта-ритм - частота 1 до 4 Гц. Амплитуда 20-200 мкВ. Такие волны особенно проявляются во время сна, избыток таких волн может свидетельствовать о наличии заболеваний нервной системы, расстройстве внимания, а также об употреблении наркотических средств.

Тета-ритм - от 4 до 8 Гц. 20-100 мкВ. Волны особенно начинают проявляться в “предсонном” состоянии, когда спокойное состояние переходит в сонливость, затем в сон.

Каппа-ритм - от 8 до 13 Гц. Амплитуда 5-40 мкВ. Наблюдается при подавлении альфа-ритма, предположительно, его активность связана с движением глаз.

Мю-ритм - Частота от 8 до 13 Гц. Амплитуда колебаний не более 50 мкВ. Такие волны регистрируются при воображении движения, то есть при представлении движения руки или другой части тела.

Тау-ритм и лямбда-ритм можно объединить в одно, так как частота их проявления находится также в рамках 8 до 13 Гц, но амплитуда в пределах от 12 до 14 Гц. Такие ритмы проявляются в фазу глубокого сна.

Все виды ритмов проявляются у здорового человека в примерно одинаковой степени. Здесь стоит подчеркнуть “здорового человека”, так как именно при изучении РМА можно поставить диагноз о заболевании. Также важным фактором может служить, что эти волны не меняются после периода взросления. Кроме определения диагноза природа ритмов позволяет, при правильном их кодировании-декодировании, использовать их в качестве интерфейса управления. Для этого нужно определиться, какие волны использовать для кодирования: по каким-то отдельным ритмам либо по по целому ряду ритмов, но оба варианта несут в себе свои плюсы и минусы.

Если использовать весь набор, который считывает ЭЭГ, это может быть хорошим вариантом, ведь для каждого человека РМА уникальны, но в пределах определенных рамок, которые называют нормой. Но при таком способе понадобится долгая предрегистрация волн, иначе результаты могут быть сильно схожи с другими людьми.

В другом варианте берется отдельный ритм (α) и получается стабильное постоянное проявление, но тут же появляется проблема самой природы альфа волн, а именно состояние спокойствия, причем все время одинаковое, если сказать точнее, в одинаковых условиях. Такой способ нельзя назвать “удобным”.

Наиболее подходящими ритмами можно назвать β, γ - ритмы. Их проявление обуславливается мозговой активностью. Но если выбрать этот способ, данные со временем будут меняться, то есть если для начального кодирования мы выбираем активность β, γ - ритмов и стимулом их проявления будет, к примеру, математическая задача, то через некоторое количество повторений данные, полученные с помощью ЭЭГ, изменятся. В этой ситуации вступает в “игру” психофизиология человека, а именно эффект привыкания к нагрузке, и как следствие, незначительное изменение показателей.

σ-ритм, τ-ритм, θ-ритм, δ-ритм можно применить не в качестве показателей кодирования, а извлечь из них полезные функции, например, води-

телю. Для безопасного передвижения во время бодрствования эти волны должны быть в минимальной степени выраженности.

Наибольший интерес представляют μ-ритмы. Уже долгое время ученые работают над нейро-протезами, управление которыми будет осуществляться непосредственно головным мозгом. Мю-волны регистрируются при сильном представлении движения, например, движении руки. Если человек будет усиленно представлять ее движение, причем детально, а именно каждый момент движения и чувства, которые он испытывает, проявление Мю-волн усиливается. Этот момент поможет кодировать полученную информацию для регистрации одного и того же ритма будет достаточно представлять одно и тоже движение. Но и этот способ может оказаться недостаточно надежным. Так как со временем мы будем иметь дело с “привыканием”, но этот процесс в итоге останавливается, и угнетение волн прекращается, так что минусом это назвать нельзя. Но также в организме человека есть зеркальные нейроны, которые “работают” на других частотах. Эти клетки станут активны, если испытуемый из-за частых представлений одного и того же движения станет неосознанно представлять не само движение, а то, как он это делал, то есть повторять сам за собой. К вышесказанному можно добавить, что для работы понадобится очень сильная концентрация сознания, что доступно далеко не всем.

Даже при успешной реализации механизмов кодирования-декодирования сигналов ЭЭГ ставится вопрос защиты данных, передаваемых энцефалографу. Как и информация в привычной нам цифровой форме, сигналы ЭЭГ тоже являются информацией, в том числе и персональной. Злоумышленник, получив информацию о характере волн жертвы сможет подделать передаваемые интерфейсу управления данные, таким образом похитив личность жертвы.

Весь метод кодирования-декодирования при помощи РМА выглядит очень привлекательным. Однако не может быть полностью реализован в настоящее время в силу недостатка изучения в области нейрофизиологии мозга, а также отсутствия хорошей методической части для интерпретации данных, полученных ЭЭГ.

Список литературы

[1] Быков М. П. Анатомия головного мозга. Фотографический атлас, Практическая медицина, 2009

[2] Сивер Дэвид. Майнд машины. Открываем заново технологию ABC

[3] Дубровинская Н.В., Фарбер Д.А., Безруких М.М. Психофизиология ребенка: Психофизиологические основы детской валеологии: Учеб. пособие для студ. высш. учеб. заведений. -- М.: Гуманит. изд. центр ВЛАДОС, 2000.

Празян Александр Арменович – студент КГУ им. К.Э. Циолковского. E-mail: prazyan@live.ru

Празян Константин Арменович – ассистент кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: prazyan.konstantin@gmail.com

К.А. Празян

ПОЛИМОРФНЫЕ ВИРУСЫ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

С прогрессом информационных технологий появляются всё новые проблемы в плане защиты компьютерных систем. Одной из таких проблем являются вирусы. С появлением вирусов появилась нужда в создании антивирусов, определяющих их по характерным симптомам. В дальнейшем вирусы были наделены специальными возможностями, что позволяло им быть незамеченными в системе. Одним из вариантов защиты от определения является полиморфизм.

Полиморфизм - высококлассная техника, позволяющая вирусу быть незамеченным по стандартной сигнатуре. Детекторы определяют вирус по характерным частям кода. В случае с полиморфными вирусами такой вариант не подходит. Два файла, зараженные одним и тем же вирусом, всегда будут иметь разный размер. Обнаружить такой вирус очень проблематично.

Все полиморфные вирусы обязательно снабжаются расшифровщиком кода, который по определенному принципу преобразует переданный ему код, вызывая при этом стандартные функции и процедуры операционной системы. Сами методы шифрования могут быть разными, но, как правило, каждая операция имеет свою зеркальную пару. В ассемблере это реализуется очень просто, и таких пар может быть много - ADD/SUB, XOR/XOR, ROL/ROR и т.п. Подобные операции проводятся для расшифровки ячеек памяти.

Немаловажной особенностью полиморфного вируса является то, что вирус содержит мусор, то есть операнды, функции и процедуры, которые служат лишь для запутывания кода. При этом реализуются две цели:

1. Сложность изучения кода при трассировке файла. Эта цель актуальна лишь для новичка, профессионал, который изучением вирусов занимался многие годы, сразу во всем разберется.

2. Увеличение элемента случайности в расшифровщике. Место их вставки имеет огромное влияние на размер кода. С мусором же появляются новые варианты компоновки кода. Размер при каждом из них будет разным.

Полиморфные вирусы используют специальные механизмы, которые затрудняют их надежное обнаружение. Обычно такие вирусы содержат код генерации шифровщика и расшифровщика собственного тела. Создаваемые генератором шифровщики (и соответствующие расшифровщики) обычно изменяются во времени. Для зашифрованной части кода вируса обязательно должна существовать подпрограмма расшифрования - рас-

шифровщик, или декриптор (decryptor). В полиморфных вирусах расшифровщик не является постоянным - для каждого инфицированного файла он свой. По этой причине зачастую нельзя установить инфицированный файл по характерной для данного вируса строке (сигнатуре). Вследствие этого некоторые антивирусные средства не ловят полиморфные вирусы.

Наиболее прославленные из полиморфных вирусов - это Phantom1, OneHalf, Satanbug. Полиморфные вирусы в зависимости от их сложности разделяют на несколько уровней.

Вирусы первого уровня полиморфизма используют постоянные значения для разных расшифровщиков. Их можно обнаружить по некоторым постоянным участкам кода расшифровщика. Такие вирусы принято называть "не совсем полиморфными", или олигоморфными.

Ко второму уровню полиморфизма относят вирусы, расшифровщик которых имеет постоянной одну или несколько инструкций. Например, он может использовать различные регистры, некоторые альтернативные инструкции в расшифровщике. Такие вирусы также можно распознать по определенной сигнатуре - заданным сочетаниям байт в расшифровщике.

Вирусы, использующие в расшифровщике команды, не участвующие в расшифровании вирусного кода, или "команды-мусора", относят к третьему уровню полиморфизма. Это такие команды ассемблера, как NOP, MOV AX, AX, STI, CLD, CLI и т.д. Данные вирусы также можно определить с помощью некоторой сигнатуры, если произвести отсеивание всех "мусорных" команд.

Вирусы четвертого уровня используют в расшифровщике взаимозаменяемые инструкции и "перемешанные" инструкции без изменения алгоритма расшифрования. Например, ассемблерная команда MOV AX,BX имеет взаимозаменяемые инструкции: PUSH BX - POP AX; XCHG AX,BX; MOV CX,BX - MOV AX,CX и т. д. Детектирование данных вирусов в принципе возможно с помощью некоторой перебираемой сигнатуры.

Пятый уровень полиморфизма включает свойства всех перечисленных уровней, а кроме того, расшифровщик может использовать различные алгоритмы расшифрования вирусного кода. Для расшифровки возможно использование основного вирусного кода, расшифровки части самого же декриптора или нескольких расшифровщиков, поочередно расшифровывающих друг друга либо непосредственно вирусный код. Как правило, обнаружение вирусов данного уровня полиморфизма с помощью сигнатуры невозможно. Процесс поиска и особенно лечения такого вируса - очень сложная задача, и она может занять весьма продолжительное время. Если для обнаружения такого вируса возможен серьезный анализ кода только самого расшифровщика, то для лечения необходимо произвести частичную или полную расшифровку тела вируса, чтобы извлечь информацию о зараженном файле.

Шестой уровень полиморфизма. К нему относятся нешифрованные вирусы - т. е. вирусы, состоящие из программных единиц-частей, которые "перемешиваются" внутри тела вируса. Данные вирусы, как "кубики", тасуют свои подпрограммы (инсталляции, заражения, обработчика прерывания, анализа файла и т. д.). Такие вирусы еще называются пермутирующими.

Помимо полиморфных вирусов, существует некоторый набор полиморфик - "генераторов", представляющих собой объектный код, который можно "подключить" к "своему" вирусу (сделав его полиморфным) и получить новый полиморфный вирус.

В наше время многие вирусы используют полиморфизм высоких уровней в своих алгоритмах. Помимо полиморфизма существуют и другие методы маскировки, например, стелс-технологии.

Список литературы

[1] Касперски К. // Компьютерные вирусы изнутри и снаружи. - СПб.: Питер, 2006. - 527 с.

[2] Касперски К. // Записки исследователя компьютерных вирусов. - СПб.: Питер, 2005. - 316 с.

[3] Косарев В. Компьютерные системы и сети. Учебное пособие. Из-во Фин. и стат. 2005. 464 стр.

[4] Крейнак Д. Интернет. Энциклопедия (2 изд.). Из-во Питер. 2004. 528 стр.

Празян Константин Арменович – ассистент кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: prazyan.konstantin@gmail.com

А.Н. Молчанов, С.В. Клюквин

ПРЕИМУЩЕСТВА АППАРАТНОГО ШИФРОВАНИЯ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Шифрование – один из самых эффективных и распространенных способов защиты информации.

Существует ряд возможных реализаций методов криптографической защиты информации:

1) Программные;

2) Аппаратные;

3) Программно-аппаратные.

Их основное различие заключается не только в способе реализации шифрования и степени надежности защиты данных, но и в цене, что часто становится для пользователей определяющим фактором[1].

Целью данной работы является анализ аппаратного шифрования и выявление преимуществ перед остальными методами криптографической защиты информации.

Безопасность. Этот показатель является главным и определяющим для шифрования, его можно разбить на пункты.

- **Физическая защита**. У алгоритма шифрования, работающего на универсальном компьютере, отсутствует физическая защита. Аппаратные устройства шифрования могут быть заключены в надежный корпус.
- **Экранирование**. Специализированные устройства шифрования могут быть экранированы, что не допускает утечки компрометирующей информации[2].
- **Неизменность алгоритма шифрования.** Существуют вредоносные программы, способные изменить алгоритм шифрования. Криптографическое ПО подвержено такой угрозе.
- **Аппаратный датчик случайных чисел (ДСЧ)**, который используется при создании криптографических ключей. Физические процессы, задействованные в аппаратном датчике, обеспечивают выдачу случайных чисел, распределение которых близко к равновероятному.
- **Прямая загрузка ключей шифрования**. Загрузка происходит в специализированный процессор аппаратного шифратора с персональных идентификаторов, минуя системную шину.
- **Хранение ключей шифрования в памяти шифропроцессора**. В случае с программной реализацией ключи хранятся ОЗУ компьютера, доступ к которым получить намного проще.

- **Функции «электронного замка».** Включают в себя:
  1) идентификация и аутентификация пользователя до загрузки операционной системы;
  2) запрет на изменение процесса загрузки компьютера;
  3) возможность контроля целостности операционной системы и прикладного программного обеспечения;
  4) ведение журнала безопасности действий пользователя, который доступен только администратору, регистрирующего попытки доступа к компьютеру[3].

Скорость. Шифрование требует много вычислительных ресурсов. Выполнение шифрования на центральном процессоре компьютера неэффективно. Использование для этого другой микросхемы, даже если эта микросхема - просто еще один такой же процессор, делает систему в целом быстрее.

Простота установки. Шифрование должно быть невидимым, оно не должно мешать пользователю. Единственный способ реализовать это требование программно - это спрятать шифрование поглубже в операционную систему. А это непросто. С другой стороны, даже новичок сможет включить блок шифрования между своим компьютером и внешним модемом[2].

Для сравнения характеристик аппаратного и программного шифрования можно обратиться к официальному сайту производителя устройств памяти Kingston.

Компания Kingston представила новую серию защищенных USB-накопителей, поддерживающих технологию аппаратного шифрования. Они помогают компаниям крупного и малого бизнеса надежно и безопасно перемещать данные. Для шифрования информации на USB-накопителях могут использоваться две различных технологии: шифрование с помощью аппаратных средств или с помощью специального ПО.

Возьмем 2 USB-накопителя емкостью 8 Гб и поддержкой USB 3.0, но с разными видами шифрования. По сводной таблице характеристик программного и аппаратного шифрования (Таблица 1) видно, что последняя имеет не только больше интересных пунктов, но и существенное преобладание надежности каждой аналогичной характеристики[4].

Таблица 1.

Аппаратное шифрование (DataTraveler Vault Privacy 3.0 8 Гб)	**Программное шифрование** (DataTraveler SE9 G2 3.0 8 Гб)
1. Используется специальный процессор, расположенный непосредственно на накопителе 2. Процессор содержит генератор случайных чисел для создания ключа шифрования, который разблокируется при помощи пользовательского пароля 3. Повышение производительности за счет освобождения хост-системы от необходимости обработки задач шифрования 4. Защита ключей и критически важных параметров безопасности производится аппаратными средствами шифрования 5. Аутентификация производится с применением аппаратных средств 6. Высокая экономическая эффективность в условиях средних и крупных предприятий, поддержка простого масштабирования 7. Постоянно доступная функция шифрования, привязанная к конкретному устройству 8. Не требуется установка дополнительных драйверов или программ 9. Данные защищены от наиболее распространенных атак, таких как "холодная" загрузка, внедрение вредоносного кода, прямой перебор паролей 10. Цена от 2800 рублей	1. Совместное использование ресурсов компьютера для шифрования данных одновременно с работой других программ – уровень защиты ПК определяет уровень защиты накопителя 2. В качестве ключа шифрования данных используется пароль, заданный пользователем 3. Может потребоваться обновление программного обеспечения 4. Уязвимость при атаках методом перебора паролей, когда компьютер пытается ограничить число попыток расшифрования, но злоумышленники могут получить доступ к памяти компьютера и обнулить счетчик попыток 5. Высокая экономическая эффективность при использовании на небольших предприятиях 6. Возможность реализации шифрования для всех типов носителей данных 7. Цена от 380 рублей

Вывод. Что же мешает широкому применению аппаратных шифраторов – или, выражаясь точнее, обусловливает их меньшую распространенность по сравнению с криптографическим ПО?

Прежде всего цена – в любом случае стоимость аппаратного шифратора будет выше, чем чисто программного решения. Так что для организаций, всерьез заботящихся об информационной безопасности, использование аппаратных шифраторов в силу перечисленных выше причин безусловно желательно – во всяком случае, для защиты наиболее важных ресурсов[5].

Список литературы

[1] Тарасюк М.В. Защищенные информационные технологии. Проектирование и применение – М.: СОЛОН-Пресс, 2004.

[2] Аппаратное или программное шифрование? // r3al.ru - [Электронный ресурс]. – Режим доступа: URL: http://r3al.ru/kripto_2/apparatnyj_i_programmnyj_sposoby.html (дата обращения 31.09.2016)

[3] Лукашов И. В. Криптография? Железно! //Журнал «Мир ПК». 2003. № 03

[4] Сравнение технологий защиты информации: аппаратное и программное шифрование// 2016 Kingston Technology Corporation. – [Электронный ресурс]. – Режим доступа: URL: http://www.kingston.com/ru/usb/encrypted_security/hardware_vs_software (дата обращения 31.09.2016)

[5] Аппаратное шифрование// Dviger.com – [Электронный ресурс]. – Режим доступа: URL: http://vos.dviger.com/virtoteka/show/c_1641.html (дата обращения 31.09.2016)

Молчанов Алексей Николаевич – ст. преп. кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: alexeymolchanov@yandex.ru

Клюквин Сергей Владимирович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: GreyHardV3@yandex.ru

А.Э. Телерман, Я.А. Бланк, А.Б. Лачихина

СИСТЕМЫ ДЕЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ ДОСТУПОМ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В современных компаниях для выполнения различных задач применяются выделенные системы, приобретаемые у различных производителей. Данные системы объединяются в рамках информационного окружения компании и применяются для решения обособленных или совместных задач.

Существуют 2 типа организации доступа к дискретным системам в рамках конкретного предприятия: централизованное управление и децентрализованное управление. В данное статье будет рассмотрена система децентрализованного управления доступом.

В отличии от централизованной модели управления доступом, в которой существует шлюз, являющийся промежуточным звеном между администратором безопасности и дискретными системами, децентрализованная модель управления предоставляет администратору прямой доступ к управлению подконтрольной системой, не ограничивая его в выполняемых действиях.

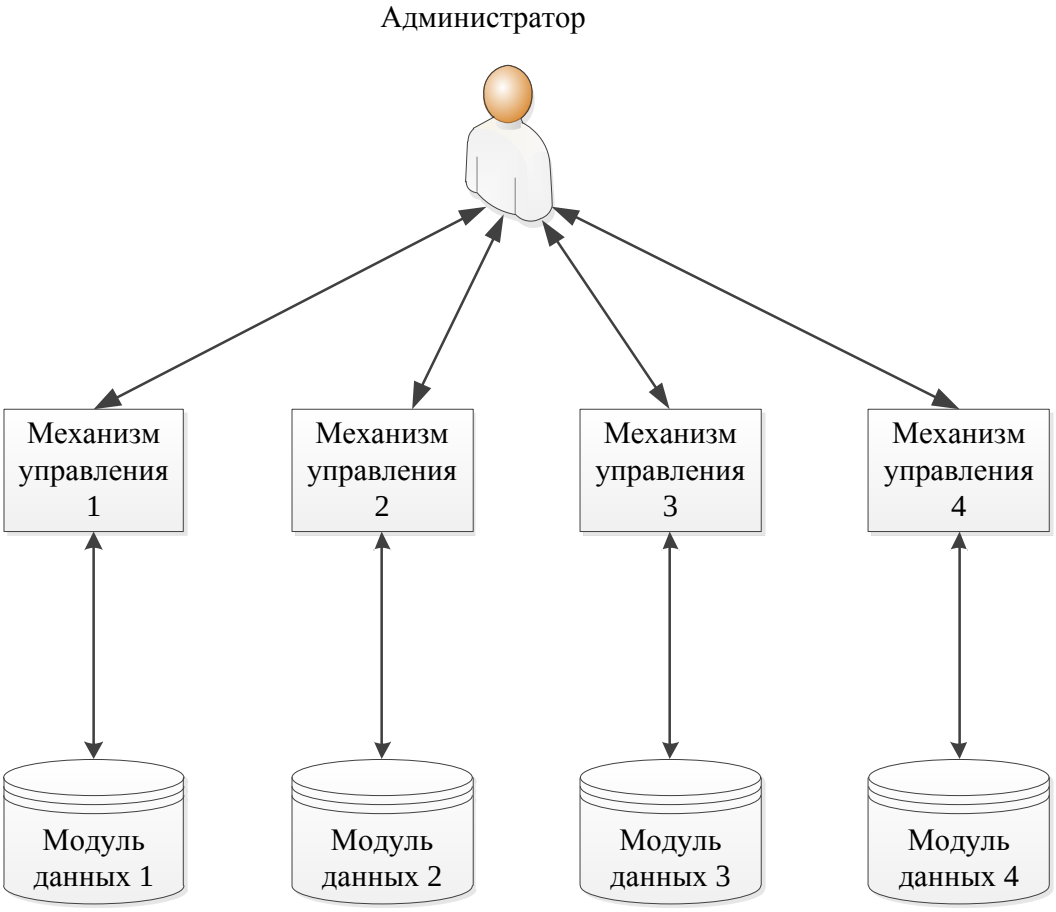


Рис. 1. Схема децентрализованного управления доступом

В децентрализованной модели все подконтрольные системы имеют свой собственный интерфейс управления. Принцип взаимодействия администратора сети и используемых систем заключается в использовании встроенных механизмов управления и получение прямого доступа к нативным функциям. Чтобы обратиться к системе с целью изменения ее настроек, администратор безопасности должен пройти процедуры аутентификации - процедура проверки принадлежности субъекту доступа предъявленного им идентификатора (имени пользователя, пароля, токена, идентификационной карты, ключа); подтверждение подлинности [1] и авторизация - получение права доступа путем проверки подлинности введенных данных пользователя [2], предусмотренные в системном модуле управления.

Характерными преимуществами предложенной модели управления доступом являются:

1. отсутствие необходимости создания шлюза и оборудования выделенного сервера под данный комплекс, т.к. для обеспечения должного уровня информационной безопасности целесообразно располагать шлюз и дискретные системы на разных серверах;
2. снижение финансовых расходов на оборудование;
3. в случае, если данные в дискретных системах не связаны, повышается уровень информационной безопасности. Получив несанкционированный доступ к одной системе, для получения полной информации злоумышленник вынужден взламывать оставшиеся системы.

В тоже время система децентрализованного доступа имеет ряд существенных недостатков:

1. снижение уровня эффективности работы администратора безопасности, т.к. для изменения настроек он вынужден обращаться к каждой отдельной системе, что увеличивает время работы;
2. в случае, если данные в дискретных системах связаны, злоумышленник, получив несанкционированный доступ к одной системе, повышает свои шансы на получение полной информации за счет найденных внутренних уязвимостей.

Применение децентрализованной модели управления доступом целесообразно на предприятиях, дискретные системы которого оперируют несвязными данными, либо в том случае, если количество систем невелико, т.к. работа с малым количеством дискретных систем слабо влияет на производительность системного администратора. Помимо этого, применение данной модели обоснованно для предприятий, не располагающих большим бюджетом.

Список литературы

[1] Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения». – М.: ГТК РФ, 1992. – 13 с.

[2] *Лачихина А.Б., Мазин А.В*. Методика рациональной настройки баз данных на примере системы "Аналитик". // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия: Приборостроение. - 2010. - № 4. - С. 91-103.

Телерман Алексей Эдуардович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: telerman.bas@yandex.ru

Бланк Яна Андреевна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: yanablank10@gmail.com

Лачихина Анастасия Борисовна – канд. техн. наук, доцент кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: anastasialach73@gmail.com

А.Р. Филатов, М.К. Савкин

СИСТЕМЫ КОНТРОЛЯ ВЕРСИЙ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

На сегодняшний день разработка более-менее крупных проектов не возможна силами одного человека. Для согласования действий при создании программного продукта используется программное обеспечение, называемое системой контроля версий (от англ. Version Control System, VCS или Revision Control System). Система контроля версий позволяет хранить несколько версий одного и того же документа, при необходимости возвращаться к более ранним версиям, определять, кто и когда сделал то или иное изменение, и многое другое. В данной статье будет дано краткое описание принципов работы различных систем контроля версий на примере наиболее популярных.

Ситуация, при которой электронный документ претерпевает несколько изменений за время своего существования, достаточна обыденна. При этом нередко требуется хранить не только последнюю версию, но и предыдущие. Самым простым способом является создание множества копий, пронумерованных в соответствующем порядке. Этот способ является неэффективным, т.к. приходится хранить одновременно практически идентичные файлы, обработка которых требует большого сосредоточения, в связи с чем возникает большое количество ошибок. Для устранения этих ошибок были разработаны автоматические системы.

Традиционные системы являются централизованными, т.е. имеется сервер, который выполняет большую часть функций по управлению версиями, и хранилище версий (репозиторий). Пользователь выбирает нужную ему версию, создается локальная рабочая копия, после завершения работы с документом на основе рабочей копии измененная версия добавляется в репозиторий. Доступ к каждой версии документа может быть получен в любой момент. Зачастую Сервер может использовать дельта-компрессию – такой способ хранения документов, при котором сохраняются только изменения между последовательными версиями, что позволяет уменьшить объём хранимых данных.

Зачастую над одним проектом одновременно работают несколько человек. Если два человека изменяют один и тот же файл, то один из них может случайно отменить изменения, сделанные другим. Системы контроля версиями отслеживают такие конфликты и предлагают средства их

решения. Большинство систем может автоматически объединить изменения, сделанные разными разработчиками. Однако, такое автоматическое объединение изменений осуществимо только для текстовых файлов при условии, что изменялись разные части этого файла. Такое ограничение связано с тем, что большинство систем управления версиями ориентированы на поддержку процесса разработки программного обеспечения, а исходные коды программ хранятся в текстовых файлах. Если автоматическое объединение выполнить не удалось, система может предложить решить проблему вручную.

Система может осуществлять управление файлами как прозрачно, т.е., не показывая пользователю уведомлений о сохранении изменений, так и открыто, т.е. уведомляя пользователя.

Большинство систем контроля версий могут предложить следующие функции:

- Создание разных версий одного документа с историей преобразований до и после точек изменений
- Возможность узнать, кто, когда и как изменил данный документ
- Ведение журнала учета изменений, в котором пользователи могут оставлять комментарии к различным изменениям
- Контроль прав пользователей, с последующим разрешением или запрещением действий в зависимости от наличия или отсутствия у них прав

Теперь рассмотрим на примерах наиболее популярные системы:

Subversion (также известная как «SVN»)

Subversion является централизованной системой контроля версий. Работа в Subversion мало отличается от работы в других централизованных системах управления версиями. Пользователи копируют файлы из хранилища, создавая локальные рабочие копии, затем вносят изменения в рабочие копии и фиксируют эти изменения в хранилище. Несколько пользователей могут одновременно обращаться к хранилищу. Для совместной работы над файлами в Subversion преимущественно используется модель копирование – изменение – слияние. В этой модели клиент каждого пользователя считывает из хранилища проект и создаёт персональную рабочую копию – локальное отражение файлов и каталогов хранилища. После этого пользователи работают, одновременно изменяя свои личные копии. В конце концов, личные копии сливаются в новую, финальную версию. Кроме того, для файлов, не допускающих слияние (различные бинарные форматы файлов), можно использовать модель блокирование – изменение – разбло-

кирование. При сохранении новых версий используется дельта-компрессия: система находит отличия новой версии от предыдущей и записывает только их, избегая дублирования данных.

При использовании доступа с помощью WebDAV (набор расширений и дополнений к протоколу HTTP, поддерживающих совместную работу пользователей над редактированием файлов и управление файлами на удаленных веб-серверах) также поддерживается прозрачное управление версиями – если любой клиент WebDAV открывает для записи и затем сохраняет файл, хранящийся на сетевом ресурсе, то автоматически создаётся новая версия.

Главными достоинствами Subversion для начинающих пользователей является возможность работы на операционной системе Windows, встроенный графический интерфейс и простота использования.

Главными недостатками является большое занимаемое пространство на локальных носителях, необходимость наличия сервера, невозможность удаления данных из хранилища без наличия административного доступа к серверу с хранилищем.

Git

Git является примером распределённой системы контроля версий, т.е. наличие центрального сервера в системе не обязательно. Такое построение системы позволяет достаточно удобно использовать её одному пользователю как систему, создающую резервные копии. При работе в системе от оригинальной ветви отделяются ветви разработчиков, а от ветви разработчиков – ветви текущих изменений. Согласование ветвей происходит достаточно гибко, что позволяем избежать многих ошибок совместимости версий.

Главным недостатками системы для начинающих пользователей является отсутствие отдельной команды переименования/перемещения файла, которая отображалась бы в истории как соответствующее единое действие (т.е. возможны разрывы в истории файла).

Главными достоинствами системы является гибкость в управлении ветвями, небольшой размер занимаемого пространства, локальность большинства операций.

Системы контроля версий продолжают совершенствоваться от версии к версии, улучшая алгоритмы управления, совместимости, добавляя поддержку разных платформ.

Подытожив все вышеперечисленное можно сказать, что не существует универсальной системы контроля версий. Для каждого проекта подойдет своя система, выбираемая исходя из задач, потребностей и возможно-

стей. Одно можно сказать наверняка – системы контроля версий были и являются незаменимым инструментом при разработке командных проектов.

Список литературы

[1] Артюхов Е., Ежедневная работа с Git, URL: https://habrahabr.ru/post/174467/ (дата обращения 29.09.2016)

[2] Руководство пользователя GIT (для версии 1.5.3 и выше) URL: http://freesource.info/wiki/RuslanHihin/gitusermanual?v=b7s (дата обращения 29.09.2016)

[3] Branching and Merging URL: https://git-scm.com/about/branching-and-merging (дата обращения 29.09.2016)

[4] Обзор систем контроля версий URL: http://all-ht.ru/inf/prog/p_0_1.html (дата обращения 29.09.2016)

[5] Коллинз-Сассман Б., Фитцпатрик Брайан У., Пилато Майкл К., Управление версиями в Subversion URL: http://svnbook.red-bean.com/nightly/ru/svn-book.html (дата обращения 29.09.2016)

Филатов Александр Романович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: afnotdead@yandex.ru

Савкин Михаил Константинович – ассистент кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: savkinmk@gmail.com

Я.А. Бланк, А.Э. Телерман, А.Б. Лачихина

СИСТЕМЫ ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ ДОСТУПОМ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В современных компаниях для выполнения различных задач применяются выделенные системы, приобретаемые у различных производителей. Данные системы объединяются в рамках информационного окружения компании и применяются для решения обособленных или совместных задач.

Существуют 2 типа организации доступа к дискретным системам в рамках конкретного предприятия: централизованное управление и децентрализованное управление. В данное статье будет рассмотрена система централизованного управления доступом.

Система централизованного управления доступом представляет собой структуру, в которой присутствует множество конечных узлов и узел-шлюз. Каждый конечных узел является системой, выполняющей определенную функцию. Шлюз является промежуточным звеном структуры, обеспечивающий взаимодействие вышеописанных систем и пользователей.

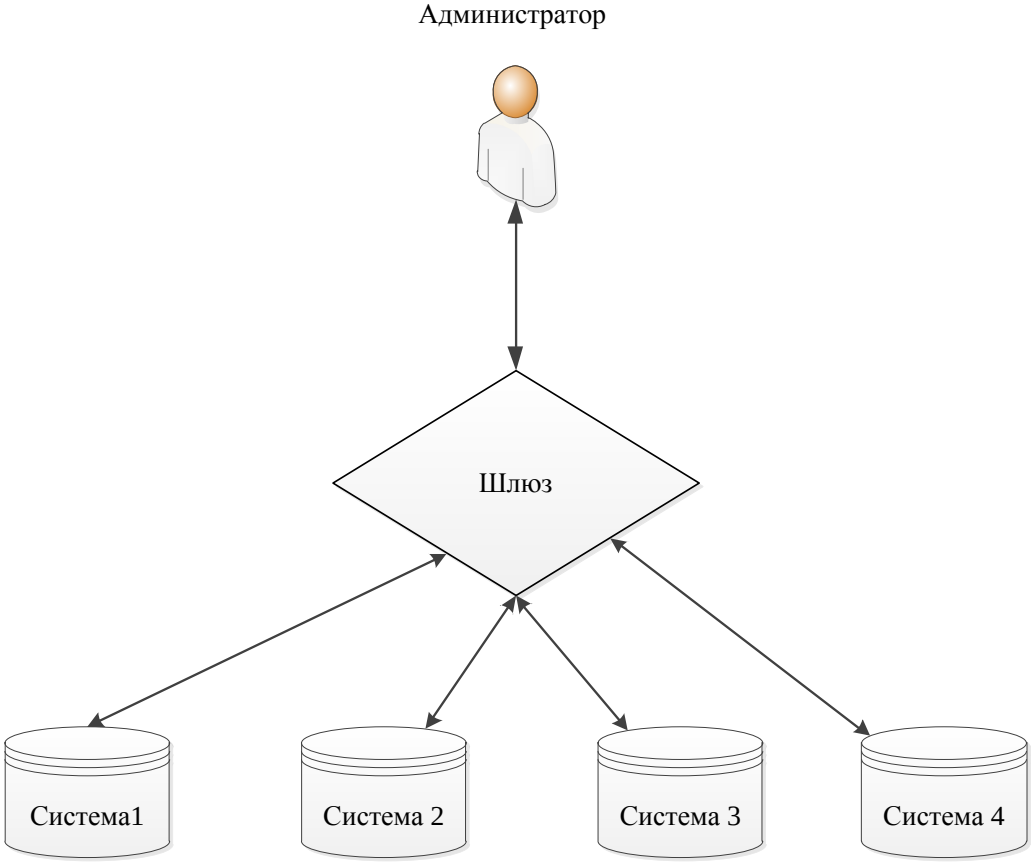


Рис. 1. Схема централизованного управления

В централизованной системе управления все подконтрольные компоненты сконфигурированы в единый интерфейс, предоставляющий администратору возможность управления подчиненными ему узлами. Принцип взаимодействия администратора сети и используемых систем заключается в использовании единого интерфейса для взаимодействия с каждой отдельной системой. Программный комплекс берет под контроль такие этапы предоставления доступа пользователям, как аутентификация - процедура проверки принадлежности субъекту доступа предъявленного им идентификатора (имени пользователя, пароля, токена, идентификационной карты, ключа); подтверждение подлинности [1] и авторизация - получение права доступа путем проверки подлинности введенных данных пользователя [2]. А также реализует алгоритмы управления политиками предоставления доступа - правилами, описывающими права пользователя на выполнение операций с информационными ресурсами и каталогом пользователей - каталогом, содержащим учетную информацию о пользователях автоматизированной системы.

Результатом применения данной методологии является:

1. снижение затрат на управление доступом и повышение эффективности работы. Происходит частичная автоматизация выполнения задач системного администратора, связанных с управлением доступом пользователей в систему;
2. повышение уровня информационной безопасности. При проектировании данного комплекса учитываются все уязвимости подконтрольных систем и предусматриваются дополнительные методы защиты, направленные на найденные уязвимости и обеспечивающие более высокий уровень защиты;
3. упрощение создания и модернизации бизнес-приложений;
4. унификация бизнес-правил предоставления доступа к разнородным информационным ресурсам компании;
5. снижение рисков несанкционированного доступа.

