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
Региональной научно-технической конференции

Том 3

ИЗДАТЕЛЬСТВО
МГТУ
им. Н. Э. Баумана
Калуга 2017

УДК 378:001.891
ББК 74.58:72
Н34

Руководитель конференции:
С.А. Кусачева (председатель совета по НИР студентов и аспирантов)

Руководители направлений:
А.И. Пономарев (ф-т КМК), *Ю.С. Белов* (ф-т ФНК), *М.Ю. Адкин* (ф-т ЭИУК), *А.Г. Вяткин* (ф-т МТК), *О.А. Артеменко* (ф-т СЭК)

Руководители секций:
Е.Н. Малышев, Г.В. Орлик, В.В. Андреев, А.А. Жинов, Ю.П. Корнюшин, Н.Е. Шубин, А.И. Пономарев, А.К. Рамазанов, А.А. Анкудинов, Б.М. Логинов, В.Г. Косушкин, А.В. Мазин, А.А. Шубин, А.К. Горбунов, А.В. Максимов, В.Н. Пащенко, М.В. Астахов, Е.Н. Сломинская, О.Л. Перерва, Г.И. Ловецкий, А.Ю. Красноглазов, В.М. Алакин

Н34 **Наукоемкие технологии в приборо- и машиностроении и развитие инновационной деятельности в вузе:** материалы региональной научно-технической конференции, 18–20 апреля 2017 г. Т. 3. – Калуга: Издательство МГТУ им. Н. Э. Баумана, 2017. – 244 с.

В сборнике материалов Региональной 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

© Коллектив авторов, 2017
© Калужский филиал МГТУ им. Н. Э. Баумана
© Издательство МГТУ им. Н. Э. Баумана, 2017

СЕКЦИЯ 12.

СОВРЕМЕННЫЕ ТЕХНОЛОГИЧЕСКИЕ ПРОЦЕССЫ И МЕТОДЫ КОНТРОЛЯ В ЭЛЕКТРОНИКЕ И МИКРОЭЛЕКТРОНИКЕ

И.В. Максимов, В.В. Андреев

ЗАЩИТА ОТ СТАТИЧЕСКОГО ЭЛЕКТРИЧЕСТВА ВРЕМЯЗАДАЮЩЕЙ МИКРОСХЕМЫ КР512ПС10

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

Важной проблемой как в производстве, так и при эксплуатации КМОП-ИС является их стойкость к воздействию разряда статического электричества. Наибольшей чувствительностью, к такого рода воздействию обладают быстродействующие микросхемы с тонким подзатворным диэлектриком, выполненные по КМОП-технологии [1].

Представителем данного типа ИМС является времязадающая микросхема КР512ПС10, она предназначена для применения в бытовых таймерах и устройствах управления временной задержкой, реле времени электромеханических часах, и в качестве генератора импульсов низкой и инфранизкой частоты [2].

Для повышения стойкости данной ИМС к воздействию статического электричества применяются цепи защиты, которые располагают в непосредственной близости к контактным окнам выводов микросхемы. Элементы защиты обычно изготавливаются вместе с другими элементами микросхемы. В настоящее время наибольшей популярностью пользуются два типа защиты: диодно-резистивная и с использованием МОП-транзисторов [1].

В данной работе рассматривается применение защиты от воздействия статического электричества на основе МОП-транзисторов для повышения степени жесткости [3] микросхем КР512ПС10.

Уязвимым местом данной микросхемы, с точки зрения воздействия статическим напряжением, являются входные управляющие МОП-транзисторы. При воздействии на них статического электричества происходит пробой тонкого подзатворного окисла, вследствие этого повреждения, микросхема перестает функционировать. КР512ПС10 имеет диодно-резистивную защиту с допустимым значением статического потенциала не более 30 В (1 степень жесткости по ОСТ 11 073.062-2001) [4]. Данный вид защиты обеспечивает низкие защитные характеристики, что уменьшает выход годных кристаллов на пластине, а также существует большая вероятность вывода микросхемы из строя при монтаже.

Для уменьшения влияния статического электричества на КР512ПС10, диодно-резистивная защита была заменена защитой с использованием МОП-транзисторов. Принцип построения схемы защиты на МОП-транзисторе с заземленным затвором [5] представлен на рис. 1.

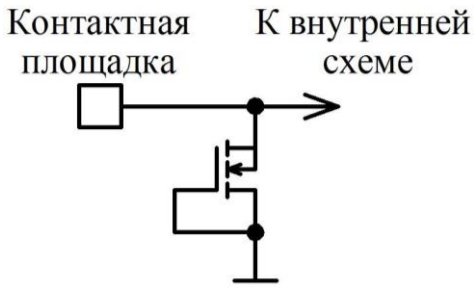

Рис. 1. Схема защиты на МОП-транзисторе.

После воздействия на выводы микросхемы, большой величины статического напряжения, потенциальный барьер между обедненными областями стока и истока уменьшается и происходит стекание статического заряда через открытые транзисторы, одновременно с этим может начаться протекание процесса пробоя подзатворного диэлектрика управляющих МОП-транзисторов. При малом времени стекания заряда в цепи защиты, этот процесс не успевает произойти, даже если он уже начался [1]. Поэтому необходимо обеспечить максимальную скорость стекания статического заряда через защитные транзисторы, она определяется длиной канала. При этом их зарядная емкость должна быть как можно меньше.

Чтобы исключить возможность срабатывания защиты от статического электричества, при напряжениях меньше предельно допустимого управляющего напряжения, в качестве защитных транзисторов, при конструировании, взяты транзисторы с пробивным напряжением выше напряжения питания микросхемы.

Цепь защиты от статического электричества, построенная с использованием нормально закрытых МОП-транзисторов представлена на рис. 2.

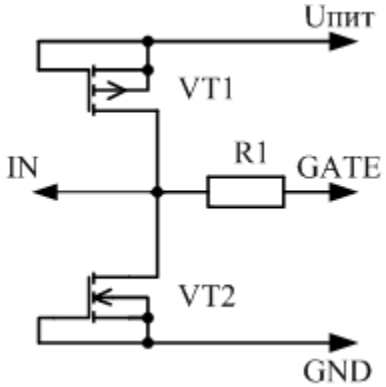

Рис. 2. Схема защиты от статического электричества на нормально закрытых полевых транзисторах

Для ограничения тока при воздействии статического заряда в цепи защиты используется резистор R1. Сопротивление цепи защиты влияет на быстродействие микросхемы, что отрицательно влияет на работоспособность данного типа микросхем, поэтому рекомендуется применять рези-

сторы номиналом от 100 до 500 Ом. Так как диффузионные резисторы занимают много места, сложны в изготовлении и оказывают влияние на подложку микросхемы, в качестве сопротивления в схеме защиты обычно используют пленочный поликремневый резистор [6].

Оценка влияния сопротивления управляющего входа на быстродействие микросхемы КР512ПС10, произведена при помощи компьютерного моделирования. Полученные результаты представлены на графике (рис. 3), где точками показаны установленные значения, прямой аппроксимация установленных значений.

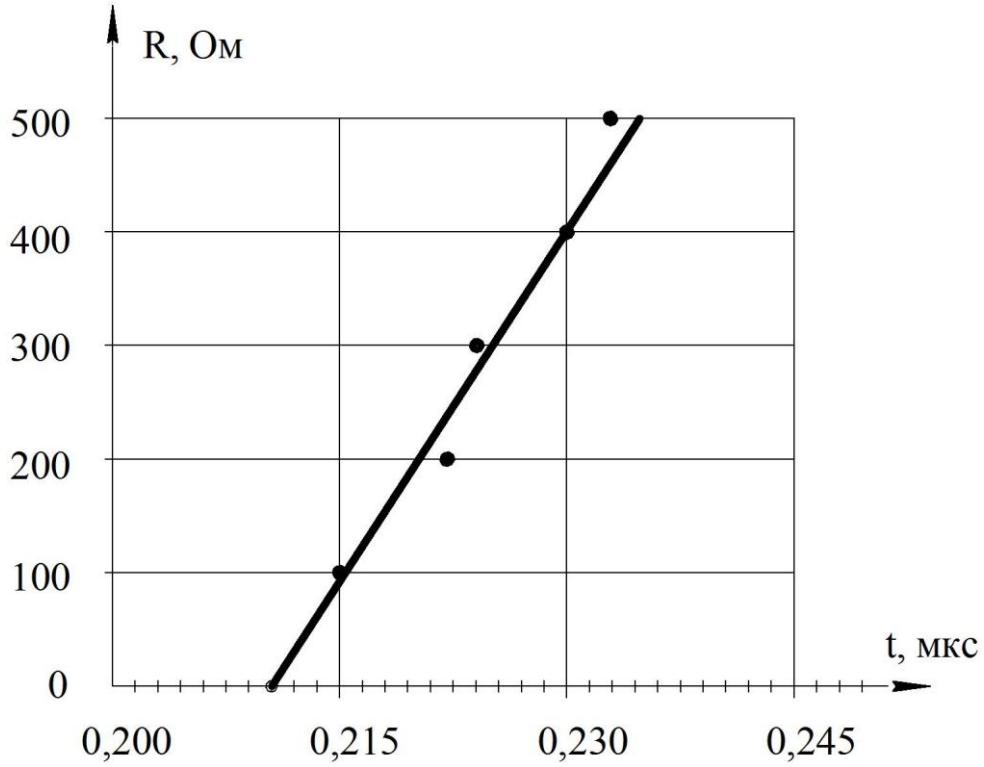

Рис. 3. Зависимость быстродействия микросхемы КР512ПС10 от сопротивления управляющего входа

Из рис. 3 видно, что с увеличением сопротивления возрастает время срабатывания. Следовательно, необходимо выбирать номинал резистора защитной цепи, удовлетворяющий производственным требованиям.

В соответствии с технологией изготовления и учитывая основные производственные параметры микросхемы КР512ПС10 разработанная защита на основе нормально закрытых МОП-транзисторов повышает степень жесткости ИМС до 3 степени по ОСТ 11 073.062-2001, что соответствует уровню статического напряжения 200 В [3].

В статье проведена оценка уровня защищенности микросхемы КР512ПС10 от воздействия разряда статического электричества, выявлены основные уязвимые элементы ИМС, рассмотрены базовые принципы построения схем защиты на основе МОП-транзисторов, описан механизм ра-

боты схемы защиты спроектированной на основе нормально закрытых МОП-транзисторов, указана необходимость применения резистивного элемента в цепи защиты и оценено его влияние на быстродействие микросхемы КР512ПС10, показана эффективность применения защиты на основе нормально закрытых МОП-транзисторов вместо диодно-резистивной защиты.

Список литературы

[1] Кечиев Л.Н., Пожидаев Е.Д. *Защита электронных средств от воздействия статического электричества.* – М.: Издательский Дом "Технологии", 2005. – Г.2, п.2.2 – 79 с.

[2] Бирюков С. Применение микросхемы КР512ПС10 // *Радио*. – 2000. – №8 – С. 44.

[3] ОСТ 11 073.062-2001 «Микросхемы интегральные и приборы полупроводниковые. Требования и методы защиты от статического электричества при разработке, производстве и применении».

[4] Бирюков С. Генератор-делитель частоты КР512ПС10 // *Радио*. – 2000. – №7 – С. 51.

[5] Максимов И.В., Андреев В.В., Столяров А.А. *Защита микросхем, изготовленных по КМОП-технологии от воздействия статического электричества.* Наукоемкие технологии в приборо - и машиностроении и развитие инновационной деятельности в вузе: материалы всероссийской научно-технической конференции, 15 - 17 ноября 2016 года. Т.1. – Калуга: Издательство МГТУ им. Н.Э.Баумана, 2016. С. 142-146.

[6] 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.

Максимов Игорь Владимирович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: igormaksimow@yandex.ru

Андреев Владимир Викторович – д-р техн. наук, профессор кафедры "Конструирование и производство электронной аппаратуры" КФ МГТУ им. Н.Э. Баумана. E-mail: andreev@bmstu-kaluga.ru

И.А. Рытиков, В.В. Андреев

ИССЛЕДОВАНИЕ ЗАВИСИМОСТИ ТОКА ПОТРЕБЛЕНИЯ МИКРОСХЕМЫ 5559ИН7Т ОТ ТЕМПЕРАТУРЫ

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

Микросхема 5559ИН7Т представляет собой сдвоенный приёмопередатчик манчестерского кода с установкой выходов приёмника в состояние низкого уровня при запрете приёма. Одним из основных параметров данной микросхемы является ток потребления (I_{CC}), который в соответствии с техническими условиями (ТУ) не должен превышать 24 мА. Следовательно, важной задачей является исследование зависимости тока потребления данной микросхемы от температуры при различных конструктивных решениях изготовления кристалла [1-3].

Данная работа посвящена исследования зависимости тока потребления микросхемы 5559ИН7Т от температуры при разных значениях номинала нагрузочного сопротивления микросхемы.

На рисунке 1 приведена часть схемы электрически принципиальной микросхемы 5559ИН7Т. Анализ этой схемы с использованием схемотехнического моделирования и макетирования показал, что ток потребления микросхемы сильно зависит от номинала резистора R22. Для определения оптимального значения номинала резистора R22 были изготовлены 4 партии микросхем 5559ИН7Т, где резистор R22 равен соответственно: 5,5 кОм, 6,5 кОм, 7 кОм, 8 кОм.

Для исследования зависимости тока потребления микросхемы 5559ИН7Т от температуры потребовалось разработать кассету для испытаний микросхемы в печи тепло-холод. Для проведения измерений параметров микросхемы в кассете и передачу данных на автоматизированную установку контроля электрических параметров микросхем на базе NI PXI EXPRESS, был разработан специальный коммутационный блок. Автоматизированная установка для контроля параметров микросхем 5559ИН7Т была разработана с использованием измерительных модулей на базе платформы NI PXI EXPRESS [4]. Исследования проводились на производственной базе АО "ОКБ МЭЛ" г. Калуга.

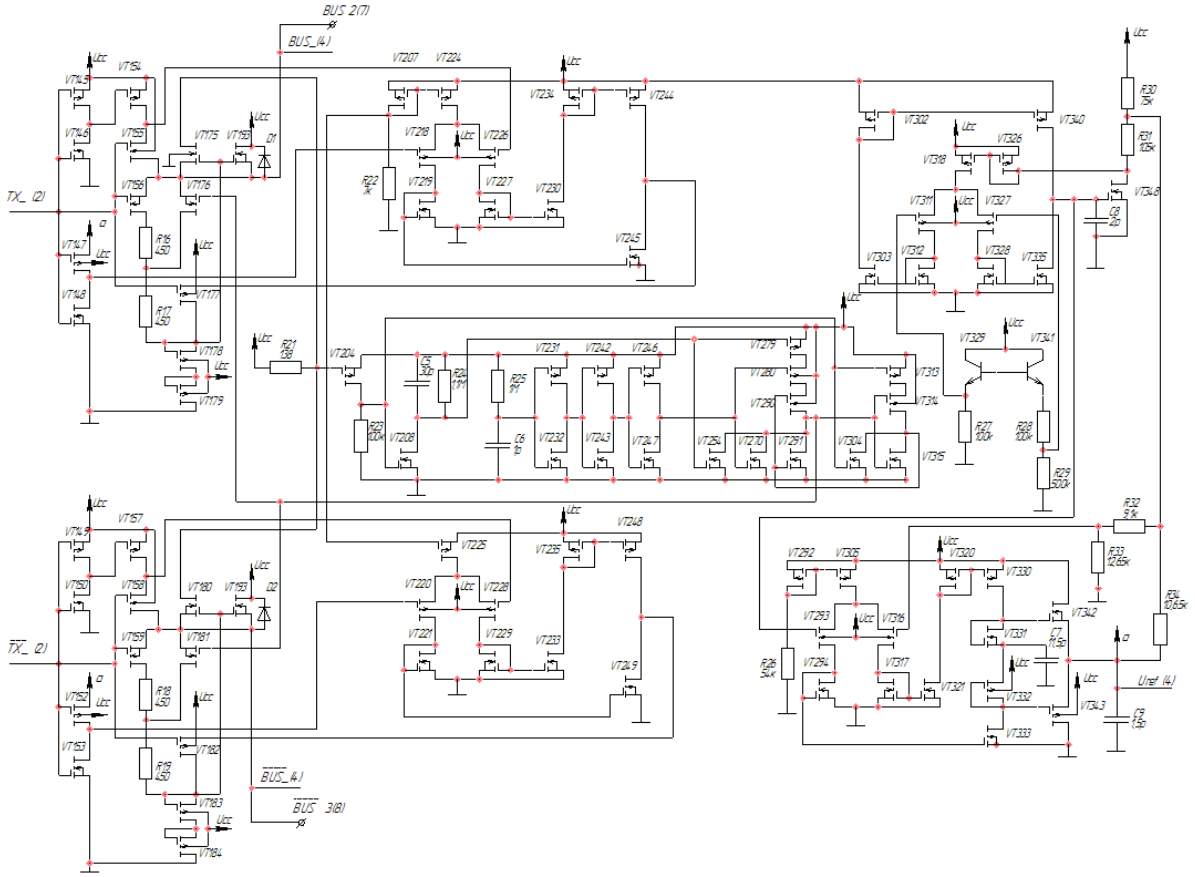

Рис. 1. Часть схемы электрической принципиальной микросхемы 5559ИН7Т

Параметры микросхемы 5559ИН7Т измерялась при значении питающего напряжения U_{CC}, равном 4,5 В. Измерения производились в диапазоне температур от -60 °С до +90 °С. В результате проведенных измерений, для четырех партий микросхем были получены зависимости тока потребления от температуры, приведенные на рисунке 2.

Из экспериментальных данных, приведенных на рис. 2, видно, что в партии микросхем с резистором R22 с номиналом 6,5 кОм ток потребления имеет более слабую температурную зависимость по сравнению с микросхемами из других партий, отличающихся значением нагрузочного резистора.

Таким образом, из полученных результатов можно сделать вывод, что оптимальным значением нагрузочного сопротивления является номинал в 6,5 кОм, поскольку при данном значении R22 слабо зависит от температуры и во всем температурном диапазоне остается ток потребления существенно ниже 24 мА.

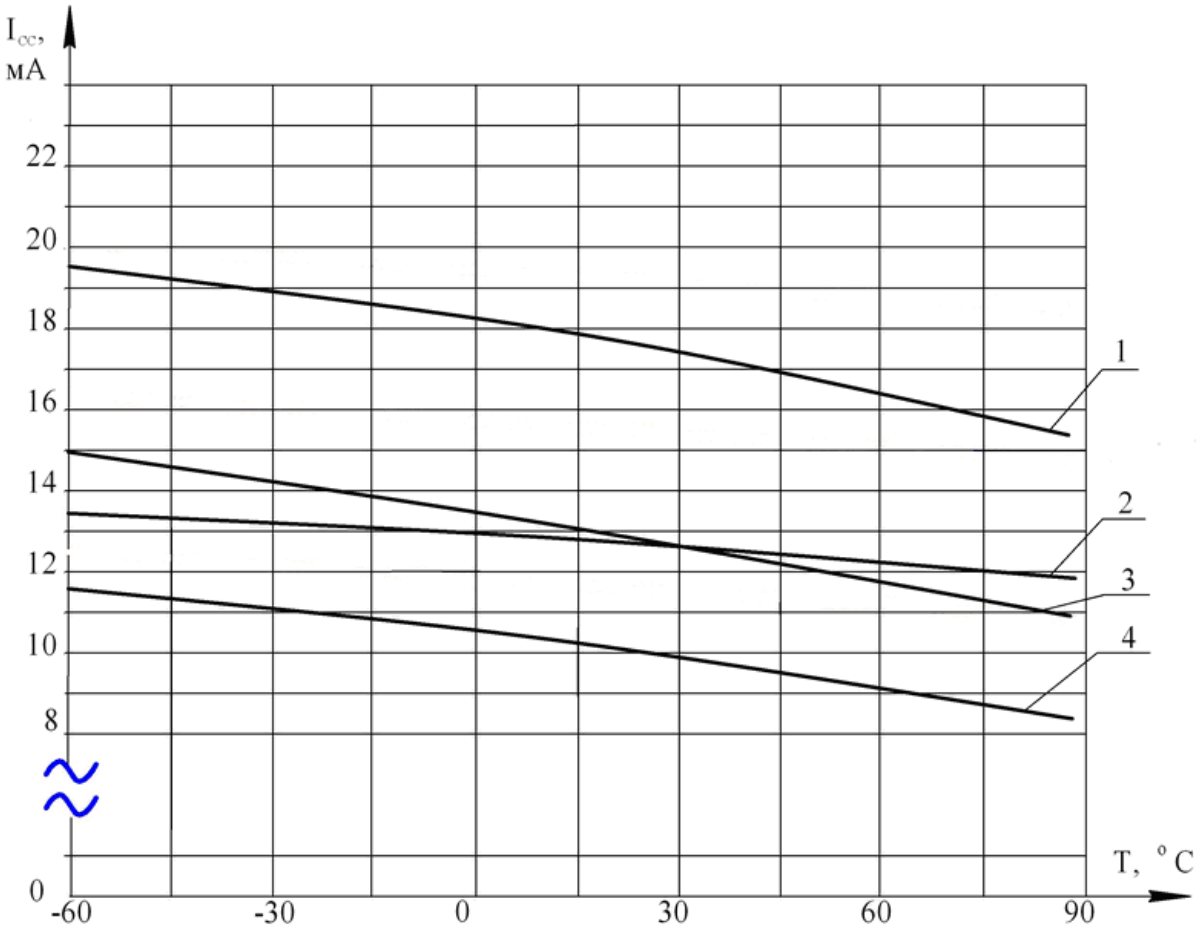

Рис. 2. График зависимости тока потребления I_{CC} от температуры при напряжении питания U_{CC}, равном 4,5 В, и различных значениях резистора R22: 1 – 5,5 кОм; 2 - 6,5 кОм; 3 - 7 кОм; 4 - 8 кОм

Список литературы

[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.

[4] http://www.okbmel.ru/wp-content/uploads/2014/11/

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

Андреев Владимир Викторович – д-р техн. наук, профессор кафедры "Конструирование и производство электронной аппаратуры" КФ МГТУ им. Н.Э. Баумана. E-mail: andreev@bmstu-kaluga.ru

А.В. Иванов, В.В. Кузнецов

ИССЛЕДОВАНИЕ СТОЙКОСТИ ЭЛЕМЕНТНОЙ БАЗЫ К ЭЛЕКТРОСТАТИЧЕСКОМУ РАЗРЯДУ

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

Целями данного исследования являются:

- ознакомление с воздействием электростатического разряда (ЭСР) на РЭА и рассмотрение ЭСР как источника электромагнитных помех.
- рассмотреть модели испытаний РЭА на воздействие ЭСР, создать модель стенда и разработать тестовые модели для имитации HBM и MM разрядов.
- произвести моделирование элемента защиты GGNMOST (n-МОП транзистор с заземлённым затвором), а также промоделировать воздействие ЭСР на целую ИМС серии 74HC.

Различают прямое и косвенное воздействие ЭСР на электронную аппаратуру. При прямом воздействии ЭСР возникают эффекты, связанные с инжекцией заряда в процессе электростатического разряда. Возникающий в результате ЭСР переходный процесс подаётся непосредственно на проводники или элементы конструкции системы. При косвенном воздействии ЭСР возникаю эффекты, связанные с электрическими и магнитными полями, порождёнными токами заряда. В этом случае эффекты связаны с излучаемыми электромагнитными помехами.

Для защиты РЭА от косвенного воздействия ЭСР применяются принципы конструирования РЭС те же, что и при защите от электромагнитных помех иного происхождения. Важна правильная экранировка электронных узлов и правильная разводка цепей заземления. Косвенное воздействие ЭСР как правило не приводит к необратимым повреждениям аппаратуры.

Наиболее опасным для электронных компонентов является прямое воздействие ЭСР. Оно может проявляться как в процессе производства, так и в процессе эксплуатации. При этом часто происходят необратимые повреждения полупроводниковых электронных компонентов.

Наиболее распространенными причинами, по которым могут возникать электростатические разряды, являются:

- люди;
- неправильное заземление;
- низкая влажность (высокая температура окружающей среды, ее сухость). При более чем 85-процентной влажности воздуха электростатические разряды практически не возникают;
- неэкранированные кабели;
- движущиеся механические детали;

– некачественные соединения.

Воздействие электростатических разрядов на полупроводниковые изделия:

Непосредственно перед ЭСР и в течение первых десятков нс разряда на изделия электронной техники (ИЭТ) действует наведённое высокое напряжение, являющееся источником тока. В связи с этим на изделие действует и потенциал электрического заряда, и ток разряда. У полупроводниковых приборов и ИС, на которые воздействовали ЭСР, могут иметь место два типа повреждений:

– катастрофические повреждения, обнаруживаемые наиболее легко, так как повреждённые изделия не выполняют своих функций;
– скрытые повреждения, затрагивающие только один из параметров: усиление, утечку и так далее, – или вызывающие некоторые изменения начальных характеристик, которые могут тем не менее не выходить за рамки допустимых отклонений. Эти повреждения обнаружить труднее, так как зачастую они проявляются лишь в результате повторяющихся разрядов или в процессе эксплуатации.

Катастрофические отказы ИЭТ при воздействии ЭСР можно разделить на отказы под действием мощности или тока, обычно обнаруживаемые по горячим точкам или расплавленным участкам на кристалле, и отказы под действием напряжения, пробивающего диэлектрик насквозь или разрушающего поверхность кристалла.

Отрицательное влияние ЭСР в первую очередь сказывается на МОП- и КМОП-приборах. Однако перечень полупроводниковых ИЭТ, особо чувствительных к воздействию ЭСР, не ограничивается указанными типами. Некоторые биполярные приборы также чувствительные к ЭСР.

Пороги чувствительности полупроводниковых приборов и ИС приведены в табл. 1.

Тип ИЭТ	Пороги чувствительности, В
МОП-транзистор	100 – 200
Арсенид-галлиевый транзистор	100 – 200
Полевой транзистор с управляющим переходом	140 – 10000
Биполярный транзистор	380 – 7000
КМОП ИС	250 – 3000
Линейные биполярные ИС	190 – 2500
ИС ТТЛ	1000 – 2500
ИС ЭСЛ	500 – 1500
ИС ТТЛШ	500 – 1500

В ходе проведения исследования был выполнен анализ НВМ и ММ моделей для исследования воздействия ЭСР на различные типы транзисто-

ров, промоделировано воздействие на КМОП инвертер импульса статического разряда; промоделирован элемент защиты GGMOST, исследовано воздействие ЭСР на целую ИМС серии 74HC.

При применении внешней защиты встроенная схема защитного элемента позволит надежно защитить КМОП микросхемы от повреждения статическим электричеством.

Литература:

[1] Горлов М.И., Андреев А.В., Воронцов И.В. Воздействие электростатических зарядов на изделие полупроводниковой электроники и радиоэлектронной аппаратуры. – Воронеж: Изд. Воронежского государственного университета. – 1997. – 160 с.

[2] Worker R.C. ESD Control: problems and solutions in the real world // Microcontamination. 1983/84. – № 4. – P. 14–15.

[3] Lyman J., Rosenblatt. A special report the drive for quality and reliability, part 1 // Electronics. – 1981. – № 10. – P. 125–131.

[4] Нойверт Л.М., Лабецкая Н.А., Рыбалов О.Я. Воздействие разрядов статического электричества на микросхемы // Электронная техника. Сер. 8. – 1978. – Вып 3. – С. 133–139.

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

В.Е. Драч, А.Е. Корчикова

МИКРОСХЕМЫ КОМПАНИИ LINEAR TECHNOLOGIES. РАЗРАБОТКА ДРАЙВЕРА НА МИКРОСХЕМЕ LT3799

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

При конструировании светодиодной лампы, любой разработчик сталкивается с задачей отвода тепла, выделяющегося в небольшом объеме светильника, т.к. перегрев светодиодам противопоказан. Кроме того, источником выделения тепла, помимо самих светодиодов, является блок питания или другими словами – светодиодный драйвер.

Ряд компаний выпускает микросхемы, ориентированные на создание недорогих источников питания светодиодов, предназначенных для применения в различных сферах. Одной из таких компаний является Linear Technologies.

80-е годы прошлого века стали временем "второй волны" в мировой электронной промышленности. Именно тогда появились такие компании как Cypress, Seeq, Sierra, Maxim, Atmel, Xilinx, "вышедшие" в большинстве своем из компаний "первой волны" - NatSemi, Intel, Signetics, AMD. Компания Linear Technologies появилась в 1981 году, фактически дав старт "второй волне".

Основателями компании были Роберт Свансон (Robert Swanson) и Роберт Добкин (Robert Dobkin). Оба более десяти лет проработали до этого в National Semiconductor, причем Свансон возглавлял всю аналоговую программу компании, а Добкин был одним из ключевых разработчиков [1].

Развитие Linear Technologies шло своеобразно и мало походило на путь других компаний в сфере производства аналоговых ИС. Хотя продукция Linear Technologies известна в России достаточно давно, она не пользовалась популярностью по той простой причине, что ни один из указываемых компанией дистрибьюторов не создавал в России заметных складов и активно не продвигал ИС с префиксом LT, как это делали, к примеру, дистрибьюторы ADI или MAXIM. Только в последние года ситуация начала меняться и хочется верить, что продукция Linear Technologies будет по достоинству оценена российскими электронщиками т.к. этой компанией выпущено очень много микросхем для создания недорогих источников питания светодиодов.

В таблице 1 приведены основные параметры некоторых ИС драйверов светодиодов компании Linear Technology [2].