Однако метод централизованного управления доступом имеет ряд недостатков:

1. высокая стоимость установки. При интеграции такой системы необходим выделенный сервер с достаточно высокими техническими характеристиками, т.к. через него будет проходить трафик всех подконтрольных систем. Также сервер должен обеспечивать высокую степень отказоустойчивости к нагрузочным и подобным типам атак;
2. понижение уровня безопасности данных при недостаточных мерах безопасности. При низкой квалификации работников, отвечающих за безопасность данных, предложенное решение не только не повысит уровень безопасности за счет закрытия уязвимостей дочерних

систем, но и создаст новые угрозы и откроет злоумышленнику доступ ко всем системам единоразово.

Управление доступом к различным информационным системам является неотъемлемой частью работы средних и крупных предприятий. Системы централизованного управления доступом оправдывают свое применение в случае наличия нескольких дискретных систем, требующих администрирования, т.к. упрощают работу администратора безопасности и увеличивают степень защиты информации.

Список литературы

[1] Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения». – М.: ГТК РФ, 1992. – 13 с.

[2] *Лачихина А.Б., Мазин А.В*. Методика рациональной настройки баз данных на примере системы "Аналитик". // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия: Приборостроение. - 2010. - № 4. - С. 91-103.

Бланк Яна Андреевна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: yanablank10@gmail.com

Телерман Алексей Эдуардович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: telerman.bas@yandex.ru

Лачихина Анастасия Борисовна – канд. техн. наук, доцент кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: anastasialach73@gmail.com

Е.Ю. Шестопалов, К.А. Празян

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПОПУЛЯРНЫХ МЕНЕДЖЕРОВ ПАРОЛЕЙ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

На сегодняшний день наиболее часто используемым инструментом защиты являются пароли. Во многих компаниях пароли зачастую охраняют наиболее важные секреты организации, например, медицинскую информацию, секретные бизнес-стратегии, финансовые данные и т.д. К сожалению, простые пароли - слабое звено в цепи безопасности систем. [1]

Серьезность проблемы паролей состоит в том, что у каждого пользователя есть не одна учетная запись и, соответственно, не один пароль. Всю эту информацию ему необходимо держать в голове. В конечном итоге, это приводит к использованию более простых паролей, т.к. их легче запоминать. В отдельных случаях, люди используют один пароль для большинства или даже всех их учетных записей. Однако данная ситуация неприемлема, потому что в случае, если злоумышленник, завладев паролем, получит доступ к одной учетной записи, он сможет использовать его для других. [2]

С целью решения данной проблемы были созданы менеджеры паролей. Их функционал позволяет хранить, генерировать, и проверять на надежность пароли.

На данный момент наиболее распространены такие менеджеры:

- KeePass;
- eWallet;
- 1Password;
- RoboForm;
- LastPass;
- Dashlane;

Для дальнейшего сравнения программ мною были выделены преимущества и недостатки каждой программы. [3] Подробную информацию можно увидеть в табл. 1.

Таблица 1. Характеристика менеджеров паролей

Критерий сравнения	Комментарий
KeePass	
Преимущества	-бесплатная; -синхронизируется с облачными хранилищами; -позволяет автоматически вводить пароли в браузерах и других программах; -обладает множеством плагинов, обеспечивающих более тесную интеграцию с браузерами; -алгоритм шифрования AES-256;
Недостатки	-старый дизайн;

eWallet	
Преимущества	-интегрируется с браузерами; -алгоритм шифрования AES-256; -позволяет автоматически подставлять логин и пароль в поле браузера;
Недостатки	-платная (стоимость 19,99$); -нет синхронизации с облачными хранилищами; -неудобный дизайн;
1Password	
Преимущества	-имеет встроенную синхронизацию базы паролей; -интегрируется с браузерами; -позволяет автоматически вводить пароли в браузерах и других программах; -имеет возможность работы с базой данных через HTML-файл, что позволяет использовать ее в любой операционной системе; -имеет приложения для большинства мобильных платформ; -позволяет хранить не только пароли, но и файлы;
Недостатки	-платная (стоимость от 49,99$); -алгоритм шифрования AES-128;
RoboForm	
Преимущества	-имеет встроенную синхронизацию базы паролей; -алгоритм шифрования AES-256; -интегрируется с браузерами; -позволяет автоматически вводить пароли в браузерах и других программах; -имеет приложения для большинства мобильных платформ;
Недостатки	-платная (стоимость 9,95$);
LastPass	
Преимущества	-бесплатная (имеется премиум пакет стоимостью 1$); -алгоритм шифрования AES-256; -возможно управление через web-интерфейс; -облачный сервис. Базы данных хранятся на серверах LastPass, что убирает необходимость синхронизации; -имеет приложения для мобильных устройств;
Недостатки	-мобильные приложения требуют покупки платной подписки;
Dashlane	
Преимущества	-позволяет автоматически вводить пароли в браузерах и других программах; -алгоритм шифрования AES-256; -имеет встроенную синхронизацию базы паролей; -имеет приложения для большинства мобильных платформ; -интегрируется с браузерами; -имеет возможность работы с базой данных через HTML-файл, что позволяет использовать ее в любой операционной системе;
Недостатки	-платная (стоимость 39,99$)

Подводя итоги обзора наиболее популярных менеджеров для защиты паролей пользователя, следует сказать, что все они удовлетворяют своей главной функции - защите данных. Выбор конкретной программы будет зависеть от предпочтений человека. Тем, кому критически важен функционал продукта, несмотря на его стоимость, следует выбрать 1Password или Dashlane, т.к. они обладают наиболее широким набором функций. Если же стоимость программы критична, то стоит обратить внимание на KeePass и LastPass.

Список литературы

[1] *Скудис Э.* – Противостояние хакерам. Пошаговое руководство по компьютерным атакам и эффективной защите: Пер. с англ. – М.: ДМК Пресс, 2003. – С.263-264.

[2] *Шаньгин В.Ф.* – Информационная безопасность. – М.: ДМК Пресс, 2014. – С.48-56.

[3] Информационный ресурс Хабрахабр https://habrahabr.ru/post/1252248/

Шестопалов Егор Юрьевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: shestopalovegor@gmail.com

Празян Константин Арменович – ассистент кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: prazyan.konstantin@gmail.com

С.В. Чупикова, А.Б. Лачихина

ТРЕБОВАНИЯ БЕЗОПАСНОСТИ В СУБД

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

21 первом веке общество находится в стадии развития, определяемой как, “Информационное общество”. Оно характерно активным использованием информации и увеличением объема используемых данных. Это привело к необходимости создания систем для упорядочивания данных, т.е СУБД. На настоящий момент существует уже больше сотни различных СУБД, но их объединяет одна общая аксиома: данные должны быть надежно защищены.

В наше время развитые информационные приложения полагаются не на файловую систему, а на многопользовательские сетевые СУБД, выполненные в формате клиент/сервер, что требует высокой степени защищенности систем и их серверных компонентов. Три главных аспекта информационной безопасности: доступность, конфиденциальность и целостность - имеют важное значение для СУБД. Общая идея защиты систем состоит в следовании рекомендациям, сформулированным для класса безопасности С2. [1] Данный класс безопасности подходит для большинства коммерческих систем. Класс С1 - это класс, обеспечивающий базовый уровень безопасности, способом разделения пользователей и данных. Информационные системы, принадлежащие к данному классу, должны отвечать следующим основным требованиям:

1. доступом именованных пользователей к именованным объектам управляет доверенная база;

2. четкая идентификация пользователей;

3. защита аутентификационной информации пользователей от несанкционированного доступа;

4. наличие у доверенной вычислительной базы для собственного выполнения изолированной области, защищенной от внешних воздействий;

5. наличие аппаратных или программных средств, позволяющих периодически проверять корректность функционирования аппаратных и микропрограммных компонентов доверенной вычислительной базы;

6. защитные механизмы протестированы на отсутствие способов обхода или разрушения средств защиты доверенной вычислительной базы;

7. описаны подход к безопасности и его применение при реализации доверенной вычислительной базы.

Класс С2 - это класс, который в дополнение к требованиям класса защищенности С1 гарантирует ответственность пользователей за свои действия и включает в себя собственные уникальные требования:

1. права доступа гранулируются с точностью до пользователя, а доступ к любому объекту контролируется;

2. устранение следов использования объекта при выделении его из пула ресурсов доверенной вычислительной базы;

3. каждый пользователь системы уникальным образом идентифицируется, а каждое регистрируемое действие ассоциируется с конкретным пользователем;

4. доверенная вычислительная база позволяет создавать, поддерживать и защищать журнал регистрационной информации, касающейся доступа к объектам, которые контролируются базой;

5. тестирование подтверждает отсутствие видимых недостатков в механизмах изоляции ресурсов и защиты регистрационной информации.

Исходя из требований класса защищенности С2, применяемого к системе, для ее защиты необходима реализация следующих механизмов ЗИ:

1. Защита паролем

Представляет простой и эффективный способ защиты БД от несанкционированного доступа. Пароли устанавливаются конечными пользователями или администраторами БД. Учет и хранение паролей производится самой СУБД. Обычно пароли хранятся в определенных системных файлах СУБД в зашифрованном виде. Поэтому просто найти и определить пароль невозможно. После ввода пароля пользователю СУБД предоставляются все возможности по работе с защищенной БД.

2. Разграничение прав доступа к объектам БД

В целях контроля использования основных ресурсов СУБД во многих системах имеются средства установления прав доступа к объектам БД. Права доступа определяют возможные действия над объектами. Владелец объекта (пользователь, создавший объект), а также администратор БД имеют все права. Остальные пользователи к разным объектам могут иметь различные уровни доступа.

3. Шифрование данных и программ

Шифрование данных (всей базы или отдельных таблиц) применяется для того, чтобы другие программы не могли прочитать данные. Шифрование исходных текстов программ позволяет скрыть от несанкционированного пользователя описание соответствующих алгоритмов.

4. Защита полей и записей таблиц самой БД.

Таким образом, при разработке собственной СУБД необходимо определять ее класс защищенности, а также учитывать все требования по мерам защиты, которые в нем содержатся.

Список литературы

[1] Классификация методов защиты информации. //Статья. - 2012. - [Электронный ресурс]. – Режим доступа: URL: http://camafon.ru/informatsionnaya-bezopasnost/metodyi-zashhityi (1.10.2016)

[2] *Блинов А.М.* Информационная безопасность. Часть 1. – СПб.: СПбГУЭФ, 2010. – 96 с.

[3] *А.Н. Наумов, А.М. Вендров, В.К. Иванов и др.* Системы управления базами данных и знаний. – М.: Финансы и статистика, 1991. – 352 с.

[4] Средства защиты баз данных. //Статья. -2013- [Электронный ресурс]. – Режим доступа: URL: http://life-prog.ru/1_13285_sredstva-zashchiti-bazi-dannih.html (2.10.2016)

Чупикова Светлана Викторовна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: victorovna.sveta@gmail.com

Лачихина Анастасия Борисовна – канд. техн. наук, доцент кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: anastasialach73@gmail.com

Н.Е. Миронов, О.Ю. Жарова

УЯЗВИМОСТИ В ОС WINDOWS 10

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Windows 10 – операционная система для персональных компьютеров, разработанная корпорацией Microsoft в рамках семейства Windows NT. Официальный запуск операционной системы Windows 10 - 29 июля 2015 года. И как почти в любой системе, в ней есть свои уязвимости.

На Windows 10 обрушился шквал критики из-за слежки операционной системы за пользователями. Пользователям не понравилось, что Windows собирает и отправляет телеметрию. Телеметрия - это ряд различных типов данных, таких как местоположение, названия открываемых программ, их электронные письма и данные различных менеджеров, данные о контактах и частота взаимодействия с этими контактами на мобильных устройствах, которые находятся под управлением Windows 10. Все эти данные автоматически отправляются на облачные сервера Microsoft. Часть критики также относится к тому, что Windows делится паролями от Wi-Fi с другими пользователями.

Через год после выхода, в обязательном обновлении "Windows 10 Anniversary Update" пользователи некорпоративных версий были лишены возможности отключить Lock Screen, на котором приложением Windows Spotlight принудительно демонстрируется реклама Microsoft. Также, после интеграции Windows Search и Cortana стало невозможным отключение Cortana, этот блок теперь постоянно отсылает вводимые данные (без входа в учетную запись cortana данные остаются "анонимными").

Уязвимость от 11 августа 2015 года. Компания Microsoft выпустила security-обновление MS15-085, которое закрывает опасную LPE уязвимость CVE-2015-1769 (Mount Manager Elevation of Privilege Vulnerability). Уязвимость присутствует на клиентских и серверных версиях Windows, начиная с Windows Vista, и заканчивая Windows 10. Она относится к типу Stuxnet-like-уязвимостей и срабатывает при подключении к компьютеру съемного диска. Для эксплуатации, в корне съемного диска должны быть расположены специальным образом сформированный файл или файлы (symbolic links).

Обновлению подлежат значительное количество системных файлов Windows 10, включая, драйвер монтирования дисков и ядро ОС: Mountmgr.sys, Ntdll.dll, Ntoskrnl.exe. Уязвимость позволяет атакующим запускать свой код с носителя, причем с системными привилегиями SYSTEM. Видимо, обновлению не присвоен уровень серьезности Critical лишь потому, что эксплуатация может быть выполнена только за счет физического доступа к ПК, т. е. с использованием съемного носителя.

Оригинальная уязвимость Stuxnet, которая была закрыта MS10-046, относилась к типу Remote Code Execution (RCE), поскольку уязвимый системный компонент Windows (Shell) позволял атакующим исполнять свой код из самых разных мест, включая, удаленные. Новая же уязвимость в MountMgr может быть использована только в случаях локальной эксплуатации, т. е. только через подключение съемного носителя к системе.

Обновление Windows 10 Anniversary вышло 2 августа 2016. Оно было выпущено через год после релиза самой операционной системы. В обновленной версии операционной системы Windows 10 Anniversary обнаружили уязвимость. Недостаточная защищенность дает хакерам возможность получить доступ к компьютеру, на котором установлена данная операционная система, похитив логин и пароль от учетной записи пользователя.

Информация, полученная благодаря уязвимости, также может быть использована для взлома учетных записей в различных сервисах компании Microsoft (в их числе – Skype, Office 365, Xbox Live и другие). Кроме того, хакеры смогут получить доступ к голосовому помощнику Cortana.

Речь идет о так называемой атаке Redirect to Server Message Block. При ее осуществлении браузер жертвы хакеров подключается к IP-адресу киберпреступников и передает на него данные.

Как сообщает издательство The Inquirer, из-за недостаточной защищенности операционной системы уязвимыми становятся также подключения к сетям VPN.

При этом отмечается, что о подобных уязвимостях в операционных системах Windows было известно еще в 1997 году.

В Windows 10 Anniversary было изменено сообщение о критической ошибке в операционной системе, известное также как BSoD, также «синий экран смерти». Ранее при выключении или перезагрузки ПК появлялся BSoD с ошибкой "Driver power state failure". Теперь на мониторе отображается QR-код, который помогает специалистам разобраться в причинах сбоя.

Следующие сразу 2 уязвимости Microsoft Windows 10 датированы 10.02.2016. Они не были столь опасны, как предшествующие. Обе уязвимости имели удаленный вектор эксплуатации. Их воздействие обеспечивало отказ в обслуживании системы и раскрытие важных данных пользователя.

Первая уязвимость существует из-за ошибки при обработке XSLT в .NET Framework. Удаленный пользователь может вставить специально сформированные XSLT в клиентскую web-часть XML, вызвав рекурсивную компиляцию трансформаций XSLT.

Вторая уязвимость существует из-за ошибки при неверной обработке иконок в NET Framework (компонент WinForms). Удаленный пользователь может отправить специально сформированные данные иконок службе .NET и раскрыть важные данные.

Список литературы:

[1] securitylab.ru
[2] theinquirer.net - Лондон, 1994-н.в.
[3] habrahabr.ru

Миронов Никита Евгеньевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: evraskinakira@yandex.ru

Жарова Ольга Юрьевна – ассистент кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: ouzharova@yandex.ru

Е.А. Коваленко, О.С. Клочко

ШИФРОВАНИЕ ДАННЫХ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В век информационных технологий человечество все больше отказывается от хранения информации в рукописном или печатном виде, предпочитая для этого электронные документы. С течением времени появляется возможность хранить и передавать все большие объемы информации. Но при этом информация становится все более уязвимой из-за возрастающих объемов хранимых и передаваемых данных или же расширения круга пользователей, которые имеют право доступа к данным.

Поэтому все большую важность приобретает проблема защиты информации от несанкционированного доступа при ее передаче и хранении. Одним из наиболее широко используемых криптографических методов сохранения конфиденциальности информации является шифрование. Человечество использует шифрование с того момента, как появилась первая секретная информация - такая, доступ к которой не должен быть публичным. [1]

Шифрование – это способ сокрытия исходного смысла сообщения от лиц, не имеющих полномочий для его просмотра, обеспечивающий искажение его первоначального содержимого. Главной целью шифрования является обеспечение конфиденциальности, целостности и доступности информации.

Для осуществления шифрования данных необходимо использовать определенный аутентичный ключ, который утверждает выбор конкретного преобразования из совокупности возможных преобразований для данного алгоритма. Пользователи являются авторизованными, то есть имеющими полномочия просматривать секретную информацию, если они обладают этим ключом. Идея шифрования состоит в том, что злоумышленник, перехватив зашифрованные данные и не имея к ним ключа, не может ни прочитать, ни изменить передаваемую информацию. В целом, шифрование состоит из двух этапов: зашифрование и расшифрование. [2]

Существует два типа алгоритмов шифрования: симметричное и асимметричное. При реализации симметричного шифрования используется один и тот же ключ как для зашифрования информации, так и для ее расшифрования. В свою очередь, асимметричное шифрование использует два разных ключа: один для зашифрования, другой для расшифрования. Первый еще называют «открытым» ключом, а второй – «закрытым». Каждый из этих подходов имеет как достоинства, так и недостатки. Выбор применяемого метода зависит от целей, с которыми информация подвергается шифрованию.

Рассмотрим работу одного из асимметричных алгоритмов шифрования RSA. RSA (Rivest, Shamir, Adleman) – криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности зада-

чи факторизации больших целых чисел. Был разработан в 1977 году. Трое ученых из Массачусетского технологического института Рональд Ривест, Ади Шамир и Леонард Адлеман занимались разработкой данного алгоритма шифрования, основная идея которого заключалась в том, насколько легко находить большие простые числа и насколько сложно раскладывать на множители произведение двух больших простых чисел. Система была названа по первым буквам фамилий ее создателей.

В алгоритме RSA открытый ключ доступен всем, а закрытый хранится только у его хозяина и неизвестен никому другому. С помощью одного ключа можно производить операции только в одну сторону. Если сообщение зашифровано с помощью одного ключа, то расшифровать его можно только с помощью другого. Имея один из ключей вероятность найти другой ключ практически нулевая, если разрядность ключа высока. [5]

Алгоритм состоит из трех этапов: генерация ключей, зашифрование, расшифрование.

- Генерация ключей:
  1. Выбор двух простых чисел p и q таких, что p не равно q.
  2. Вычисление модуля – произведение p и q: n = p * q.
  3. Вычисление функции Эйлера: f = (p - 1) * (q - 1).
  4. Выбор числа E – открытой экспоненты. Это число должно отвечать следующим критериям: оно должно быть простое, оно должно быть меньше f, оно должно быть взаимно простое с f.
     Пара {E, n} – открытый ключ.
  5. Вычислить число D, обратное E по модулю f. То есть остаток от деления по модулю f произведения D * E должен быть равен 1: (D * E) mod f = 1.
     Пара {D, n} – закрытый ключ.
- Зашифрование:

Пусть A – это исходная информация, которую необходимо зашифровать. Тогда: $B = A^E \pmod n$ – зашифрованная информация.

- Расшифрование:

Расшифрование зашифрованной информации происходит с помощью закрытого ключа по следующей формуле: $A = B^D \pmod n$.

Замечание: необходимым условием корректной работы данного алгоритма является то, что кодируемое сообщение A не должно быть больше числа n. [3]

Обобщенная схема работы алгоритма RSA, отображающая Обобщенная последовательность действий, которые включает в себя данный алгоритм, продемонстрирована на рисунке 1.

С целью детально рассмотреть алгоритм RSA и продемонстрировать его работу на примере, было создано приложение на языке программирования C# в среде разработки программного обеспечения Visual Studio.

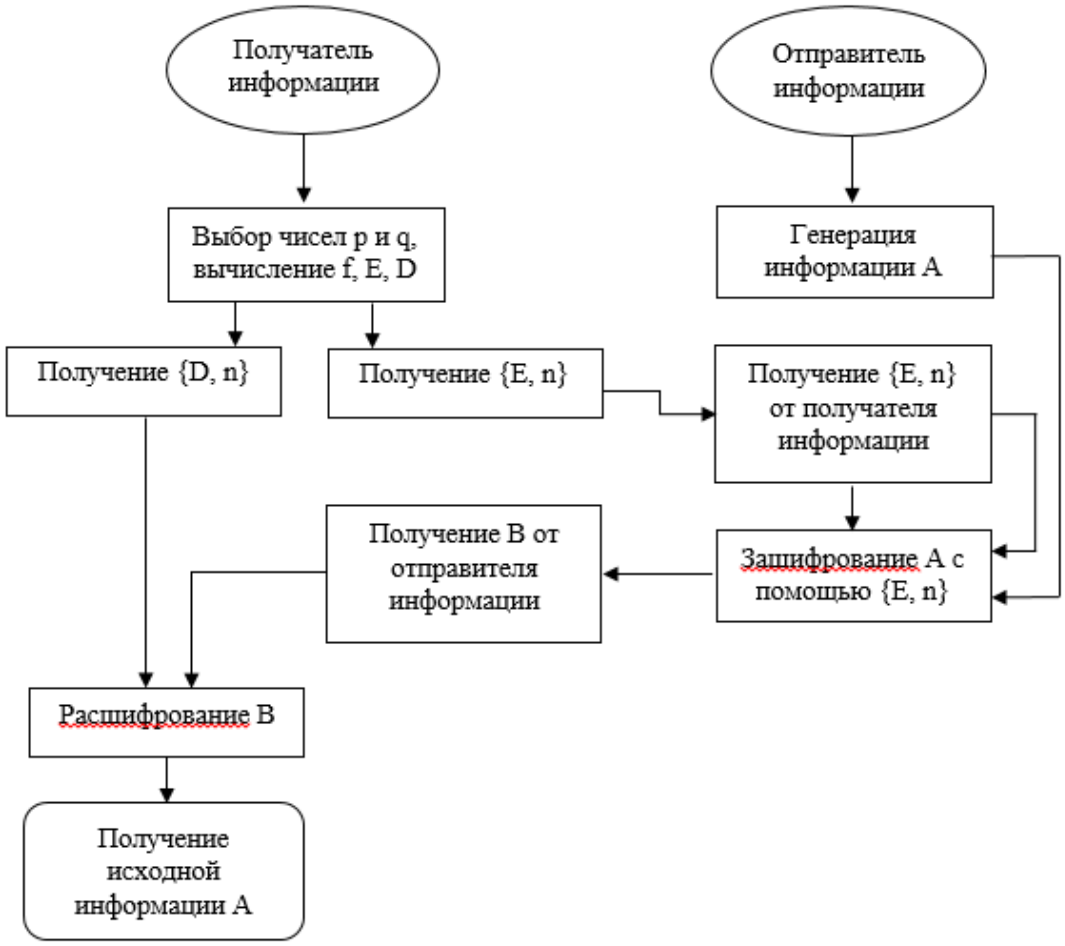


Рисунок 1. Обобщенная схема работы алгоритма RSA

В приложении имеются две формы, олицетворяющие собой отправителя сообщения (Sender) и получателя сообщения (Recipient). Алгоритм работы приложения разработан таким образом, чтобы смоделировать передачу ключей от получателя к отправителю и передачу зашифрованных данных от отправителя к получателю.

Для того, чтобы создать ключи на форме Recipient необходимо ввести простые числа p и q, а затем нажать кнопку «Сгенерировать ключи». После того, как создание ключей завершено, на этой же форме нужно нажать кнопку «Отправить открытый ключ», после чего автоматически появится форма Sender. Затем, нажав кнопку «Принять открытый ключ» на форме Sender, отправитель получит открытый ключ. Теперь он может вводить сообщение в поле «Исходный текст» и приступать к его зашифрованию с помощью полученного открытого ключа, нажав кнопку «Зашифровать текст».

Классический алгоритм шифрования RSA слишком слаб. Причина кроется в том, что один и тот же символ шифруется одним и тем же числом. Это позволяет злоумышленнику, перехватившему сообщение, догадаться о его содержимом. Чтобы избежать этого, используются специальные дополнительные алгоритмы, суть которых в том, что каждая предыдущая часть сообщения начинает влиять на следующую. В данном приложении перед зашифрованием

к каждой части сообщения применяется следующее правило: b = (b + a) % n, где a – предыдущая часть сообщения, а b – следующая. При расшифровании применяется обратная операция модифицирования: b = (b - a) % n. [4]

Таким образом, перед шифрованием, необходимо преобразовать каждый символ текстового сообщения в его числовое представления, согласно таблице ASCII (American Standard Code for Information Interchange). Затем, применяя вышеуказанный дополнительный алгоритм, необходимо модифицировать каждое число сообщения перед шифрованием.

При реализации данного алгоритма можно столкнуться с проблемой хранения очень больших чисел, не помещающихся ни в один тип числовых данных. Это происходит вследствие того, что одним из основных факторов надежности этого алгоритма является использование больших чисел p и q, а значит формируемые ключи также будут представлены большими числами. Как уже упоминалось выше, в формулах зашифрования и расшифрования применяется возведение в степень. Как раз при возведении в степень и получаются очень большие числа. Соответственно, чтобы не хранить большие числа, нужно избежать необходимость возведения в полную степень. Для этого применяется алгоритм быстрого возведения в степень.

Алгоритм вычисления $a^E \pmod n$:

1. Число E необходимо представить в двоичной системе счисления: $E = E_0 * 2^r + \ldots + E_{r-1} * 2 + E_r$, где E_i – цифры в двоичном представлении, $E_0 = 1$.
2. Положить $a_0 = a$, а затем для $i = 1, \ldots, r$ вычислить $a_i = (a_{i-1})^2 * a^{Ei} \pmod n$.
3. a_r есть искомое число $a^E \pmod n$. [6]

Работа данного приложения продемонстрирована на рисунках 2 и 3.

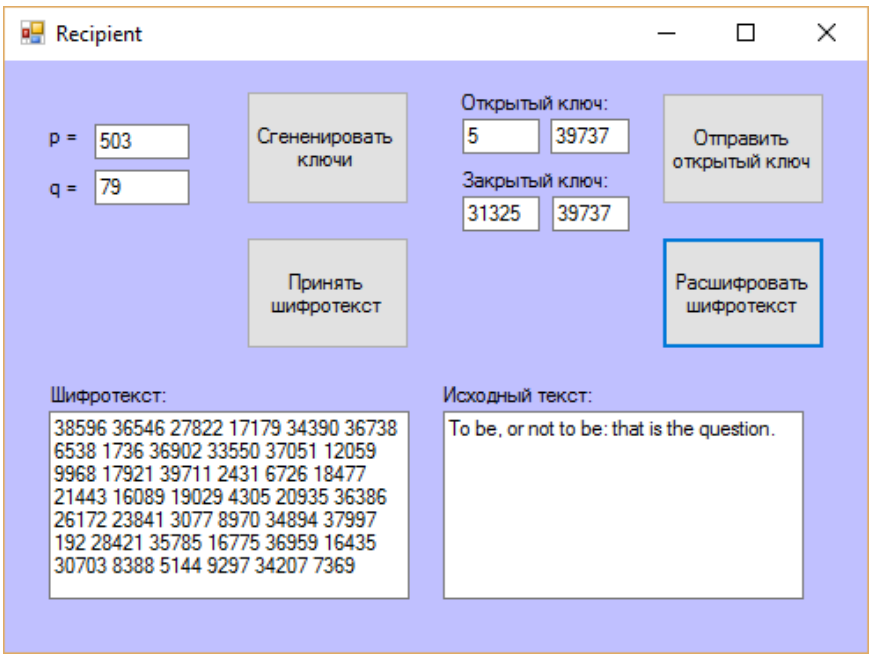


Рисунок 2. Пример работы формы Recipient

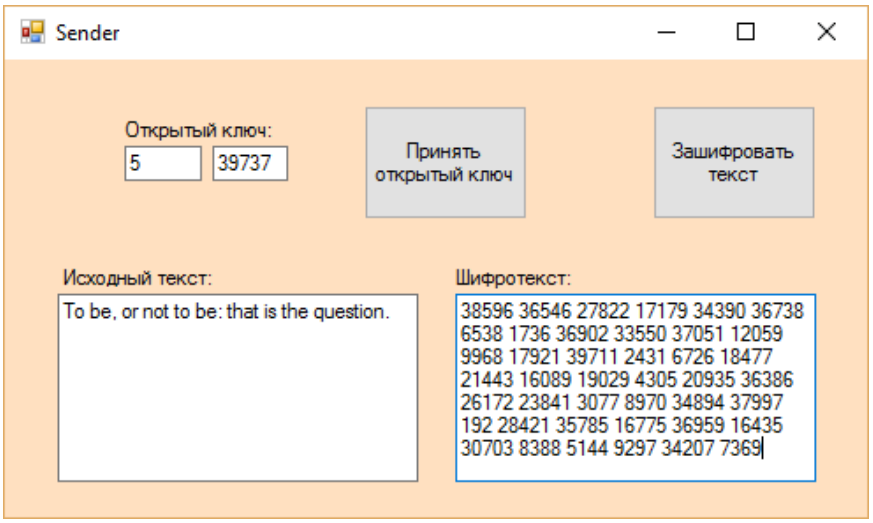


Рисунок 3. Пример работы формы Sender

В заключение следует отметить, что алгоритм шифрования RSA применяется для защиты программного обеспечения и в схемах цифровой подписи. [1]

Список источников:

[1] Б. Шнайер Прикладная криптография

[2] А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин Основы криптографии

[3] http://www.krukovo.ru/stat/cript

[4] http://www.ixbt.com/soft/alg-encryption.shtml

[5] http://shifrovanie.narod.ru/articles/5n96y3a.htm

[6] http://www.michurin.net/computer-science/rsa.html

[7] http://www.paveldvlip.ru/algorithms/rsa.html

Коваленко Елизавета Александровна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: www.yoursmile@yandex.ru

Клочко Ольга Сергеевна - ассистент кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: klochkoolgakaluga@gmail.com

СЕКЦИЯ 14.

ДИНАМИКА, ПРОЧНОСТЬ И НАДЕЖНОСТЬ ПОДЪЕМНО-ТРАНСПОРТНЫХ, СТРОИТЕЛЬНЫХ, ДОРОЖНЫХ МАШИН И ОБОРУДОВАНИЯ

Д.Г. Мокин, Д.В. Суранов

АВТОМАТИЗАЦИЯ ГРУЗОВОГО ЛИФТА

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Объектом исследования является грузовой лифт и возможность его автоматического управления.

Цель работы - повышение качества работы лифта, плавности его движения, точности остановки, для создания максимальной производительности.

В процессе работы необходимо будет провести экспериментальные исследования автоматизации лифта и разработать автоматическое управление лифтом при помощи программного модуля LabVIEW.

Программный модуль LabVIEW был выбран из соображений его удобства и легкости в процессе работы.

В данной работе рассматривается грузовой лифт, который устанавливается в жилых и общественных зданиях и служащий для перевозки грузов. Объектом управления является асинхронный двигатель с редуктором, канатоведущим шкивом, канатом, кабиной и противовесом. Следовательно, можно сказать, что объектом управления САУ является асинхронный двигатель совместно с механической частью системы.

Система управления лифтом должна решать задачи безопасного и комфортного передвижения пассажиров. Передвижение должно осуществляться с допустимым ускорением, требуемой скоростью и отсутствие ощутимых рывков. Для выполнения приведённых требований необходимо получать информацию о положении и скорости движения кабины с помощью различных датчиков.

Большое внимание необходимо уделить вопросу безопасности передвижения в случаях пожаров и землятресений, обрыва канатов, срабатывания ловителей.

Режим работы электропривода лифта характеризуется частыми включениями и отключениями. При этом можно выделить следующие этапы движения [1] (рис. 1.):

- разгон электродвигателя до установившейся скорости $\upsilon_{уст}$;
- движение с установившейся скоростью;
- уменьшение скорости при подходе к этажу;
- торможение и остановка кабины лифта на этаже назначения с требуемой точностью.

Прежде чем создать алгоритм работы электропривода лифта, на начальном этапе необходимо разработать функциональную схему системы управления и алгоритма управления процессом грузового лифта.

Алгоритм функционирования лифтовой установки можно представить в виде блок диаграммы [2] (рис. 2.).

Блок диаграмма состоит из систем действий и условий, при которых это действие совершается, и работать она должна следующим образом.

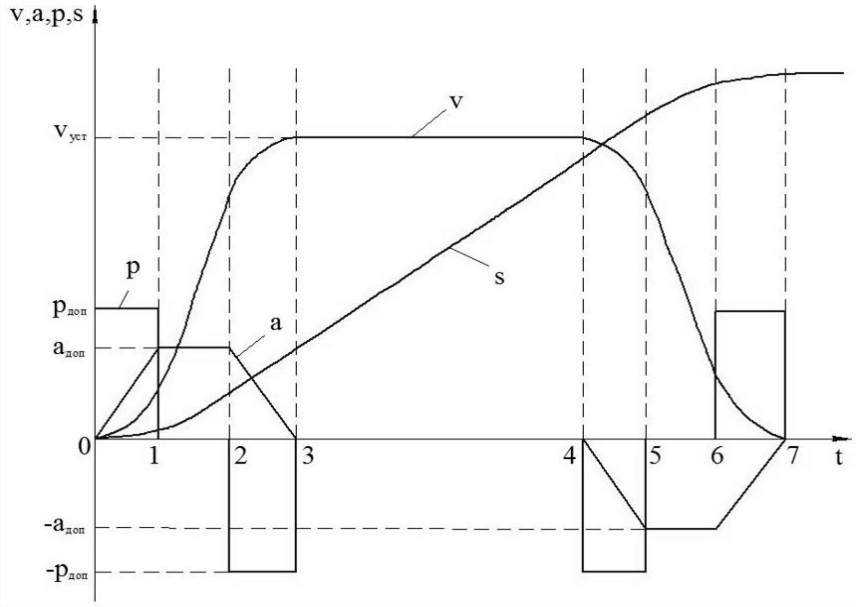


Рис. 1. Оптимальный график движения кабины

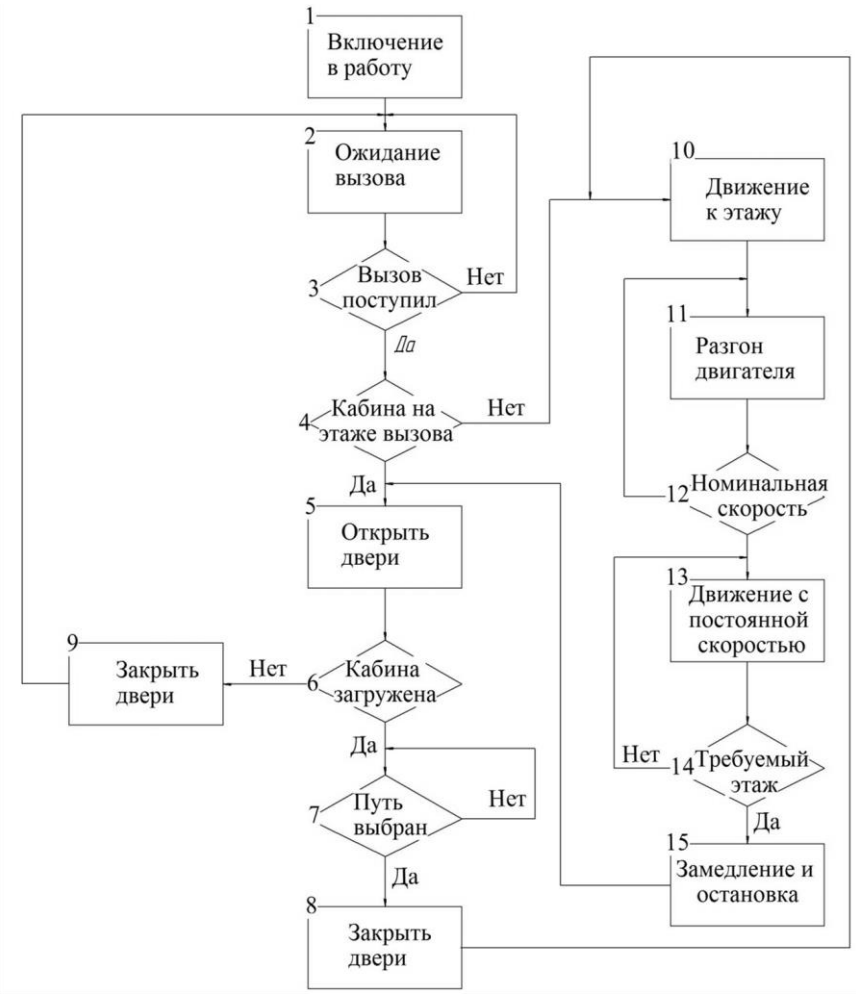


Рис. 2. Алгоритм функционирования лифтовой установки

Лифт находится в рабочем режиме и на начальном этапе ожидает вызова. При нажатии кнопки вызывного аппарата в электроаппаратуру управления лифтом подается электрический импульс (вызов). Если кабина находится на остановке, с которой поступил вызов, открываются двери кабины и шахты на данной остановке. Если кабина в другом месте, подается команда на её движение. В обмотку электродвигателя лебёдки и катушки электромагнитных тормозов подаётся напряжение, тормоза отпускают, и ротор электродвигателя приходит в движение.