Таблица 1. Параметры ИС драйверов светодиодов

Тип ИС	Число выходов	$U_{вх.мин.}$ (В)	$U_{вх.макс.}$ (В)	$I_{вых}$, А	$U_{вых}$, В	Топология	Число светодиодов	Корпус
LT1618	1	1,6	18	2	36	Boost, Sepic, Flyback	20	MS-10, DFN-10
LT1932	1	1	10	0,55	36	Boost	8	ThinSOT
LT1937	1	2,5	10	0,22	36	Boost	4	ThinSOT, SC-70
LT3003	3	3	40	0,35		Ballaster		MS-10E
LT3465	1	2,7	16	0,34	30	Boost	6	ThinSOT
LT3466	2	2,7	24	0,4	39,5	Boost	2 × 10	DFN10
LT3474/ FEAT.	1	4	36	2,1	15	Buck	4	TSSOP16
LT3475-1	2	4	36	2	25	Buck	4	TSSOP20
LT3476	4	2,8	16	4	36	Boost, Buck-Boost, Buck	4 × 8	QFN38
LT3477	1	2,3	25	6,3	40	Buck, Boost, Buck-Boost	12	QFN-20, TSSOP-20
LT3478	1	2,8	36	6,3	42	Boost, Buck-Boost, Buck	6	TSSOP-16
LT3486	2	2,4	24	1,2	35,4	Boost	2 × 10	DFN-16, TSSOP-16
LT3491	1	2,5	12	0,35	24	Boost	6	SC-70, DFN-6
LT3492	3	3	30	1	60	Buck, Boost, Buck-Boost	3 × 10	QFN-28, TSSOP-28
LT3496	3	3	30	1	45	Boost, Buck-Boost, Buck	3 × 10	QFN-28, TSSOP-16
LT3518	1	2	40	2,8	45	Buck, Boost, Buck-Boost	10	QFN-16
LT3519	1	3	30	0,98	45	Boost, Sepic, Buck-Boost, Buck	10	MS-16
LT3590	1	4,5	55	0,115	55	Buck	10	SC-70, DFN-6
LT3956/ FEAT	3	6	60	0,51	44	Boost, Sepic	3 × 10	QFN-52
LT3799/ NEW	6	3,2	30	0,33	44	Boost, Sepic	6 × 10	QFN-24
LT3598/ FEAT	1	3,2	30	2	44	Boost, Sepic	10	QFN-24
LT3599/ FEAT	1	3	30	2,5	44	Boost, Sepic	10	QFN-32, TSSOP-28

LT3741	1	6	60	25	34	Buck	10	QFN-20
LT3743/ FEAT	1	6	36	20	30	Buck	10	QFN-28, TSSOP-28
LT3745/ NEW	16	6	36		36	Buck	16 × 10	QFN-40

Микросхема LT3799 также совместима со стандартным настенным симисторным регулятором освещения (TRIAC Dimmer). Уникальная схема считывания тока на этой микросхеме выдает хорошо стабилизированный ток и обходится без оптопары. Кроме уменьшения итоговой стоимости системы, повышается ее надежность за счет использования минимума внешних компонентов [3].

Вариант схемотехнического решения представлен на рис. 1.

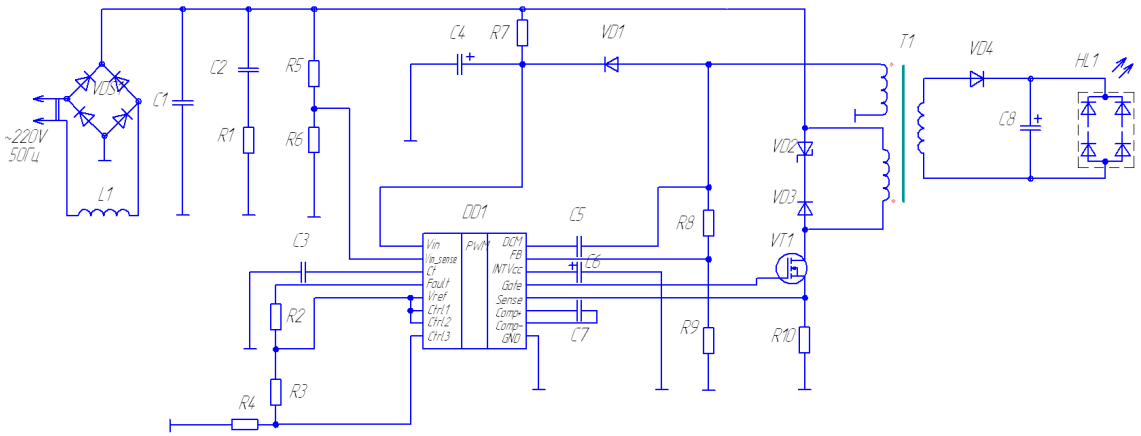

Рис. 1. Схема электрическая принципиальная LED-драйвера

В принципе, схемотехническое решение практически полностью совпадает с рекомендованным производителем включением ИМС-драйвера [4].

Были промоделированы характеристики законченного устройства такие как:

1. Оценка помех, вносимых драйвером в электрическую сеть, продемонстрирована на спектрограмме тока потребления (рис. 2).

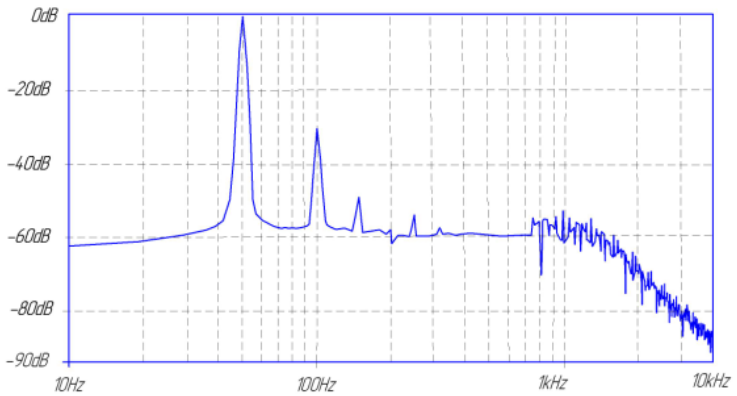

Рис. 2 Спектр гармоник, порождаемый драйвером

Как видно, работа ККМ настолько эффективна, что на графике присутствует, по сути, лишь 2-ая гармоника, все остальные гармоники фактически на уровне шумовой полки.

2. Работа активного ККМ хорошо отображается на совмещенном графике тока потребления и напряжения питания, приведенного на рис. 3.

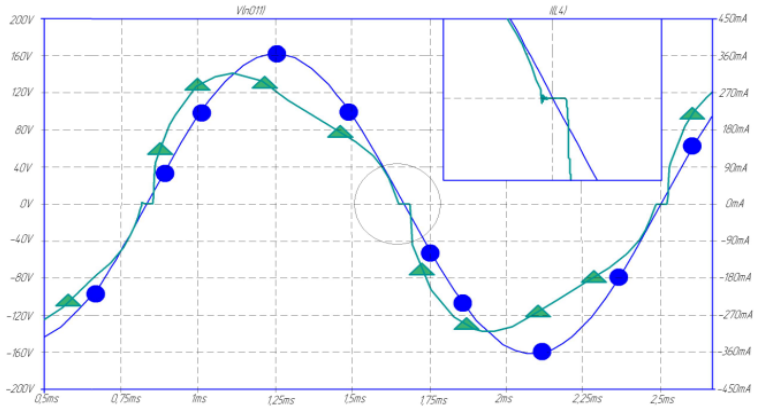

Рис. 3. Форма тока потребления от источника синусоидального напряжения

Видно, что за счет работы ККМ потребление тока почти равно синусоидальному в такт источнику питания, что приводит, в конечном итоге, к почти активному характеру нагрузки.

3. При этом, используя возможности моделирования, легко получить токи и напряжения в самых электронагруженных узлах устройства: в индукторе, ключевом транзисторе, демпферной цепочке (рис. 4), диоде в цепи питания светодиодной матрицы (данный график будет приведен ниже).

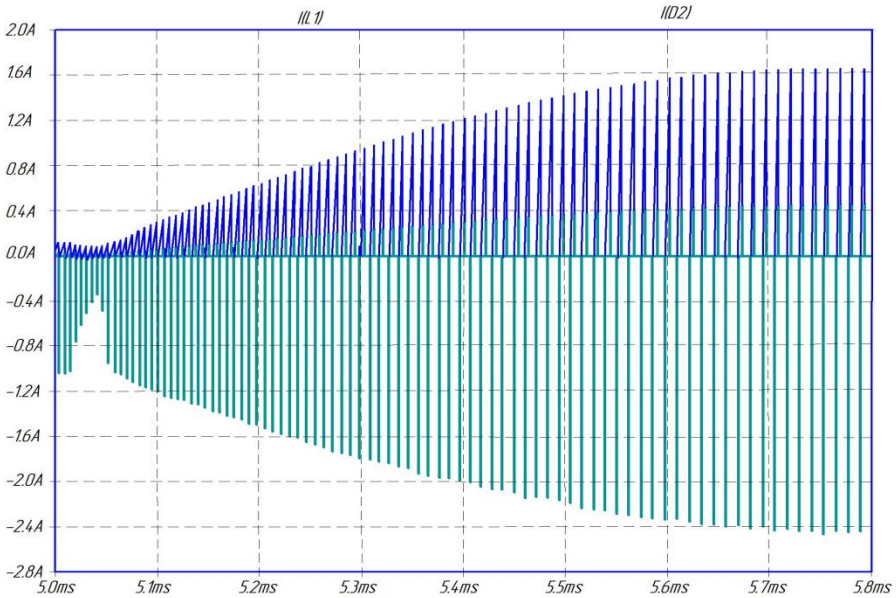

Рис. 4. Токи в индукторе (стоке ключевого транзистора) и демпферной цепочке

4. Режимы работы светодиодной матрицы для номинального питающего напряжения и для пониженного (-20%, -40%, -60%) приведены на рис. 5.

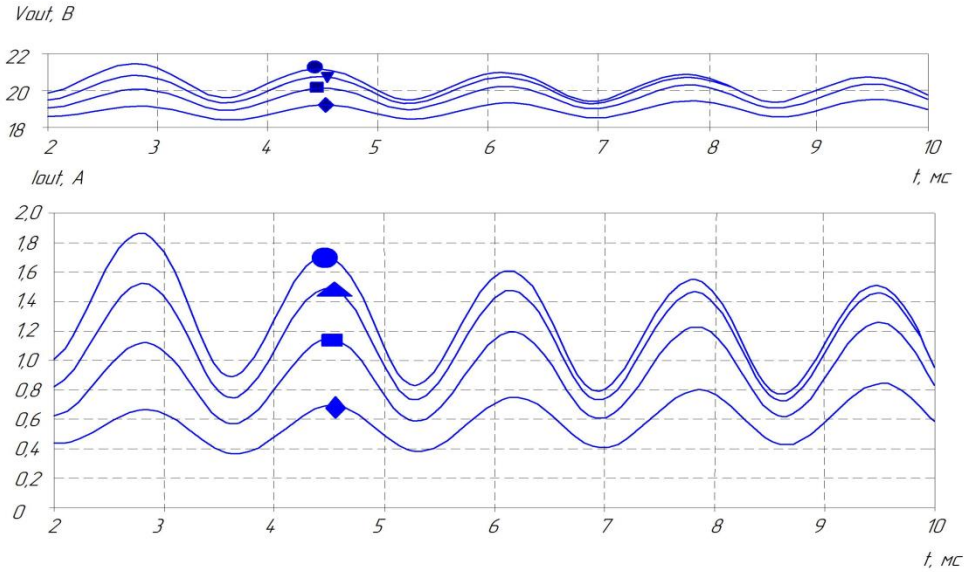

Рис. 5. Режимы работы светодиодной матрицы при разных напряжениях питания

5. При необходимости, пульсации тока через светодиодную матрицу можно значительно уменьшить, а также получить плавный пуск, что также благоприятно скажется на надежности светодиодной матрицы (рис. 6).

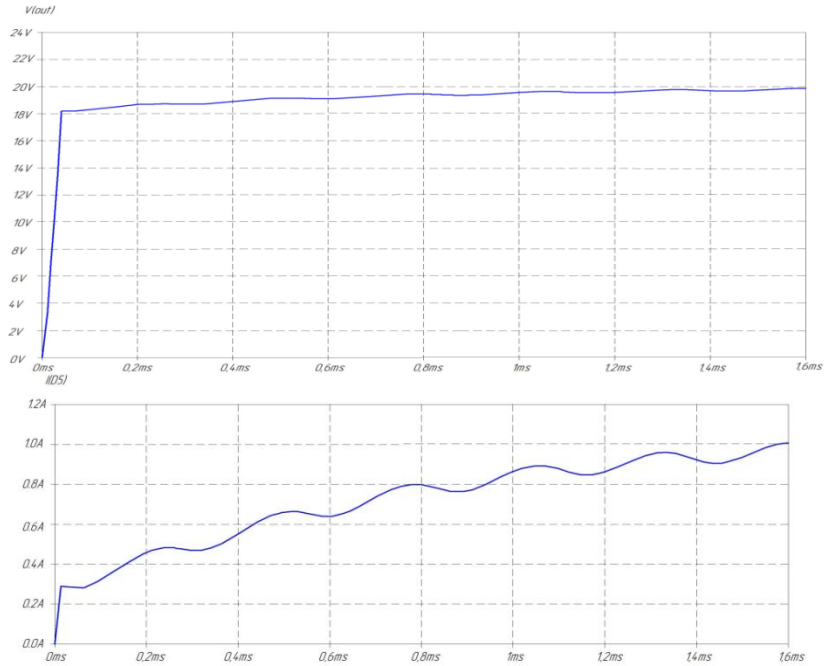

Рис. 6. Режим плавного пуска

Данный режим легко организовать, добавив дополнительный CLC-фильтр в цепи питания светодиодной матрицы.

Заключение

В результате проделанной работы авторами предложена схема светодиодного драйвера для источника внешнего освещения мощностью 20Вт. Преимуществами данного драйвера являются: 1) наличие активного корректора коэффициента мощности (ККМ), позволяющего резко снизить помехи, излучаемые в промышленную сеть и увеличить энергоэффективность; 2) гальваническая развязка цепей питания светодиодной матрицы, в некоторых случаях данное обстоятельство является критичным; 3) возможность использования стандартных регуляторов яркости (диммеров) совместно с данным драйвером.

В результате моделирования получены режимы работы элементов драйвера, что позволило оптимизировать выбор элементов, а также оценить полученный результат с точки зрения потребительских свойств.

Список литературы

[1] Келл Г. Linear Technology: портрет компании // Новости электроники. – 2006. – №5.

[2] Петропавловский Ю. Драйверы светодиодов компании Linear Technology // Современная Электроника. – 2012. №3. – С.10-17.

[3] Корчикова А.Е., Драч В.Е. Моделирование драйвера сверхъярких светодиодов в среде LTSpice // Наукоемкие технологии в приборо– и машиностроении и развитие инновационной деятельности в вузе. – 2016. Том 3. – С.23-25.

[4] Лоскутов С.А., Драч В.Е., Корчикова А.Е. Драйвер светодиодного светильника // Электромагнитные волны и электронные системы. – М.: Радиотехника. – 2016. – Том 21. – №10. – С.43-49.