При подходе кабины к требуемой посадочной площадке система управления лифтом по сигналу датчиков точной остановки переключает электродвигатель лебёдки на работу с пониженной частотой вращения ротора. Скорость движения кабины снижается, подаётся команда на остановку, и в момент, когда порог кабины совмещается с уровнем порога двери шахты, кабина останавливается, вступает в действие тормоз, включается в работу привод дверей, и двери кабины и шахты открываются. На лифте с системой управления от контроллера происходит бесступенчатое регулирование частоты вращения ротора двигателя посредством системы частотного регулирования, что обеспечивает плавные остановку и пуск кабины.

При нажатии кнопки приказа на панели управления, расположенной в кабине, закрываются двери кабины и шахты, кабина отправляется на посадочную площадку, кнопка приказа которой нажата.

После прибытия на требуемую посадочную площадку и выхода пассажиров двери закрываются, кабина стоит до тех пор, пока не будет нажата кнопка любого вызывного аппарата.

Движение кабины возможно только при исправности всех блокировочных и предохранительных устройств. Срабатывание любого предохранительного устройства приводит к размыканию цепи управления и остановке кабины.

В зависимости от поступивших вызовов и приказов происходит управления оборудованием лифта по заданной программе.

В результате разработки системы автоматизированного управления можно будет анализировать статистические данные по работе лифтовой установки. Данная программа будет иметь широкий диапазон логических действий для осуществления такого анализа.

Список литературы

[1] *Бесекерский В.А.*, *Попов Е.В.* Теория систем автоматического управления. Изд. 4-е, перераб. и доп. – СПб, Изд-во «Профессия», 2004. – 752с.

[2] *Белов М.П.,* Автоматизированный электропривод типовых производственных механизмов и технологических комплексов: Учебник для вузов – М.: Академия, 2004. – 576 с.

Мокин Дмитрий Геннадьевич – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: mdg-80@yandex.ru

Суранов Дмитрий Владимирович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: moisieienko1992@mail.ru

С.Л. Заярный, А.А. Голосов

АСПЕКТЫ ПРИМЕНЕНИЯ КОМПОЗИТНЫХ МАТЕРИАЛОВ В ЭЛЕМЕНТАХ МЕТАЛЛОКОНСТРУКЦИИ КРАНА

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В статье рассматривается конструктивные, технологические и эксплуатационные особенности и условия применения композитных материалов в элементах металлоконструкций инженерных сооружений с целью улучшений их технико – экономических показателей.

Стержни ферм и оболочки металлоконструкций представляют собой идеальные элементы для изготовления из волокнистых, композиционных материалов, т. к. такие материалы особенно эффективны при нагружении в продольном направлении. При этом, их прочность может быть использована максимально [1].

При анализе прочности сжатых стержней и оболочек необходимо учитывать возможность потери устойчивости: общей для длинных и гибких стержней и местной для тонкостенных оболочек [2].

Рассмотрим некоторые аспекты применения композиционных материалов из стеклопластика в металлоконструкциях инженерных сооружений.

Стеклопластиковый профиль - это перспективный композитный материал, который имеет большую гамму применения. Стеклопластик на основе полиэфирной смолы обладает низкой теплопроводностью, прочностью стали, биологической стойкостью, влагостойкостью и атмосферостойкостью полимера, не имея недостатков, присущих термопластам.

Профиль представляет собой изделие из стеклопластика с постоянным поперечным сечением заданной длины, может выпускаться сплошным или полым. Конфигурация поперечного сечения – круглая, прямоугольная, фигурная. [3]

Таблица 1. Сравнение материалов

Факторы	**Стеклопластик**	**Сталь**	**Алюминий 6061-Т651 и 6061-Т6**
Коррозия	Выдерживают широкий спектр химических веществ и не зависит от влажности или погружения в воду	Окисление и коррозия. Требуется окраска или гальваническое покрытие	Может вызвать гальваническую коррозию (анодирование или другие покрытия увеличивают стойкость к коррозии)

Прочность	Прочность на изгиб и в продольном направлении сравнимая со сталью и большая чем у алюминия	Гомогенный материал	Гомогенный материал
Вес	Вес на 75 % меньше, чем вес стали и на 30 % меньше веса алюминия	Может потребоваться подъемное оборудование для передвижения и установки	Легкий вес
Электропроводимость	Не проводник. Высокий диэлектрический потенциал	Проводит ток. Предполагается заземление	Проводит ток. Предполагается заземление
Термические свойства	Хороший изолятор с низкой термической проводимостью	Проводит тепло. Термическая проводимость	Проводит тепло. Термическая проводимость
Жесткость	Модуль упругости: 23 х 106 Па	Модуль упругости: 29 х 106 Па	Модуль упругости: 10 х 106 Па
Ударопрочность	Распределяет ударную нагрузку, что предотвратить повреждение поверхности, даже при отрицательных температурах	Может постоянно деформироваться под воздействием	Легко деформируется под воздействием
Цвет	Цвет продукту придается в массе еще на стадии производства; не требуется дальнейшая покраска	Необходимо красить, а со временем и подкрашивать	Механические, химические и электрохимические покрытия могут быть использованы
Цена	Более низкие затраты на монтаж, меньше обслуживания и длительный срок службы продукта	Низкие начальные материальные расходы	Стоимость частично сравнима со стеклопластиком
Изготовление конструкций	Может быть изготовлена с использованием простых строительных инструментов	Требует сварки, резки и специфльного оборудования для установки	Хорошая обработка (сварка, пайка или механическое соединение)

Рассмотрение характеристик композитных пултрузионных тянутых профилей позволяет сделать вывод о возможности и целесообразности их применения в инженерных конструкциях [4].

Список литературы

[1] Композитные материалы: В 8-ми т. Пер. с англ./ Т. 7. Анализ и проектирование конструкций. Ч.1/ Под ред. К. Чамиса. – М.: Машиностроение. 1978. - 300 с.: ил..

[2] Композитные материалы: В 8-ми т. Пер. с англ./ Т. 8. Анализ и проектирование конструкций. Ч.2/ Под ред. К. Чамиса. – М.: Машиностроение. 1978. - 264 с.: ил.

[3] *Производство металлопластиковых труб* URL: http://www.meto.ru/tecnology.htm (дата обращения 29.09.2016)

[4] *Стеклопластиковые пултрузионные профили EUROGRATE* http://www.eurograte.ru (дата обращения 29.09.2016)

Заярный Сергей Леонидович – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: texnakon@yandex.ru

Голосов Алексей Алексеевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: Alex-1993g@yandex.ru

С.Л. Заярный, А.А. Шубин, Н.С. Гладышев

ВАРИАНТЫ ВИБРОПРИВОДА ОЧИСТНЫХ УСТРОЙСТВ ЩЕБНЕОЧИСТИТЕЛЬНЫХ МАШИН

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Верхнее строение железнодорожного пути служит для восприятия силовых воздействий от колес подвижного состава, и включает в себя рельсошпальную путевую решетку (РШП) с балластной призмой.

Балластная призма необходима для обеспечения устойчивости шпал под воздействием нагрузок, упругости подрельсового основания и отвода от него поверхностных вод.

В процессе эксплуатации балластная призма засоряется мелкими фракциями земляного грунта, разрушенного щебня и просыпанного груза с подвижных составов, что ухудшает её эксплуатационные характеристики. Это требует периодической очистки балластной призмы при капитальном ремонте пути. [1]

Для выполнения этих работ используются различные путевые щебнеочистительные машины: СЧ-601, СЧ-800, ЩОМ-1200, ЩОМ-1400, RM-80, RM-95F, RM-2002 и т. д. Вне зависимости от их технических характеристик, и конструктивного исполнения их основными элементами являются очистной и добывающей модули.

Очистной модуль состоит из грохотов, которые производят очистку щебня механическим способом рис. 1.

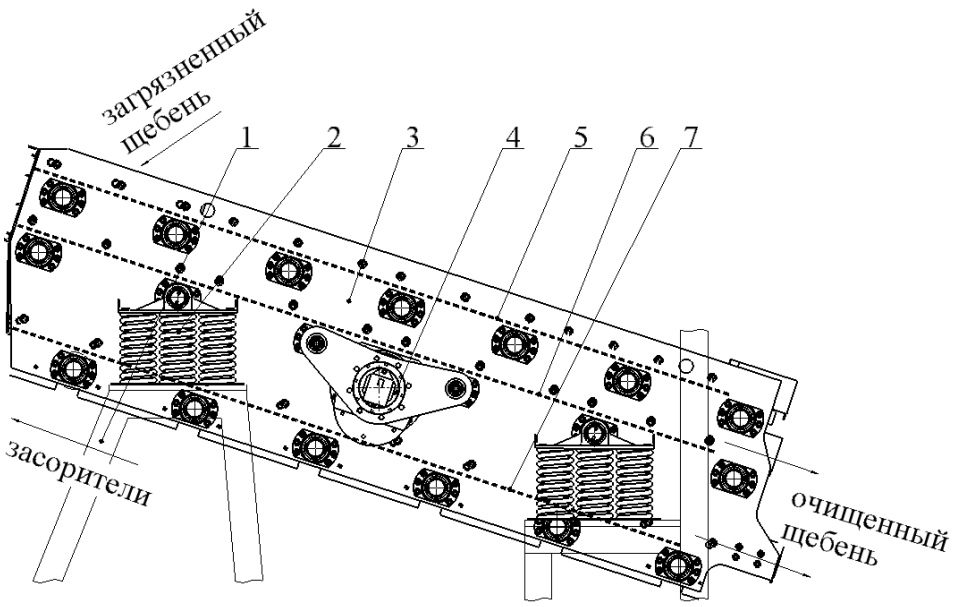


Рис 1 Устройство наклонного вибрационного грохота:
1–опорная рама, 2–комплект пружин, 3–короб, 4 – дебалансный вал,
5–7 – просеивающие сита грохота

Наклонный вибрационный грохот состоит из короба внутри которого закреплены просеивающие сита. Короб установленный на опорной раме с пружинными комплектами образует колебательную систему.

Колебания в этой системе могут возбуждаться множеством способов одним из которых основан на применение дебалансного вибратора принципиальная схема которого представлена на рис. 2

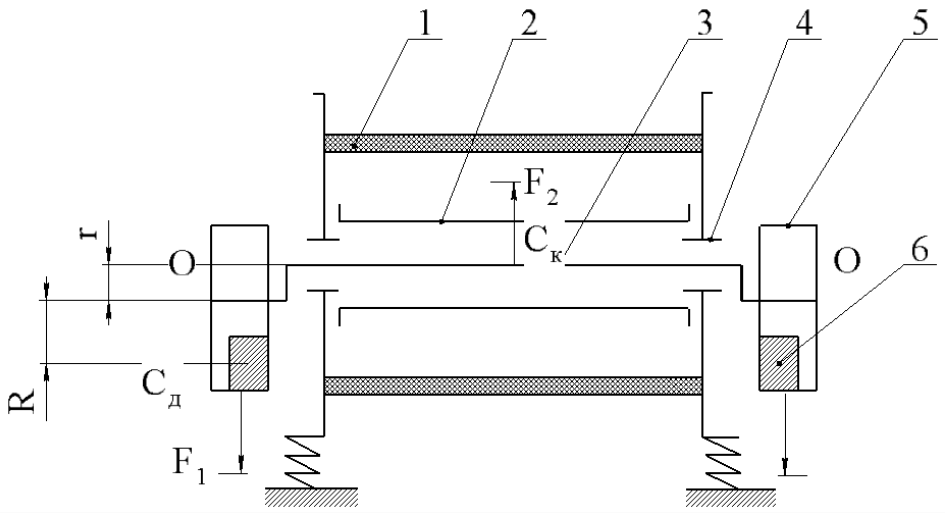


Рис. 2 Принципиальная схема действия дебалансного вибратора:
1–грохот, 2–труба, 3–вал, 4–опорный узел, 5–шкив, 6–дебалансный груз

Дебалансный привод вибрационного грохота, работая в пылящей среде, имеет ряд недостатков, к которым можно отнести большое число вращающихся быстро изнашиваемых элементов, большие нагрузки на подшипники качения, испытывающие дополнительную нагрузку от вибраций, создаваемых дебалансным валом, высоким уровнем шума.

Эти недостатки частично устраняются в гидравлических вибровозбудителях колебаний, исполнительным органом которых является цилиндр, в котором в свою очередь перемещается поршень со штоком. Рис.3

Цилиндр устанавливается на опорной раме путевой машины, а шток соединен с опорными кронштейнами грохота. Поршень под действием рабочей жидкости совершает возвратно-поступательные движения, которые через шток и опорный кронштейн грохота сообщают ему колебания. Возвратно-поступательные движения поршня создаются либо посредством использования пульсирующего потока рабочей жидкости рис. 3а, либо путем прерывания потока рабочей жидкости постоянного расхода с помощью золотниковых и клапанных устройств.

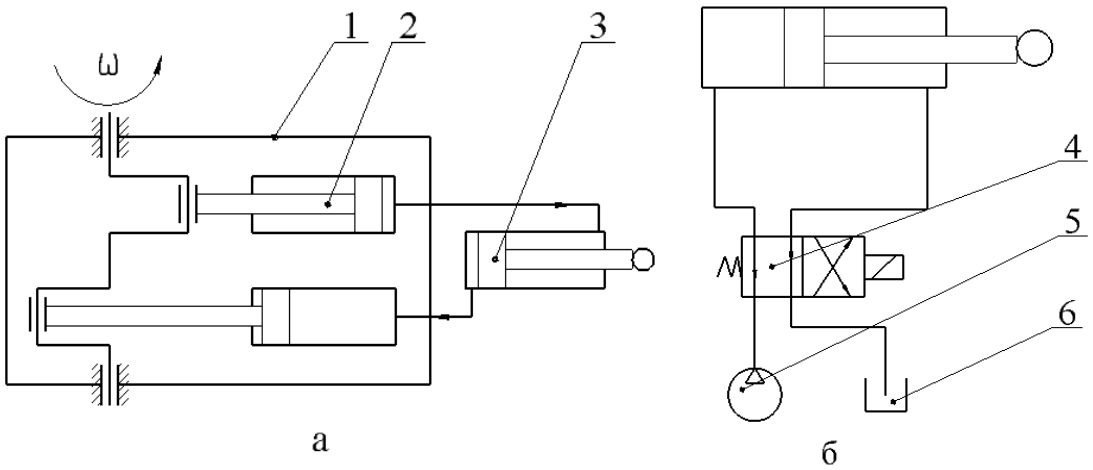


Рис. 3 Принципиальная схема действия гидравлических вибровозбудителей: а)–с плунжерным насосом, б–с электромагнитным клапаном: 1–плунжерный насос, 2–плунжер, 3–гидроцилиндр, 4–электромагнитный клапан, 5–насос, 6–сливной бак

Для уменьшения инерционности и устранения механических управляющих устройств особый интерес представляет гидравлический вибровозбудитель, в котором в качестве рабочей жидкости используется магнитная жидкость, способная мгновенно затвердевать при воздействии на нее электрического поля рис. 3б. Механические клапаны в этом вибровозбудителе заменены на электромагнитные. Частота колебаний вибровозбудителя задается частотой переключения управляющих устройств, а величина возмущающей силы–давлением рабочей жидкости в магистрали. [3]

К достоинствам таких вибровозбудителей можно отнести малые размеры, снижение затрат энергии затрачиваемых на колебания и снижение уровня шума. Недостатком пульсационных вибровозбудителей таких конструкций является наличие подвижных трущихся элементов.

Эффективным вариантом возбуждения вертикальных колебаний короба могут служить комплекты трубчатых пружин, которые совмещают в себе функции колеблющегося элемента и стабилизирующей опоры рис. 4а. Меняя расположение этих пружин можно добиться различных траекторий колебания короба.

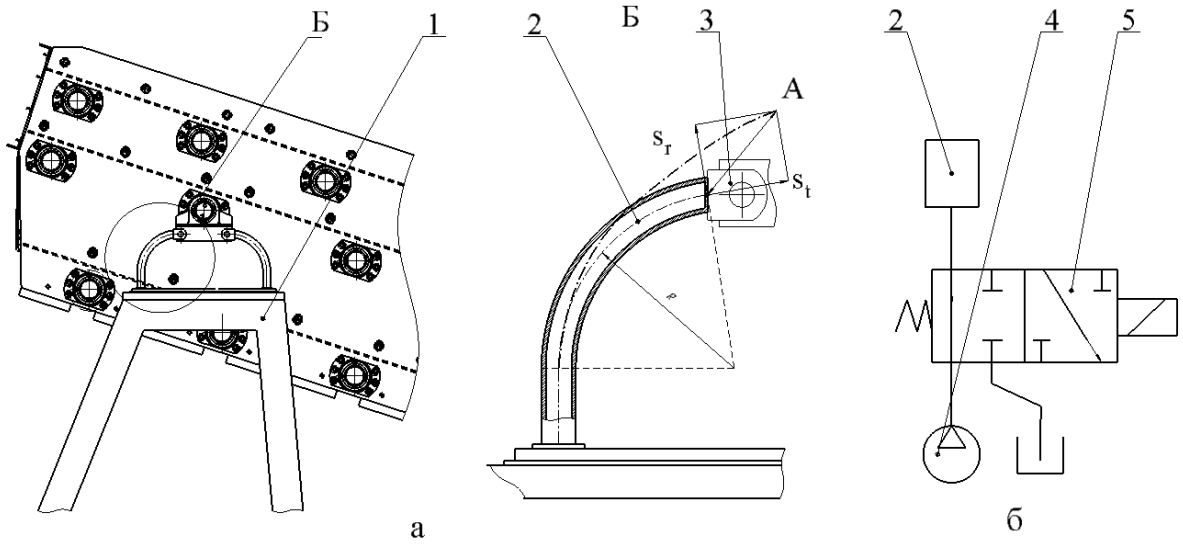


Рис. 4 Принцип действия трубчатой пружины:
а–колебания, совершаемые трубчатой пружиной, б–принципиальная схема работы трубчатой пружины: 1–опорная рама, 2–трубчатая пружина, 3–шарнир, 4–гидронасос, 5–электромагнитный клапан

Под воздействием гидростатического давления пружина деформируется и её конец получает перемещение А. При оттоке жидкости конец пружины возвращается в исходное состояние. Грохот соединенной шарнирно с пружинами совершает вертикальные колебания, создаваемые разницей между двумя конечными состояниями пружин с амплитудой А.

$$A = \sqrt{s_r^2 - s_t^2} = \frac{\Delta\gamma}{\gamma} R\Gamma \ мм, \qquad (1)$$

Где s_r и s_t –перемещения пружины в радиальном направление и направление касательном к оси пружины; $\frac{\Delta\gamma}{\gamma}$ – относительный угол изменение кривизны оси пружины и линейное перемещение ее конца; R-радиус кривизны; Г-коэффициент. [2]

Применение трубчатых пружин позволяет в процессе работы изменять амплитудно–частотные характеристики, как и в случае электромагнитного вибровозбудителя с помощью управляющих устройств, и, следовательно, подстраивать процесс грохочения под параметры (размер частиц, степень загрязнения и д. р.) очищаемого материала рис. 5б. Так же трубчатые пружины позволяют убрать из конструкции стабилизирующие опоры.

При наличии обратной связи можно реализовать частоты колебаний близкие к резонансным, что существенно снизит энергозатраты на процесс грохочения.

Замена дебалансного вибратора, применяемого на современных путевых машинах, комплектом трубчатых пружин позволит за счет упрощения конструкции значительно повысить надежность и долговечность очистного устройства, а также снизить уровень шума в процессе работы.

Список литературы

[1] Путевые машины: Учебник для вузов ж.-д. транс/ С.А. Соломонов, М.В.Попович, В.М. Бугаенко и др. Под ред. С.А. Соломонова. – М.: Желдориздат 2000 – 756 с.

[2] «Региональный Центр Инновационных Технологий» Путевые машины применяемые в ОАО «РЖД» Конструкция, теория и расчет. http://rcit.su/techinfo33.html

[3] Гончаревич, И. Ф. Вибрация - нестандартный путь: Вибрация в природе и технике / И. Ф. Гончаревич, Э Г. Гудушаури - М.: Наука, -1986. - 207с.

[4] Пономарев С. Д., Андреева Л. Е. Расчет упругих элементов машин и приборов. – М.: Машиностроение, 1980. – 326 с, ил. – (Б-ка расчетчика).

Заярный Сергей Леонидович – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: texnakon@yandex.ru

Шубин Александр Анатольевич – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: shubin55@mail.ru

Гладышев Никита Станиславович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: naik14@yandex.ru

В.А. Раевский

ГЕОМЕТРИЧЕСКИЙ СИНТЕЗ ПЕРЕДНЕГО ПЛЕЧА СТРЕЛОВОЙ СИСТЕМЫ ПОРТАЛЬНОГО КРАНА

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В работе [1] разработана и предложена аналитическая методика кинематического синтеза шарнирных стреловых систем (ШСС). Эта методика позволяет точно получить размеры звеньев ШСС, однако, не учитывает некоторые параметры при синтезе механизма в произвольном положении.

Для проверки адекватности данной методики в пакете АРМ WinMachine была создана модель шарнирно-стреловой системы. Расчетная траектория точки конца хобота и траектория, полученная в пакете АРМ WinMachine, значительно отличались друг от друга. Это связано с тем, что расчетная схема, приведенная в [1], не учитывает, что в реальных конструкциях хобот соединен со стрелой корпусом шарнира, который имеет свою высоту, т.е. шарниры находятся не на одной линии. На рис. 1 представлена доработанная модель первого механизма в произвольном положении.

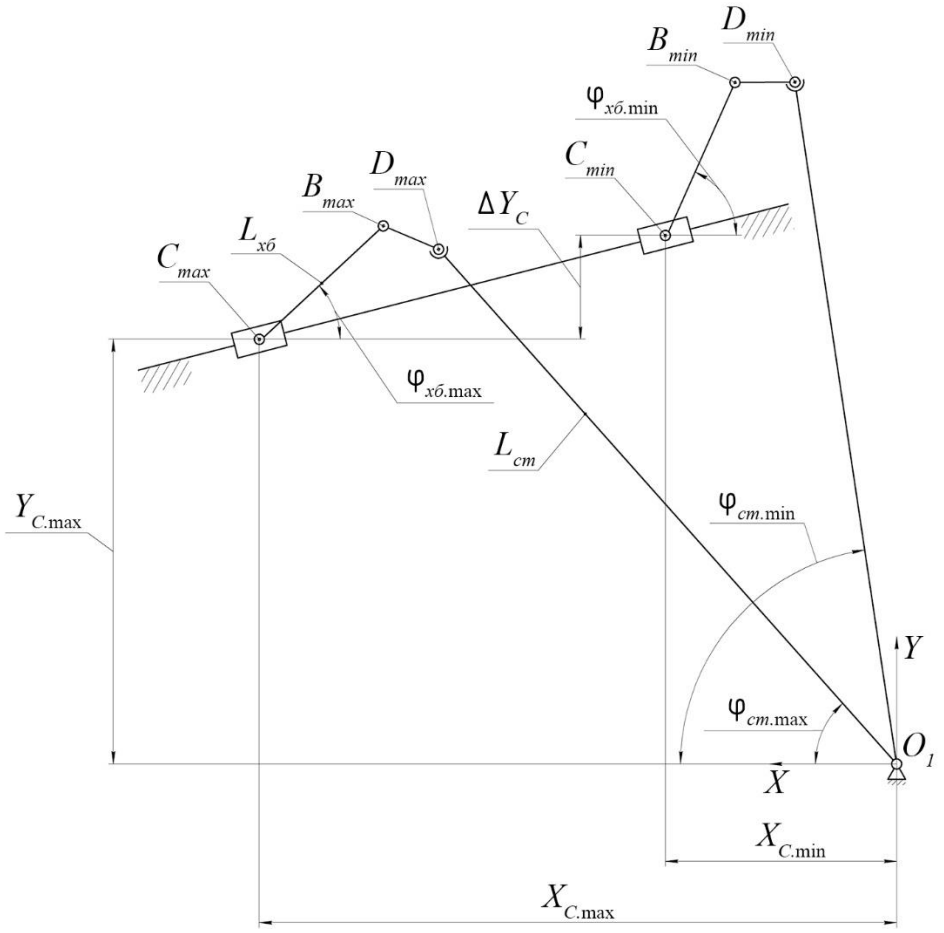


Рис. 1. Расчетная схема для определения размеров переднего плеча хобота и стрелы с учетом высоты «шарнира»

Перед тем, как составить векторное равенство, описывающее механизм, указанный на рис. 1, рассмотрим механизм в любом произвольном положении для получения дополнительных зависимостей.

По теореме косинусов найдем расстояние между точками *C* и *D:*

$$L_{CD} = \sqrt{h_ш^2 + L_{хб}^2 - 2h_ш^2 L_{хб}^2 8\cos\left(\frac{180^0 + \beta_n}{2}\right)}, \qquad (1)$$

где $h_ш$ – расстояние между точками *B* и *D*.

По теореме синусов найдем угол α_1 ($\angle BCD$):

$$\alpha_1 = \arcsin\left[\frac{h_ш \sin\frac{180^0 + \beta_n}{2}}{L_{CD}}\right]. \qquad (2)$$

Векторное равенство, описывающее механизм, показанный на рис.1, спроектированное на оси координат, с учетом зависимостей (1) и (2) дает четыре уравнения:

$$\begin{aligned}
X_{C.\max} &= L_{cm}\cos(\varphi_{cm.\max}) + L_{CD}\cos(\varphi_{хб.\max} - \alpha_1),\\
X_{C.\min} &= L_{cm}\cos(\varphi_{cm.\min}) + L_{CD}\cos(\varphi_{хб.\min} - \alpha_1),\\
Y_{C.\max} &= L_{cm}\sin(\varphi_{cm.\max}) - L_{CD}\sin(\varphi_{хб.\max} - \alpha_1),\\
Y_{C.\max} + \Delta Y_C &= L_{cm}\sin(\varphi_{cm.\max}) - L_{CD}\sin(\varphi_{хб.\max} - \alpha_1).
\end{aligned} \qquad (3)$$

Численное решение системы (3) было выполнено в пакете MathCAD блоком Given…Find.

При одних и тех же начальных параметрах доработанная математическая модель описывает реально существующий объект с меньшей ошибкой.

Список литературы

[1] Стрелов В.И. Расчет шарнирных стреловых систем портальных кранов (аналитический метод кинематического синтеза). – Калуга: Облиздат. – 1998, 188 с.

Раевский Владимир Алексеевич – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: var-77@mail.ru

С.Л. Заярный, Г.Ю. Грачев

ИСПОЛЬЗОВАНИЕ ЧИСЛЕННЫХ МЕТОДОВ В РЕШЕНИИ ЗАДАЧ РАСЧЕТА ИНЖЕНЕРНЫХ КОНСТРУКЦИЙ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В расчетах инженерных конструкций используются различные численные методы. Присущие этим методам особенности, предполагают и области инженерных расчетов для их применения. Однако даже в этих, традиционных, областях, разнообразие реальных инженерных конструкций и решаемых задач, зачастую, не позволяет рассчитывать на их эффективное решение. В связи с этим является актуальным, выявление возможности комплексного применения различных численных методов.

Большинство численных методов относят к классу сеточных методов. Понятие сетки является основным при построении большой группы приближенных методов решения задач математической физики и расчета инженерных конструкций. В таких методах непрерывное пространство распределения искомых величин представляется совокупностью их значений в узлах пространственной сетки. При этом математическую формулировку задачи сводят к системе уравнений, относительно искомой переменной [1].

Наиболее широко применяемый вариант метода сеток-метод конечных разностей (МКР). Согласно этого метода производные искомых функций, входящие в дифференциальные уравнения и краевые условия, аппроксимируются в каждом узле сетки конечными разностями. Получаемая при этом система алгебраических уравнений является предметом исследования. К недостаткам МКР относят необходимость предварительного получения аналитических формулировок поставленной задачи в виде дифференциальных уравнений [1].

Другим сеточным методом, является метод конечных элементов (МКЭ). Этот метод является достаточно эффективным и удобным вычислительным методом решения прикладных задач механики деформируемого твёрдого тела применительно к расчёту инженерных конструкций. Преимущество МКЭ проявляется в универсальности техники вычислений при использовании различных конечных элементов (КЭ) [2]. Конечно-элементные модели различных конструкций могут быть сведены к стержневым, пластинчатым, оболочечным или объёмным системам, находящимся под действием произвольных нагрузок. МКЭ позволяет рассчитывать сложные инженерные конструкции с единых позиций, т. е. в возможности образования плоских, а также пространственных расчётных моделей на основе стержневых и плоских КЭ, так как матричный аппарат метода носит стандартный характер для КЭ различной формы [3].

Однако МКЭ имеет границы эффективного применения. Так, существует широкий класс задач, решение которых содержит резкие неоднородности,

проявляющиеся на мелких пространственных масштабах не только по отношению к размеру области, но и по отношению к приемлемому шагу сетки. Такие неоднородности задачи иногда могут быть выделены явно, как, например, инородные включения в композитных материалах, стержни и оболочки в металлоконструкциях и т.п. Численное решение этих задач сеточными методами требует специальных сеток для разрешения особенностей. В то же время проявления этих особенностей зачастую являются локальными, сосредоточенными в мелкомасштабных подобластях. При решении таких задач может быть эффективным использование модификации МКЭ - метод конечных супер- элементов (МКСЭ). При этом расчетная область разбивается на некоторое количество подобластей-конечных супер-элементов (КСЭ) таким образом, чтобы особенности решения задачи были целиком сосредоточены внутри суперэлемента, а на их границах решение являлось достаточно гладкой функцией. Каждый КСЭ оснащается системой “базисных” функций, которые являются решениями рассматриваемого уравнения в КСЭ с некоторыми граничными данными. “Базисные” функции Φ_i являются решениями системы уравнений рассматриваемой модельной задач) внутри КСЭ, а на его границе совпадают с некоторыми функциями $\varphi_i = \left\{ \varphi_i^{(1)},\ \varphi_i^{(2)},\ \varphi_i^{(3)} \right\}$:

$$\begin{aligned} &\mathrm{A}\ \Phi_i(x) = 0 \quad \forall \mathrm{x} \in \Omega_k \,/\, \partial\Omega_k, \\ &\Phi_i(x)\big|_{\mathrm{x}\in\Omega_k} = \varphi_i(x)\big|_{\mathrm{x}\in\Omega_k} \end{aligned} \qquad (1)$$

Функции φ_i будем называть граничными базисными функциями.

Полученное таким образом приближенное решение внутри каждого КСЭ Ω_k заведомо удовлетворяет дифференциальному уравнению исходной задачи. На границах КСЭ рассмотренная схема МКСЭ позволит обеспечить непрерывность аппроксимации перемещений [2].

Расчет инженерных конструкций, превосходящих определенную степень сложности, требует других подходов. Для расчета целесообразно использовать метод супер – элементов (МСЭ). Расчетная схема в этом случае строится не сразу для всей конструкции, а в несколько этапов-уровней. При этом ее описание КЭ и конечными супер-элементами выполняется на нижних уровнях, а полная конструкция представляется в виде совокупности иерархически соподчиненных конструкций различных уровней [4].

Слабая сторона МКЭ, сужающая область его эффективного применения, состоит в необходимости выполнять дискретизацию всего тела. Это ведет к представлению ее чрезвычайно большим количеством элементов, особенно в трехмерных задачах с удаленными границами [2]. Для устранения этого недостатка при реализации МКЭ, наряду с МКСЭ и МСЭ, целесообразно использовать метод граничных элементов (МГЭ). При этом, в любой однородной области требуется дискретизировать только сопрягаемую поверхность, так что область становится одним большим сложным «элементом» [4]. Тогда переменные, описывающие решение, будут изменяться непрерывно в этой области и все аппроксимации будут иметь место

только на ее внешних границах. При этом однако требуется вывод граничных интегральных уравнений, что само по себе является сложно математической задачей. Но эта задача может быть реализована в алгоритмах решения интегральных уравнений для каждого конкретного случая. При этом МГЭ может быть реализован в различных вариантах. В прямом варианте МГЭ неизвестные функции, входящие в интегральное уравнение, имеют физический смысл. Например, функции напряжений в теории упругости. При этом решение интегрального уравнения должно сразу давать все усилия и смещения на границе. В полу-прямом варианте МГЭ возможно составление неизвестных функций по аналогии с функции напряжений в теории упругости. При этом дифференцирование полученного решения даст распределение внутренних напряжений. В непрямом варианте МГЭ интегральные уравнения полностью выражаются через фундаментальное сингулярное решение (например, функция Грина для неограниченной области) исходных дифференциальных уравнений распределенные с неизвестной плотностью по границам рассматриваемой области [4]. При этом использование прямого и непрямого методов является предпочтительным. Этими методами могут быть решены статические и динамические задачи теории упругости. Несмотря на некоторые математические трудности реализации, МГЭ обладает четко выраженными преимуществами по сравнению с МКЭ и МКСЭ для областей большого размера. Поэтому МГЭ может быть использован в сочетании с МКЭ и МКСЭ, преимущества которых проявляется в объектах конечного размера и в зонах быстрого изменения свойств.

Из приведенного анализа видно, что комплексное применение различных численных методов может в существенной мере повысить эффективность решение задач расчета инженерных конструкций.

Список литературы

[1] Бахвалов Н. С. Численные методы / Н. С. Бахвалов, Н. П. Житков, Г. М. Кобельков. - 3-е изд., доп. И перераб. - М.: БИНОМ. Лаборатория знаний, 2004, - 636 с., ил.

[2] Зенкевич О.С. Метод конечных элементов в технике - М.: Мир, 1975. – 543 с.

[3] Норри Д., де Фриз Ж. Введение в метод конечных элементов: Пер. с англ. - М.: Мнр, 1981. - 304 с. Ил.

[4] Постнов В.А. Метод супперэлементов в расчетах инженерных сооружений. / В.А. Постнов, С. А. Дмитриев, Б. К. Елтышев, А. А. Родионов. Под общей редакции В.А. Постнова. - Л.: Судостроение, 1979. - 2888 с., ил.

Заярный Сергей Леонидович – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: texnakon@yandex.ru

Грачев Георгий Юрьевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: goshangrachev@gmail.com

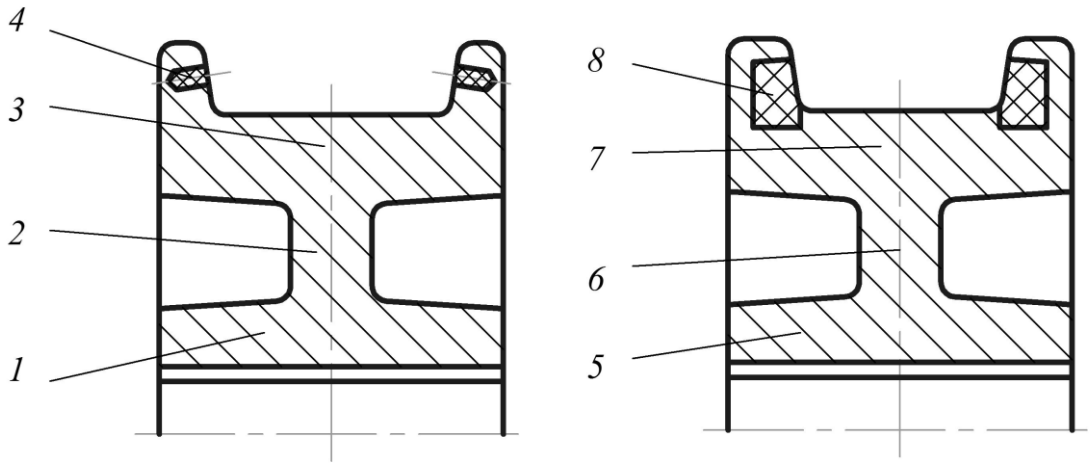
В.А. Ермоленко, А.А. Голиков

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ УМЕНЬШЕНИЯ ИЗНОСА РЕБОРД КРАНОВЫХ КОЛЁС

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

При перекосе мостовых кранов в процессе движения возникает силовое взаимодействие реборд ходовых колес с боковыми поверхностями головок рельсов, сопровождающееся их взаимным изнашиванием. Рассмотрим возможные методы, направления исследования и технические решения, способствующие уменьшению интенсивности изнашивания реборд крановых колёс и рельсов.

Известно применение смазки реборд. Для этого к рельсу прижимают карандаш с пастой, включающей в себя твёрдую смазку – дисульфид молибдена MoS_2 (рис.1а). Твёрдая смазка автоматически наносится на поверхность реборд и боковую грань рельса, образуя прочную пленку. Она уменьшает коэффициент трения скольжения, повышает несущую противозадирную способность трущихся поверхностей, а, следовательно, и срок их службы [1]. Твердая смазка может располагаться по всему диаметру реборды в проточке в виде ласточкина хвоста (рис.1б). В качестве наполнителя, удерживающего смазку, применяется эпоксидный отвердитель со стеклотканью или стеклянными нитями. Но твёрдая смазка частично попадает на поверхность качения и вызывает скольжение (буксование крановых колёс) при торможении.



а) б)

Рис.1. Ходовые колёса с твёрдой смазкой:
1,5–ступица; 2,6–диск; 3,7–обод; 4–карандаш с пастой; 8– эпоксидный отвердитель

Известно крановое колесо, которое состоит из ступицы 1, диска 2 и обода 3. Между ободом 3 и ребордами 4 расположен упругий элемент 5. Реборды 4 крепятся к ступице 3 болтами 6. Применение таких ходовых колёс позволяет снизить динамические нагрузки на ходовую часть крана за счёт наличия между ступицей колеса и ребордами упругих промежуточных элементов и уменьшить износ реборд [2].

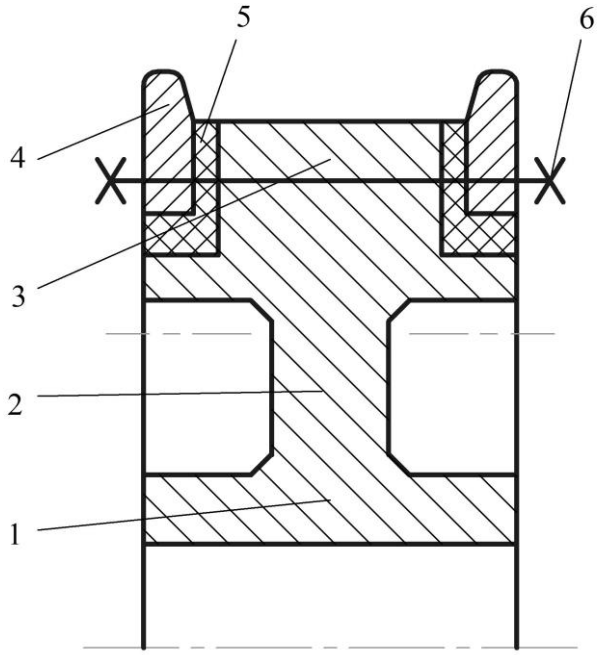


Рис. 2. Крановое колесо с упругими элементами

Известны крановые колёса со сменными ребордами, крепящимися к ступице колеса через упругие промежуточные элементы [3]. Крановое колесо (рис.3) содержит обод 1, съёмные реборды 2, упругие элементы 3, расположенные между ободом 1 и ребордами 2, и крепёжные элементы 4, установленные в отверстиях 5 обода 1 и отверстиях 6 реборд 2. Отверстия 5 в ободе 1 выполнены сквозными, а реборды 2 соединены между собой крепёжными элементами 4, концы которых установлены в отверстиях 6 реборд 2 с минимальным зазором, закреплены гайками 8 и шплинтами 9. Реборды 2 имеют на внутренней боковой поверхности кольцевые выступы 10,которые образуют с поверхностью обода 1 зазор 11, обеспечивающий подвижность реборд 2 и крепёжных элементов 4 относительно обода 1 . При воздействии колебаний вертикальной силы и горизонтальной боковой нагрузки происходит их гашение упругими элементами 3. Для уменьшения износа боковых поверхностей рельса и реборд предлагаются крановые колеса, у которых реборды вращаются независимо от кранового колеса [4].

Одна из реборд кранового колеса выполнена в виде диска, свободно вращающегося на подшипниках (рис.4). Колесо крана состоит из ската 1,

подшипника 2, установленного на ступице, и вращающейся реборды 3. Подшипник 2 закреплен фланцем 4 и болтами 5. Реборда 3 прижата гайкой 6, фиксируемой стопором 7. В данной конструкции уменьшается сила трения реборды о подкрановый рельс за счет отсутствия жесткой связи между ободом и ребордой. Однако, полностью избежать трения скольжения между ребордой и подкрановым рельсом не удаётся вследствие разных окружных скоростей точек контакта стенки реборды по ее диаметру и цилиндрической дорожки катания колеса. Кроме того, конструкция такого колеса сложна.

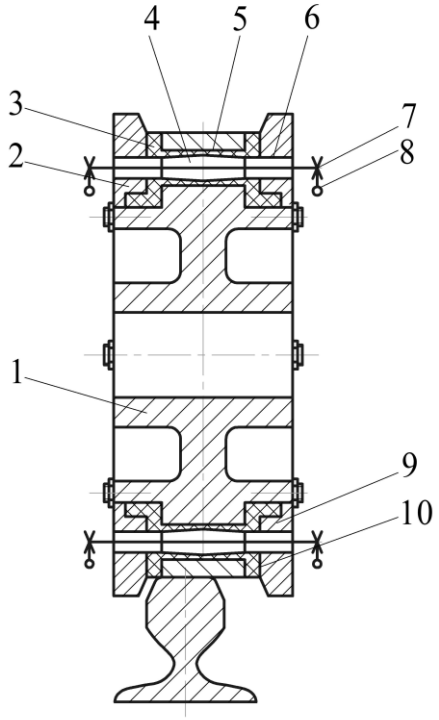


Рис. 3. Крановое колесо с промежуточными упругими элементами

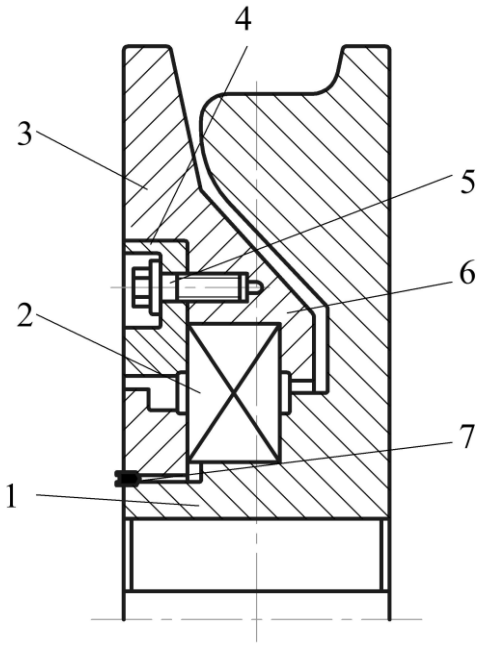


Рис. 4. Крановое колесо с вращающейся ребордой

Предлагается крановое колесо, снабженное сменными телами качения, равномерно распределенными по окружности реборды. Трение скольжения преобразуется в трение качения в паре реборда-рельс при возникновении контакта между ними (рис.5). Колесо 1 выполнено с ребордой 2, в которую вмонтированы тела качения 3,7 равномерно расположенные по окружности и выступающие частично над поверхностью качения стенки реборды со стороны головки подкранового рельса. Тела качения 3,7 помещают в гнездах 6, перпендикулярных продольной оси рельса. Для смазки шариков имеется групповое смазочное устройство 4 с пресс-масленкой 5. При движении крана контакт между ребордой и боковой гранью головки рельса осуществляется через тела качения. Такая конструкция кранового

колеса позволяет значительно уменьшить износ боковых поверхностей подкранового рельса и исключить износ реборды.

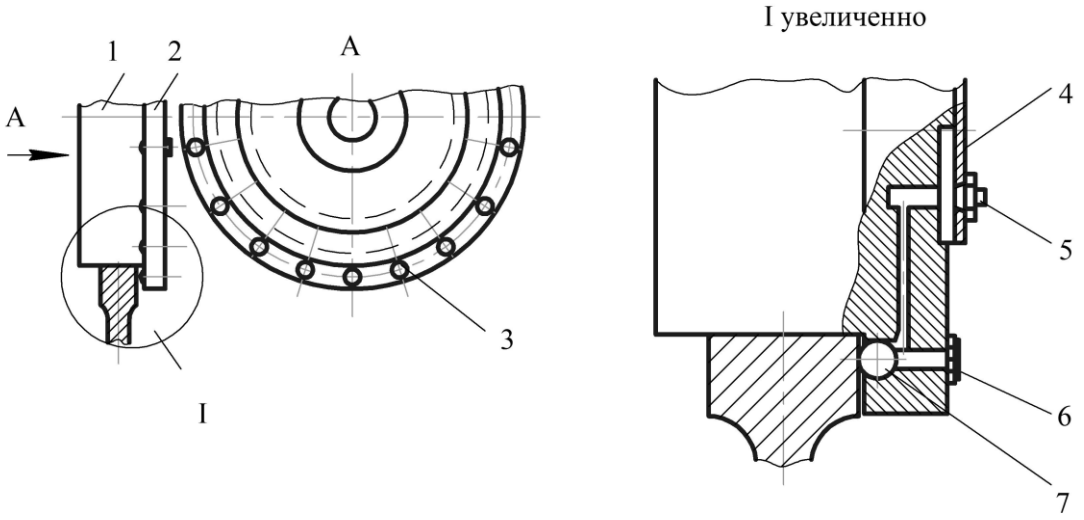


Рис. 5. Крановое колесо с шариками в реборде

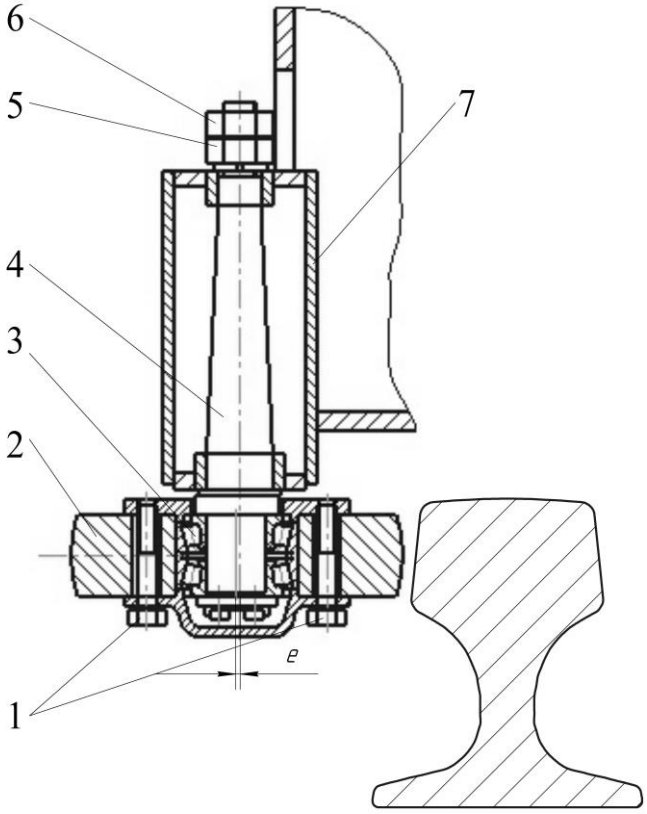


Рис. 6. Боковой направляющий ролик с эксцентриком:
1–болт; 2–ролик; 3–подшипник; 4–эксцентрик; 5–гайка;
6–контргайка; 7–рама

Предлагаются также боковые направляющие ролики с эксцентриками (рис.6). Тележка или кран имеют по обе стороны ходового колеса ролики со сферической поверхностью качения, примыкающие к боковым поверхностям рельсов с зазором 2…3 мм, который регулируется эксцентриком в процессе износа ролика. Реборды при этом не касаются рельса и не изнашиваются. Это техническое решение является наиболее эффективным.

Таким образом, применение в крановых колесах сменных частей (реборд) из более прочного материала увеличивает долговечность, но вместе с тем, приводит к усложнению конструкции кранового колеса. Оценивая меры, направленные на совершенствование ходовой части кранов можно признать целесообразными технические решения, направленные на уменьшение сил трения в зоне контакта реборд *с* рельсами. Использование этих технических решений с соответствующей конструктивной доработкой помогут существенно повысить долговечность ходовой части грузоподъёмных кранов за счет уменьшения сил трения в зоне контакта реборд о рельсы и уменьшения износа крановых колёс и рельсов.

Список литературы

[1] А.с. 604799 (СССР). Ходовое колесо с ребордами. /В.А. Ромащенко и др.–Заявл. 30.12.74, №2090368/29-11; Опубл. 30.04.78, Б.И. №16, Кл.^{2} В 66 С 9/08.

[2] А.с. 500168 (СССР). Ходовое колесо. / В.А. Серёгин и др.–Заявл. 13.02.74, №1997301/27-11; Опубл. 25.01.76, Б.И. №3, Кл.В 66 С 9/08

[3] Шабашов А.П., Лысяков А.Г. Мостовые краны общего назначения. –М.: Машиностроение, 1980. –304 с.

[4] А.с. 819045 (СССР). Ходовое колесо с ребордами. /Л.А. Фавстов и др.–Заявл. 10.01.79, №2712417/29-11; Опубл. 07.04.81, Б.И. №13, Кл.^{3} В 66 С 9/08

Ермоленко Владимир Алексеевич – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: tvermolenko@rambler.ru

Голиков Антон Аркадьевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: toxa2017a@yandex.ru

Д.В. Татару, Д.Г. Мокин

МОДЕЛИРОВАНИЕ ДВИЖЕНИЯ ХОДОВОГО КОЛЕСА

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Для суждения о возможности и целесообразности применения в заданных условиях эксплуатации того или иного типа колеса для существующего или проектируемого механизма необходимо установить параметры, пользуясь которыми можно объективно оценивать эксплуатационные качества, определять соответствие его функциональному назначению и предъявляемым требованиям. Остановимся лишь на основных, наиболее важных параметрах, используемых при оценке эксплуатационно-технических качеств ПТМ. К ним относятся:

- его надежность;
- тяговые (динамические) качества;
- экономические качества и др.;

Существует несколько видов взаимодействия колеса с опорной поверхностью

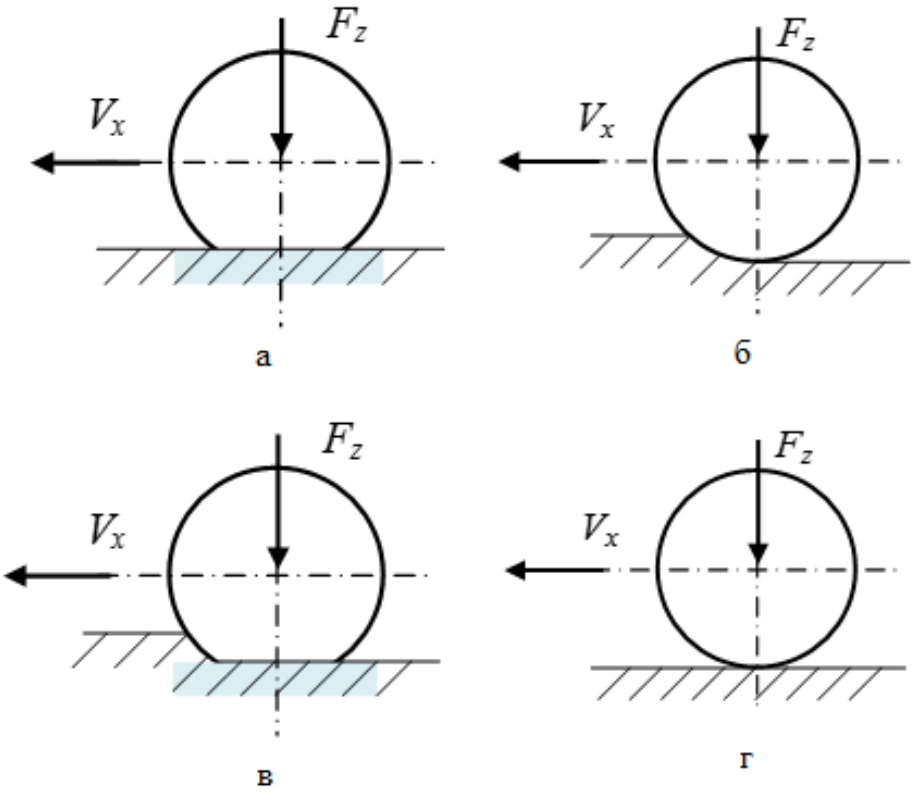


Рис.1 Воздействие колеса с опорной поверхностью
а) Эластичное колесо по недеформируемой поверхности
б) Жесткое колесо по деформируемой поверхности
в) Эластичное колесо по деформируемой поверхности
г) Жесткое колесо по недеформируемой поверхности

1.Движение колеса, деформируемого под действием нормальной реакции, по твердой опорной поверхности. Например, движение пневмоколесного транспорта по асфальтобетонному покрытию.

2.Движение жесткого колеса по деформируемой поверхности, когда нормальная деформация колеса мала в сравнении с деформацией опорной поверхности. Например, движение транспорта с жесткими шинами по снежной целине, песчаным и другим рыхлым грунтам.

3. Движение эластичного колеса по деформируемой поверхности, когда деформации колеса и опорной поверхности соизмеримы. Движение пневмоколесного транспора с малым давлением воздуха в шинах по снегу, песку и т.д.

4.Движение жесткого колеса по недеформируемой поверхности. Например, качение стального колеса крана или тележки по рельсовому пути.

В соответствии с написанным было принято решение рассмотреть движение жесткого колеса по недеформируемой поверхности и разработать программу, подбирающую оптимальные параметры для нужного механизма передвижения.

При вращении колеса возможно несколько видов перемещения, зависящих от кинематического радиуса

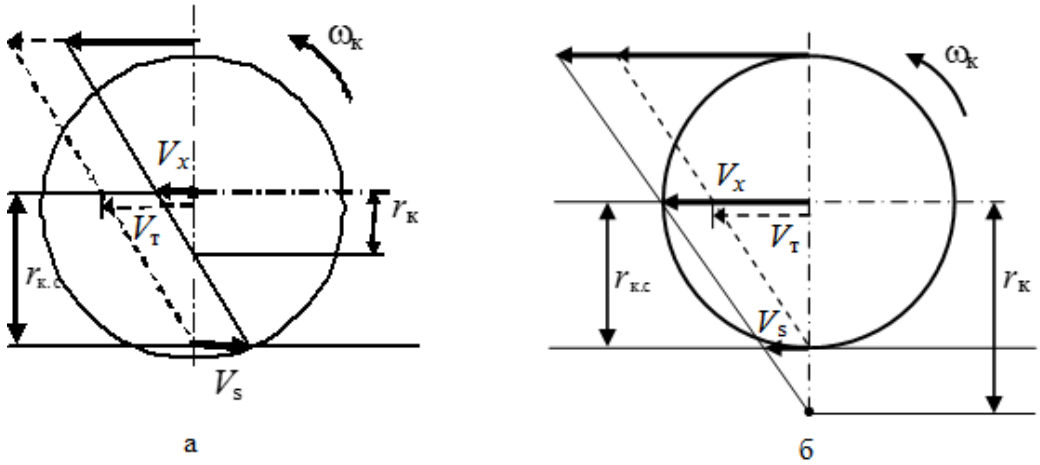
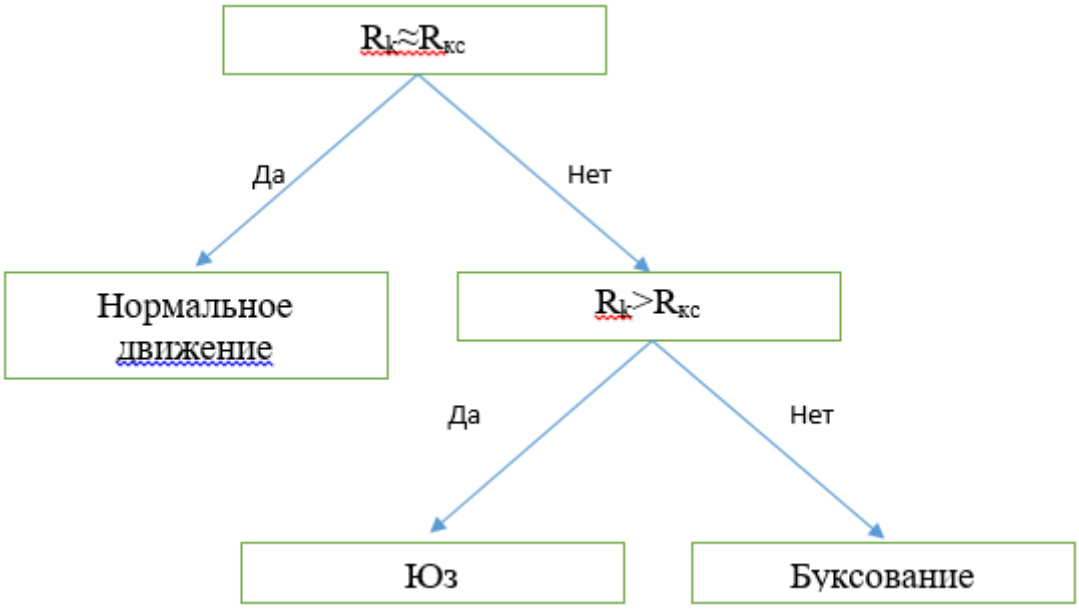


Рис. 2 Виды перемещения колеса
а) Буксование колеса
б) Юз тормозящего колеса

Программа производит расчет при введении входных данных (крутящий момент, диаметр ходового колеса, масса и др.) образуя тип движения колеса, что занимает очень мало времени, так как происходит практически в реальном времени. По выходным параметрам можно увидеть вид движения колеса и, основываясь на это, подбирать нужные значения. Принцип работы программы показан в следующей схеме.

Схема работы программы



R_k – кинематический радиус
$R_{кс}$ – радиус колеса

Список литературы

[1]. *Хусаинов А.Ш. Селифонов В.В.* Теория автомобиля. – Ульяновск: УлГТУ, 2008. – 121 с.

Татару Драгош Вячеславович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: tatarudorel@mail.ru

Мокин Дмитрий Геннадьевич – канд. техн. наук, доцент кафедры "Детали машин и подъемно-транспортное оборудование" КФ МГТУ им. Н.Э. Баумана. E-mail: tvermolenko@rambler.ru

В.А. Раевский, В.Ю. Горичев

МОСТОВОЙ КРАН-ШТАБЕЛЕР С ТЕЛЕСКОПИЧЕСКОЙ КОЛОННОЙ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В современных экономических условиях в последние годы произошло резкое сокращение объема промышленного производства: по данным Росстата в 2015 году сокращение годовом исчислении составило 4,5%. При этом эмбарго на ввоз в Россию ряда продовольственных товаров привело к значительному росту выпуска пищевых продуктов [1].

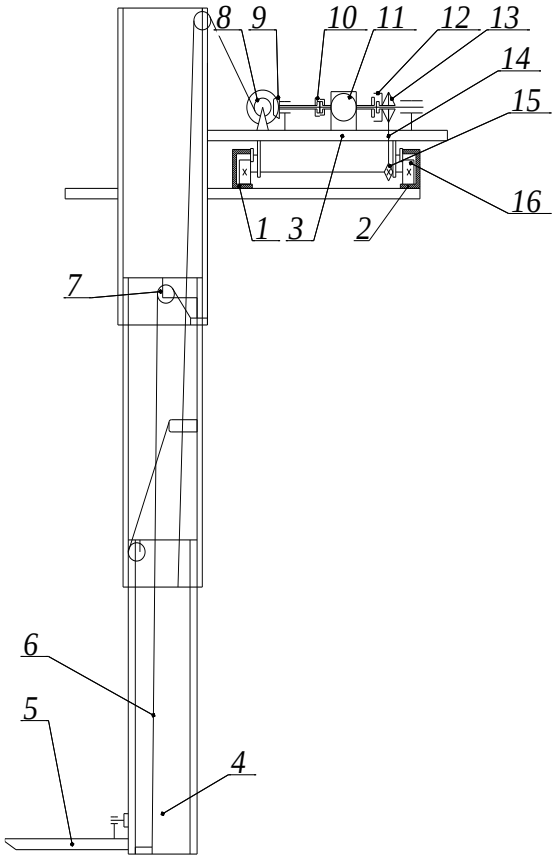
При этом усиливается тенденция к заключению сделок built-to-suit между девелоперами складской недвижимости и крупными торговыми компаниями [2], а также покупка и модернизация выбывающих цеховых помещений и их оборудования под складские нужды [3].

В таких помещениях продавец обычно оставляет мостовые краны, которые могут быть перепроектированы и после доработки конструкции использоваться как краны-штабелеры, если будущий склад предназначен для упакованных или палетированных грузов.

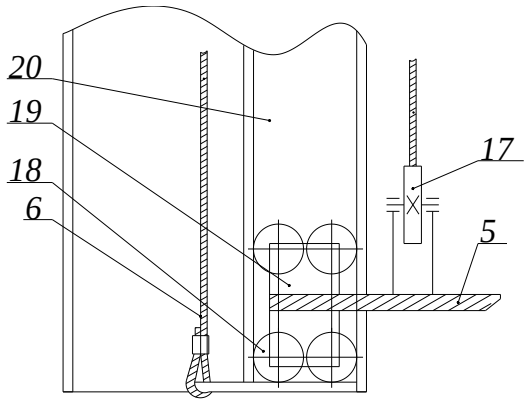
Также для вновь проектируемых помещений по сделкам built-to-suit девелоперы активно предлагают в качестве встроенного грузоподъемного оборудования использовать мостовые краны-штабелеры, так как они обладают следующими преимуществами по сравнению с напольными электроштабелерами [4]:

- наибольшее использование рабочей площади склада за счет уменьшения ширины проезда;
- отсутствие специальных требований к полам;
- верхние стеллажи могут быть опорами для подкрановых путей;
- простота управления краном и низкая стоимость обслуживания и эксплуатации;
- возможность авторизации учета грузов и автоматизации процесса складирования;
- меньшая стоимость крана-штабелера по сравнению с напольным электроштабелером.

Предлагается в перепроектированных мостовых кранах-штабелерах для обеспечения жесткой связи между грузоподъемником и поворотной платформой, а также управления вертикальным положением грузоподъемника использовать телескопические колонны (рис. 1, а).



а) Телескопическая колонна с грузовой платформой



б) Продольное сечение внутреннего выдвижного звена телескопической колонны с грузовой платформой

Рис.1. Мостовой кранах-штабелер с телескопической колонной

Перемещение секций телескопической колонны 4 и подъемно-опускной грузовой платформы 5 осуществляется стальными канатами 6 через блоки 7, барабан 8, коническую зубчатую передачу 9, взаимодействующую со сцепляемой управляемой двухсторонней электрической муфтой 10, и привод включающий редуктор 11 с двумя выходными валами и реверсивный электродвигатель с дистанционным управлением. Причем электродвигатель с дистанционным управлением имеет возможность через сцепляемую управляемую двухстороннюю электрическую муфту 12, взаимодействующую со звездочкой 13, посредством цепи 14 и звездочки 15, неподвижно закрепленной на оси приводных колес 16 ходовой тележки, перемещать последнюю по горизонтальным направляющим 1,2 с возможными остановками в заданных точках.

Предлагаемая компоновка привода крана-штабелера дает возможность посредством соответствующего включения двух двухсторонних электрических муфт 10 и 12, сочетать как одновременное поднятие (опускание) грузовой платформы 5 вместе с телескопической колонной 4 и перемещением ходовой тележки 3 по горизонтальным направляющим 1 и 2,

так и возможность совершать указанные перемещения поочередно, каждое в отдельности.

Для обеспечения нормального положения подъемно-опускной грузовой платформы 5 в случае неравномерной вытяжки ветвей каната 6, на платформе 5 закреплены два уравнительных блока 17 (Рис.1, б).

Для сохранения геометрического положения грузовой платформы 5 относительно телескопической стрелы 4, в концевой выдвижной секции последней смонтированы опорно-направляющие желоба 20, в которых посредством регулируемых прижимных опорно-направляющих роликов 18 перемещается каретка 19, жестко связанная с грузовой платформой 5. В центре телескопической колонны 4 на средней ее секции, смонтирована штанга, служащая для заделки свободных концов каната 6 подъемно-опускной грузовой платформы 5 (Рис.1, б).

Такая конструкция колонны позволит производить погрузку и разгрузку напольных транспортных средств, автомобилей, обслуживать склады с разными отметками пола по высоте (склады с рампами); переносить грузы над препятствиями – оборудованием, перегородками.

Список литературы

[1] Официальный сайт РБК: http://www.rbc.ru/economics/25/01/2016/56a5da3e9a7947628cf80a83 (дата обращения 8.10.16)

[2] Официальный сайт корпорации Стерх: http://sterh-corp.ru/news/skladskie-potrebnosti.php (дата обращения 9.10.16)

[3] Официальный сайт Трейд40: http: //трейд40.рф/page/Proiz_skld_pom.html (дата обращения 10.10.16)

[4] Степыгин В.И., Чертов Е.Д., Елфимов С.А. Проектирование подъемно-транспортных установок.Учебное пособие. – М.: Машиностроение, 2005. – 288 с.; ил. https://e.lanbook.com/reader/book/761/ (дата обращения 11.10.16)

[5] Зерцалов, Андрей Иванович. Краны с жестким подвесом груза [Текст]. - Москва: Машиностроение, 1979. - 191 с.; ил. (дата обращения 11.10.16)

Раевский Владимир Алексеевич – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: var-77@mail.ru

Горичев Василий Юрьевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: vasily.gorichev@yandex.ru

С.Л. Заярный, А.А. Логвинов

ОПРЕДЕЛЕНИЕ НАДЕЖНОСТИ РАСТЯНУТОГО КОМПОЗИТНОГО СТЕРЖНЯ МЕТОДОМ СТАТИСТИЧЕСКОГО МОДЕЛИРОВАНИЯ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Рассмотрены модели определения надежности растянутого композитного стержня из условия прочности слабого звена и живучести. Представлен алгоритм определения условий отказа методом статистического моделирования при различных законах распределения прочности армирующего волокна.

Перспективным направление исследования металлоконструкций является рассмотрение возможности применения в них конструктивных элементов, изготовленных из композитных материалов. Для реализации такой возможности идеальными элементами являются стержни ферм. Наилучшим образом преимущества стержня, изготовленного из композитного материала, проявляются при его растяжении.

Определение распределения нагрузки между нитями композитного стержня в общем случае представляет собой статически неопределимую задачу. Раскрытие статической неопределимости, возможно только путем составления уравнений, дополняющих число уравнений статики до числа неизвестных. Эти дополнительные уравнения отражают особенности геометрических связей, наложенных на деформируемую систему (уравнения перемещений). Расчетная схема композитного стержня представлена на рис. 1. [3]

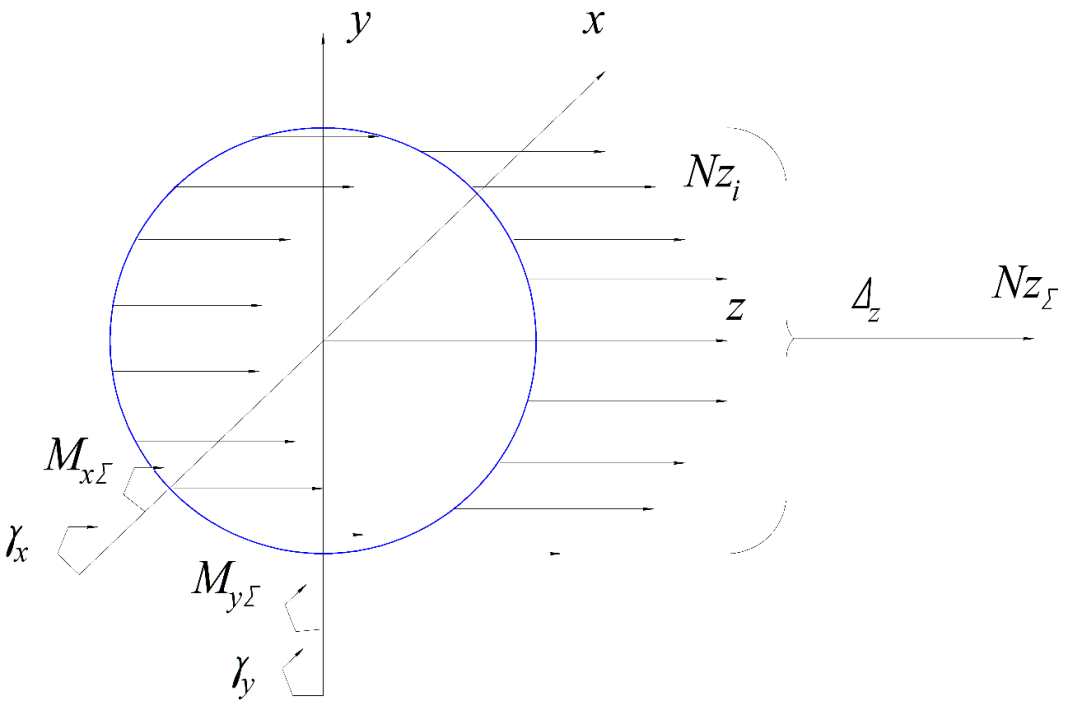


Рис. 1. Расчетная схема растянутого композитного стержня

Уравнения перемещений должны отражать тот факт, плоскость x-y должна быть общей для всех элементов системы. В этом случае, концы нитей после нагружений остаются в плоскость x-y.

Условия равновесия отсеченной части стержня определяется как:

$$\sum N_i = N_{z\sum};\ M_{x\sum} = 0;\ M_{y\sum} = 0, \qquad (1)$$

где $\sum N_z = \sum_{i=1}^{n} N_i;\ \sum M_x = \sum_{i=1}^{n} N_i y_i;\ \sum M_y = \sum_{i=1}^{n} N_i x_i$.