Корчикова Анастасия Евгеньевна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: korchickowa@yandex.ru

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

А.А. Корнеев, В.В. Кузнецов

МОДЕЛИРОВАНИЕ ЗАДАЮЩЕГО ГЕНЕРАТОРА СТЕНДА ПРОВЕРКИ ИНДУКТИВНЫХ ДАТЧИКОВ И КАБЕЛЕЙ В ПАКЕТЕ QUCS-S

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

При разработке современной радиоэлектронной аппаратуры актуальной задачей является моделирование работы схемы перед её окончательным запуском в производство. В связи с этим необходимо, чтобы результаты моделирования наиболее достоверно отражали протекающие процессы в реальном устройстве. То есть применяемые пакеты САПР должны обладать определёнными характеристиками, обеспечивающими данное требование.

Темой данной работы является обзор и сравнение возможностей виртуального симулятора работы электронных схем QUCS-S [1].

Научная новизна исследования заключается в постановке и решении приоритетных задач комплексной оценки процессов, происходящих при работе устройства, а также их сравнение в виртуальной среде.

Разработка любого устройства сопровождается, как правило, физическим или математическим моделированием. Физическое моделирование связано с большими материальными затратами, поскольку требуется изготовление макетов и их исследование, которое может быть весьма трудоемким. Поэтому часто применяют математическое моделирование с использованием средств и методов вычислительной техники.

Практическая значимость данного исследования является в том, что после сравнения возможностей виртуального симулятора Qucs-S и реальных осциллограмм стенда проверки индуктивных датчиков и кабелей, можно применять данный САПР при разработке новых электронных изделий минуя материальные затраты на эксперимент [2].

Вследствие этого было принято решение перед реализацией данного устройства собрать и промоделировать составляющие части такого изделия и сравнить их результаты анализов.

Исследования выходных сигналов производились при помощи цифрового запоминающего двухканального осциллографа Tektronix TDS2012S. Он обладает стандартным набором возможностей – включая порт USB, 16 автоматических измерений, контроль предельных значений, регистрацию данных и контекстную справку.

Рассмотрим подробнее схему задающего генератора опорного сигнала, а также его осциллограммы выходных сигналов с трех разных точек (1’,2’ и 3’). В данном схемотехническом решении был применён транс-

форматор, предназначенный для гальванической развязки выходного сигнала:

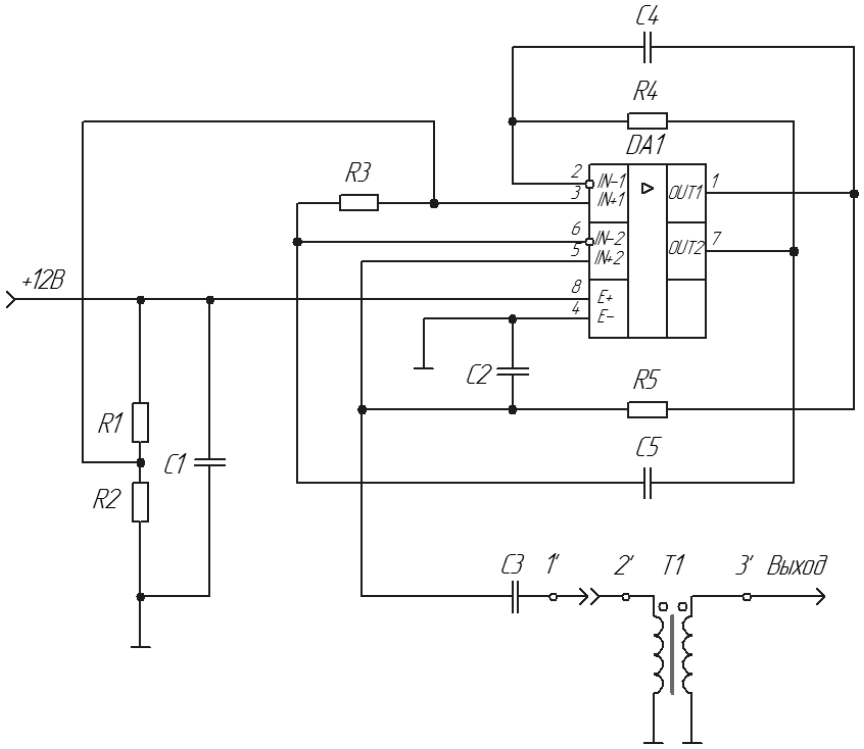

Рис.1. Схема генератора задающего генератора.

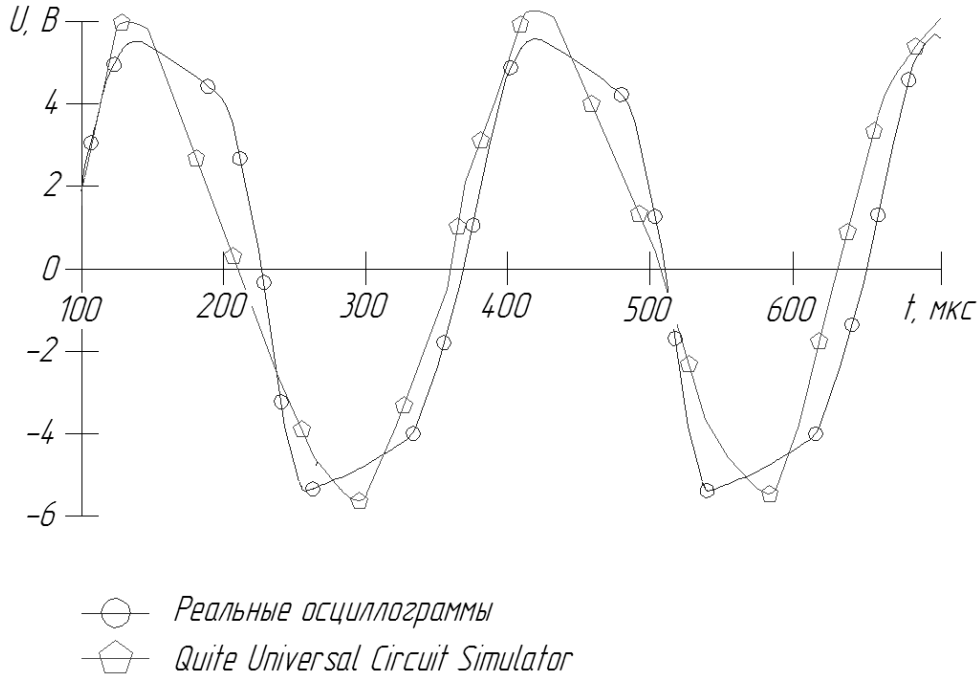

Рис.2. Осциллограмма выходного сигнала в контрольной точке 1'.

Из результата моделирования, изображенном на рисунке 2, можно сделать следующее заключение: форма сигнала, полученная опытным путём - пилообразная. Период такого сигнала приблизительно равен

$T = 273,4$ *мкс* , частота – $f = 3,657$ *кГц*. QUCS-S незначительно увеличил амплитуду.

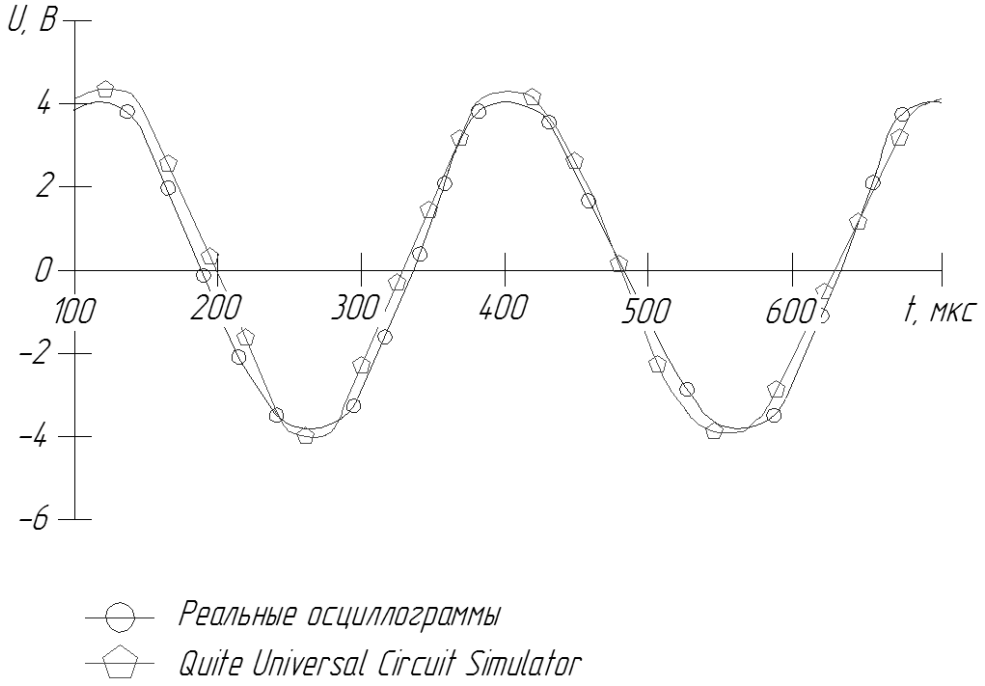

Рис.3. Осциллограмма выходного сигнала в контрольной точке 2'.

Из результата моделирования, изображенном на рисунке 3, можно сделать следующее заключение: форма реального графика - синусоидальная. Период равен $T = 243,9$ *мкс*, частота – $f = 4,112$ *кГц*. QUCS-S снова увеличил амплитуду.

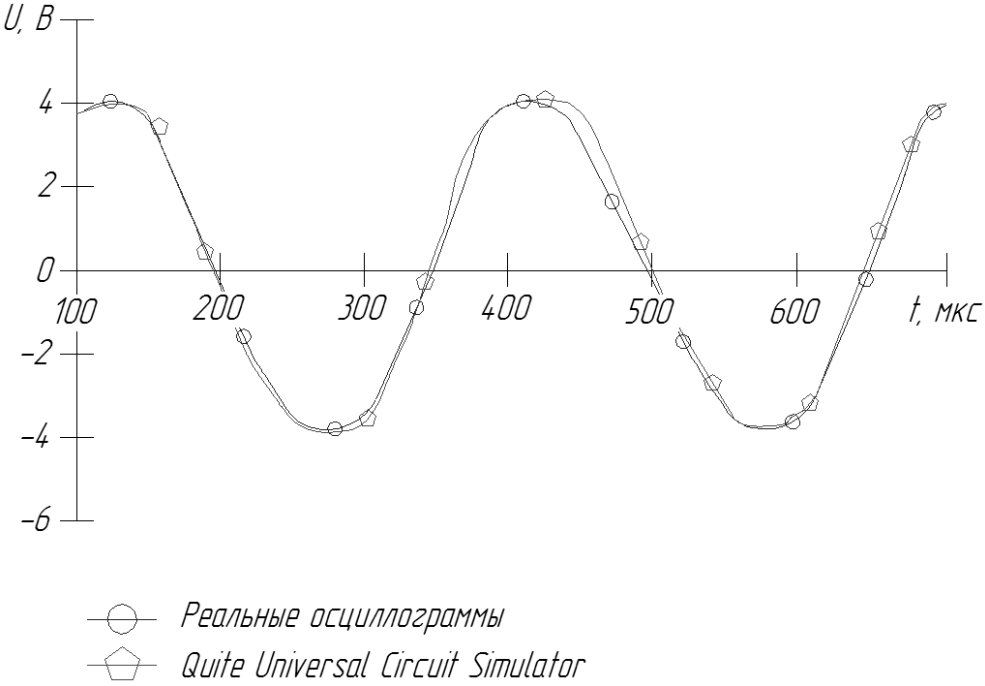

Рис.4. Осциллограмма выходного сигнала в контрольной точке 3'.

Из результата моделирования, изображенном на рисунке 4, можно сделать следующее заключение: форма реального графика - синусоидальная. Период равен $T = 238,6$ *мкс*, частота – $f = 4,119$ *кГц*. В QUCS-S значение амплитуды практически равно реальному значению, форма сигнала, частота и период почти не изменились.

В результате проведенных исследований выходных сигналов данного устройства получились группы осциллограмм и временных диаграмм выходных сигналов, которые представлены выше в виде совмещенных графиков. В заключении хотелось бы отметить, что QUCS-S практически идеально подходит для моделирования схем электрических принципиальных в похожих схемотехнических решениях. При использовании данного пакета можно свести к минимуму трудоемкость воспроизведения схемы устройства и материальных затрат.

Литература:

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

[2] Кузнецов В.В., Крючков Н.М. Qucs: Использование свободного ПО для моделирования электронных схем в учебном процессе/ XI конференция разработчиков свободных программ: Тезисы докладов/ Калуга, 26–28 сентября 2014 года. М.: Альт Линукс, 2014.

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

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

Е.Н. Дрожжова, А.Н. Мозохин

ПРОЕКТИРОВАНИЕ ЦИФРОВОГО УСТРОЙСТВА КОНТРОЛЯ ДВИЖЕНИЯ ТРАНСПОРТНОГО СРЕДСТВА

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

В России автобусы с числом мест более 8 и грузовые транспортные средства с разрешённой полной массой более 3.5 тонн (приказ Минтранса России от 13 февраля 2013 г. № 36) должны быть оборудованы цифровыми устройствами контроля движения транспортного средства, с целью обеспечения безопасных условий.

Данное устройство представляет собой контрольный бортовой регистрирующий прибор, в составе транспортного средства, предназначенный для контроля и регистрации следующих параметров как: скорость движения, пробег автомобиля, периоды труда и отдыха водителей.

Целью работы является разработка и усовершенствование 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.

При всем богатстве разнообразия моделей цифровых устройств на рынке, на май 2016 г не многие из них имеют сертификат на эксплуатацию в России:

- Штрих-Тахо RUS SM в металлическом и пластиковом корпусах;
- КАСБИ DT 20M;
- Меркурий ТА 001;
- VDO DTCO 3283;
- ТЦА 02 НК;
- Атол Drive 5;
- EFAS V2 Rus.

КАСБИ способен выдавать отчеты о скорости, технических параметрах и режимах водителя в виде графиков. Простота подачи информации в графическом виде позволяет наглядно проанализировать работу автомобиля за отчетный период. Данное устройство может выдать отчет о неисправностях и ошибках в виде списка. Протокол навигационного модуля открыт для настройки любого программного обеспечения. Само устройство позиционируется для установки на грузовые автомобили, перевозящие взрывоопасные и легковоспламеняемые грузы. Кроме того, калибровать КАСБИ можно без применения дорогого оборудования. Это уменьшает стоимость установки и калибровки прибора и сокращает общие затраты на устройство. Возможность перепрошивать один и тот же СКЗИ продлевает срок его службы на данном автомобиле. И, опять-таки, сокращает общие расходы по его содержанию. В конструкции устройства заложены такие схемы и программные платформы, которые можно модернизировать

без замены самописца. Не смотря, на большое количество преимуществ данного устройства, есть необходимость постоянного конкурирования.

Любое устройство может выйти из строя, не исключая и данное. Защита от помех в данном устройстве осуществляется на базе защитного диода VD7(1N5404) и супрессора VD10(SM8S33A) в диапазоне от 30…36 В. Технические характеристики представлены в таблице 1 и 2. При превышении напряжения питания порогового значения, диод выходит из строя.