Усилие в i-нити композитного стержня определяется соотношением $N_i = E_i A_i \varepsilon_i$, где E_i, A_i, ε_i- модуль упругости, площадь сечения и относительная деформация нити.

Механические характеристики нитей, в составе композитного стержня, определяются как их собственными характеристиками, так и условия их упаковки в матрицу. Поэтому усилие в i нити композитного стержня определим соотношением $N_i = E_i^* \varepsilon_i$, E_i^*- обобщенный модуль упругости нити композитного стержня. Относительные деформации нитей в общем случае деформирования композитного стержня из геометрических соображений определяются как

$$\varepsilon_i = \left(\Delta_0 + \gamma_x y_i + \gamma_y x_i\right) \Big/ l_0, \qquad (2)$$

где $\Delta_0 \gamma_x \gamma_y$-осевые и угловые деформации композитного стержня; l_0- длина стержня композитного стержня.

Таким образом, при заданных $N_{z\sum}$, E_i^* и параметрах l_0, x_i, y_i, система уравнений (1) имеет решение относительно параметров $\Delta_0 \gamma_x \gamma_y$.

При этом условием локальной прочности композитного стержня, согласно модели слабого звена, является условие $N_i \le [N]$.

Рассмотрим две модели отказа композитного стержня: 1- модель слабого звена; 2- модель потери несущей способности (разрушение).

Впервой модели варьируемы факторами являются параметры армирующей нити: приведенный модуль упругости при растяжении; предел прочности материала; площадь поперечного сечения. Указанные факторы является случайными величинами, а их изменения в установленных пределах подчиняются выбранным законам распределения.

Растягивающее усилие является детерминированной величиной и изменятся дискретно по i уровням

$$N_i = \frac{1}{k_i} \sum_{j=1}^{n} \sigma_{ekj} A_j,$$

где σ_{ekj}, A_j- предел прочности материала и площадь поперечного сечения j-й армирующей нити; k_i-коэффициент запаса по нагрузке i-го уровня.

На каждом расчетном цикле проверяется условие $\sigma_j \ge \sigma_{ekj}$. Справедливость (несправедливость) этого соотношения устанавливает факт воз-

никновения (не возникновения) отказа по условию прочности композитного стержня согласно модели слабого звена.

По результатам статистического моделирования строятся гистограммы и определяется вероятность отказа композитного стержня для различных уровней детерминированной нагрузки. [1]

Во второй модели, варьируемы факторами, так же как и в первой модели, являются параметры армирующей нити. Однако при этом растягивающее усилие $N_{\alpha i}$ является случайной величиной с математическим ожиданием α -го уровня $\bar{N}_{\alpha}$. На каждом расчетном цикле i проверяется условие $\sigma_j \geq \sigma_{ekj}$. Справедливость (несправедливость) этого соотношения устанавливает факт разрушения (не разрушения) j-ой армирующей нити. В случае если на расчетном цикле i установлено, что $\sigma_{j=m} \geq \sigma_{ekj=m}$, то на цикле $i+1$ расчет композитного стержня повторяется без изменения варьируемых параметров при условии $A_m = 0$.

При этом если на расчетном цикле $i+1$ установлено $\sigma_{j=l} \geq \sigma_{ekj=l}$, то расчет на цикле $i+2$ повторяется как и для цикла i. если на расчетном цикле $i+1$ установлено $\sigma_{j=l} \leq \sigma_{ekj=l}$, то расчет на цикле $i+2$ повторяется с изменением варьируемых параметров при условии $A_m = 0$.

Отказа по условию прочности композитного стержня согласно модели потери несущей способности (разрушение) композитного стержня определяется условием $\sigma_{j\in 1\ldots n} \geq \sigma_{ekj\in 1\ldots n}$.

По результатам статистического моделирования строятся гистограммы и определяется вероятность отказа композитного стержня для различных уровней α случайной нагрузки для $\bar{N}_{\alpha}$. [2]

Выводы. Предложенные способы статистического моделирования позволяют оценить надежности композитного стержня для различных моделей отказа.

Список литературы

[1] Композитные материалы: В 8-ми т. Пер. с англ./ Т. 7. Анализ и проектирование конструкций. Ч.1/ Под ред. К. Чамиса. -М.: Машиностроение. 1978.-300 с.: ил..

[2] Композитные материалы: В 8-ми т. Пер. с англ./ Т. 8. Анализ и проектирование конструкций. Ч.2/ Под ред. К. Чамиса. -М.: Машиностроение. 1978.-264 с.: ил.

[3] Строительная механика: В 2 кн. Кн 1. Статика упругих систем: Учеб. для вузов/В.Д. Потапов, А. В. Александров, С. Б. Косицын, Д. Б. Долотказин; Под ред. В. Д. Потапова. - М.: Высш. шк. 2007.-511 с.: ил..

Заярный Сергей Леонидович – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: texnakon@yandex.ru

Логвинов Александр Андреевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: paradoksme@yandex.ru

М.А. Качан, А.А. Шубин

ОПТИМИЗАЦИЯ ПРОЦЕССА ВОССТАНОВЛЕНИЯ ПРОФИЛЯ ПОВЕРХНОСТИ КАТАНИЯ КОЛЁС КРАНОВ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

В процессе эксплуатации подъемных кранов происходит износ и повреждения их ходовых частей и, в частности, профиля поверхности катания колес. Появление у колес предельного износа или других дефектов вызывает необходимость их периодической обточки по профилю катания. Проблема повышения эффективности технологического процесса механической обработки по профилю катания ходовых колес подъемных кранов при их изготовлении и ремонте является составной частью общей проблемы повышения надежности ПТМ.

Взаимодействие пути и механизма передвижения крана осуществляется через верхние слои металла колеса и рельса. В зоне пятна контакта колеса с рельсом возникает большое удельное давление. Такие нагрузки, которым подвергается каждый участок поверхности катания колеса с большой частотой циклов, вызывают износ, пластические деформации и различные виды контактно-усталостных повреждений. В целом, неисправности и дефекты крановых колес во многом схожи с дефектами железнодорожных колёсных пар, для фиксации которых разработан классификатор ИТМ1-В[1] Диагностирование осуществляется визуально, а также путём контрольных измерений. При эксплуатации допускаемый износ поверхности катания, визуально проявляющийся в виде шелушения, составляет не более 15-20% толщины обода [2] Любое повреждение поверхности катания отрицательно влияет на режимы резания при восстановлении его профиля.

Технологический процесс обточки крановых колес с целью восстановления профиля поверхности катания имеет ряд особенностей, обусловленных переменной величиной снимаемого припуска, изменением физико-механических свойств вдоль обрабатываемой поверхности и сложностью конфигурации профиля колеса, которые затрудняют проведение исследований по его совершенствованию. При обточке по профилю катания изношенных колес величина припуска колеблется в широких пределах.

Основной критерий обрабатываемости материалов – скорость резания, допускаемая режущим инструментом при определенной стойкости и других постоянных параметрах. В настоящее время для определения обрабатываемости используются различные методы, которые либо продолжительны во времени, либо недостаточно точны, что ограничивает их использование. После проведения ряд экспериментальных исследований, было установлено, что существует взаимосвязь между скоростью резания и остаточными напряжениями на обработанной поверхности, причем максимум остаточных сжимающих напряжений соответствует оптимальной скорости резания (Рис. 1), что позволило разработать способ определения оптимальной скорости резания для колесных сталей.

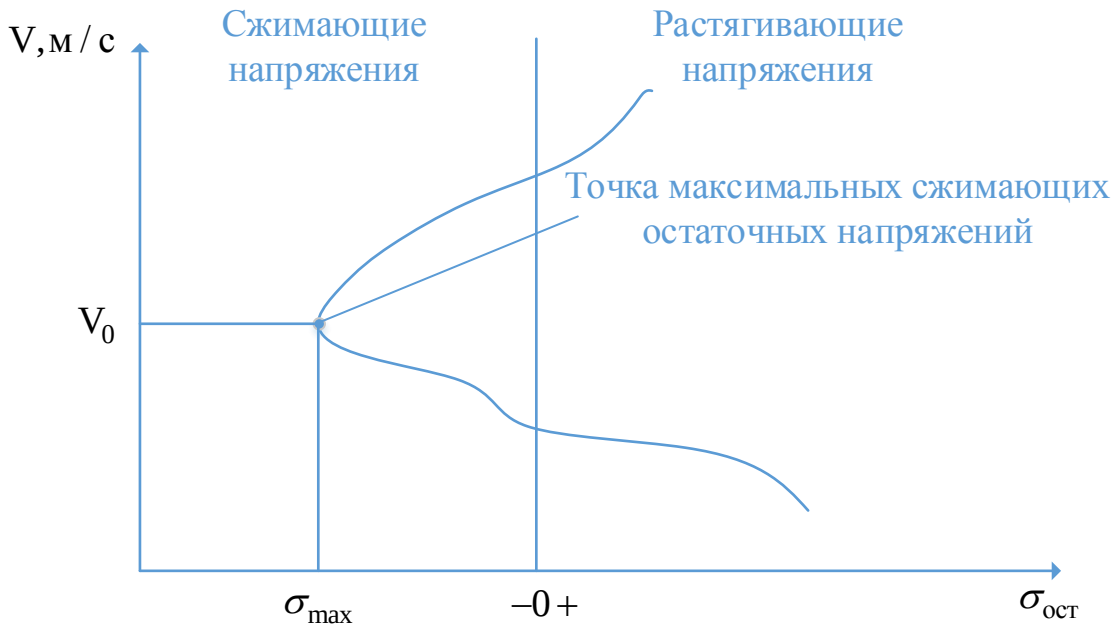


Рис. 1 Определение оптимальной скорости резания по остаточным напряжениям

Суть способа состоит в том, что при торцевом точении диска из колесной стали с постоянной угловой скоростью и подачей резца в радиальном направлении определяется скорость резания, соответствующая максимальной величине остаточных сжимающих напряжений. Эта скорость соответствует оптимальной скорости резания. Исследования проводились на экспериментальной установке (Рис. 2), в которой, помимо прочего, была предусмотрена возможность снятия показаний температуры в зоне резания с помощью естественной хромель-алюмелевой термопары.

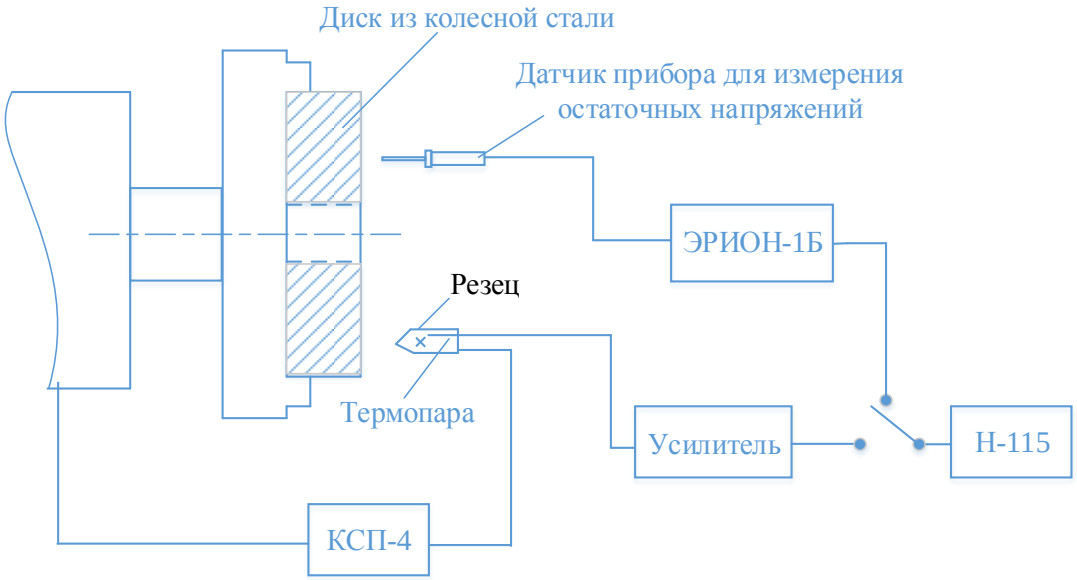


Рис. 2 Схема экспериментальной установки для определения оптимальной скорости резания

Оптимизация процесса резания для повышения стойкости инструмента представляет собой использование режимов, при которых износ инструмента был бы минимален. Для определения тепловой и силовой нагрузок на инструмент при восстановлении профиля поверхности катания, а также для выбора параметра, наиболее полно отражающего динамику процесса резания, была проведена серия производственных экспериментов. В результате были выявлены наиболее сложные участки с точки зрения тепловой и силовой нагрузок на инструмент. Для обеспечения нормального протекания техпроцесса была предпринята попытка регулирования процесса с целью поддержания в зоне резания определенной температуры. Результаты испытаний показали возможность регулировки температуры за счет изменения режимов резания.

Дальнейший анализ показал, что оптимальная температура резания может быть использована в качестве критерия оптимизации, что наметило значительный прогресс в области определения обрабатываемости и выбора режимов резания. В результате для каждой пары «обрабатываемый материал - инструментальный материал» стали применяться уже два соответствующих критерия – Оптимальная скорость резания и оптимальная температура резания. [3] Помимо этого, осуществление контроля в зоне резания может быть автоматизировано. Это позволит создать перспективные системы автоматического управления с обратной связью, регулирующие режимы резания для поддержания постоянной температуры, что обеспечит максимальную долговечность режущего инструмента.

Вопрос экспериментального определения оптимальных температур резания в настоящее время разработан недостаточно и определяется либо по результатам стойкостных испытаний, либо по значению оптимальной скорости резания. Однако, для получения температуры должен производиться трудоемкий процесс тарировки термопары, что отрицательно сказывается на точности результатов.

Для экспериментального определения оптимальной температуры резания при обработке колесных сталей был разработан принципиально новый способ, заключающийся в снятии показаний температуры с помощью срезных термопар при торцевом точении диска из колесной стали. Для реализации данного способа была сконструирована экспериментальная установка (Рис. 3), которая производила запись термо-ЭДС срезных термопар, а также значение термо-ЭДС естественной термопары.

Принципиальное отличие срезной термопары от естественной заключается в отсутствии рабочего спая, как такового. Рабочие элементы изначально изолированы друг от друга и от диска лаком, и замыкаются между собой непосредственно резцом при точении

Принцип работы установки заключался в следующем: В диске из колесной стали по радиусу устанавливались хромель-алюмелевые срезные термопары, которые через токосъемник выводятся к регистрирующей аппаратуре. Диск крепится в патроне станка и производится обточка его торцевой поверхности режущим инструментом.

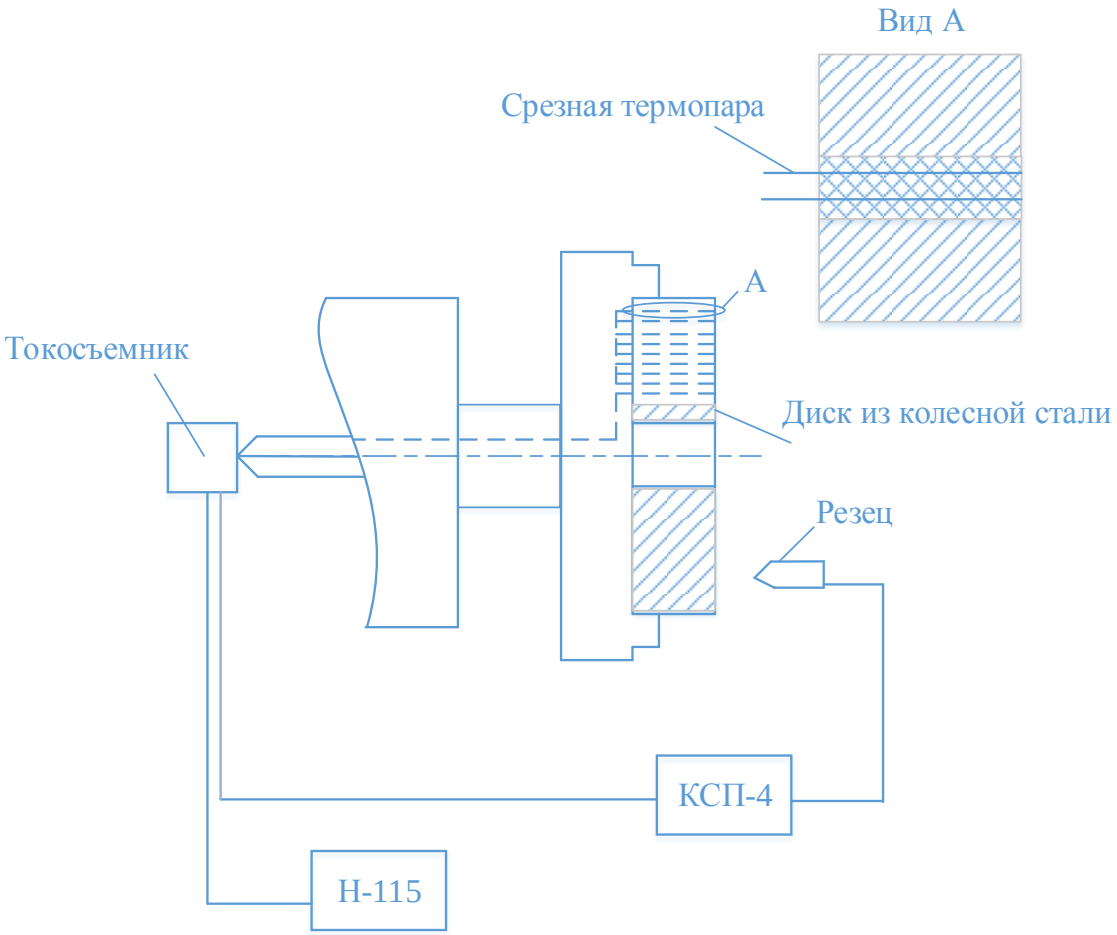


Рис. 3 Схема установки для определения оптимальной температуры резания

Результаты исследований могут быть использованы для упрощения процесса и повышения точности определения оптимальной температуры резания при разработке методики расчета и оптимизации параметров процесса обточки крановых колес, а также при создании систем автоматизированного регулирования процесса восстановления профиля поверхности катания колеса.

Список литературы

[1] *Богданов А.Ф., Чурсин В.Г.* Эксплуатация и ремонт колесных пар – железнодорожный транспорт, №1, 1979, с. 52-54

[2] *Сероштан В.И., Огаря Ю.С.* Диагностика грузоподъемных машин. – М.: Машиностроение, 1992, с. 87-89

[3] *Резников А.Н.* Теплофизика процессов механической обработки металлов. – М.: Машиностроение, 1981, 279с.

Качан Максим Аркадьевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: red-blade@yandex.ru

Шубин Александр Анатольевич – канд. техн. наук, заведующий кафедрой "Детали машин и подъемно-транспортное оборудование" КФ МГТУ им. Н.Э. Баумана. E-mail: shubin55@mail.ru

С.Л. Заярный, И.О. Лесовский

ПОСТРОЕНИЕ РАСЧЕТНОЙ МОДЕЛИ ВИБРАЦИОННОГО МЕХАНИЗМА С ТРУБЧАТОЙ ПРУЖИНОЙ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Процесс уплотнения балласта, в пределах рельсошпальной решётки железнодорожного пути, является сложным многофакторным процессом взаимодействия вибрационных рабочими органами (ВРО) путевой машины и балласта [1]. На практике наибольшее распространение получили ВРО в которых вибрационное воздействия реализуется совместно с поступательным движением уплотнительной поверхности рабочего органа.

Модели процесса вибрационного уплотнения позволяют решать практические задачи создания и модернизации рабочих органов путевых машин. Кинематический и силовой анализ взаимодействия поступательно движущейся вибрирующей лопатки подбойки и подверженного ее воздействию балласта позволяет найти решение многих задач проектирования рабочего органа.

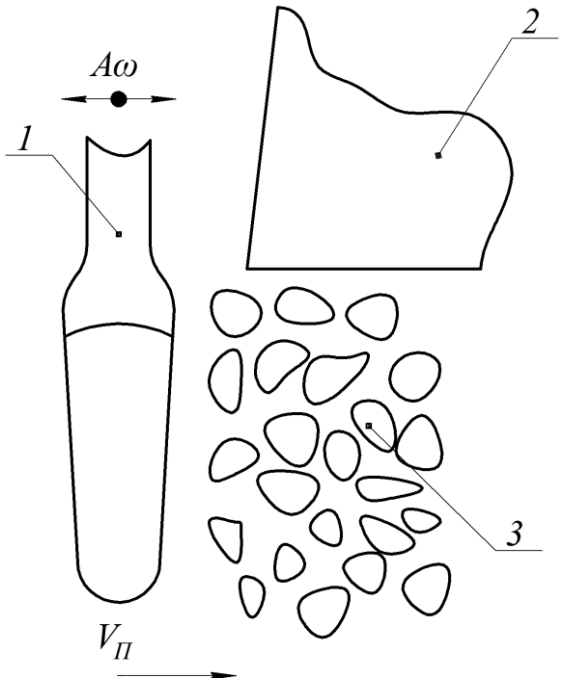


Рис. 1 Вибрационное и поступательное движение лопатки подбойки:
1 – подбойка; 2 – шпала; 3 – уплотняемый объем балласта

Для оценки характера взаимодействия лопатки с балластом используется параметр C режима, значение которого с учетом упругой отдачи балласта определяется по формуле

$$C = \frac{V_П + V_б}{A\omega} .$$

В числителе этого выражения приводится скорость взаимного сближения лопатки и балласта, а в знаменателе – амплитудное значение скорости вибрирования. Как показывает опыт эксплуатации уплотнительных рабочих органов машин, эффективное уплотнение происходит при взаимодействии лопатки и балласта с отрывом и ударами, что соответствует $C<1$. При безотрывном режиме взаимодействия лопатки и балласта эффективность уплотнения резко падает, так как контакты частиц друг с другом малоподвижны, частицы оказываются взаимно заклиненными. При отрывном режиме взаимодействия контакты частиц становятся подвижными, имеют возможность перестроиться, образуя более плотную текстуру.

Экспериментально установлено, что результат уплотнения несвязного материала (щебня), выраженный через относительную осадку E_y является случайной гиперболической функцией от общего количества относительных перемещений частиц материала, происходящих под действием внешних силовых импульсов с учетом сил инерции и внутреннего трения (активные перемещения), а также сил упругости и веса, вызывающих отдачу щебня при циклических разгрузках (пассивные перемещения), и выражается формулой

$$E_y = \frac{\chi\lambda(\omega t_B)_{\min}}{A + B(\omega t_B)_{\min}},$$

где $\chi = 0-2$ – коэффициент, определяющий степень использования для уплотнения пассивных и активных относительных перемещений частиц; $\lambda = 0-1$ – коэффициент, определяющий долю объема материала, охваченного относительными перемещениями; $(\omega t_B)_{\min}$ – минимально необходимое количество вибрационного воздействия для рабочих органов циклического действия, умноженное на 2π; (t_B – время воздействия на балласт, с; A, B – эмпирические коэффициенты, зависящие от рода уплотняемого материала и способов вибрационного воздействия.

По прежнему актуальной является задач создания эффективного вибрационного механизма (ВМ), который может быть реализован в качестве ВРО путевой машины. При этом представляется перспективным реализация в них механических эффектов, позволяющих существенно снизить энергопотребления ВРО в сочетании с высокой эффективностью. Особого внимания заслуживает ВМ, в котором может быть реализовано явление резонанса [2]. Функциональная схема одного из вариантов такого ВМ представлена на рис. 2. Структура такой ВМ представляет собой двухмассовую колебательную систему, упругий элемент которой выполнен в виде трубчатой пружины [3]. Функциональными элементами ВМ являются: 1 – станина, обеспечивающая связь ВМ с путевой машиной; 2 – трубчатая пружина; 3 –гидроцилиндры привода рычагов ВМ; 4 – рычаг; 5 – башмак, обеспечивающий передачу вибрационных воздействий на балласт; 6 – подбойка, установленные в рычаге 5, обеспечивающие перемещение балласта под шпалу.

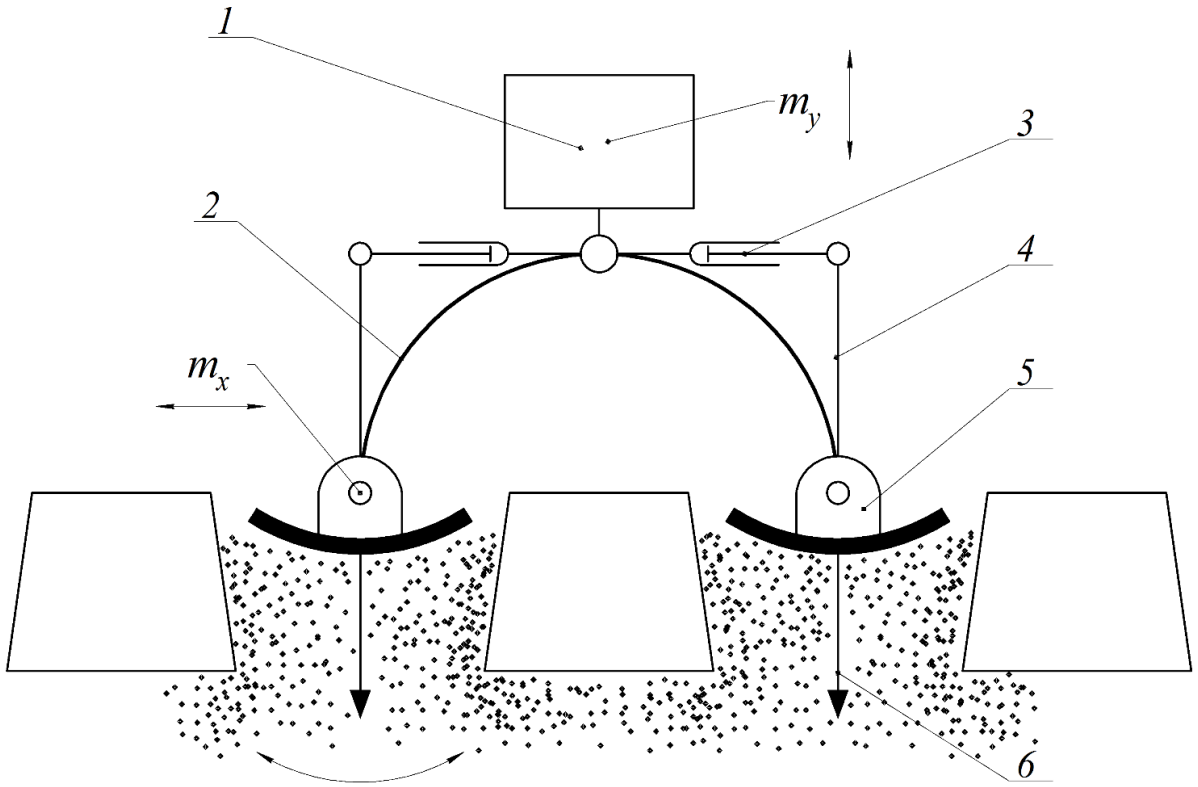


Рис. 2 Функциональная схема вибрационного механизма с трубчатой пружиной

Расчетная схема вибрационного механизма с трубчатой пружиной представлена на рис.3. Она представляет собой двухмассовую колебательную систему с двумя степенями свободы диссипативными факторами. Возбуждение системы обеспечивается циклическим, знакопеременным, расходом рабочей жидкости, поступающей в полость трубчатой пружины.

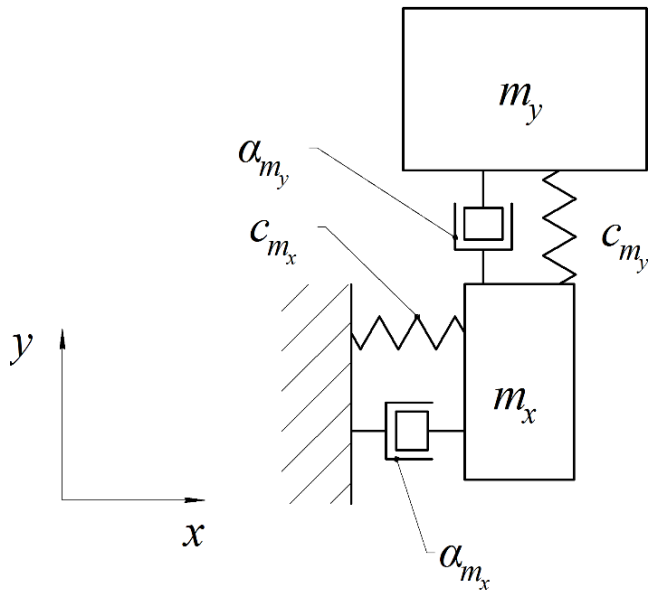


Рис. 3 Расчетная схема вибрационного механизма с трубчатой пружиной

Общее дифференциальное уравнение движение вибрационного механизма согласно расчетной схемы рис. 3 имеет вид:

$$\begin{cases} m_x\ddot{x} + \alpha_x\dot{x} + R_x\nu\,\mathrm{sgn}\,\dot{x} + cx = \dfrac{k_q}{r}\left[F(t) - k(x+y)\right] \\ m_y\ddot{y} + \alpha_y\dot{y} + cy = \dfrac{k_q}{r}\left[F(t) - k(x+y)\right] \end{cases}$$

где $R_x = m_y\ddot{y}$ – реактивная сила; $F(t) = \int_0^t q\,\mathrm{sgn}(\sin\omega\tau)\,d\tau$ – периодическая интегральная функция; ω, q – частота пульсации и расход рабочей жидкости поступающей в полость трубчатой пружины; k, k_q – коэффициенты изменения объема полости трубчатой пружины при внешнем и внутреннем воздействии; ν – коэффициент трения по поверхности балласта; α_x, α_y – коэффициенты эквивалентного жидкого трения.

Исследования математической модели рассмотренного вибрационного механизма позволят:

- определение рациональных геометрических параметров и режимов работы;
- оценка достигаемого эффекта уплотнения для разных конструкций верхнего строения пути.
- выработать рекомендации по конструктивному исполнению ВРО для уплотнения балласта верхнего строения пути.

ЛИТЕРАТУРА

[1] Путевые машины: Учебник для вузов ж.-д. транс/ С.А. Соломонов, М.В.Попович, В.М. Бугаенко и др. Под ред. С.А. Соломонова. – М.: Желдориздат 2000 – 756 с.

[2] Заярный С.Л., Ноткин В.С. *Шпалоподбивочная машина*. Пат. № 2043449 Российская Федерация, 1995, бюл. № 25, 5 с.

[3] Аксеральд Э.Л. *Гибкие оболочки*. Москва, Наука, 1976, 376 с.

Заярный Сергей Леонидович – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: texnakon@yandex.ru

Лесовский Игорь Олегович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: igor@lesovsky.ru

В.А. Ермоленко, А.В. Гавриков

ПРОЕКТИРОВАНИЕ ФРИКЦИОННОЙ МУФТЫ ПОДЪЁМНОГО КРАНА

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Известен механизм консольно-поворотного крана с муфтой предельного момента, встроенной внутрь корпуса червячного редуктора. [1], с. 5; с. 59 Недостатком данного механизма является то, что при необходимости регулировки муфты, при замене пружин или фрикционных дисков потребуется трудоемкий ремонт (вскрытие) редуктора. Другим недостатком этого устройства является наличие большого количества шпилек, пружин и гаек, требующих равномерной затяжки. Это увеличивает трудоемкость обслуживания муфты. Так как фрикционная муфта находится внутри, то редуктор и муфта являются специальными, а не универсальными, и это ограничивает область применения редуктора и муфты в отдельности.

Известна также предохранительная фрикционная муфта [2], которая содержит фрикционные диски, прижатые с помощью пружин и гаек, установленных на регулировочных болтах. Это устройство отличается сложностью равномерной затяжки множества пружин и большим диаметром шестерни, охватывающей фрикционные диски. Это обусловливает еще больший диаметр последующего зубчатого венца поворотного устройства, так как шестерня на фрикционной муфте является частью понижающей зубчатой передачи.

Целью данного технического решения является уменьшение габаритов фрикционной муфты и уменьшение трудоемкости ее обслуживания.

Технический результат достигается за счет того, что фрикционная муфта подъемного крана содержит ведущий зубчатый венец, соединенный с фрикционными дисками и ведущим валом посредством скользящих шлицов и пружин, при этом диаметр зубчатого венца максимально приближен к диаметру выходного вала редуктора механизма поворота крана (рис. 1), а диаметр фрикционных дисков увеличен относительно диаметра зубчатого венца. Корпус фрикционной муфты представляет собой двухступенчатый полый цилиндр, на малом внешнем диаметре которого имеется ведущий зубчатый венец, а на внутреннем диаметре большого цилиндра выполнены шлицевые зубья. На ведущий вал редуктора механизма поворота крана, посредством шпонки посажен цилиндрический стакан длиной, превышающей длину свободной пружины на несколько миллиметров, с заплечиками внутри и снаружи цилиндров. На стакане выполнены шлицы, а подшипниковая втулка выполнена разъемной из двух половин – полуколец.

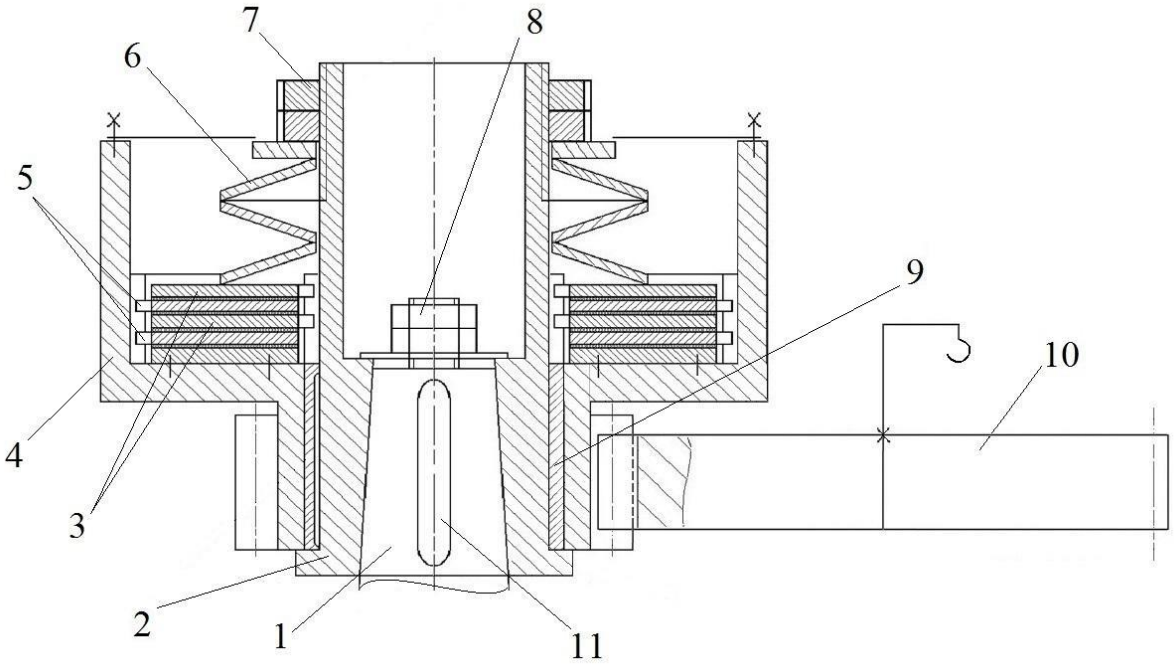


Рис. 1. Фрикционная муфта механизма поворота подъёмного крана

Фрикционная муфта подъемного крана (рис. 1) содержит выходной вал редуктора механизма поворота крана 1; стакан с наружными шлицами 2; фрикционные диски с внутренними шлицами 3; корпус с ведущим зубчатым венцом и внутренними шлицами 4; стальные диски с наружными шлицами 5; пружину 6; регулировочные гайки 7; концевые гайки 8; подшипниковую втулку 9; зубчатый венец механизма поворота грузоподъемного крана 10; шпонку 11.

Муфта работает следующим образом: ведущий вал 1 редуктора механизма поворота подъемного крана поворачивает через наружные шлицы стакана 2 фрикционные диски с внутренними шлицами 3. Эти диски в результате затяжки гаек 7 и пружины 6 прижимаются к стальным дискам с наружными шлицами 5. Если регулировочный момент трения дисков не превышает регулировочный крутящий момент, то происходит вращение корпуса 4 с ведущим зубчатым венцом и внутренними шлицами и поворот или торможение зубчатого венца 11 механизма поворота подъемного крана.

Сила затяжки пружины:

$$F = \frac{T}{zfR} = \frac{1000}{4 \cdot 0,3 \cdot 0,08} \approx 10^4 \text{ Н},$$

где $T = 1000$ Нм – крутящий момент, при котором проскальзывает фрикционная муфта (выходной момент редуктора); $z = 4$ – число пар трущихся поверхностей; f – коэффициент трения. Выбираем ленту асбестовую тормозную “ЛАТ-2” или “ЭМ-1”. Она имеет высокий коэффициент трения $f \approx 0,4$; при случайном образовании масляной пленки, можно принять

$f \approx 0,3$; конструктивно примем $R = 0,08$ м – средний радиус фрикционных дисков, равный диаметру тарельчатой пружины №231 ГОСТ 3057. Она допускает усилие до 13430 Н при деформации 20%.

В результате применения предлагаемой муфты достигается:

– уменьшение габаритов фрикционной муфты по сравнению с прототипом за счет того, что зубчатый венец перенесен с диаметра, превышающего диаметр фрикционных дисков на значительно меньший диаметр, незначительно превышающий диаметр ведущего вала редуктора. Это позволяет уменьшить диаметр большого зубчатого венца механизма поворота грузоподъемного крана при сохранении передаточного числа открытой зубчатой передачи.
– защита от внешних повреждений пружин фрикционной муфты, так как имеется удлиненный корпус, внутри которого скрыты зубчатые шлицы, пружины и фрикционные диски.
– применение одной крупной (например, составной тарельчатой) пружины вместо нескольких мелких витых пружин. Таким образом, достигается уменьшение трудоемкости обслуживания фрикционной муфты (затягиваем одну крупную гайку с контргайкой вместо нескольких гаек).

Муфта может быть применена в подъемно-транспортных машинах, в частности в механизмах поворота стреловых кранов, а также в качестве предохранительных муфт других машин.

Список литературы

[1] *Александров М.П., Решетов Д.Н.* Подъемно-транспортные машины. Атлас конструкций. – М.: Машиностроение, 1987. – 122 с.

[2] Патент RU 2049940 кл. F16D7/02 предохранительная фрикционная муфта.

Ермоленко Владимир Алексеевич – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: tvermolenko@rambler.ru

Гавриков Александр Витальевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: blackskorpion@mail.ru

УДК 621.86

В.А. Ермоленко, П.В. Витчук, Е.Е. Майоров, М.В. Донченко, А.А. Давтян

РАЗРАБОТКА КАНАТНОГО ТОРМОЗА

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Известны тормоза, устанавливаемые на быстроходном валу механизмов подъема [1, с. 245]. Недостатком такой конструкции является то, что разрушение муфты или редуктора механизма подъема приводит к падению груза.

Чтобы исключить аварию, в шахтных подъемных машинах тормоз устанавливают непосредственно на валу барабана. В качестве замыкающего устройства используют пружины, а в качестве размыкающего устройства используют гидроцилиндры [2, с. 188,224].

Известен также механизм поворота грузоподъемного крана, в котором тормозной шкив кинематически отделен от поворотной платформы тремя боковыми зазорами в зубчатых зацеплениях [3]. В случае изменения направления ветра может произойти неуправляемый поворот стрелы крана на угол, соответствующий сумме этих зазоров, приведенных к стреле крана, так как тормоз на поворотной платформе отсутствует [1, с. 442,443] и А.с. СССР 1258957 [3]. Известны ленточные тормоза, имеющие цилиндрический шкив и гибкий стальной элемент, концы которого связаны с силовым рычагом [1], с.240. Такие тормоза имеют ряд существенных недостатков:

1. Усилия, действующие на концы ленты со стороны привода и опор ленты направлены в одну сторону, на тормозной вал действует сила, равная геометрической сумме натяжений концов ленты. Эта сила создает изгибающий момент, со временем приводящий к разрушению вала.

2. Тормозной момент зависит от направления вращения цилиндрического шкива.Это следует из формул, приведенных в литературе [1].

3. Лента является одноэлементным изделием, поэтому ее обрыв влечет за собой непрогнозируемый отказ тормоза. По этой причине применение ленточных тормозов запрещено для многих грузоподъемных машин, например, лифтов.

Известен ленточный тормоз [4, с.216] и устройство [5], содержащие тормозной стальной шкив, огибаемый гибкой тормозной лентой, концы которой посредством рычажной системы кинематически связаны с приводами замыкания и размыкания тормоза. Такая конструкция имеет еще один недостаток – при монтаже длинных лент на тормозных шкивах большого диаметра возникают трудности разматывания и установки ленты.

Целью данной работы является разработка тормоза, свободного от указанных недостатков.

Нами предлагается конструкция канатного тормоза (рис. 1), содержащего три многопроволочных каната 1, 2 и 3. Концы канатов кинематически связаны с приводом равных усилий 6. Канаты соединены с помощью разветвителя 5, наложенного на тормозной шкив 4.

Такой тормоз можно устанавливать непосредственно на рабочем органе механизма, например, на опорно-поворотном устройстве крана или экскава-

тора (рис. 2). В качестве тормозного шкива канатного тормоза может быть использована любая вращающаяся цилиндрическая поверхность опорно-поворотного устройства, например, наружное кольцо кинематически связанного со стрелой грузоподъемного крана подшипника 4, опирающегося катками 12 на неповоротную платформу 11. Внизу цилиндрической поверхности установлен упор 13, на который опирается канат 1, затем на первый канат опирается средний канат 2 и следующий за ним канат 3. Средний канат 2 имеет площадь поперечного сечения вдвое больше, чем площадь поперечного сечения каждого из двух крайних канатов. Фиксация канатов на цилиндрической поверхности осуществляется, при помощи разветвителя 5, состоящего из трех клиновых зажимов 7, 8, 9. Для увеличения тормозного момента предусмотрена фрикционная накладка 10, соединенная с разветлителем 5.

Канатный тормоз работает следующим образом. Привод равного усилия 6 (например, состоящий из 2-х гидроцилиндров и гидронасоса) натягивает концы канатов 1, 2 и 3 (рис. 1). При этом, усилия привода, приведенные к геометрической оси цилиндрического шкива 4 взаимно уничтожаются.

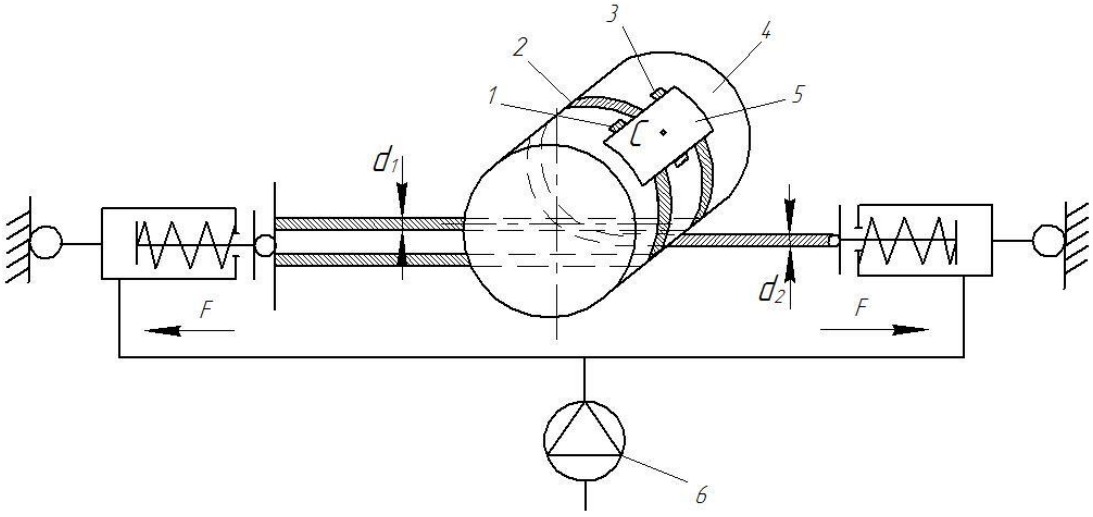


Рис. 1 – Предлагаемый канатный тормоз: 1, 2, 3 – канаты; 4 – тормозной шкив; 5 – разветвитель; 6 – привод равного усилия, С-центр разветвителя

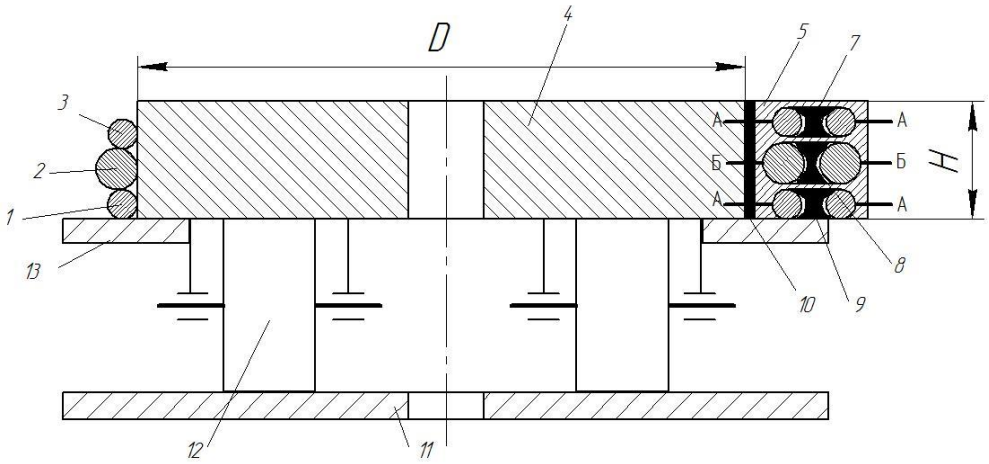


Рис. 2 – Установка канатного тормоза на опорно-поворотном устройстве: 1, 2, 3 – канаты; 4 – поворотный круг; 10 – накладка фрикционная; 5– разветвитель; 7, 8, 9 – зажимы клиновые; 11 –неповоротная платформа; 12 – каток; 13 – упор

В случае обрыва нескольких проволок канатов (например, 10…20 обрывов на длине каната, равной шести диаметрам каната) прочность каната практически не уменьшается. Число обрывов проволок накапливается постепенно и визуально отслеживается. Поэтому обрыв каната переходит из класса внезапных отказов в класс постепенных отказов, то есть становится прогнозируемым. Канат может быть заменен при плановом ремонте и отказ тормоза предотвращен. Высота цилиндрической части поворотного круга, занимаемая сечениями трех канатов и разветвителем достаточно мала по сравнению с шириной стальной ленты, используемой в ленточных тормозах. Поэтому, канатный тормоз может быть расположен на поворотной части крана (наружной части подшипника, который обычно имеет небольшую ширину). При монтаже канатного тормоза, в отличие от ленточного тормоза, длина каната и диаметр цилиндрического шкива могут быть значительно большими. Это позволяет расширить область применения канатного тормоза. Большой тормозной момент обеспечивается благодаря большому углу обхвата цилиндрического шкива канатами (около 360°) и вследствие большого усилия, которое выдерживает канат, а также благодаря применению специального каната без смазки. Если применять тормоз в качестве стояночного или аварийного, то абразивного износа каната практически не будет, ввиду малого пути скольжения каната по цилиндрической поверхности тормозного шкива. Схема предлагаемого ленточного тормоза симметрична относительно плоскости, проходящей через ось вращения тормозного шкива и центр разветвителя 4 (рис. 1). Поэтому центр разветвителя С считаем условно неподвижной точкой, в которой приложена сила наибольшего натяжения канатов. Тогда по терминологии [1, с.240] имеем «простой ленточный тормоз». Различие в том, что вместо ленты нами предложены канаты, а тормоз сдвоен относительно разветвителя 5.

Для фрикционных передач с гибким элементов и цилиндрическим шкивом, усилие, развиваемое канатным тормозом, может быть рассчитано с использованием формулы Эйлера.

Замыкающее усилие в канате F, направленное вправо примем равным приблизительно усилию двух канатов, направленному влево (рис.1) и равном усилию каждой из двух пружин.

Тормозной момент

$$M = \left(e^{\beta \cdot f} - 1\right) \cdot FD, \qquad (1)$$

где β=π=3.14 радиан- угол обхвата тормозного шкива одной из симметричных частей тормоза; f = 0.2- коэффициент трения специального каната (без смазки) по стальному тормозному шкиву; D – диаметр тормозного шкива.

В отличие от формулы, приведенной Александровым М.П [1, с.241] вместо радиуса R нами принят диаметр тормозного шкива D, так как имеем как бы два симметричных простых ленточных тормоза. Плечо усилие ленты a=R. Плечо замыкающей силы также равно a. В нашем случае

$2a$=2R=D. В остальном, формула (1), предложенная нами, вытекает из формулы Александрова М.П для простого ленточного тормоза.

По формуле(1) получим:

$$M = \left(2{,}72^{0{,}2\cdot 3{,}14} - 1\right)\cdot FD = 1{,}87FD, \qquad (2)$$

По формуле (2) можно выбрать усилие пружин F. Например, имеем диаметр поворотной части опорно-поворотного устройства, используемого в качестве тормозного шкива D=2м (рис.2). Пусть задан максимальный тормозной момент $M=2\cdot 10^5$ Н·м, действующий на стрелу грузоподъемного крана при штормовом ветре (скорость ветра 30м/с). Из формулы (2) получим:

$$F = \frac{M}{1{,}87D} = \frac{2\cdot 10^5}{1{,}87\cdot 2} = 5{,}35\cdot 10^4\, H$$

Примем коэффициент использования каната (коэффициент запаса прочности) Zp=2,5 [1].

Получим условие выбора одинарного каната:

$$[F] \geq F\cdot z_p = 5{,}35\cdot 10^4\cdot 2{,}5 = 13{,}4\cdot 10^4 \text{Н},$$

где [F]-разрывное усилие каната в целом, принимаемое из ГОСТ 2688 для маркировочной группы 1770 МПа. Примем диаметр одинарного каната (справа по рис.1) d_2=15мм; $[F]=15{,}2\cdot 10^4$Н.

Условие выбора сдвоенного каната (слева по рис1):

$$[F] \geq F\cdot z_p / 2 = 5{,}35\cdot 10^4\cdot 2{,}5/2 = 6{,}7\cdot 10^4\, H.$$

Из ГОСТ 2688 получим d_1=11мм; $[F]=8{,}32\cdot 10^4$Н. Высота разветвителя

$$H = 2\left(d_1 + 2d_2\right) = 2\left(15 + 2\cdot 11\right) = 74\text{мм}.$$

Это приемлемо, так как ширина типовых подшипников диаметром 2 м, применяемых для опорно-поворотных устройств не менее Н (см.рис.2).

На рис. 3 показан разрез Б-Б по разветвителю 5 (след секущей плоскости Б-Б показан на рис.2).

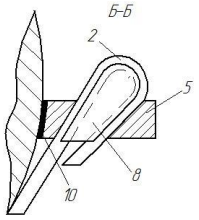


Рис.3

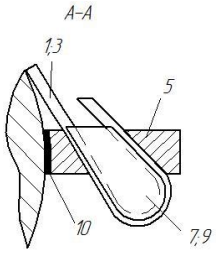


Рис.4

На рис.4 показан разрез А-А по разветвителю 5 (два следа секущих плоскостей А-А показаны на рис.2).

Разветвитель 5 имеет среднее отверстие клиновидной формы (рис.3), в которое вводят петлю каната 2 и клин 8, расширенный внизу. Поверхность разветвителя 5, прилегающая к поворотной части опорно-поворотного устройства 4 оснащена тормозной накладкой 10. Разветвитель 5 имеет

также два крайних отверстия клиновидной формы меньшего размера (рис.4) в которые вводят канаты 1;3 и клинья 7 и 9, расширенные вверху.

Тормозная накладка 10 увеличивает коэффициент трения и тормозной момент. Клинья 7, 8 и 9, установленные противоположно, удерживают канаты 1; 2 и 3 направленные в разные стороны.При этом линия каната 2 (рис.3) является касательной к двум цилиндрам, шкиву и расширенной части клина 8. То же относится к рис.4 для канатов 2 и 3.

Применение предлагаемого канатного тормоза позволит уменьшить вероятность обрыва гибкого элемента ленточного тормоза, устранить усилие, изгибающее вал тормозного шкива или усилие, действующее на опорно-поворотное устройство, а также упростить монтаж гибкого элемента на крупногабаритных поворотных платформах и применить готовое изделие (канат) вместо ленты на тормозных шкивах большого диаметра.

Список литературы

[1] Александров М.П. Грузоподъёмные машины. -М.: Изд-во МГТУ им. Н.Э. Баумана – Высшая школа, 2000. 552 с.

[2] Траубе Е.С, Найденко И.С. Тормозные устройства и безопасность шахтных подъемных машин. -М.: Изд-во Недра, 1980. 256 с.

[3] Опорно- поворотное устройство: свид-во. на полез. модель № 1258957 Рос. Федерация: МПК E02F9/12.

[4] Александров М.П. Тормоза подъемно-транспортных машин. -М.: Машиностроение, 1976. 383 с.

[5] Пат.2383794 Рос. Федерация: F16D49/08, B66D5/10. Ленточный тормоз/ Тарасов Ю.Д.; Заяв. 03.12.2008; Опубл. 10.03.2010

Ермоленко Владимир Алексеевич – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: tvermolenko@rambler.ru

Витчук Павел Владимирович – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: zzzventor@ya.ru

Майоров Евгений Евгеньевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: maybesovsky@yandex

Донченко Михаил Владимирович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: donchenkomv@mail.ru

Давтян Артем Арцрунович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: artem.davtian@yandex.ru

Т.В. Гаах, Д.М. Глазунов

СНИЖЕНИЕ ДИНАМИЧЕСКИХ НАГРУЗОК НА РАМУ ЭКСКАВАТОРА С АКТИВНЫМ РАБОЧИМ ОРГАНОМ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Для разработки мерзлых и прочных грунтов широкое распространение получили экскаваторы, оснащенные гидромолотами. Сфера использования гидравлического молота очень обширна (демонтаж стен и дорожных одежд, установка свай и пр.), поскольку позволяет в больших пределах регулировать энергию и частоту ударов гидроимпульсной системы [1].

Машины ударного действия с гидравлическим приводом имеют высокий КПД и повышенную долговечность, обусловленную работой ударного устройства при постоянной смазке [2]. Высокая маневренность экскаваторов II и III группы позволяют выполнять строительные и ремонтные работы в стесненных условиях. Современные гидромолоты обладают значительными энергетическими возможностями со сравнительно невысокими удельными массами, что позволяет использовать их на базовых моделях экскаватора II размерной группы. Но малая масса базовой машины приводит к значительным реакциям отдачи, что может отрицательно сказаться на работе элементов конструкции экскаватора (раму, стрелу). В связи с этим снижение вибраций и как следствие динамических нагрузок, передаваемых на машину и оператора, является актуальной задачей. Снижение уровня вибрации платформы экскаватора можно достигнуть путем установки демпфирующей подвески гидромолота (рис.1).

Гидромолот 4, связан с кареткой 3 гидроцилиндра 7 с помощью шарнира 2. Поршень со штоком 5 также имеет связь с гидромолотом 4 посредствам шарнира 6. К гидроцилиндру 7 со стороны поршневой полости присоединен гидропневмоаккумулятор 1, а между ними расположены обратный клапан 8 и дроссели 9.

Подвеска работает следующим образом. В начальном положении гидромолот вывешивается к разрабатываемой поверхности с начальным контактом. Прижатие гидромолота и дальнейший запуск удара задается подачей жидкости в поршневую полость гидроцилиндра. При отдаче гидромолота происходит вертикальное перемещение корпуса гидромолота - штока, и вытеснение жидкости из поршневой полости через дроссели в гидропневмоаккумулятор. Жидкость перетекает через дроссели, которые повышают сопротивление ее перетеканию и уменьшают скорость перемещения штока. Одновременно происходит сжатие агента (N_2) гидропневмоаккумулятора, что обеспечивает дополнительное гашение ударной нагрузки до номинального уровня. При прижатии гидромолота каретка возвращается в начальное положение за счет срабатывания гидропневмоаккумулятора с

одновременным открытием обратного клапана. Это увеличивает скорость возврата гидромолота до первоначального положения. В дальнейшем цикл повторяется [3].

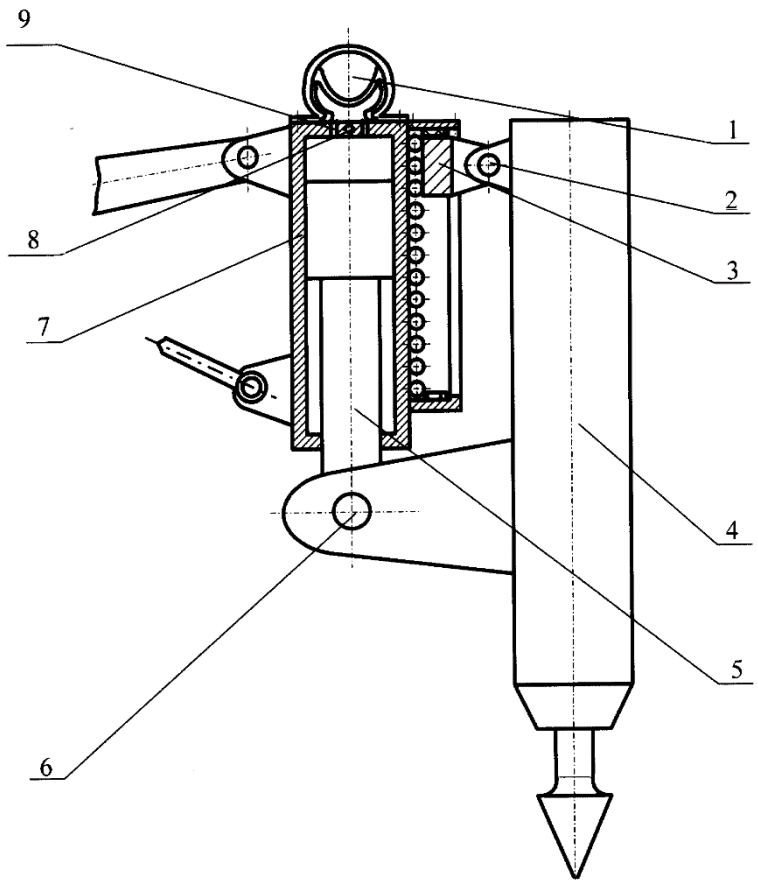


Рис.1 Подвеска гидромолота

Дифференциальное уравнение, описывающее динамику рабочего процесса экскаватора и его элементов имеет вид:

$$A_q\ddot{\vec{q}} + B_q\dot{\vec{q}} + C_q\vec{q} = \vec{Q}_f,$$

где A_q , B_q, C_q - матрицы коэффициентов дифференциальных уравнений размером $l \times l$; $\ddot{\vec{q}}$, $\dot{\vec{q}}$, $\vec{q}$ - матрицы размером $l \times 1$, представляющие собой малые значения соответственно ускорений, скоростей и обобщенных координат; $\vec{Q}_f$ - матрица сил размером $l \times 1$.

В результате численного решения системы дифференциальных уравнений получены зависимости перемещения рамы экскаватора от времени. Расчет произведен для случаев установки гидромолота с жесткой и демпфирующей подвесок. (рис. 2) [4].

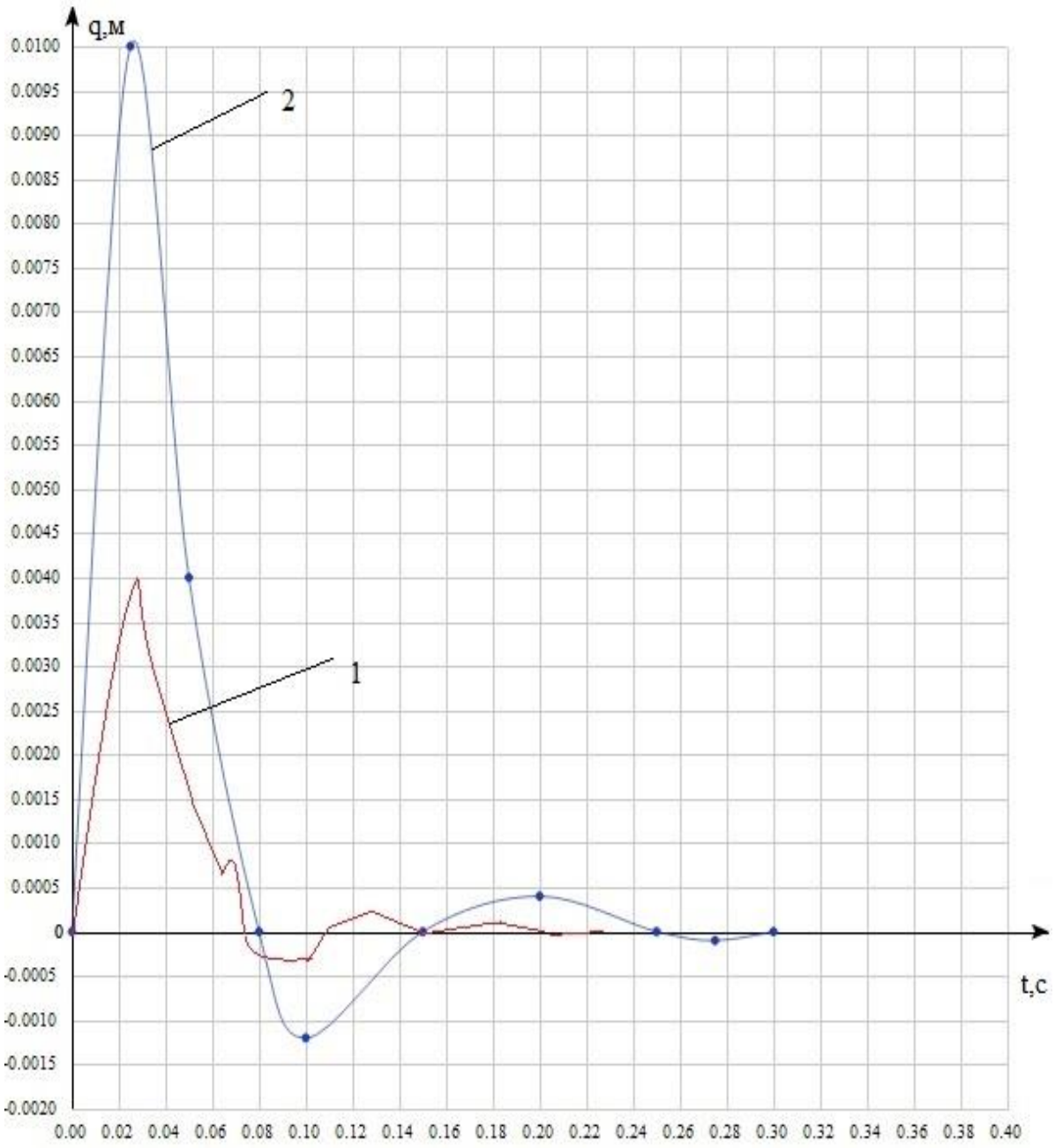


Рис. 2. Графические зависимости перемещения рамы экскаватора от времени: 1 – с амортизирующей подвеской; 2 – с жесткой подвеской

На рисунке видно, что жесткость амортизирующей подвески значительно влияет на вертикальное отклонение рамы экскаватора, таким образом использование подвески позволяет снизить негативное воздействие вибраций.

Список литературы

[1] Высокопроизводительные гидропневматические ударные машины для прокладки инженерных коммуникаций / Д.Н. Ешуткин, Ю.М. Смирнов, В.И. Цой, В.Л. Исаев. М.: Стройиздат, 1990. 171 с.

[2] Перевязкин В.Н., Дмитриевич Ю.В. Анализ рабочих циклов гидравлических и гидропневматических молотов // Повышение эффективности ударных машин: Науч. тр. М.: ВНИИстройдормаш, 1986. Вып. 107.

[3] Пат. 58564 на полезную модель. РФ, МПК[51] E 02 F 9/22. Подвеска гадромолота / Д.В. Поступинских, С.Ю. Тимаков, А.И. Грамовик.

[4] В.Н. Кузнецова, Д.В. Поступинских. Исследование влияния динамических нагрузок на раму экскаватора с активным рабочим органом. // Строительные и дорожные машины. - 8/2008. – С. 40-43.

Гаах Татьяна Владимировна – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: zzzventor@ya.ru

Глазунов Дмитрий Михайлович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: glapple@yandex.ru

П.В. Витчук, К.А. Фарафонтова

СОВРЕМЕННЫЕ КОНСТРУКЦИИ ГРУЗОВЫХ ЛИФТОВ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Лифт представляет собой разновидность грузоподъёмной машины, используемую для вертикального или наклонного перемещения грузов на специальных платформах, передвигающихся по жестким направляющим, угол наклона которых к вертикали не превышает 15° [1, 2].

Грузовые лифты часто применяют для механизации грузоперевозок в производственных и складских помещениях. Их могут использовать для перевозки грузов с сопровождающим персоналом (проводником) или только грузов (перевозка людей запрещена).

В соответствии с [3] грузовые лифты выполняют с номинальной грузоподъемностью 500; 630; 1000; 1600; 2000; 2500; 3200; 3500; 5000 кг и скоростью движения кабины 0,25; 0,40; 0,50; 0,63; 1,0; 1,60; 1,75; 2,5 м/с.

Приводные системы современных грузовых лифтов имеют весьма разнообразную конструкцию. Так, имеются сведения о применении в грузовых лифтах следующих типов приводов: электрические редукторные с тяговым барабаном или канатоведущим шкивом и тяговым канатом; электрические безредукторные с канатоведущим шкивом и тяговым канатом; электрические редукторные с тяговой звездочкой и цепью; гидравлические прямого действия и с канатным мультипликатором; пневматические. Рассмотрим наиболее распространенные из них.

Лифты с лебедками барабанного типа (SKG и др.) [4] характеризуются тем, что канаты, на которых подвешены кабина и противовес, раздельно жестко закреплены на барабане и при подъеме кабины ее канаты наматываются на барабан, а канаты противовеса сматываются (рис. 1).

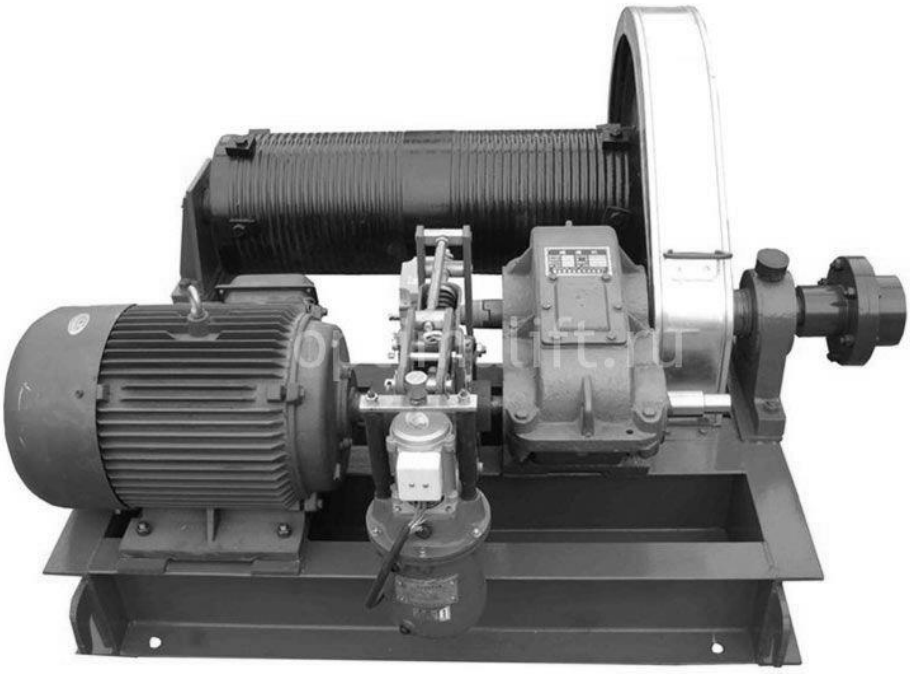


Рис. 1. Лебедка грузового лифта с тяговым барабаном

При опускании кабины канаты работают в обратном порядке. Основной недостаток барабанных лебедок – значительная длина барабана, возрастающая с увеличением высоты обслуживаемого лифтом здания, а также большая длина тяговых канатов. Поэтому такие лебедки применяют только на лифтах с малой высотой подъема кабины.

Лифты с лебедками, оборудованными канатоведущими шкивами (BKG, SKG, КМЗ, Могилевлифтмаш и другие) [4,5,6,7] характеризуются отсутствием жесткого крепления канатов на канатоведущем шкиве (рис. 2). Тяговое усилие в канатах, необходимое для подъема кабины и противовеса, создается силами трения между канатами и рабочими поверхностями канатоведущего шкива. Такая лебедка позволяет подвешивать кабину и противовес на нескольких канатах, без усложнения ее конструкции. Это важно для лифтов повышенной грузоподъемности в многоэтажных зданиях, так как высота обслуживаемого здания несущественно влияет на конструкции лебедок.

Рис. 2. Лебедка грузового лифта с канатоведущим шкивом и выносной подшипниковой опорой

Лифты с тяговой звездочкой и цепью (SKG, BKG) [4,5], характеризуются тем, что у этой лебедки тяговая сила создается за счет зацепления звездочки с тяговой цепью (рис. 3).

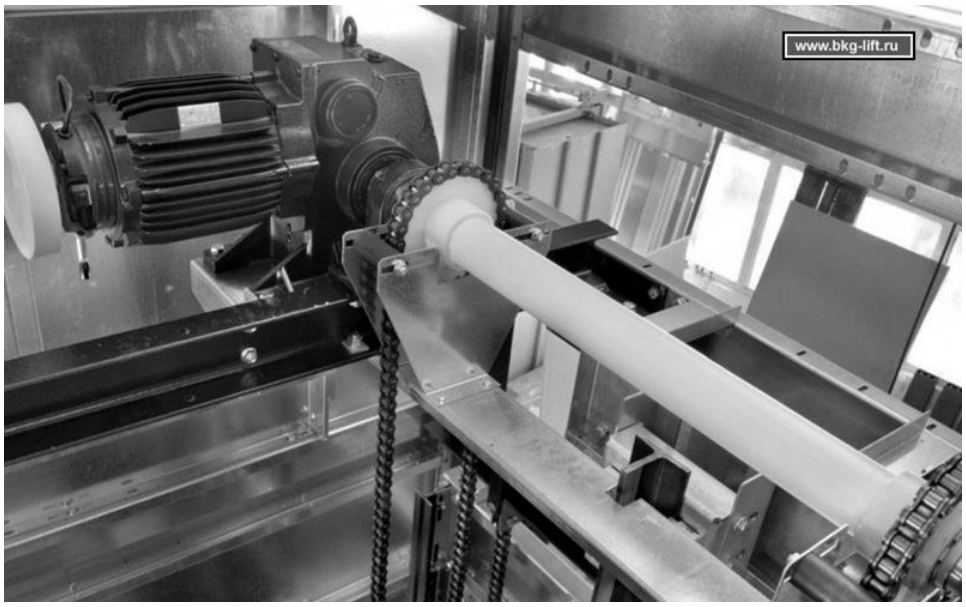


Рис.3. Лифт с тяговой звездочкой и цепью [5]

В последние годы, из-за минимальных нагрузок на строительную часть конструкции здания, расширилась сфера применения в грузовых лифтах гидравлических приводов прямого действия и с гидравлическими мультипликаторами [8] (рис. 4).