Таблица 1. Технические характеристики диода 1N5404

Материал	кремний
Максимальное постоянное обратное напряжение, В	400
Максимальное импульсное обратное напряжение, В	525
Максимальный прямой (выпрямленный за полупериод) ток, А	3
Максимально допустимый прямой импульсный ток, А	200
Максимальный обратный ток, мкА 25гр	5
Максимальное прямое напряжение, В	1.2
при Iпр., А	3
Рабочая температура, С	-65…150
Способ монтажа	в отверст.
Корпус	DO-201AD

Таблица 2. Технические характеристики диода SM8S33A

Минимальное пробивное напряжение, В	36,7
Максимальное пробивное напряжение, В	40,6
Обратное напряжение, В	33
Максимальный обратный ток, мкА	10
Максимальный импульсный ток, А	124
Корпус	DO-218AB

Одной из основных причин поломки устройства в эксплуатации, связана с выходом из строя защитного диода VD10(SM8S33A), он сгорает, или не срабатывает, в следствие чего, выходит из строя микросхема DA3. Рассмотрим применение схемы защиты цепи питания, представленную на рис. 1, направленную не на рассеивания мощности, а на отключение по входу цепи питания при воздействии защиты высокого напряжения. Происходит отключение питания менее чем, на 200 мс.

Напряжение питания бортовой сети ТС через разъем XP1 и фильтр защити от синфазных помех L1 подается на схему защиты от превышения напряжения. В случае превышения значения напряжения питания БУ свыше 45,5±05 В через стабилитрон VD1 начинает протекать ток, транзистор VT1 открывается, что приводит к закрытию высоковольтного ключа VT2. В нормальных условиях, при напряжении питания бортовой сети ниже 45 В резистивный делитель R4 – R5 обеспечивает разность потенциалов исток-затвор VT2. Исключение из схемы перемычки R8 обеспечивает повышение уровня стабилизации напряжения на 0,5 В. Стабилитрон VD3 защищает переход затвор-исток от перенапряжения.

Благодаря данному решению, мы сможем защитить входные цепи цифрового устройства от высоковольтных помех.

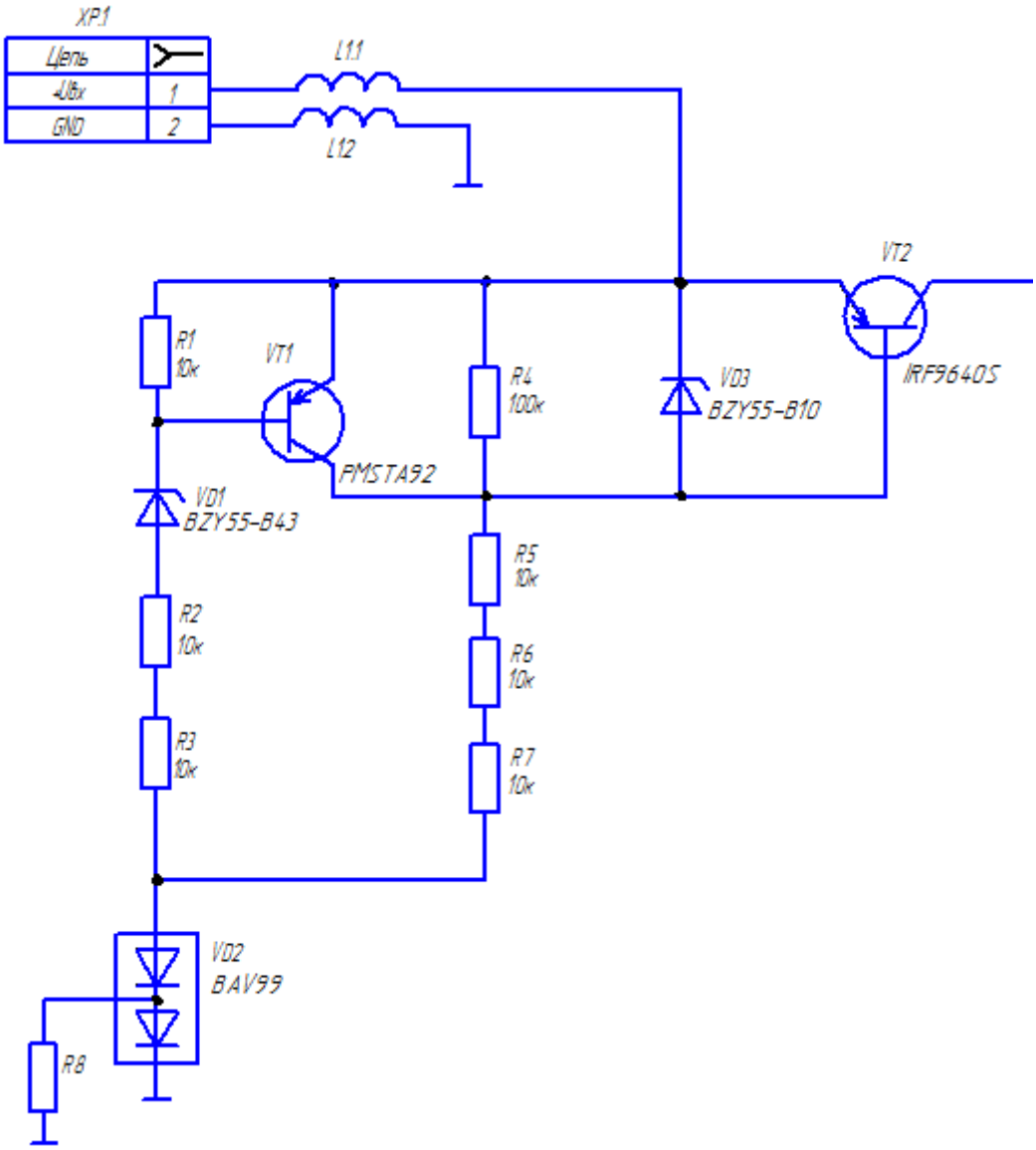

Рис.1 Схема защиты цепи питания

Библиографический список

[1] Контрольное устройство «КАСБИ DT-20M» стр. 101

[2] Тахографы URL: http://gruzavtoperevozki.ru/vybor-tahografa (дата обращения 31.03.2017)

[3] Surface Mount Automotive Transient Voltage Suppressors URL: http://html.alldatasheet.com/html-pdf/852105/SHUNYE/SM8S33A/216/1/SM8S33A.html (дата обращения 30.03.2017)

[4] Diodes 1N5404 URL:http://www.datasheetlib.com/datasheet/193295/1n5404_diodes.html#datasheet (дата обращения 30.03.2017)

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

В.В. Кузнецов, Д.Е. Бородин

РАЗРАБОТКА МОДЕЛИ ФОТОДИОДА ФПУ 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 – разработать модель фотодиода с возможностью настройки интенсивности падающего светового потока и его длины волны. На текущем этапе исследований создана грубая модель фотодиода, проводится ее тестирование и согласование параметров с реальным фотодиодом. Моделирование фотодиода проводится в симуляторе электронных схем Qucs-S [2].

За основу модели была взята обобщенная модель фотодиода [3], пригодная для моделирования характеристик p–n- и p–i–n-фотодиодов, фотодиодов с управляющим МДП-затвором (ФДУЗ) и имеющая эквивалентную схему, представленную на рисунке 1. Она имеет 4 вывода: анод A, катод C, затвор G и световой F – и состоит из следующих элементов: Gph – источник фототока; Dpn – диод, описывающий p–n-переход; Cpn – ёмкость p–n-перехода; Rpn – суммарное сопротивление p- и n-областей; Rleak – паразитное поверхностное сопротивление утечки; Rcont – сопротивление контакта p+–p–; Cmos – ёмкость МОП-структуры.

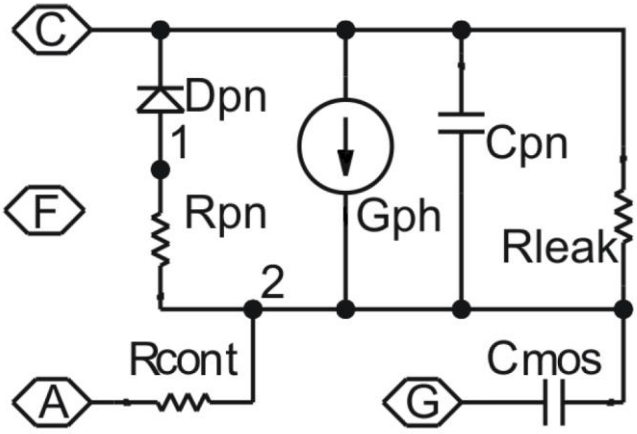

Рис. 1. Эквивалентная схема модели фотодиода

Выражение для фототока (Gph) имеет вид:

$$I_{\Phi} = k\Phi, k = A_S \cdot \eta(\lambda) \cdot S_0 \cdot f(U_3), \quad (1)$$

где I_{Φ} – фототок, А; Φ – плотность мощности светового потока, Вт/см^2; A_S – площадь фоточувствительной поверхности, см^2; $\eta(\lambda)$ – внутренний квантовый выход фотоэффекта; S_0 – фоточувствительность, А/Вт (в случае источника с широким спектром используется интегральная фоточувствительность, вычисляемая на основе спектральной фоточувствительности); $f(U_3)$ – функция, учитывающая влияние напряжения затвора U_3.

В нашем случае у фотодиода отсутствует управляющий МДП-затвор, отсюда упрощением выражения (1) получаем конечное выражение для фототока:

$$I_{\Phi} = k\Phi, k = A_S \cdot \eta(\lambda) \cdot S_0. \quad (2)$$

Далее с помощью инструмента «Edit Circuit Symbol» симулятора электронных схем Qucs-S была создана модель фотодиода ФПУ высотомера, подсхема и схема включения которой представлены на рисунках 2 и 3 соответственно:

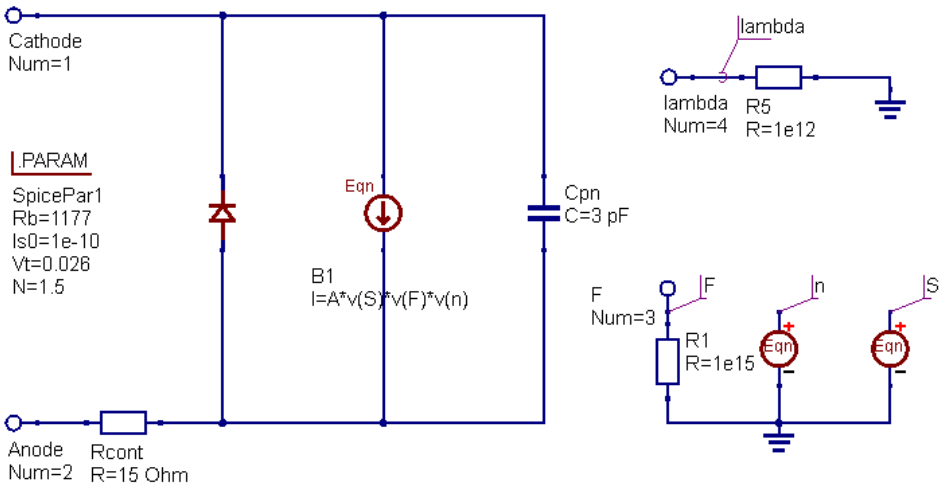

Рис. 2. Подсхема модели фотодиода ФПУ высотомера в Qucs-S

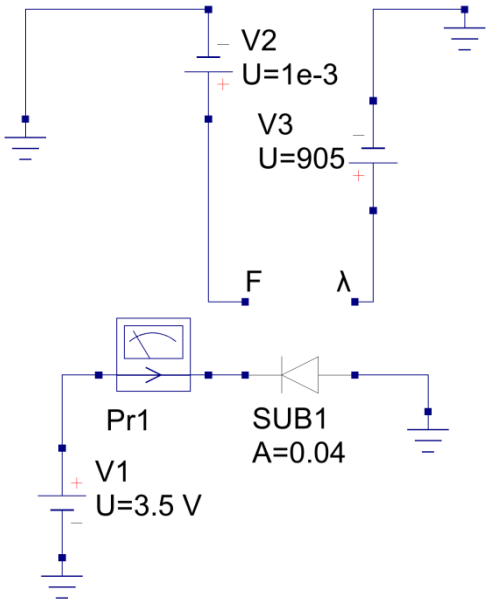

Рис. 3. Схема включения модели фотодиода в Qucs-S

Модель имеет 4 порта: анод, катод, порт для задания плотности мощности светового потока и порт для задания длины волны светового потока. Модель поддерживает диапазон длин волн от 400 до 1100 нм. Следующим шагом с модели были сняты следующие характеристики: статическая прямая и обратная ВАХ, световая характеристика фотодиода, зависимость фототока от длины волны светового излучения, семейство обратных ветвей ВАХ при $\Phi = const$ и при $\lambda = const$, примеры которых представлены на рисунках 4-7:

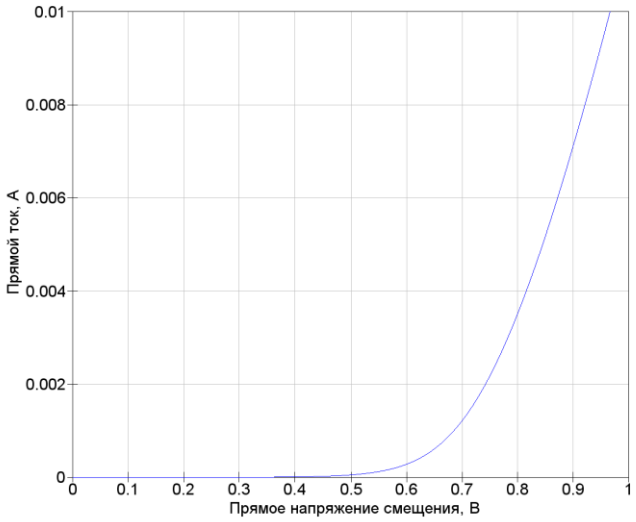

Рис. 4. Статическая прямая ВАХ модели фотодиода

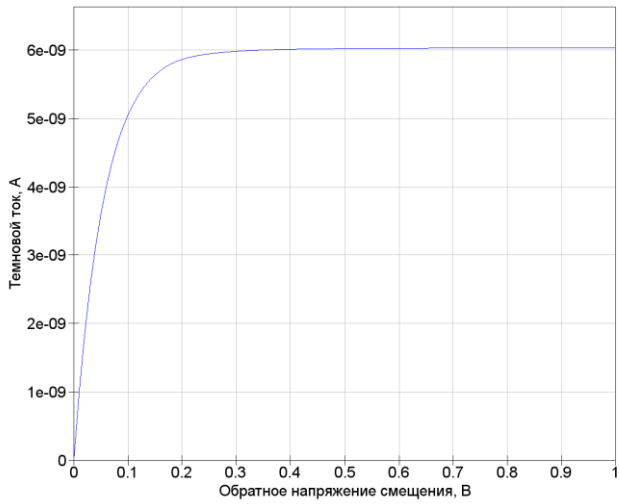

Рис. 5. Статическая обратная ВАХ модели фотодиода

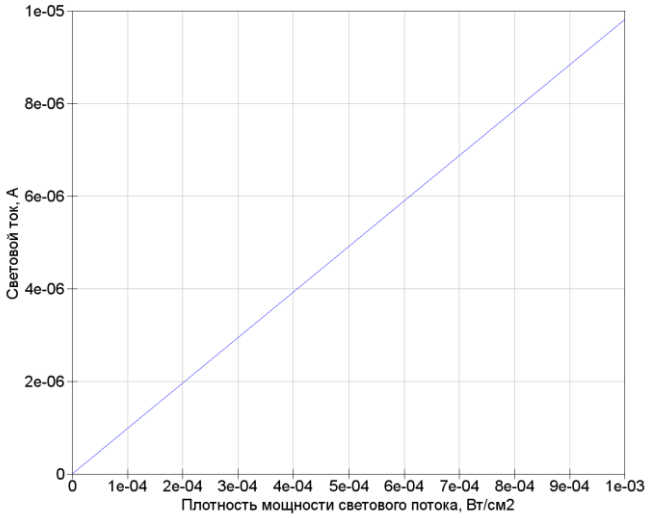

Рис. 6. Световая (энергетическая) характеристика модели фотодиода

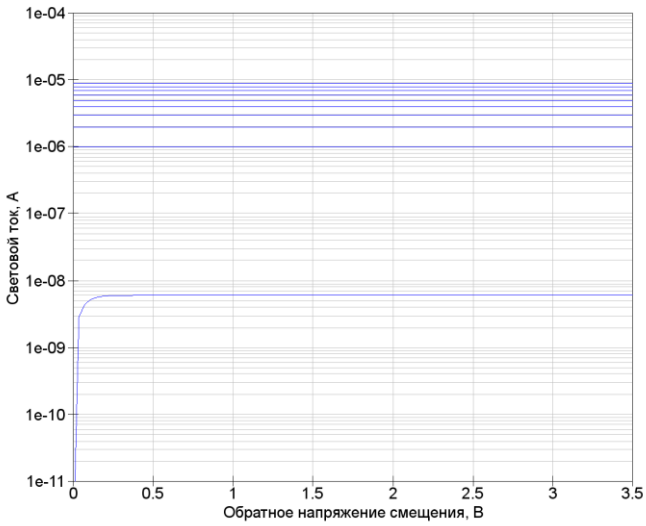

Рис. 7. Семейство обратных ветвей ВАХ модели фотодиода при $\lambda = 905 нм$

Таким образом, снятые с модели характеристики позволяют сделать вывод, что модель работает правильно, но пока является достаточно грубым приближением. В настоящее время планируется уточнить параметры модели фотодиода, провести анализ исходных схем ФПУ высотомера с учетом данной модели.

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] Самбурский Л.М. SPICE-модели оптоэлектронных элементов для расчёта фоточувствительных КМОП-ФД БИС // МЭС – 2005. Сб. научных трудов. – М.: ИППМ, 2005. – стр. 196–203

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

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

С.А. Лоскутов, В.Э. Толоконников

СРАВНИТЕЛЬНЫЙ АНАЛИЗ УСТРОЙСТВ ВЫВОДА ИНФОРМАЦИИ НА ПРИМЕРЕ СИМВОЛЬНОГО И ГРАФИЧЕСКОГО ДИСПЛЕЕВ.

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

Как правило для вывода информации символьного дисплея DV-20400S2FBLY от компании DATAVISION, установленного в устройстве блока концентратора данных, более чем достаточно. Но иногда требуется изобразить картинку, график или любую другую графическую информацию. Данная задача решается применением графического дисплея. Одним из самых простых и доступных является дисплей на контроллере KS0107 или аналоге. С целью расширения возможностей отображения графической информации, мной был выбран WG12864A от Winstar. Дисплей имеет довольно большой размер (диагональ около 80мм) и разрешение 128x64 пикселя. Относительно не высокая стоимость и достойные технические характеристики склоняют нас к его выбору.

Выбор данного дисплея так же обусловлен тем, интерфейс управления дисплеем параллельный и совпадает с ранее установленным, что дает нам возможность не перерабатывать печатную плату, а всего лишь ограничиться изменением программного обеспечения для микроконтроллера.

Целью данной статьи являются краткий обзор и сравнительный анализ дисплеев DV-20400S2FBLY и WG12864A.

Рассмотрим основные характеристики двух дисплеев и проведем сравнительный анализ.

Воспользуемся для этого технической документацией, представленной компаниями разработчиками DATAVISION [1] и Winstar [2].

Рассмотрим механические характеристики дисплеев. Дисплей DV-20400S2FBLY, являясь символьным способен отобразить 20 x 4 символов, а графический дисплей WG12864A отображает 128 x 64 точек.

Размеры пикселей для дисплея. установленного в устройстве блока концентратора данных равны 0.55 мм на 0.55 мм, а для нового дисплея – 0.41 мм на 0.41 мм. Расстояние между пикселями для символьного модуля составляет 0.05 мм, а для графического модуля – 0.03 мм.

Габаритные размеры первого модуля (по горизонтали, вертикали и толщине) равны 98.0 x 60.0 x 14.5 мм, из них видимая область экрана 76.0 мм на 25.2 мм, для второго 75.0 x 52.7 x 8.9 мм, из них видимая область экрана 60.0 мм на 32.6 мм.

Из этого следует, что дисплей WG12864A обладает меньшим размером пикселей, т.е. пиксельная плотность выше, и, следовательно, качество

отображаемого изображения лучше. Так же это дисплей имеет значительно меньшую толщину.

Таблица 1 – Электрические характеристики

	DV-20400S2FBLY		WG12864A	
Напряжение питания для логики (В)	4.5 - 5.5		4.5 - 5.5	
Входное напряжение высокого уровня (В)	2.2 - 5.5		2.0 - 5.5	
Входное напряжение низкого уровня (В)	0 - 0.6		0 - 0.8	
Выходное напряжение высокого уровня (В)	2.4 - 5.5		2.4 - 5.5	
Выходное напряжение низкого уровня (В)	0 - 0.4		0 - 0.4	
Ток питания (мА)	1.0 - 6.0		2.0 - 4.0	
Напряжение питания (В)	0 °C	5.1 (max)	-20 °C	9.6 (max)
	20 °C	4.6 (typ)	25 °C	8.0 (typ)
	50 °C	4.2 (min)	70 °C	7.6 (min)

По электрическим характеристикам оба дисплея имеют схожие параметры, но WG12864A способен воспринимать немного больший диапазон входных значений для высокого и низкого логических уровней.

Одной из важных проблем в работе раннее установленного дисплея DV-20400S2FBLY является невозможность его корректного функционирования при отрицательных температурах. Поэтому мной был проведен сравнительный анализ температурных характеристик двух раннее представленных дисплеев.

Для дисплея DV-20400S2FBLY рабочая температура составляет от 0 до +50 °C, для дисплея WG12864A от -20 до +70 °C. Температура хранения для первого дисплея равна от -20 до +70 °C, для второго – от -30 до +80 °C.

Следовательно, WG12864A в отличии от DV-20400S2FBLY способен работать в большем диапазоне температур, и что наиболее важно сохраняет свою работоспособность при отрицательных температурах.

Таблица 2 – Оптические характеристики

		DV-20400S2FBLY	WG12864A
Контрастность (при 20 °C)		1.34 - 4.99	3 - 5
Частота кадров (Гц)		64	64
Время отклика (мс)		250	200
Угол обзора (градус)	(V)θ	10 - 30	20 - 40
	(H)φ	- 25 - 25	-30 - 30

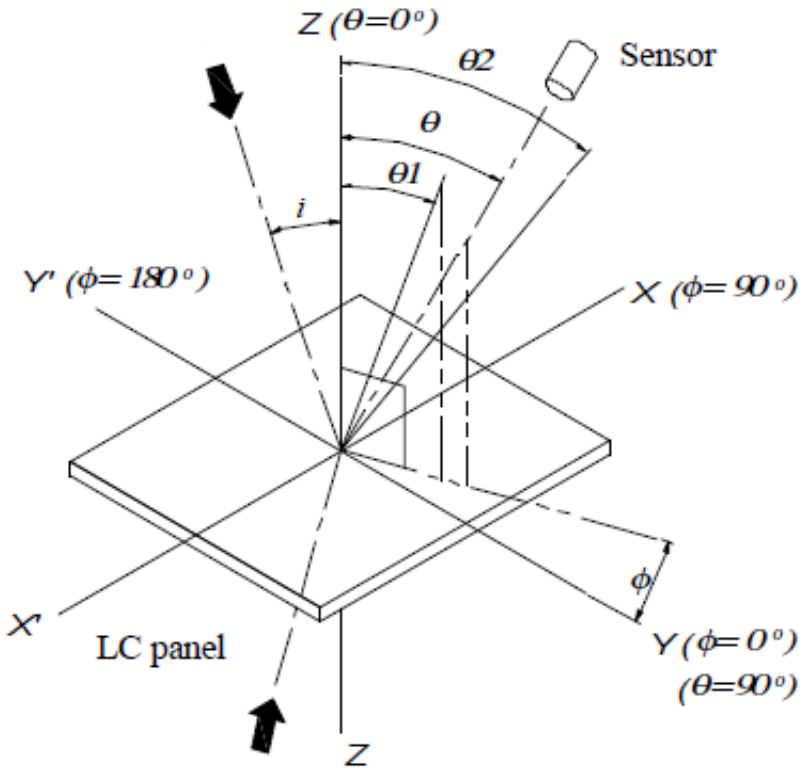

Рисунок 1 – Углы обзора дисплея

WG12864A обладает наилучшим временем отклика, имеет большие углы обзора по сравнению с DV-20400S2FBLY, но не значительно проигрывает ему в контрастности.

Сделав сравнительный анализ параметров и характеристик дисплеев WG12864A и DV-20400S2FBLY можно сделать вывод, что выбранный для замены дисплей полностью удовлетворяет поставленные цели и задачи. Также он превосходит установленный ранее экран по множеству параметров, основными из которых являются температурные и оптические характеристики.

Электронные ресурсы

[1] Технические характеристики модуля ЖК дисплея DV-20400S2FBLY: http://platan.ru/pdf/datasheets/datavision/DV-20400.pdf (дата обращения 15.03.2017).

[2] Технические характеристики модуля ЖК дисплея WG12864A: http://www.winstar.com.tw/uploads/files/875d5acf8585e64b2f 601a787afe81ae.pdf (дата обращения 15.03.2017).

Лоскутов Сергей Александрович – канд. техн. наук, доцент кафедры "Конструирование и производство электронной аппаратуры" 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

А.В. Рытикова, В.В. Андреев

ТЕСТОВЫЙ КОНТРОЛЬ МДП-ТРАНЗИСТОРОВ

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

При операционном контроле технологического процесса изготовления изделий микроэлектроники широкое применение нашли тестовые схемы, состоящие из тестовых структур.

Тестовая структура представляет собой совокупность определенным образом спроектированных и соединенных элементов (резисторов, конденсаторов, транзисторов, проводников и т.д.), изготавливаемых совместно с реальными изделиями по анализируемому технологическому процессу и предназначенных для определения погрешностей формирования геометрических размеров и физических характеристик, а также характеристик дефектности физической структуры реального изделия [1,2].

Цель данной работы составить методику измерения параметров МДП-транзистора с помощью тестовой структуры. Измерения выполняются на автоматизированной зондовой установке ЭМ6020 с использованием измерительной установки «Вахта».

До начала измерения параметров необходимо провести проверку контактирования и короткого замыкания между иглами. После этого можно переходить к измерению параметров транзистора. Сначала снимаются параметры контактного сопротивления n- и p-канальных МДП-транзисторов. Далее следует измерение поверхностного сопротивления. После измерения всех сопротивлений следует перейти к измерению вольт-амперных характеристик (ВАХ) транзистора (пороговое, пробивное, прямое напряжения и ток стока). После проведения всех измерений проверка считается законченной. Полученные результаты сверяются с нормой.

Предложенная методика была реализована при контроле партии КМДП микросхем серии 1564, изготовленной на АО «Восход» - Калужский радиоламповый завод. Тестовый модуль в этих микросхемах состоит из двух частей, топология которой представлена на рисунке 1. В тестовый модуль включены транзисторы, имеющие конструкцию аналогичную транзисторам, используемым в рабочем кристалле ИС. В таблице 1 приведены нормы электрических параметров для рабочих n- и p-канальных МДП-транзисторов в микросхемах данной серии.

Если при контроле параметров МДП-пранзисторов в тестовом модуле они выходили за диапазон, приведенный в таблице 1, то данные полупроводниковые пластины браковались, как не соответствующие нормам. В таблице 2 приведены результаты измерений параметров n- и p-канальных МДП-транзисторов, которые соответствовали нормам, приведенным в таблице 1. Последующая разбраковка рабочих кристаллов на данной полупро-

водниковой пластине показала выход годных кристаллов более 60 %, а их последующие испытания показали их высокую надежность. В то же время, контроль электрических параметров на пластинах, забракованных по результатам тестового контроля, дал выход годных менее 10%.

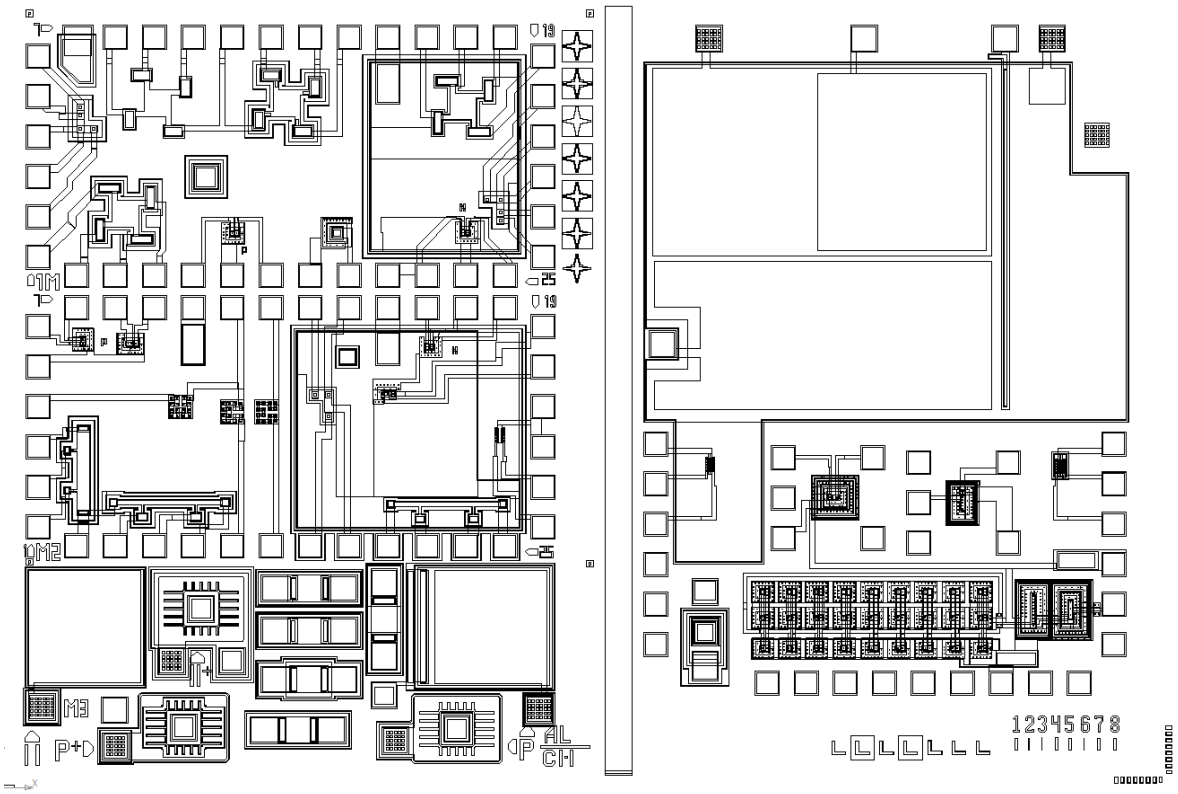

Рис. 1. Топология тестового модуля для контроля качества КМДП ИМС с поликремневым затвором

Таблица 1 - Нормы электрических параметров

Поверхностное сопротивление			
R_{sp-} кОм/кв	R_{ss}* кОм/кв	R_{sp+} кОм/кв	R_{sn+} кОм/кв
1200-1800	10-30	270	25-50
ВАХ p-канальных транзисторов			
U_{n1p} ,В	U_{np1p} ,В	I_{p13} ,мА	U_{lp} ,В
0.7-1.2	>14	>0.4	<2.7
ВАХ n-канальных транзисторов			
U_{np1p} ,В	I_{n13} ,мА	U1n1 ,В	Sn1
>14	>2.15	<2.5	>0.25
Контактное сопротивление			
R_{kp+} ,Ом	R_{kn+} ,Ом	R_{ks*} ,Ом	
<30	<10	<5	

Таблица 2 - Результаты измерения электрических параметров

Поверхностное сопротивление			
R_{sp-} кОм/кв	R_{ss}* кОм/кв	R_{sp+} кОм/кв	R_{sn+} кОм/кв
1586	14	203	26.3
ВАХ p-канальных транзисторов			
U_{n1p} ,В	U_{np1p} ,В	I_{p13} ,мА	U_{lp} ,В
1.12	20.7	0.49	1.84
ВАХ n-канальных транзисторов			
U_{np1p} ,В	I_{n13} ,мА	U1n1 ,В	Sn1
20.9	>2.5	<1.64	>0.47
Контактное сопротивление			
R_{kp+} ,Ом	R_{kn+} ,Ом	R_{ks*} ,Ом	
17.2	2.4	2.4	

Таким образом, полученные в работе результаты показывают, что использование контроля тестовых элементов в производстве КМОП интегральных микросхем серии 1564 позволяет оперативно управлять технологическим процессом, а также обеспечивать изготовление более надежных интегральных микросхем.

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

Список литературы

[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] Strong A.W., Wu E.Y., Vollertsen R., Suñé J., Rosa G.L., Rauch S.E., Sullivan T.D. Reliability wearout mechanisms in advanced CMOS technologies. Wiley-IEEE Press. 2009. ISBN: 0471731722. 624 p.

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

Андреев Владимир Викторович – д-р техн. наук, профессор кафедры "Конструирование и производство электронной аппаратуры" КФ МГТУ им. Н.Э. Баумана. E-mail: andreev@bmstu-kaluga.ru

В.С. Кулагин, П.В. Кондрашов, В.В. Андреев

УСТАНОВКА КОНТРОЛЯ ВОЛЬТ-АМПЕРНЫХ ХАРАКТЕРИСТИК МДП-ТРАНЗИСТОРОВ

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

Полевой транзистор является одним из основных элементов цифровых интегральных микросхем. Наиболее часто используются транзисторы со структурой металл-диэлектрик-полупроводник [1-4].

Для расчета некоторых параметров транзисторов используются вольт-амперные характеристики. К таким характеристикам относится пороговое напряжение МДП транзисторов с индуцированным каналом. Это напряжение на затворе, которое приводит к образованию канала между стоком и истоком.

Пороговое напряжение используется при управлении транзистором. Оно определяет минимально допустимое значение напряжения питания, уровень токов потребления, помехозащищённость.

Приведенная установка позволяет снимать вольт-амперные характеристики МДП-транзисторов, а также определять величину порогового напряжения.

Алгоритм, написанный в среде разработки LabVIEW, подразумевает использование цикла для снятия ВАХ характеристик транзистора и получения данных в цифровом, либо графическом виде. Соответственно, выполнение программы возможно прервать в любой момент времени, в случае возникновения непредвиденных ситуаций.

Пороговое напряжение определяется методом постоянного тока. Он заключается в последовательном изменении напряжения затвор-исток. Таким образом, осуществляется последовательный подбор напряжения затвор-исток с одновременным измерением тока стока. Алгоритм измерения завершится при достижении током стока определенного значения, например, 10 мкА. Схема определения порогового напряжения показана на рисунке 1.

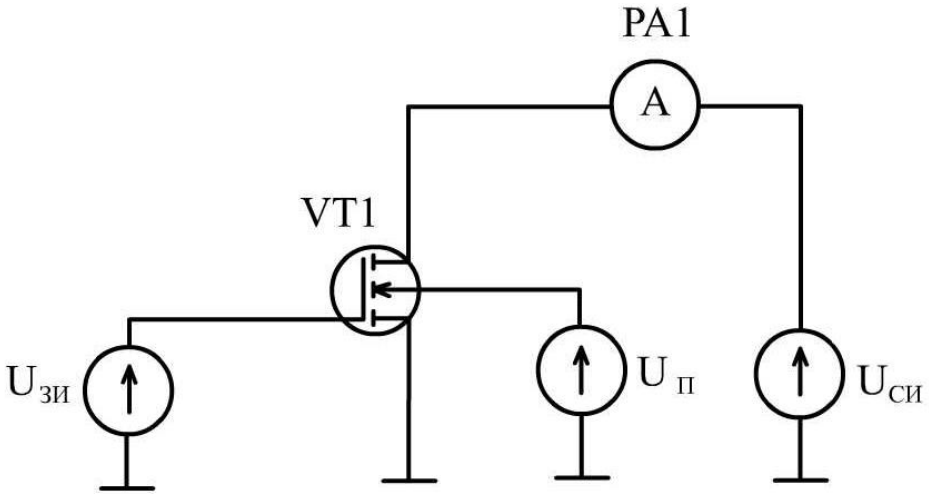

Рис. 1. Схема для получения ВАХ и определения порогового напряжения.

Установка реализуется при помощи модулей National Instruments NI PXI-6259 (АЦП/ЦАП), NI PXI-4132 (Высокоточный измеритель/источник питания), среды разработки LabVIEW.

Во время измерения на подложку подаётся нулевое смещение. Напряжение сток-исток поддерживается постоянным. Далее происходит постепенное увеличение напряжения затвор-исток с одновременным контролем тока стока. Если ток стока начинает превышать определенное значение (10 мкА), измерения прекращаются, а текущее значение напряжения затвор-исток будет являться пороговым для транзистора.

Напряжения затвор-исток, сток-исток, а также смещение подложки создаются с помощью ЦАП NI PXI-6259. Максимальная скорость обновления при таком режиме работы устройства составляет 1.54 Мвыб/сек на канал. Разрядность каждого канала составляет 16 бит. Диапазон допускаемых напряжений лежит в пределах от -10 до +10 В. Точность ЦАП на полном диапазоне – 2,08 мкВ.

Для контроля подаваемых напряжений на вход АЦП (NI PXI-6259) поступают три сигнала, формируемые ЦАП. Максимальная скорость обновления при работе с несколькими каналами составляет 1.25 Мвыб/сек на канал. Разрядность АЦП – 16 бит. Чувствительность – 1,92 мкВ.

Снятие тока стока осуществляется высокоточным измерителем NI PXI-4132. При этом максимальная точность измерения тока составляет 10 пА с интервалом измерения 1 мкс.

Управление модулями NI, задание значений необходимых напряжений, установка предельного значения тока стока осуществляется через алгоритм, написанный в среде LabVIEW.

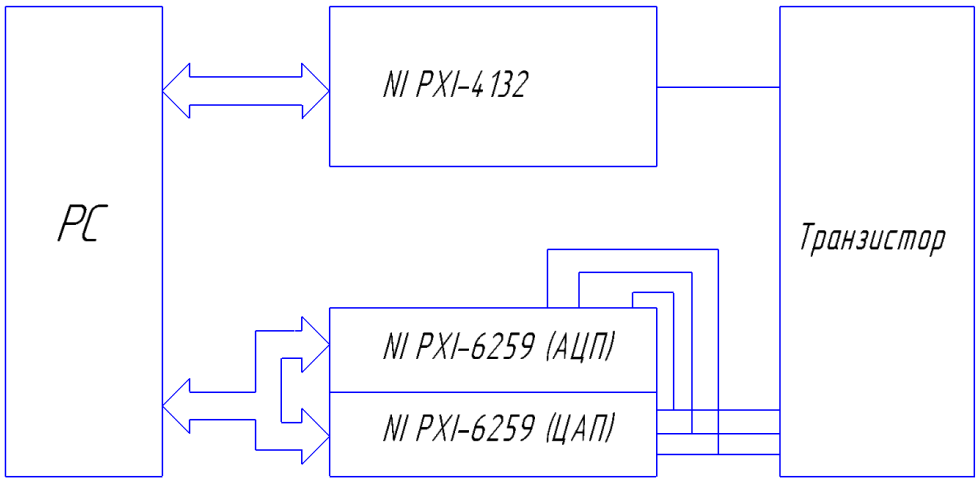

Рис. 2. Структурная схема установки измерения ВАХ

Установка предназначена для проведения научных исследований, а также может использоваться для контроля параметров промышленно выпускаемых МДП-транзисторов.

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

Список литературы

[1] Зи С.М. *Физика полупроводниковых приборов.* – Москва: Мир, 1984. – 449 с.

[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] Андреев В.В., Бондаренко Г.Г., Столяров А.А., Васютин Д.С., Михальков А.М. *Исследование влияния режимов инжекционной модификации на зарядовое состояние подзатворного диэлектрика МДП-приборов* // Перспективные материалы. 2009. № 2. С.45-51.

[4] Столярский Э. *Измерения параметров транзисторов* – Москва: Р. и С., 1992. – 122 с.

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

Кондрашов Павел Вячеславович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: p.kondrashov.radio@yandex.ru

Андреев Владимир Викторович – д-р техн. наук, профессор кафедры "Конструирование и производство электронной аппаратуры" КФ МГТУ им. Н.Э. Баумана. E-mail: andreev@bmstu-kaluga.ru

СЕКЦИЯ 13.

ЗАЩИТА ИНФОРМАЦИИ

Р.Р. Ахтямов

DLP-СИСТЕМЫ

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

Системы информационной безопасности в наше время используют принцип комплексной защиты информации. Должным образом установленные и настроенные средства защиты информации (СЗИ) обеспечивают высокий уровень надёжности защиты от атак злоумышленников или вирусов. Но, тем не менее, проблема внутренних нарушителей довольно актуальна. В прошлом, на фоне компьютерных вирусов, хакеров и прочих злоумышленников, угрозы безопасности, исходящие со стороны собственных сотрудников, представлялись малореальными. Но в современном мире их действия, совершенные непреднамеренно или же, что встречается нередко – преднамеренно, могут повлечь за собой реальные угрозы для организации, в которой они работают [1].

DLP-системы проверяют рабочие операции на соответствие корпоративным политикам по соблюдению нормативных требований [2]. В автоматическом режиме выводятся различные предупреждения, в случаях нарушений политики безопасности, либо в случаях подвергания технологических ценностей и конфиденциальной информации риску несанкционированного доступа и различного рода действий, направленных на их уничтожение или компрометацию.

Центр аналитики Zecurion Analytics представил [3] предварительные итоги ежегодного исследования утечек информации. Только за 11 месяцев 2015 года зафиксирован рекордный ущерб от хакерских атак и случайных утечек – более $27 млрд, сообщает компания Zecurion Analytics. Средний ущерб от одной утечки в мире также увеличился и составил $33,22 млн. В 2014 г. одна утечка в среднем стоила компаниям $25,29 млн. Одной из причин резкого увеличения денежных потерь послужил возросший интерес киберпреступников к конфиденциальным данным организаций и уменьшение доли атак на отдельных пользователей. Это объясняется тем, что объёмы украденной корпоративной информации оказываются намного больше по сравнению с данными отдельно взятых людей, при этом трудоёмкость получения информации одного человека существенно ниже, пояснили в компании. В целом количество преднамеренных утечек существенно не изменилось по сравнению с 2014 годом и составило 36,8% всех инцидентов.

Тем не менее, ущерб от утечек, совершённых преднамеренно, заметно больше. В результате целенаправленных атак и случайных утечек в 2014 г. чаще всего "утекали" финансовые сведения физлиц. Их доля за 2015 год возросла почти в два раза, с 10,8% до 19,2%. Такая информация обычно

легко монетизируется и высоко котируется на чёрном рынке, отметили в Zecurion Analytics. Прочие персональные данные, например, e-mail, телефон, паспортные данные, по-прежнему лидируют среди типов скомпрометированной информации, доля которых составила 59,6%. Анализируя эти данные, несложно объяснить рост интереса к DLP-системам в последние несколько лет.

DLP-системы проверяют рабочие операции на соответствие корпоративным политикам по соблюдению нормативных требований. В автоматическом режиме выводятся различные предупреждения, в случаях нарушений политики безопасности, либо в случаях подвергания технологических ценностей и конфиденциальной информации риску несанкционированного доступа и различного рода действий, направленных на их уничтожение или компрометацию.

Программное обеспечение, входящее в состав DLP-систем, как правило, обеспечивает следующие возможности:

- мониторинг рабочего стола;
- мониторинг сетевой активности;
- мониторинг доступа к USB – носителям и внешним устройствам;
- мониторинг запущенных процессов и приложений;
- мониторинг локальных действий.

Мониторинг рабочего стола может быть реализован 2 различными способами - администратор в своей системе в реальном времени наблюдает то же изображение, которое в настоящий момент видит пользователь, или же анализирует сделанные ранее скриншоты экрана. В дальнейшем полученные данные могут быть использованы как вещественные доказательства нарушения условий трудового договора. Также имеются иные способы сделать снимок экрана, к примеру, утилита ScreenCapture.

Мониторинг сетевой активности. Сеть Интернет является крайне распространённым каналом утечки конфиденциальной информации, в связи с чем системы контроля за действиями пользователей контролируют различные вариации сетевой активности сотрудников.

Мониторинг посещаемых сотрудником интернет-ресурсов позволяет обнаружить нецелевое использование рабочего времени, а отслеживание запросов сотрудника в различных поисковых системах позволяет проверить их соответствие рабочим нуждам. Сохраняются адреса посещённых сайтов, их заголовки, а также время и дата их посещения.

Мониторинг электронной почты. Осуществляется журналирование всех сообщений электронной почты. Зачастую это достигается путём перехвата сообщений используемой почтовой программы-клиента, но возможно перехватить и сообщения, отправляемые (полученные) с использованием веб-браузера, что может быть реализовано 2 способами:

1. Перехват собственно сетевого трафика программным или аппаратным путём (неприменимо в случае использования защищённого соединения);

2. Перехват содержания полей ввода, web-форм и др. При использовании данного метода скрыть получаемые (передаваемые) сообщения крайне сложно.