Рис. 4. Грузовой лифт с гидравлическим приводом [13]:

К основным преимуществам лифтов на гидравлическом приводе можно отнести [8, 9]: высокая энергетическая эффективность; шахта лифта с гидравлическим приводом может иметь лишь одну несущую стену; возможность размещения машинного помещения на значительном удалении от шахты и на любом из этажей здания; высокая надежность механизмов при относительной простоте конструкции; плавность и бесшумность хода кабины; большая грузоподъемность.

Недостатками конструкции лифтов с гидравлическими приводами являются [8, 9]: незначительная скорость хода и высота подъема кабины; необходимость в использовании значительного количества масла (до двухсот литров); повышенные требования пожарной безопасности; в ряде случаев возникает потребность в установке дополнительного оборудования (охладителей и т.д.).

Перспективным для грузовых лифтов может являться использование ленты в качестве тягового органа. Впервые подобная конструкция была разработана и апробирована в СССР в 1970-х годах [10]. В качестве тягового органа была применена стальная лента. Это позволило значительно снизить размеры и массу лебедок, повысить срок службы самого тягового органа и снизить его металлоемкость. В результате были изготовлены несколько опытных образцов лифтов, но в серийное производство они не пошли. Вероятно, это обусловлено тем, что обрыв стальной ленты носит случайный характер и не может быть спрогнозирован.

В 2000 году двумя зарубежными компаниями (OTIS и SCHINDLER) были выпущены пассажирские лифты с ленточным тяговым органом. В качестве тягового органа была применена полиуретановая лента, армированная стальными канатами малого диаметра [11] (рис. 5). Привод таких лифтов безредукторный с тяговым барабаном, выполнен по полиспастной схеме.

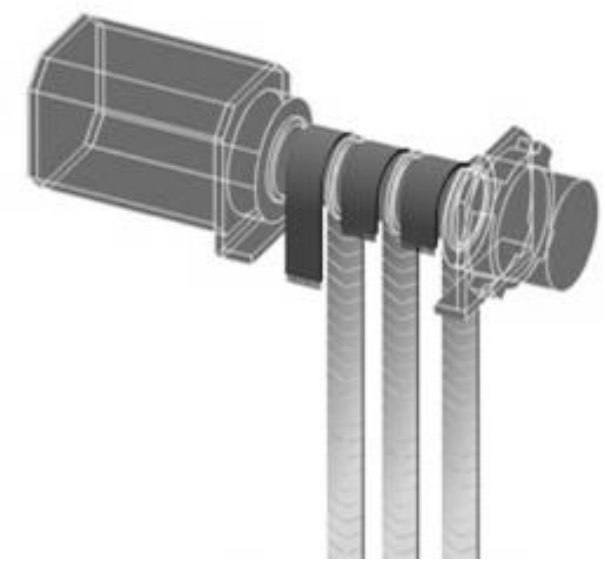


Рис. 5. Лебедка лифта с полиуретановыми ремнями [11]

Данная конструкция обладает всеми недостатками лифтов с лебедками барабанного типа. Перспективным может являться использование полиуре-

тановой ленты в качестве элемента передачи трением. Это позволит существенно упростить конструкцию привода лифта и уменьшить его габариты.

Весьма специфическую конструкцию имеют лебедки грузовых лифтов с большой грузоподъемностью. Они могут дополнительно оборудоваться ременной передачей и включать в свою конструкцию редуктора с червячно-зубчатой передачей [12].

Подобное разнообразие конструкций приводов грузовых лифтов свидетельствует об отсутствии единого алгоритма выбора их наиболее рациональных параметров, а также критериев, обуславливающих целесообразность применения того или иного конструктивного исполнения. Это, несомненно, обуславливает актуальность разработки рекомендаций по выбору и обоснованию параметров приводов грузовых лифтов.

Список литературы

[1] Лифты. Учебник для вузов /под общей ред. Д.П.Волкова. –М.: Изд-во АСВ, 1999. -480 с.

[2] Павлов Н. Г. Лифты и подъемники. Основы конструирования и расчета. – М.: Машиностроение, 1965. -204 с.

[3] ГОСТ Р 53771-2010 (ИСО 4190-2:2001). Лифты грузовые. Основные параметры и размеры –М.: Стандартинформ, 2010. -24 с.

[4] Официальный сайт SKG. URL: http://www.skglift.ru/index.html (дата обращения: 9.10.16).

[5] Официальный сайт компании BKG. URL: http://www.bkg-lift.ru/produktsiya/gruzovye_lifty/ (дата обращения: 9.10.16).

[6] Официальный сайт КМЗ лифт. URL: http://www.kmzlift.ru/winches/ (дата обращения 9.10.16).

[7] Официальный сайт Могилевлифтмаш. URL: http://www.liftmach.by/catalog/lebyedki-liftov/ (дата обращения: 9.10.16).

[8] Г. Г. Архангельский. Гидравлические лифты: конструкция, монтаж и обслуживание. Учебное пособие. –М.: МГСУ, 2013. – 272 с.

[9] Портал лифтовиков России. URL: http://prolift.ru/gidravlicheskiy-lift/lifty-s-gidravlicheskim-privodom-konstruktsiya-i-osobennosti.html (дата обращения: 10.10.16).

[10] Борохович А. И. Грузоподъемные установки с ленточным тяговым органом. –М.: Машиностроение, 1980. -191 с.

[11] Лифт GeN2™ Comfort. URL: http://www.eska-lift.ru/userfiles/Gen2.pdf (дата обращения: 10.10.16).

[12] Яновски Л. Проектирование механического оборудования лифтов. Третье издание. -М.: Монография. Издательство АСВ, 2005. -336с.

[13] Официальный сайт Kleemann Hellas S.A. URL: http://www.kleemannlifts.com/index.php?lang=en (дата обращения: 10.10.16).

Витчук Павел Владимирович – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: zzzventor@ya.ru

Фарафонтова Ксения Андреевна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: fakssa@yandex.ru

К.С. Рыжов, П.В. Витчук

СПОСОБЫ ИЗМЕРЕНИЯ ОТКЛОНЕНИЙ КРАНОВЫХ ПУТЕЙ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Подкрановый путь предназначен для эксплуатации в промышленном производстве, машиностроении и на объектах энергетики при эксплуатации мостовых и козловых кранов, башенных кранов, а также других грузоподъемных устройств и механизмов. Нормами эксплуатации подкрановых путей устанавливается периодическая диагностика подкрановых путей с условием обязательного проведения геодезического промера рельсовых путей кранов с целью проверки их геометрических параметров. Любой проект подкрановых путей должен предусматривать возможность их инструментального и визуального обследования и контроля. [1]

При постоянном использовании технические свойства крановых путей могут сильно отклоняться от установленной нормы, что чревато серьезными последствиями не только для крановой грузоподъемной техники, но и для работников, обслуживающих ее. [2] Нивелирование подкрановых путей должно в обязательном порядке проводиться в абсолютном соответствии с графиком работы грузоподъемного оборудования, а значит – циклично. [1]

Нивелировка крановых путей начинается с выноса на местность конечных точек оси в соответствии с проектной документацией. Параллельно выполнению нивелировки подкрановых путей рекомендуется произвести геодезическую съемку основных параметров самих подъемных механизмов (кранов, кран-балок), непосредственно эксплуатирующих подкрановый путь. [3] Такая съемка позволит определить текущее эксплуатационное состояние кранов, их геометрические характеристики (разность в осевых длинах и расстояния, подъем (прогиб балки) и т.д.). Также каждый отчетный период (для подъемных машин разного типа интервал инспектирования может отличаться, средняя периодичность 1 раз в год) необходимо заключение крановой инспекции которое невозможно получить без соответствующей геодезической съемки. [4] При выполнении нивелировки крановых путей устанавливается их фактическое положение согласно плану и составляются профили.

Нивелировка подкрановых путей выполняется не только для выявления отклонения от прямолинейности, но и для измерения остальных геометрических параметров пути крана. При измерении подкранового пути исследуются следующие показатели: как ширина колеи, стыковые зазоры, уклон рельсового пути, высотные отметки вдоль пути и поперек пути, несовпадение рельсов по высоте в стыках и множество дополнительных кри-

териев, которые обозначаются в инструкции по эксплуатации грузоподъемных кранов.

На данный момент для определения отклонений крановых рельсов от проектного положения наиболее часто применяются следующие приборы:

- Теодолиты;
- Нивелиры;
- Нивелирные рейки;
- Уровни различных конструкций;
- Лазерные измерители расстояний.

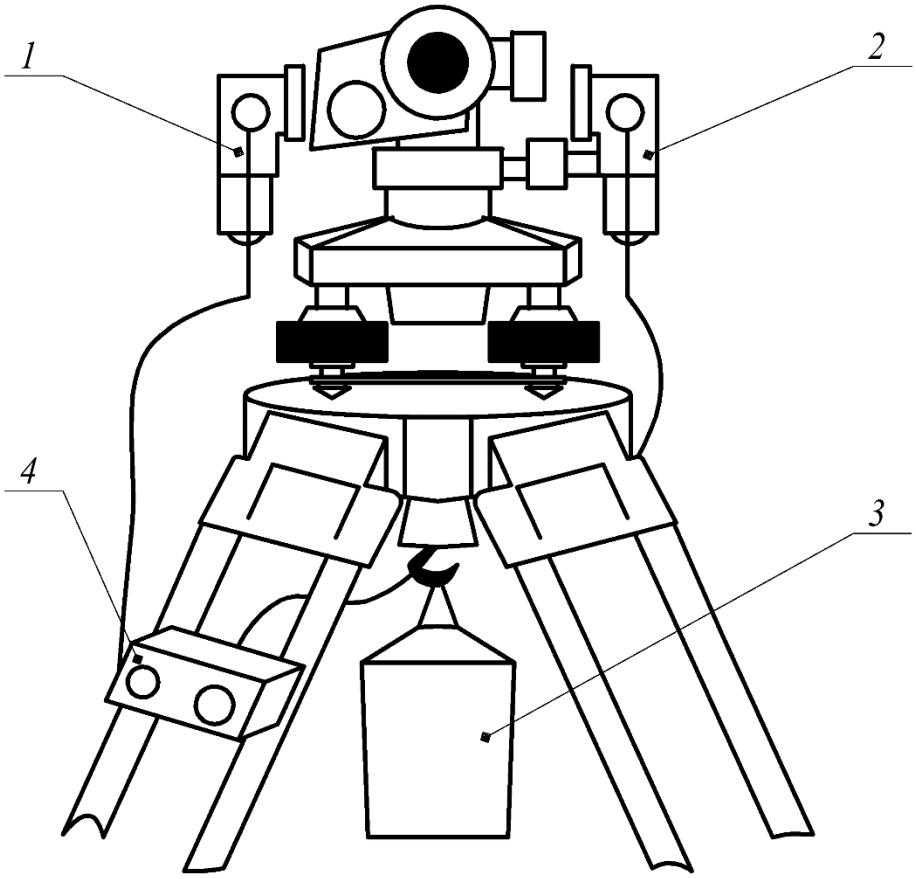


Рис. 1 Нивелир Н3 с приспособлением для подсветки

На рисунке 1 показано приспособление для подсветки круглого уровня при приведении нивелира в рабочее положение и цилиндрического уровня перед взятием отсчетов по рейке во время работы с инструментом в условиях слабой освещенности. В комплект приспособления входят осветительные головки 1 и 4, выключатели 2 и источник питания 3. В качестве последнего могут быть использованы батарейки или соответствующий аккумулятор. Осветительная головка снабжена электрической лампой, заключенной в кожух. Авторами использовались серийно изготавливаемые промышленностью осветительные головки, блоки управления 2 и аккумуляторы. Небольшие масса и габаритные размеры аккумулятора позволяет

подвешивать его непосредственно к становому винту. Для применения готового комплекта требуется изготовление всего двух скобок для крепления головок на приборе. [5]

А.М. Русковым предложена специальная подставка под геодезические приборы пластина 2 которой с прокладкой 1 крепится струбциной к плоскости строительной конструкции так, чтобы пузырек круглого уровня 8 был на середине в направлении, параллельном оси 4. Окончательная установка уровня производится вращением гайки 5, которая перемещает уголок 6, закрепленный на площадке 7, вдоль болта 3. Консоль 15 может поворачиваться в горизонтальной плоскости и имеет прорезь 17 для станового винта 16. Зажимной винт 10 служит для фиксирования консоли в определенном положении. Поворотом консоли 15 и смещением станового винта 16 в прорези 17 можно добиться наиболее удобного для наблюдений расположения прибора. Винтом 14 можно изменять положение консоли 15 с установленным на ней прибором (теодолит, нивелир) в пределах 20-25 мм по высоте. Для определения величины этого перемещения служит шкала 11, по которой берут отсчеты, поочередно совмещая винтом 14 горизонтальную нить сетки нивелира с высотой инструмента в нивелируемых точках. Разность отсчетов дает превышение между точками. Измерение превышений можно автоматизировать, если использовать диск 13 с магнитами и герметизированный контакт (геркон) 9, соединенный с микрокалькулятором.

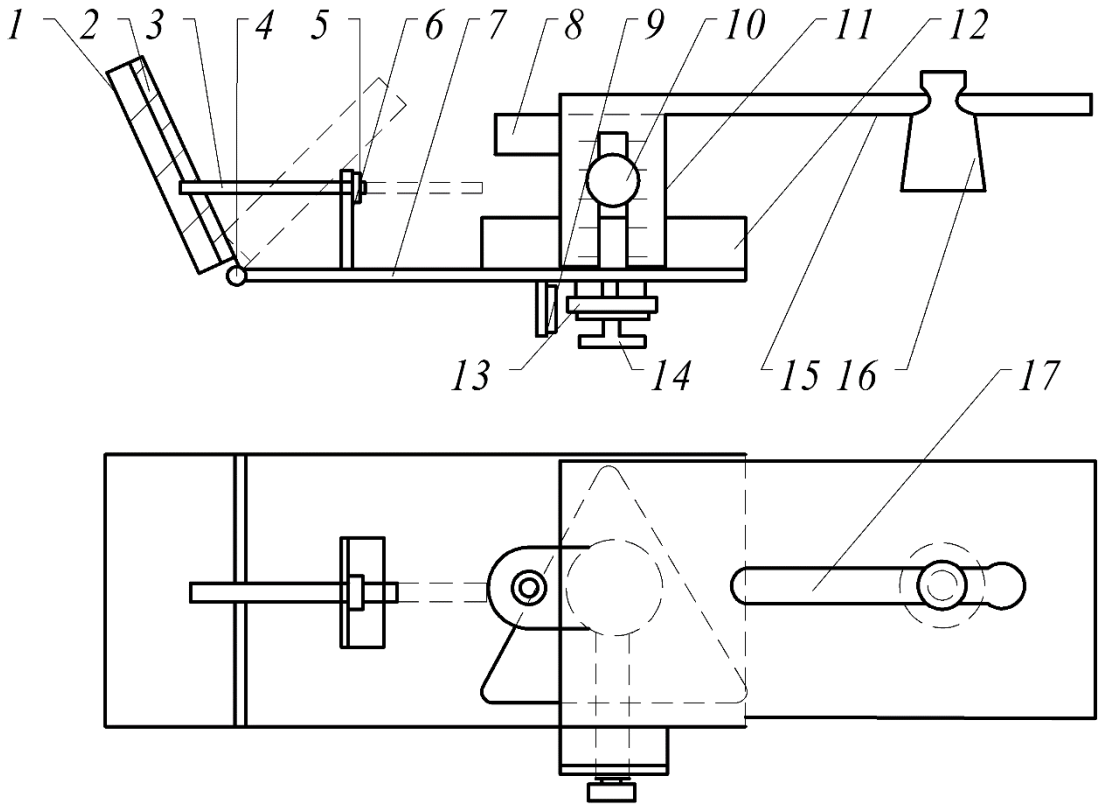


Рис. 2 Подставка для геодезических приборов

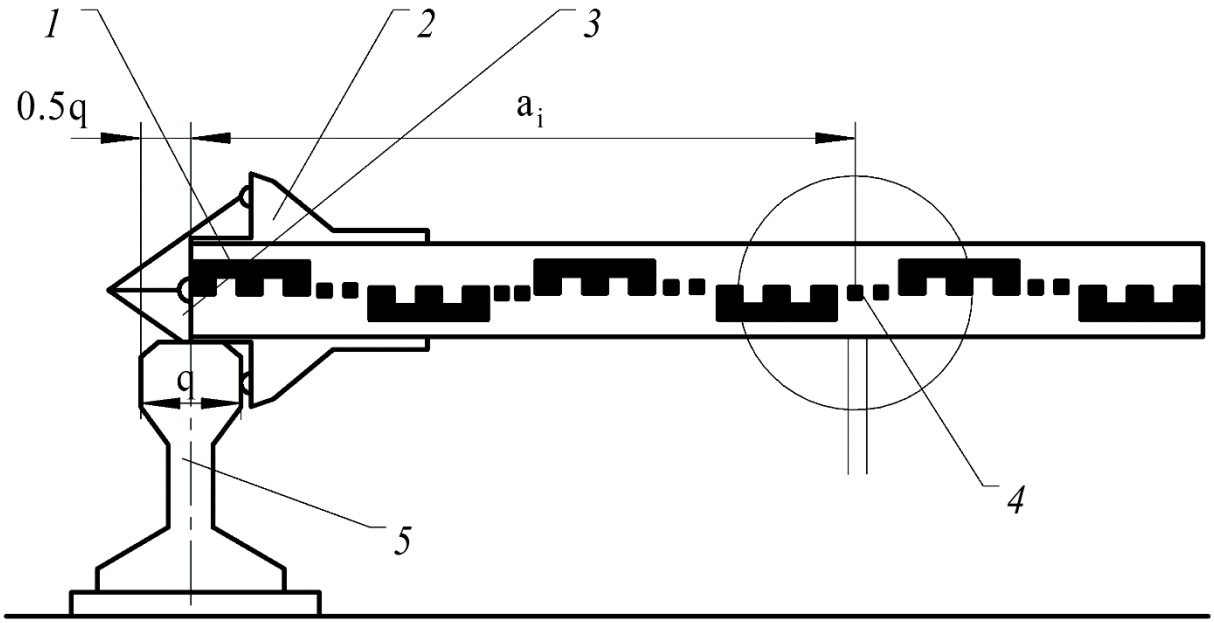


Рис. 3 Приспособление для бокового нивелирования подкрановых рельсов

На рисунке 3 показано простое приспособление для бокового нивелирования подкрановых рельсов при контроле их прямолинейности путем измерения отрезков, от визирного луча или иного створа до оси рельса. Для этого В.Н.Соустин предложил использовать половину стандартной нивелирной рейки 1 со специальным контактным устройством на ее пятке. Оно представляет собой шаблон 2 с шурупами 3, упирающимися в боковую грань головки рельса 5. Отсчеты по рейке берут по вертикальной нити сетки 4, поворачивая рейку черной и красной стороной. [5] Следует заметить, что точечный контакт рейки с рельсом может отрицательно сказаться на точности измерений вследствие коррозии или иных нарушений его боковой грани.

Существует также устройство, состоящее из двухсторонней рейки и плоского зеркала, установленных на прямоугольной раме так, что в поле зрения трубы теодолита одновременно видны передняя и отраженная в зеркале задняя плоскости рейки. Но в условиях плохой освещенности здесь возникает задача подсветки не одной, а двух плоскостей рейки.

Также используется следующее приспособление.

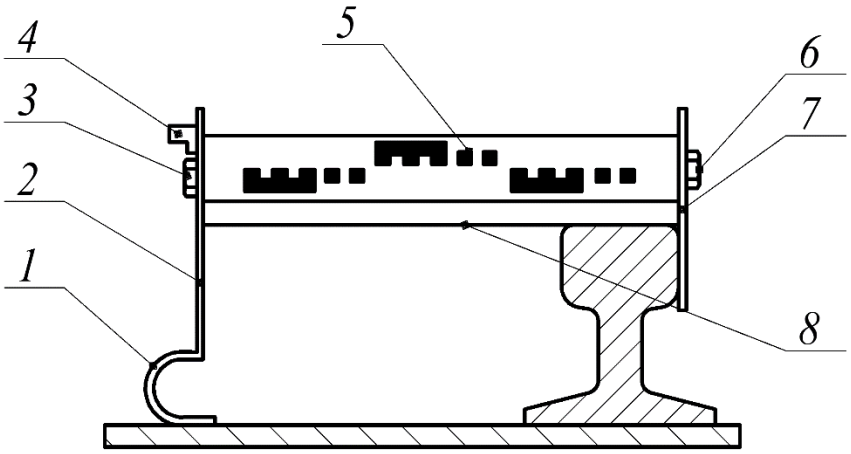


Рис .4 Приспособление для бокового нивелирования подкрановых рельсов.

Оно состоит из двух вертикальных щек 1 и 2, соединенных горизонтальной поперечиной 3. Между щеками болтами 4 и 5 закреплен отрезок двухсторонней нивелирной рейки 6 с возможностью вращения ее вокруг продольной оси. В горизонтальное положение рейка устанавливается по уровню 7 с помощью подпятника 8 в виде дугообразной пластинчатой пружины. Вращая рейку вокруг продольной оси, можно брать отсчеты по ее черной и красной сторонам. Ширина щеки 2 при плотном ее прилегании к боковой грани головки рельса обеспечивает перпендикулярное положение рейки к его оси и исключает влияние, локальных повреждений этой грани на результаты измерений. [5]

Другое приспособление отличается возможностью изменения его габаритных размеров в процессе съемки и для удобства транспортировки.

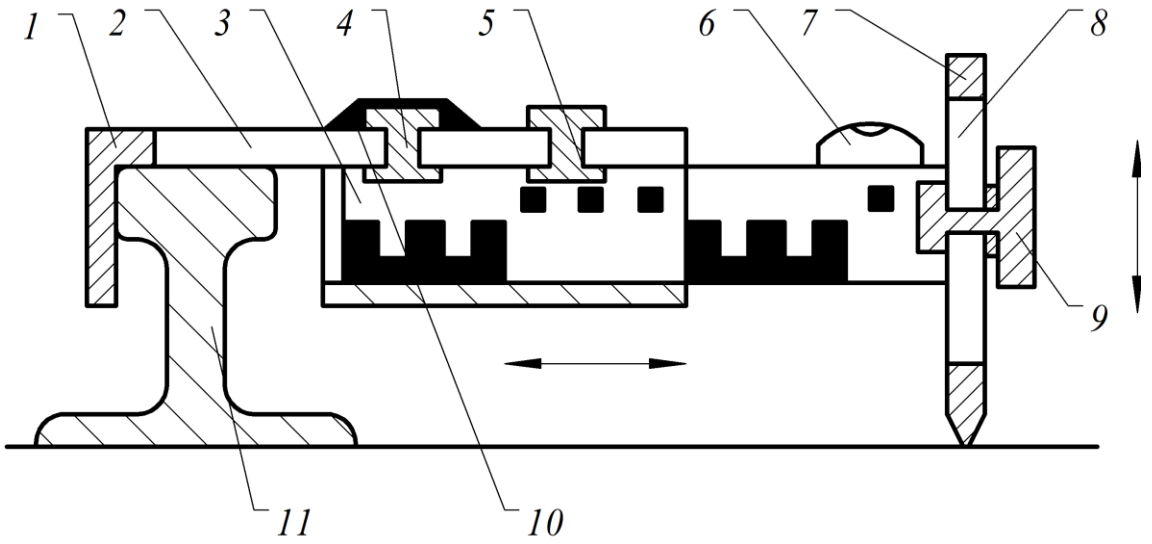


Рис .5 Приспособление для бокового нивелирования подкрановых рельсов.

Оно содержит коробчатый каркас 1 с продольной прорезью 2 на верхней его плоскости. Внутри каркаса закреплена укороченная нивелирная рейка 3, которая имеет возможность передвижения влево-вправо с после-

дующей фиксацией в требуемом положении винтами 4 и 5. Рейка снабжена уровнем 6 и вмонтированной с торца гайкой. Для приведения пузырька уровня в нульпункг служит щека 7 с прорезью 8 и стопорным винтом 9. На верхней плоскости каркаса закреплена линейка с миллиметровыми делениями, а на винте 5 имеется отсчетный индекс 10. Если визирный луч не попадает на рейку или по условиям съемки необходимо изменить длину устройства, то, открепив винты 4, 5, смещают рейку влево или вправо. Это смещение фиксируется по металлической линейке. В собранном виде приспособление удобно для транспортировки, в т.ч. и в городском транспорте. [5]

Анализ известных способов измерения отклонений подкрановых путей показывает, что работы по их техническому обследованию на данный момент являются самым опасным и наименее производительным видом работ из входящих в комплекс по диагностированию грузоподъемных машин и их структурных единиц. Это обуславливает несомненную актуальность разработки специальных устройств для механизации и автоматизации работ по экспертному обследованию подкрановых путей.

Список литературы

[1] РД 22-28-35-99 «Конструкция, устройство и безопасная эксплуатация рельсовых путей башенных кранов». -М.: Изд-во ЗАО НТЦ «Промышленная безопасность», 2005. 98 с.

[2] Диагностирование грузоподъемных машин / В.И. Сероштан [и др.] / под. ред. В.И. Сероштан, Ю.С. Огаря. -М.: Машиностроение, 1992. 192 с.

[3] Рахаев В.В., Головин А.И. Устройство крановых путей грузоподъемных машин: учебное пособие. – М.: Издательство МГТУ им. Н.Э. Баумана, 2012. 48с.

[4] РД 10-138-97 «Комплексное обследование крановых путей грузоподъемных машин. Часть 1. Общие положения» -М.: Изд-во ЗАО НТЦ «Промышленная безопасность», 2010. 145 с.

[5] Г.А. Шеховцов. Современные методы геодезического контроля ходовой части и путей мостовых кранов. Монография. Нижний Новгород, 1999. 164 с.

Рыжов Кирилл Сергеевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: ryjov.kirill@yandex.ru

Витчук Павел Владимирович – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: zzzventor@ya.ru

Н.А. Витчук, Н.Н. Курдюбов

СПОСОБЫ ОПРЕДЕЛЕНИЯ ТЯГОВОЙ СПОСОБНОСТИ ПЕРЕДАЧ ТРЕНИЕМ С ГИБКИМ ЭЛЕМЕНТОМ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Передача трением с гибким тяговым элементом – это способ передачи вращательного движения (или преобразования вращательного движения в поступательное) и момента через гибкую связь на основе использования сил трения между тяговым элементом и шкивами [1]. Примерами применения таких передач могут служить ременные передачи, вариаторы скорости, лифтовые канатоведущие шкивы, приводные барабаны ленточных транспортеров, ленточные тормоза грузоподъемных кранов и другие [1–4].

Интегральным показателем работоспособности передачи трением с гибким элементом, а также количественной мерой оценки ее тяговой способности служит коэффициент тяговой способности $e^{f\alpha}$, который выражается из классической формулы (неравенства) Эйлера [5]:

$$\frac{T_1}{T_2} \le e^{f\alpha},$$

где e = 2,72... – основание натурального логарифма; T_1 – большая сила натяжения гибкого элемента; T_2 – меньшая сила натяжения гибкого элемента; α – угол обхвата гибким элементом поверхности трения; f – приведенное значение коэффициента трения между гибким элементом и поверхностью трения.

В реальных передачах трением тяговая способность зависит от многих конструктивных параметров гибкого элемента и поверхности трения (например, от толщины гибкого элемента, радиуса изгиба и др.), которые не учитываются формулой Эйлера [6]. Это обуславливает необходимость экспериментального исследования тяговой способности этих передач.

Одна из простейших установок для экспериментального исследования тяговой способности передач трением с гибким тяговым элементом разработана и изготовлена на кафедре «Подъемно-транспортные системы» МГТУ им. Н.Э. Баумана (рис. 1) [7]. Она включает в себя червячный редуктор с рукоятью, установленный на стойке, рычажную систему, динамометр, грузы, набор сменных гибких тяговых элементов и поверхностей трения (шкивов). В качестве гибких тяговых элементов используют стальные круглопрядные канаты, специальный резиновый жгут с метками и стальную ленту с наклеенными на ее поверхности тензодатчиками.

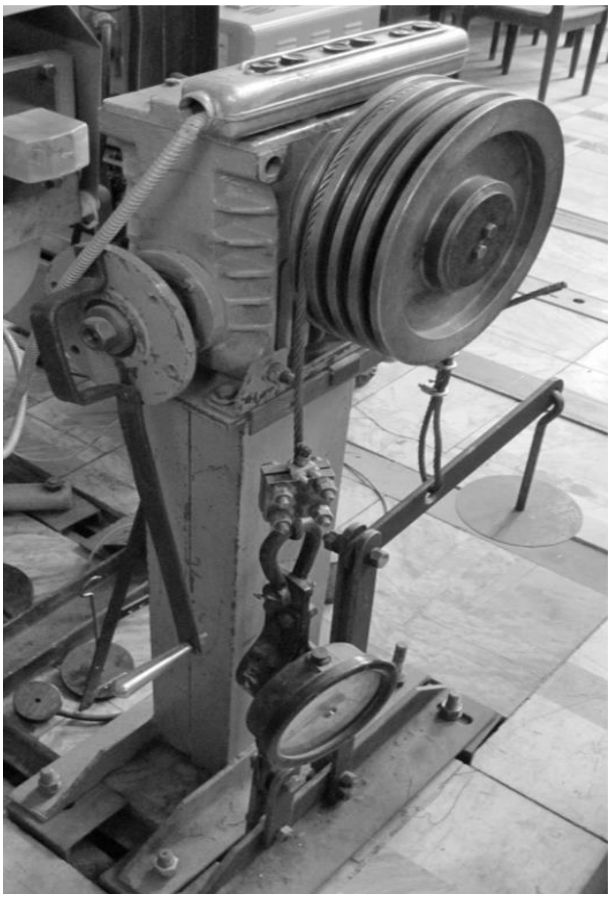


Рис. 1. Установка для исследования тяговой способности передач трением (МГТУ им. Н.Э. Баумана) [7]

На кафедре «Транспортно-технологические машины и оборудование» Пензенского государственного университета (ПГУ) исследование тяговой способности лифтового канатоведущего шкива в зависимости от величины угла обхвата α, профиля ручья и натяжения сбегающей ветви T_2 осуществляется на экспериментальной установке, которая выполнена в виде лебедки с канатоведущим шкивом (рис. 2) [8]. Тяговая способность канатоведущего шкива исследуется путем измерения натяжения набегающей ветви T_1, при различных значениях T_2, f, α в момент кратковременного включения двигателя лебедки пускателем 9. При этом канат плавно натягивается за счет большого передаточного отношения редуктора, а затем проскальзывает по ручью.

На кафедре «Подъемно-транспортные машины и оборудование» Тульского государственного университета исследование тяговой способности приводного барабана ленточного конвейера проводится в зависимости от наличия или отсутствия отклоняющего и прижимного роликов, а также тяговых усилий в набегающей и сбегающей ветвях конвейерной ленты (рис. 3) [8].

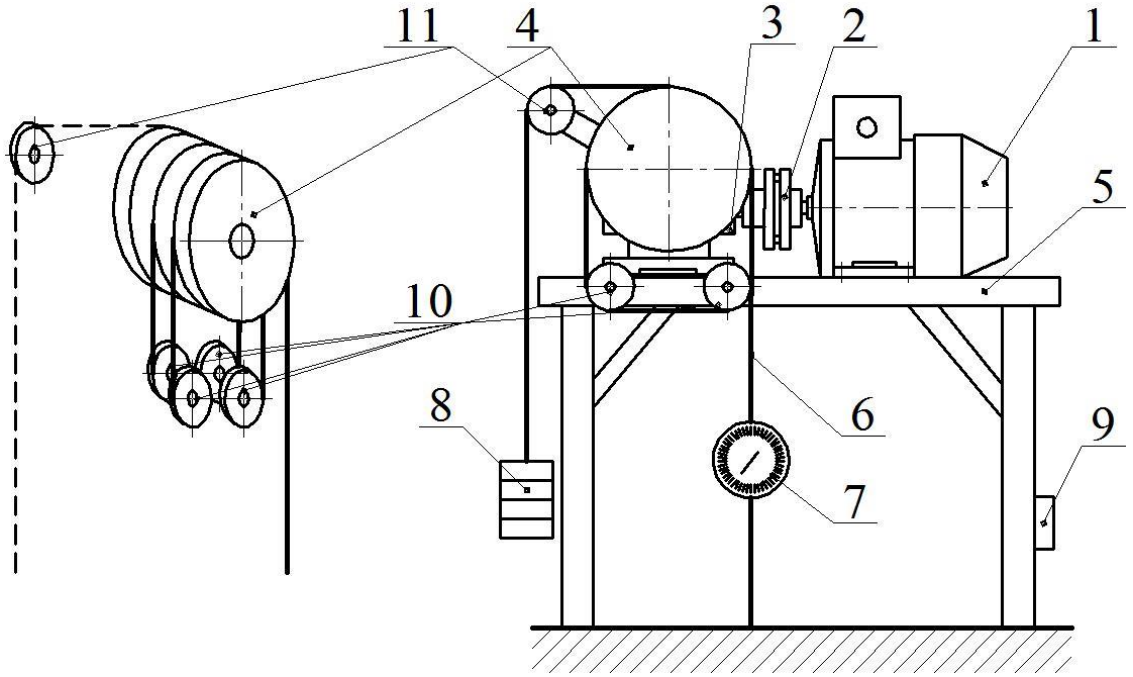


Рис. 2. Установка для экспериментального определения тяговой способности лифтового канатоведущего шкива (ПГУ): 1 – двигатель; 2 – муфта; 3 – редуктор; 4 – канатоведущий шкив; 5 – рама; 6 – канат; 7 – динамометр; 8 – подвеска; 9 – пульт управления лебедкой; 10 – оси с двумя холостыми блоками; 11 – ось с одним холостым блоком [7]

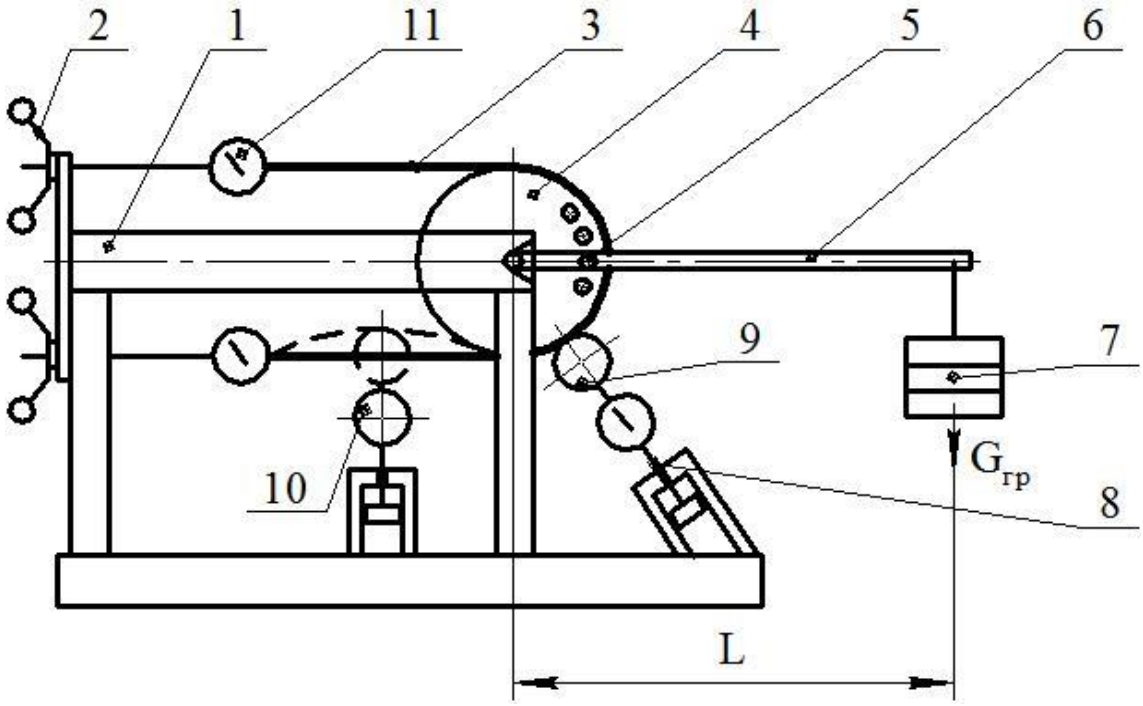


Рис. 3. Установка для исследования тяговой способности приводного барабана ленточного конвейера (ТулГУ): 1 – рама; 2 – винтовая пара; 3 – лента; 4 – барабан; 5 – фиксатор; 6 – рычаг; 7 – груз; 8 – динамометр; 9 – прижимной ролик; 10 – отклоняющий ролик; 11 – динамометр

Известна также конструкция трибометра [6] для непосредственного определения тяговых характеристик трения гибких материалов в расширенном диапазоне изменения угла обхвата направляющей гибким телом и сравнительного анализа характеристик трения гибких тел разной формы с учётом условий их нагружения в различных ремённых передачах с предварительным натяжением ремня. Конструкция данного устройства представлена на рис. 4 и рис. 5. На рис. 4 представлена кинематическая схема трибометра, а на рис. 5 показана схема взаимодействия подпружиненной собачки с храповым колесом, сблокированным с поворотным шкивом, образующим пару трения с испытуемым изогнутым гибким телом.

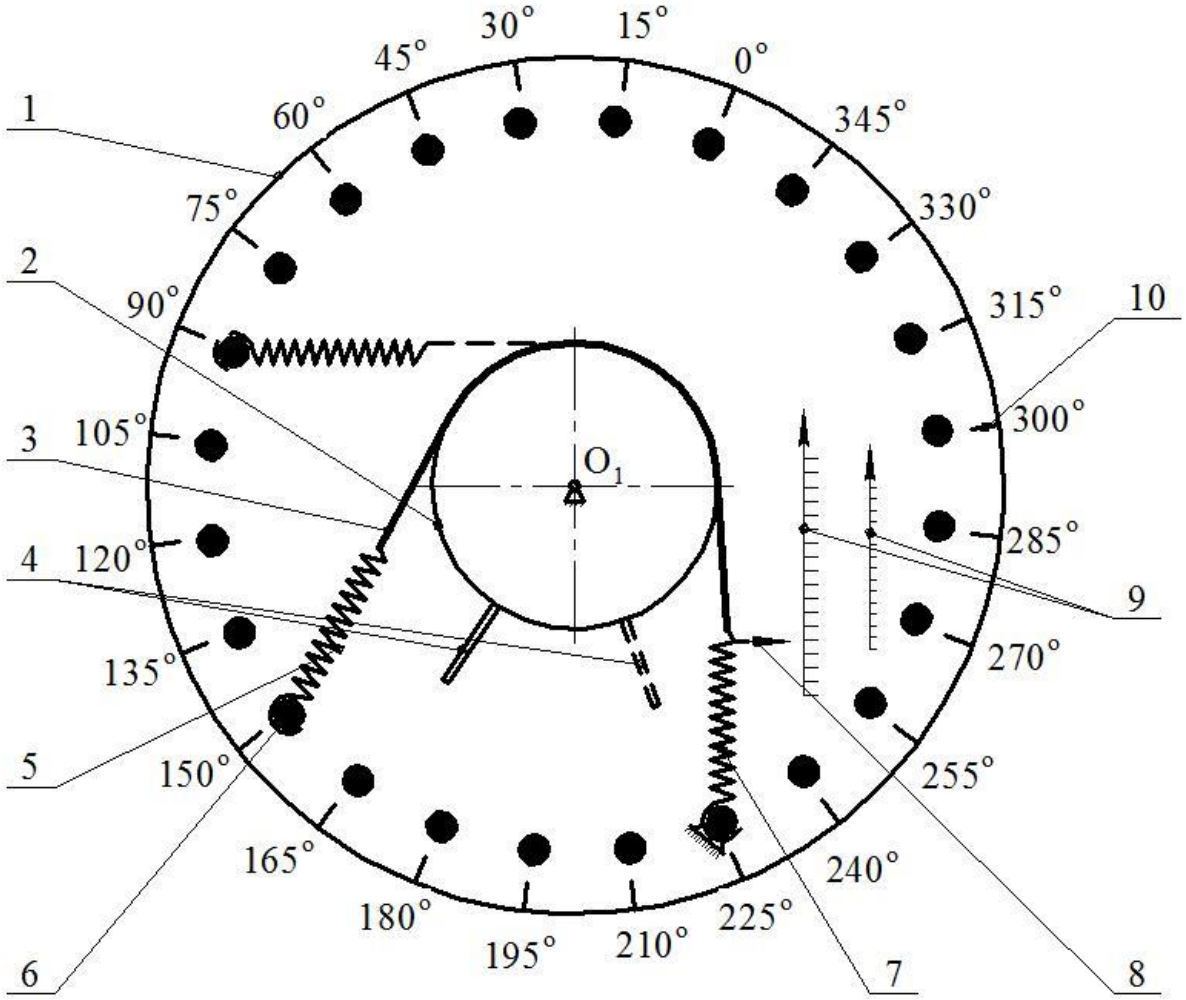


Рис. 4. Устройство трибометра

Указанный трибометр содержит корпус 1, установленную на корпусе направляющую (в виде поворотного шкива 2) для размещения на ней испытуемого гибкого тела 3 и привод ее поворота в виде рычага углового поворота 4.

Узел нагружения гибкого тела 3 состоит из шарнирно присоединенного к корпусу 1 упругого элемента 5, соединяющего концы гибкого тела 3 с шарнирными опорами фиксаторов 6 упругого элемента 5.

Узел измерения натяжения включает в себя динамометр 7 с измери-

тельной стрелкой 8 и сдвоенную шкалу-линейку 9 для одновременного измерения нескольких характеристик трения.

Помимо этого, трибометр содержит узел изменения угла обхвата α в виде расположенных на окружности корпуса 1 вокруг оси O_1 фиксаторов 6, совмещенных с круговой измерительной шкалой угла обхвата 10.

Кроме рассмотренных выше, существует множество устройств для определения тяговой способности передач трением с гибким элементом. Эти устройства следует использовать при проектировании новых и модернизации существующих устройств, в основе которых лежит принцип передачи трением с гибким элементом. Кроме того, подобные экспериментальные исследования позволят уточнить формулу Эйлера на основе введения в нее соответствующих коэффициентов и, тем самым, повысить ее точность при решении конкретных проектных задач.

Список литературы

[1] Иванов М.Н. Детали машин. – М.: Высшая школа, 2000. 383 с.

[2] Иоффе Е.Я. Высокоскоростные лифты. –М.: Стройиздат, 1988. 92 с.

[3] Зенков Р.Л. Машины непрерывного транспорта: учеб. для студентов вузов / Р.Л. Зенков, И.И. Ивашков, Л.Н. Колобов. –М.: Машиностроение, 1987. 432 с.

[4] Лалаянц Р.А. Расчеты крановых механизмов и их деталей. – СПб.: ВНИИПТМАШ. 1993. 324 с.

[5] Исследование тяговой способности канатоведущего шкива лебедки: метод. указания к лаб. работе по курсу «Подъемники» / Курносов Н.Е., Лобачев В.В. [и др.] / Под. ред. Н.Е. Курносова. –Пенза: Изд-во ПГУ, 2009. 12 с.

[6] Пожбелко В.И. Экспериментальное исследование тяговых свойств трения без смазки гибких тел в ременных передачах // Вестник ЮУрГУ серия «Машиностроение». –Челябинск: Изд-во ЮУрГУ, 2015. №15 (1). С. 26-34.

[7] Семенов Л.Н. Передача силы трением гибкого элемента о шкив: метод. указания к лаб. работам. – М.: МГТУ им. Н.Э. Баумана, 1970. 22 с.

[8] Толоконников А.С. Машины непрерывного транспорта: метод. указания к лаб. работам. – Тула: Изд-во ТулГУ, 2012. 53 с.

Витчук Наталья Андреевна – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: vitchuk.natalya@yandex.ru

Курдюбов Николай Николаевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: nkurdyubov@gmail.com

А.А. Шубин, В.В. Фадеев

ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ЭФФЕКТИВНОСТИ ЭЛЕКТРОШПАЛОПОДБОЙКИ ВИБРАЦИОННОГО ТИПА

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

На железнодорожном транспорте для выполнения работ, связанных с очисткой или заменой материала балластной призмы, широко применяются высокопроизводительные щебнеочистительные и выправочно-подбивочно-рихтовочные машины и комплексы тяжелого типа. В то же время, для поддержания пути в рабочем исправном состоянии и обеспечения безопасности движения, срока службы рельсов и шпал, необходимо выполнять достаточно большие объемы работ при устранении перекосов, просадок и других дефектов, а также по ремонту и удалению с пути шпал, вышедших из строя и замены их новыми.

Для выполнения этих работ применяется разнообразный путевой инструмент и мобильные машины. Одной из ключевых технологических операций является уплотнение балласта под шпалой. Для этого используются шпалоподбойки различных модификаций [1]. Их работа основана на принципе ударного вибрационного уплотнения. Недостатком данной конструкции является расположение на значительном удалении источника возмущающих колебаний (дебаланса) от зоны уплотнения, а также малая производительность, вследствие уплотнения балласта только непосредственно в зоне подбивочного полотна.

В работах [2, 3] предложена новая конструкция шпалоподбойки с размещением дебаланса, максимально приближенным к зоне уплотнения и заменой ударного уплотнения вибрационным.

Процесс уплотнения осуществляют изменением относительного положения частиц балласта в некотором объеме: частицы начинают более плотно прилегать одна к другой, уменьшаются размеры воздушных промежутков между ними. Происходит это при вибрационном перемещении частиц под действием колеблющегося и внедряющегося внутрь балласта подбивочного полотна шпалоподбойки. Этот процесс сложно описать точными математическими зависимостями, так как он осуществляется при не постоянном силовом воздействии на балласт со стороны оператора и переменном сопротивлении частиц балласта (особенно щебеночного, ракушечного и т.п.) из-за неоднородной их формы, размера и пр.

В работе [4] приведены зависимости для расчета шпалоподбойки ударного типа. Использовать данную методику при расчете шпалоподбойки вибрационного типа не представляется возможным, вследствие различающихся принципов уплотнения балласта.

Наиболее полно теория уплотнения балласта подбивочными элементами вибрационного типа исследовано применительно к подбивочным машинам тяжелого типа [5]. Исследования ВНИИЖТ позволили установить, что основными параметрами виброуплотнения являются: амплитуда колебаний рабочего органа, частота колебаний, скорость обжатия балласта, время вибрирования, заглубления клина по вертикали, считая от постели шпал до нижней кромки подбойки, геометрические размеры клина.

Из приведенных параметров для расчета шпалоподбойки определяющими можно считать амплитуду и частоту колебаний, а также время вибрирования. Оптимальное значение амплитуды соответствует максимальному уплотнению балласта. Увеличение амплитуды больше оптимальной не приводит к повышению эффекта уплотнения. ВНИИЖТ по результатам исследований установлено, что среднее значение амплитуды для путевых машин составляет 4,5 мм, что согласуется с рекомендациями по амплитуде колебаний шпалоподбоек (от 3,2 до 4,5 мм).

Процесс уплотнения материала во времени происходит крайне неравномерно (рис 1); в первые 3-5 секунд его интенсивность наибольшая, затем постепенно уменьшается и процесс приобретает затухающий характер.

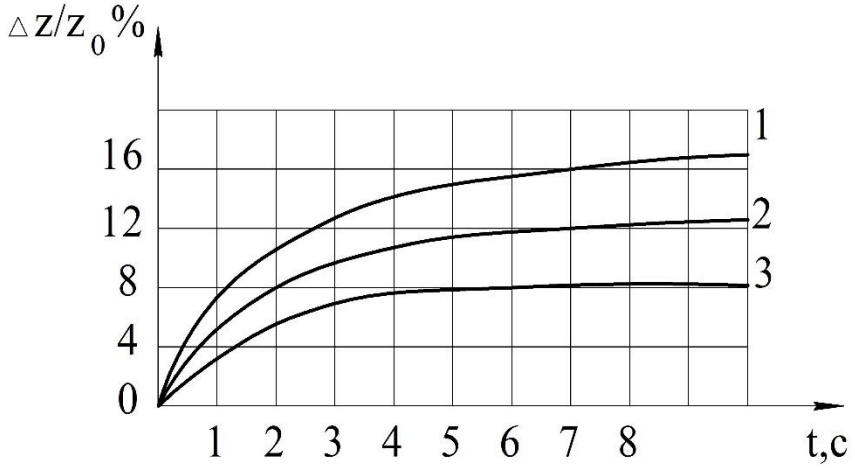


Рис.1. Зависимость эффекта уплотнения от времени вибровоздействия рабочего органа на балласт:

1- при A = 5 мм, ω = 200 $с^{-1}$, $V_{обж}$ = 120мм/с(оптимальные параметры)

2- при A = 3,8 мм, ω = 200 $с^{-1}$, $V_{обж}$ = 120мм/с

3- при A = 2,5 мм, ω = 200 $с^{-1}$, $V_{обж}$ = 120мм/с

Время вибрирования и частота колебаний определяют число вибровоздействий, передаваемых уплотняемому материалу, которое пропорционально произведению частоты на время ωt. Зависимость эффекта уплотнения от числа вибровоздействий имеет такой же характер, как приведенная на рис. 1. Число ωt определяет общее число активных и пассивных относительных перемещений частиц, происходящих в уплотняемом объеме за время вибрирования[6]. Для разных режимов виброобжатия общее число относительных перемещений, даже при одинаковом числе виб-

ровоздействий, может быть различным и зависит от условий использования пассивных относительных перемещений и охвата вибрированием уплотняемого материала.

Зависимость эффекта уплотнения от числа вибровоздействий можно представить в виде:

$$\Delta z / z_0 = \alpha\beta\omega t / (A' + B'\omega t), \qquad (1)$$

где $\Delta z / z_0$ - степень уплотнения балласта;

Δz - осадка слоя балласта при уплотнении;

z_0 - толщина рыхлого слоя;

α - коэффициент, определяющий степень использования для уплотнения пассивных и активных относительных переменных частиц;

β - коэффициент, определяющий долю объема материала, охватываемого относительными перемещениями;

A' и B' - эмпирические коэффициенты, зависящие от рода уплотняемого материала и способа вибровоздействия.

Соотношение (1) выражает зависимость эффекта уплотнения от произведения ωt, пропорционального числу вибровоздействий, передаваемых уплотняемому материалу, с учетом использования для уплотнения пассивных и активных относительных перемещений частиц и охвата относительными перемещениями уплотняемого объема материала. Это соотношение справедливо для всех возможных режимов и способов уплотнения и подтверждается экспериментально.

При полном использовании отдачи балласта каждому вибровоздействию и связанным с ним активным относительным перемещениям соответствует такое же число пассивных относительных перемещений, т. е, общее число относительных перемещений удваивается (коэффициент α = 2). Если отдача балласта не используется (безотрывные режимы взаимодействия), периодические активные и пассивные относительные перемещения частиц не происходят и материал не уплотняется (коэффициент α = 0).

Коэффициент β изменяется от 0 до 1 и определяет долю уплотняемого объема балласта, охватываемого относительными перемещениями. При $\beta = 1$ весь уплотняемый объем охватывается вибрированием; при $\beta = 0$ частицы балласта не имеют относительных перемещении и уплотнение не происходит.

Предельное уплотнение при бесконечно большом числе вибровоздействий имеет вид:

$$(\Delta z / z_0)_{пр} = \lim_{\omega t \to \infty} \Delta z / z_0 = \lim_{\omega t \to \infty} \alpha\beta\omega t / (A' + B'\omega t) = \alpha\beta / B'. \qquad (2)$$

Следовательно, предельное уплотнение материала зависит от коэффициентов α и β, которые для разных режимов различны. Поэтому предельное уплотнение также различно для разных режимов. Для щебе-

ночного балласта эмпирические коэффициенты A' и B' соответственно равны 3300 и 10, следовательно, предельное уплотнение при $\alpha=2$ и $\beta=1$ по формуле (2) составляет 0,2 или 20% по относительной осадке.

В процессе выполнения данной работы были определены факторы, влияющие на эффективность виброуплотнения балласта, а также выбран критерий оценки эффекта уплотнения.

Список литературы

[1] Путевой механизированный инструмент: справочник. В.М. Бугаенко, Р.Д.Сухих, И.М. Пиковский и др. / – под ред. В.М. Бугаенко, Р.Д.Сухих-М.: Транспорт, 2000. 368с.

[2] Шубин А.А., Витчук П.В., Фадеев В.В. Повышение эффективности работы вибрационной шпалоподбойки// Научный альманах. Издательство: ООО «Консалтинговая компания Юком» Тамбов. ISSN: 2411-7609 [http:www.elibrary.ru/item.asp?id=25314254]

[3] В.В. Фадеев, А.А Шубин, Н.М. Борискина. Совершенствование конструкции вибрационной шпалоподбойки// Наукоемкие технологии в приборо- и машиностроении и развитие инновационной деятельности в вузе: материалы Региональной начно-технологической конференции студентов, аспирантов и молодых ученых МГТУ им. Н.Э.Баумана, 2016- с.184-186.

[4] Путевые механизмы и инструменты / Р.Д. Сухих, В.М. Бугаенко, Ю.С. Огарь, В.Д. Ермаков, И.М. Пиковский, А.В. Пронченко; под общей ред. Р.Д. Сухих. – М.: УМК МПС, 2002. – 428 с.

[5] Путевые машины для выправки железнодорожного пути, уплотнения и стабилизации балластного слоя. Технологические системы: Учебное пособие для вузов ж.-д. Транспорта/ А.В. Атаманюк, В.Б. Бредюк, В.М. Бугаенко и д.р.; Под ред. М.В. Поповича, В.М. Бугаенко. – М.: ГОУ «Учебно-методический центр по образованию на железнодорожном ранспорте», 2008-285с.

[6] Новые путевые машины: (Подбивочно - выправочные и рихтовочная ВПР-1200, ВПРС-500 и Р-2000) / Ю.П. Сырейщикова. - М.: Траспорт. 1984.-317 с.

Шубин Александр Анатольевич – канд. техн. наук, заведующий кафедрой "Детали машин и подъемно-транспортное оборудование" КФ МГТУ им. Н.Э. Баумана. E-mail: shubin55@mail.ru

Фадеев Владимир Владимирович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: fadeev.volodya2010@yandex.ru

А.О. Петрухин, Д.Г. Мокин

УМЕНЬШЕНИЕ РАСКАЧИВАНИЯ ГРУЗА ПРИ ПОДЪЕМЕ СТРОИТЕЛЬНЫМ ПОРТАЛЬНО-СТРЕЛОВЫМ КРАНОМ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Портальные краны применяют на погрузочно-разгрузочных работах на заводах стройиндустрии и в гидротехническом строительстве. В настоящее время большую часть грузоподъемной техники составляют морально устаревшие краны. Покупать новую технику зачастую представляется трудно решаемой задачей, а имеющиеся краны не соответствуют современным требованиям. Решение этой проблемы является модернизация существующих портальных кранов.

Одной из наиболее серьезных проблем, которые необходимо решить это уменьшить раскачивание груза при подъеме/опускании. Необходимо это для того чтобы обеспечить точность подачи груза на требуемое место, тем самым можно уменьшить время работы и уменьшить износ механизмов крана.

Рассмотрим возможные методы технического решения, способствующие уменьшению раскачивания груза при выполнении подъема/опускания.

Одним из основных средств для предотвращения раскачиваний груза является пространственная запасовка канатов. Эта тенденция особенно проявилась в связи с появлением большой группы кранов, оборудованных автоматическими захватами.

При проектировании пространственных схем стремятся запасовать канаты в виде буквы “Y” для создания наибольшей жесткости подвеса в направлении движения груза. Такая “Y” – образная запасовка эффективна лишь при значительных углах наклона канатов, которые часто ограничиваются конструктивными соображениями.

Известны схемы с раздвижными тележками и блоками, которые позволяют регулировать угол наклона канатов. Применяются схемы с дополнительными оттяжными канатами, которые имеют много разновидностей: дополнительные канаты могут крепиться к подвижным противовесам, следящим барабанам или грузогидродемпферам. Кроме ограничения раскачиваний они часто служат для разворота груза и демпфирования крутильных колебаний. Существуют грузовые подвески крана с шарнирно закрепленными на тележке гидроцилиндрами, которые служат для уменьшения колебаний грузозахватного органа.

Для уменьшения раскачивания груза при изменении его пространственного положения можно достигнуть, обеспечив плавное протекание

переходных процессов, которое может осуществляться за счет регулирования угла наклона канатов с помощью углового датчика. Вся суть этого метода заключается в том, что при превышении угла наклона канатов отключаются механизмы, участвующие в подъеме груза, до тех пора, пока угол наклона не достигнет допустимого, затем операции, связанные с изменением пространственного положения груза, продолжают выполнять.

Также возможно предотвратить раскачивание груза в продольном и поперечном направлениях установив устройство для гашения колебаний груза. Оно содержит корпус, внутри которого через подшипники, симметрично установленные относительно центральной вертикальной оси устройства, установлена с возможностью поворота относительно центральной поперечной горизонтальной оси устройства горизонтальная рама. Технический результат - повышение эффективности гашения колебаний и расширение конструктивных особенностей.

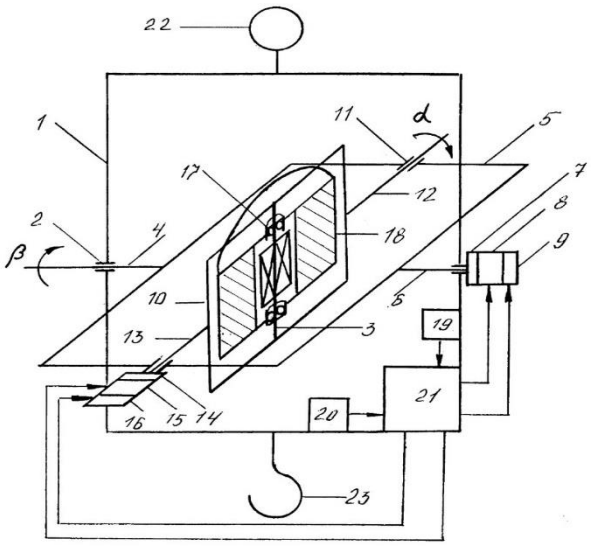


Рис.1 Устройство для гашения колебаний груза.

1 - корпус, 2 - горизонтальная рама, 3 - подшипники, 4, 8, 13 - вал, 5, 9, 10 - ось, 6 - вертикальная рама, 7, 17 - подшипники, 11, 20 - датчик периода колебаний, 12, 22 - подвеска, 14 - редуктор, 15 - прецессионный двигатель, 16 - тормоз,18 - асинхронный двигатель, 19 - датчик угла наклона, 21 - микропроцессорный блок, 23 - грузовой крюк.

Оценивая меры, направленные на решение данной проблемы можно признать целесообразным устанавливать устройство для гашения колебаний в продольном и поперечных направлениях. Использование этого технического решения позволит повысить долговечность механизмов крана, участвующих при подъеме груза.

Список литературы

[1] Ерзутов Александр Васильевич, Затравкин Михаил Иванович, Каминский Леонид Станиславович, Пятницкий Игорь Андреевич, Фёдоров Игорь Германович Патент №2422354 Способ уменьшения раскачивания груза при подъеме стреловым краном и система для его осуществления.

[2] Голдобина Любовь Александровна, Орлов Павел Сергеевич, Орлов Артем Павлович Патент №2280607 - Устройство для гашения колебаний груза, подвешенного на канате строительного крана.

Мокин Дмитрий Геннадьевич – канд. техн. наук, доцент кафедры "Детали машин и подъемно-транспортное оборудование" КФ МГТУ им. Н.Э. Баумана. E-mail: mdg-80@yandex.ru

Петрухин Артем Олегович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: artem-petruhin@mail.ru

Н.П. Сибилёв

УСТРОЙСТВО ДЛЯ ПОЛУЧЕНИЯ ИЗДЕЛИЙ ИЗ КОМПОЗИЦИОННЫХ МАТЕРИАЛОВ

КФ МГТУ им. Н.Э. Баумана, Калуга, 248000, Россия

Устройство для получения изделий из композиционных материалов

В качестве конструкционных материалов в настоящее время находят широкое применение композиционные материалы (КМ). Среди них значительный интерес вызывают волокнистые композиционные материалы (ВКМ) с металлической матрицей [1]. У этих ВКМ армирующими элементами могут быть тонкие проволоки из вольфрама, бериллия, титана, стальные и из других металлов, волокна борные, углеродные, карбидокремниевые (SiC), а матрицей - алюминиевые сплавы и другие металлы [2]. Сочетания армирующих элементов, обладающих высокими прочностными и жесткостными характеристиками с матрицами малой плотности, дает возможность получить ВКМ со своими новыми свойствами.

Рассмотрим ВКМ системы алюминий-бор (Al-B), у которого армирующим компонентом служат борные волокна, а матрицей сплавы алюминия. Получение ВКМ также является и процессом получения конструкционных элементов, например, труб, широко используемых в различных конструкциях из трубчатых стержней. Однако технологический процесс получения труб круглого сечения из ВКМ имеет свои особенности, которые накладывают определенные требования на устройства и оснастку используемые при их изготовлении.

В качестве заготовок труб используют плазменно-напыленные полуфабрикаты (ПНП), которые получают плазменным напылением алюминиевой матрицы на борные волокна, намотанные с принятым шагом на барабан[3]. Известно, что плазменное напыление является процессом нестационарным, поэтому слои матрицы в ПНП имеют отклонения от номинальных параметров по толщине и плотности[4].

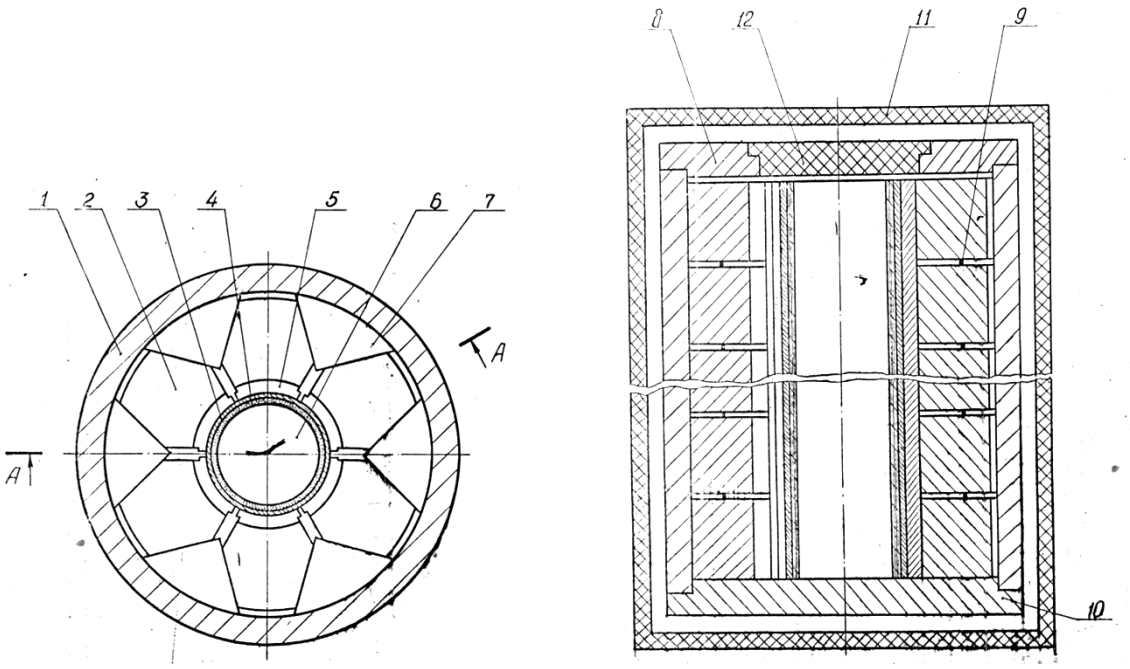
Сборку заготовки трубы проводят наворачиванием на цилиндрическую оправку в виде рулона ПНП наложенного на фольгу из алюминиевого сплава АМг2Н толщиной 100*мкм*, к которой встык прикреплена фольга толщиной 30*мкм* и в конце рулона также встык прикреплена фольга толщиной 150*мкм*.Фольга толщиной 150*мкм* и толщиной 100*мкм* предназначены для антикоррозионной защиты трубы. Кроме того наружный слой из фольги толщиной 150*мкм* предназначен для соединения трубы с закон-

цовками, необходимыми для сборки трубы из ВКМ в узле изделия. При сборке заготовки трубы ПНП располагают так, чтобы волокна были параллельны оси трубы.

Ширину фольги в направлении наворачивания рулона принимают: для фольги толщиной 100*мкм* - равной ширине развертки первого от оправки оборота в рулоне, для 30*мкм* - равной ширине развертки второго и последующих оборотов в рулоне, с количеством оборотов необходимых для толщины стенки трубы, толщиной 150*мкм* - равной ширине развертки последнего в рулоне оборота плюс 8...12*мм* для нахлеста, с целью получения на нем возможности предотвращения разворачивания рулона путем постановки на нахлесте нескольких точек точечной сварки.

Собранная заготовка трубы имеет неплотности, которые необходимо устранить при компактировании её в термокомпрессионной установке. Возможным для получения трубчатых изделий является метод термокомпрессионного компактирования ВКМ, который заключается в деформировании неплотных заготовок под действием перемещения рабочих деталей оснастки, выполненных из материалов, обладающих различными значениями термического коэффициента линейного расширения (ТКЛР). Этот метод обеспечивает возможность статического горячего компактирования армированных заготовок и может быть использован для изготовления длинномерных трубчатых изделий. Основным недостатком этого метода является малая величина абсолютных тепловых перемещений рабочих деталей и их малая скорость. Для решения этой задачи в процессе горячего прессования трубы используют компенсирующую оболочку в виде цилиндрических втулок из Al. Втулки надевают на собранную на оправке заготовку трубы из ВКМ, плотно прижимая их друг к другу в осевом направлении. Для того чтобы полностью прошел процесс горячего прессования стенки трубы, т.е. чтобы матрица затекла во все имеющиеся пустоты, подверглась уплотнению и прочному адгезионному соединению с поверхностями волокон, необходимо иметь расчетный избыток материала компенсирующей оболочки, который при достижении нужного давления должен истекать в облойные полости. Это достигается созданием условий всестороннего радиального обжатия заготовки трубы при изотермическом процессе.

С целью получения труб из ВКМ предложена термокомпрессионная установка (Рис. 1)



а) б)

Рис.1 Схема термокомпрессионного устройства
а - горизонтальное сечение термокомпрессионного устройства; б - вертикальное сечение (А-А) термокомпрессионного устройства; 1 - обойма: 2 - рабочие клиновые вкладыши; 3 - технологическая оболочка; 4 - заготовка; 5 - сегментные проставки; 6 - оправка; 7 - опорные вкладыши; 8 - верхняя плита; 9 - компенсационные прокладки; 10 - нижняя плита; 11 - теплозащитный кожух; 12 - крышка

Устройство состоит из массивной обоймы из прочного материала с относительно низким значением термического коэффициента линейного расширения (ТКЛР). Обойма установлена на нижнюю плиту; в полости обоймы размещены сопрягающиеся по участкам скосов рабочие подвижные клиновые и неподвижные опорные вкладыши из материала, например, марки 70ГНДХ, с высоким значением ТКЛР. В осевой зоне полости обоймы расположена цилиндрическая оправка из того же материала с высоким значением ТКЛР. На оправке установлена сборная заготовка трубы из ВКМ, находящаяся в технологической оболочке.

Между оболочкой и рабочей поверхностью клиновых подвижных вкладышей размещена система сегментных проставок, между которыми образованы радиальные облойные полости, в которые происходит истечение избытка материала технологической оболочки. Рабочие подвижные и неподвижные вкладыши выполнены секционными, между секциями расположены кольцевые, проволочные компенсационные прокладки. Система "вертикальной компенсации" позволяет снизить контактные растягивающие напряжения, действующие на обойму и проставки, а через них на технологическую оболочку, матрицу и на волокна ВКМ, так как ТКЛР мате-

риала вкладышей значительно больше той же характеристики материалов обоймы и проставок. Кроме того, эта система позволяет компенсировать возможные различия теплопередачи при работе нагревателей на установках большой высоты, позволяет выполнять обойму сборной из колец высотой равной высоте клиновых секций или кратных им. Для уменьшения теплопотерь из рабочей зоны устройства, на обойму устанавливают верхнюю плиту с крышкой.

Процесс компактирования в устройстве рассматриваемой конструкции происходит следующим образом. При нагреве устройства, осуществляемом с помощью кольцевой вертикальной печи электросопротивления, в камеру которой помещается устройство, или с помощью системы термоэлектрических нагревателей (ТЭНов), размещаемых в вертикальных отверстиях опорных вкладышей (на рис. 1 ТЭНы не показаны) происходит тепловое расширение всех элементов устройства. В случае нагрева устройства ТЭНами, оно заключается в теплозащитный кожух (показан на рис. 1б).

Так как ТКЛР материала обоймы относительно мал, происходит встречное перемещение в радиальном направлении рабочих поверхностей оправки и подвижных клиновых вкладышей, причем перемещение последних обусловлено не только высоким ТКЛР их материала, но и наличием сопряжения участков скосов с поверхностями неподвижных вкладышей, материал которых имеет также высокий ТКЛР. В результате - сужается кольцевая полость между поверхностью оправки и внутренней поверхностью сегментных проставок, происходит компактирование трубной армированной заготовки, а фактический избыток материала технологической оболочки образует радиальные облойные выступы.

Определение параметров термокомпрессионной установки и элементов ее оснастки подтвердили ожидаемые результаты.

Список литературы

[1] Материаловедение: учебник для вузов / Б.Н. Арзамасов и др.; Под общ. ред. Б.Н. Арзамасова, Г.Г. Мухина. 8-е изд., стереотип. М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. 648с.

[2] Буланов И.М., Воробей В.В. Технология ракетных и аэрокосмических конструкций из композиционных материалов: Учеб. для вузов. М.: Изд-во МГТУ им.Н.Э. Баумана, 1998. - 516 с.

[3] Н.П. Сибилев, А.А. Шубин, А.А. Косенко Известия ТулГУ. Технические науки. Вып.11: в 2ч. Ч.2. Тула: Изд-во ТулГУ, 2014.с 506-512

[4] Механические свойства матрицы АД1, полученной плазменным напылением / В.В. Кудинов и др. // Композиционные материалы. М.: Наука, 1981.С.133-136

Сибилев Николай Пантелеевич – канд. техн. наук, доцент КФ МГТУ им. Н.Э. Баумана. E-mail: nikolaysibilev2@gmail.com

СОДЕРЖАНИЕ

НАУКОЕМКИЕ ТЕХНОЛОГИИ
В ПРИБОРО - И МАШИНОСТРОЕНИИ
И РАЗВИТИЕ ИННОВАЦИОННОЙ
ДЕЯТЕЛЬНОСТИ В ВУЗЕ

Материалы
Всероссийской научно-технической конференции

Том 3

Научное издание

Все работы публикуются в авторской редакции. Авторы несут ответственность за подбор и точность приведенных фактов, цитат, статистических данных и прочих сведений

Подписано в печать 15.11.2016.
Формат 60x90/16. Печать офсетная. Бумага офсетная. Гарнитура «Таймс».
Печ. л. 16. Усл. п. л. 14,88. Тираж 50 экз. Заказ № 174

Издательство МГТУ им. Н.Э. Баумана
107005, Москва, 2-я Бауманская, 5

Оригинал-макет подготовлен и отпечатан в Редакционно-издательском отделе
КФ МГТУ им. Н.Э. Баумана
248000, г. Калуга, ул. Баженова, 2, тел. 57-31-87