Instant Messaging (сокращённо – IM). Для предотвращения, либо последующего доказательства произошедшей утечки конфиденциальной информации, осуществляется перехват и сохранение сообщений многих распространённых IM-мессенджеров и протоколов, таких, как Skype, Jabber, Miranda, ICQ и пр. Данные операции выполняются либо с помощью программных средств, либо с помощью анализа сетевого трафика, проходящего через шлюз.

Социальные сети (ВКонтакте, Одноклассники, Facebook, Twitter и пр.). Наряду с нецелевой растратой рабочего времени, через социальные сети может происходить утечка конфиденциальной информации. Для противодействия этому система отслеживает и сохраняет следующие данные: посещённые профили, диалоги и передаваемые (или получаемые) в них файлы.

Мониторинг доступа к USB – носителям и внешним устройствам. Легко подключаемые и удаляемые USB-носители могут напрямую угрожать безопасности конфиденциальной информации. Многие системы мониторинга предоставляют возможность фильтрации устройств, запрета доступа ко всем внешним устройствам, и журналирование использования USB-носителей. Часто, в случае наличия доступа, все данные, копируемые на съёмный носитель, скрытно сохраняются в другом месте, что в дальнейшем может быть использовано для расследования нарушений внутренней политики компании. Это может быть реализовано следующими способами:

- полная блокировка через системный реестр;
- полная блокировка через прямой запрет записи в определённые системные файлы (например, %SystemRoot%\Inf\Usbstor.inf);
- использование соответствующего USB-драйвера.

Мониторинг запущенных процессов и приложений контролирует запущенные приложения и процессы, записывая различные параметры: время запуска, время работы, название, ID процесса и т.д. С помощью этих данных возможно оценить эффективность использования сотрудником рабочего времени или вовремя распознать потенциальную вирусную угрозу, способную нанести непоправимый ущерб. Многие системы дают возможность блокировать запуск заранее определённых приложений и процессов, наряду с возможностью удалённого завершения уже запущенных сотрудником приложений и процессов.

Мониторинг локальных действий.

Мониторинг нажатий клавиатуры (опционально – мыши). Система отслеживает все нажимаемые пользователем клавиши (в том числе и системные), помимо этого, записывается название окна, которое было активно в

момент ввода, язык ввода и т.п. Подобные программы реализуются с использованием так называемых «хуков», когда между нажатием клавиши и отправкой сообщения окну о факте нажатия внедряется специальная функция, фиксирующая нажатие клавиши.

Печать файлов. Через напечатанный сотрудником документ возможна утечка конфиденциальной информации, достаточно просто вынести его с предприятия или отправить с помощью факса. В связи с этим целесообразно хранить названия выводимых на печать файлов, наряду со временем печати. В дополнение к этой мере, эти файлы могут быть скрытно сохранены в другом месте. Для этого имеется Print Spooler API, используемый для контроля очереди печати.

Мониторинг действий над файлами: создание файлов, удаление, копирование, открытие, изменение и т.д. Даёт возможность определять использованные сотрудником для рабочих (или нерабочих) нужд файлы и выявить потенциальную вирусную угрозу.

Буфер обмена. Система мониторинга отслеживает и сохраняет все скопированные в буфер обмена данные, что позволяет не допустить утери информации и выявить разглашение конфиденциальной информации. Для этих целей существует специальная функция SetClipboardViewer.

Практика показывает, что большая часть ставших известными утечек (порядка 3/4) происходит не по злому умыслу, а из-за ошибок, невнимательности, безалаберности, небрежности работников. Выявлять подобные утечки проще. Остальная часть связана со злым умыслом операторов и пользователей информационных систем. Понятно, что эти внутренние нарушители, как правило, стараются преодолеть средства DLP-систем. Исход этой борьбы зависит от многих факторов. Гарантировать успех здесь невозможно. Применение специальных программных средств может поднять на новый качественный уровень систему комплексной безопасности предприятия.

Список литературы

[1] Горбачевская, Е.Н., Краснов, С.А. Анализ структуры системы информационной безопасности предприятия с централизованной авторизацией пользователей // Вестник Волжского университета имени В.Н. Татищева. – №4(22). – С. 63-74.

[2] Жадаев, А.Г. Как защитить компьютер на 100%. – СПб.: Питер, 2014. – 304 с.

[3] Глобальное исследование утечек конфиденциальной информации за 2015 год. URL: https://www.anti-malware.ru/news/2015-12-23/17652

Ахтямов Ренат Рашидович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: renat08051993@gmail.com

К.А. Празян, А.Б. Лачихина

XML-ИНЪЕКЦИИ

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

Веб-сервисы становятся неотъемлемой частью Всемирной Паутины. Веб-разработчики используют новые технологии хранения и обработки данных. Одной из таких технологий является XML (eXtensible Markup Language - универсальный расширяемый язык) [4, 5]. Этот язык во многом схож с языком разметки гипертекстовых страниц (HTML), что послужило его широкому распространению. Язык XML является унифицированным языком, и на сегодняшний день существует огромное количество библиотек для работы с ним. Как правило, файл формата XML содержит информацию об объектах, выраженную описательным языком. Все свойства объектов находятся внутри “тегов”, которые позволяют задать имя свойства и его атрибуты.

Типовой файл XML может содержать следующий код:

```
<?xml version="1.0"?>
<catalog>
  <book id="bk101">
   <author>Gambardella, Matthew</author>
   <title>XML Developer's Guide</title>
   <genre>Computer</genre>
   <price>44.95</price>
   <publish_date>2000-10-01</publish_date>
   <description>An in-depth look at creating applications
   with XML.</description>
  </book>
  <book id="bk102">
   <author>Ralls, Kim</author>
   <title>Midnight Rain</title>
   <genre>Fantasy</genre>
   <price>5.95</price>
   <publish_date>2000-12-16</publish_date>
   <description>A former architect battles corporate zombies,
   an evil sorceress, and her own childhood to become queen
   of the world.</description>
  </book>
</catalog>
```

В данном примере описан книжный каталог, содержащий автора, название, жанр, цену, дату публикации и описание каждой книги. XML позволяет создавать собственные теги и атрибуты.

Таким образом, удобство и схожесть XML с HTML дало возможность веб-разработчикам использовать XML для хранения данных. Иными словами, обходиться без СУБД. Такой подход предлагает свои преимущества:

отпадает необходимость беспокоиться об уязвимости языка запросов SQL, а также об уязвимостях самих СУБД.

Для упрощения работы с XML как контейнерами данных была создана специальная библиотека XPath. Она позволяет работать с файлом XML как с базой данных, совершая запросы и получая ответы из файла [3].

Например, веб-сервис с авторизацией пользователей может содержать следующий файл XML с авторизационными данными пользователей (accounts.xml):

```
<?xml version="1.0"?>
<users>
  <user id="12345">
   <login>Root</login>
   <pass>sTrongPassword</pass>
   <firstName>Admin</firstName>
  </user>
  <user id="12346">
   <login>User</login>
   <pass>weakpass</pass>
   <firstName>User_One</firstName>
  </user>
  <user id="12347">
   <login>foo</login>
   <pass>bar</pass>
   <firstName>foobar</firstName>
  </user>
</users>
```

Содержимое файла довольно простое: в качестве информации о пользователе используется логин, пароль и имя пользователя. Составленный специальным образом запрос к этому файлу позволит проверить существование пользователя и правильность ввода пароля.

Скрипт, обрабатывающий запросы на авторизацию серверу, может выглядеть следующим образом:

```
<?php
$login = $_POST['login'];
$pass = $_POST['pass'];
$xml = simplexml_load_file('accounts.xml');
// Формируем XPath-запрос
$query = "//users/user[login/text()='$login' and password/text()='$pass']";
// Выполняем запрос
$result = $xml->xpath($query);
if(!$result)
{
die("User credentials are not correct");
}
$user_data = $result[0];
```

```
$id = $user_data->id;
$firstname = $user_data->firstname;
/**/
?>
```

В данном случае переменные *login* и *pass* никак не фильтруются и идут в запрос в неизменном виде, позволяя злоумышленнику отправить особым образом сформированные данные. В отличие от SQL-injection [1, 2], в котором достаточно было написать в поле ввода, например, следующее содержимое:

admin’ OR 1=1 -- ,

где символы “--” означают начало комментария и позволяют обойти проверку пароля для пользователя admin. В XPath не существует возможности добавить комментарии к запросу, но достаточно изменить текст в поле ввода на

‘ or ‘1’=’1 ,

и в результате запрос в XPath изменится и будет выглядеть:

//users/user[login/text()=admin and password/text()=’‘ or ‘1’=’1′] .

В результате выполнится запрос or 1=1, который является заведомо верным, и злоумышленник получит доступ без знания пароля для пользователя admin.

В статье был показан пример использования XML как хранилища данных, а также уязвимость в способе получения данных из XML. В общем случае инъекции в XML во многом похожи на SQL-injection [1, 2], однако, в силу отсутствия в XPath некоторых механизмов, эксплуатация усложняется, но остается осуществимой.

Список литературы

[1] Празян К.А., Лачихина А.Б. Классификация атак SQL-инъекцией. Расширенные способы атак. – Вопросы радиоэлектроники, серия общетехническая, 2015, вып.6. С.82-88.

[2] Празян К.А., Лачихина А.Б. Классификация атак SQL-инъекцией. Типовые примеры классических атак. – Вопросы радиоэлектроники, серия общетехническая, 2015, вып.6. С.88-94.

[3] Празян К.А., Лачихина А.Б. JSON-уязвимости формата NoSQL. – Вопросы радиоэлектроники, серия общетехническая, 2016, вып.2.

[4] “Extensible Markup Language (XML) 1.0 (Second Edition) - W3C Recommendation, 6 October 2000”, http://www.w3.org/TR/REC-xml

[5] “XML Path Language (XPath) 2.0 – W3C Working Draft, 12 November 2003”, http://www.w3.org/TR/xpath20/

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

П.А. Чувак

АЛГОРИТМЫ СИСТЕМЫ КОНТРОЛЯ УПРАВЛЕНИЯ ДОСТУПОМ С РАСПОЗНОВАНИЕМ ЛИЧНОСТИ ПО ЛИЦУ

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

На объекте с высшим уровнем безопасности приоритетом служит надежность идентификации пользователей. Очевидно, что в СКУД таких объектов применение биометрии не только возможно и желательно, но и жизненно необходимо. Однако здесь на первый план выходят технологии, обеспечивающие наименьший уровень ошибок FAR (идентификация по отпечаткам пальцев, радужной оболочке глаз и др.), и технология распознавания по лицу используется как одна из составляющих мультибиометрических решений.

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.

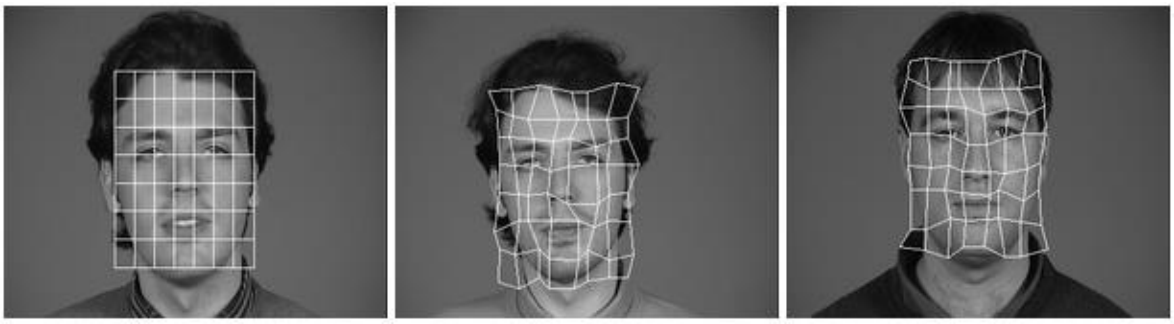

Рис. 2. Пример деформации графа в виде регулярной решетки

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.

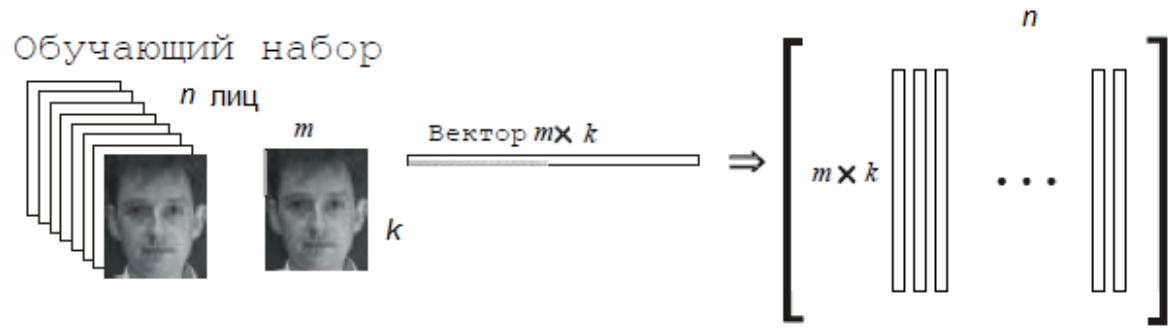

Рис. 3. Преобразования обучающего набора лиц в одну общую матрицу X

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.

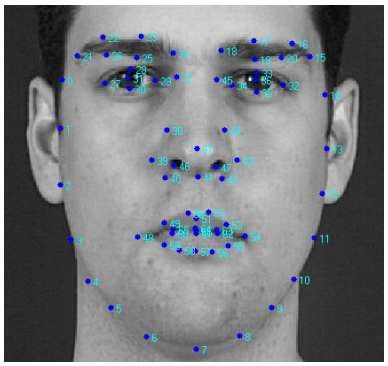

Рис. 4. Пример разметки изображения лица из 68 точек, образующих форму AAM

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

А.А. Корнеев, А.В. Мазин

АНАЛИЗ МЕТОДОВ МОДЕЛИРОВАНИЯ ЭЛЕКТРИЧЕСКИХ СХЕМ, ОБЕСПЕЧИВАЮЩИХ ФУНКЦИОНАЛЬНУЮ БЕЗОПАСНОСТЬ СИСТЕМ

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

Разработка грамотного и технически правильного схемотехнического решения при производстве электронной аппаратуры является одной из наиболее важных задач, особенно, если к изделию предъявляются повышенные требования к надежности, или оно служит для обеспечения безопасности, в той или иной степени. Проверка работоспособности узла или схемы в целом экспериментальным путем не является возможной или очень трудоемка и несёт за собой иногда большие материальные затраты.В таких случаях следует прибегнуть к математическому моделированию в виртуальных пакетах.

Темой данной работы является сравнение возможностей симуляторов электронных схем с реальными, полученными опытным путём.

Главной задачей перед физической реализацией необходимого устройства следует выбрать наиболее оптимальные и распространенные системы автоматизированного проектирования, собрать в каждой из них узел или схему целиком, промоделировать ее составляющие, сравнить результаты анализа с реальными и исключить наиболее недостоверные.

В качестве объекта исследования выбран генератор опорного сигнала [1]. Данное устройство можно реализовать на множестве простейших операционных усилителях. Форма выходного сигнала - пилообразная, с частотой ~4 кГц.

Исследования выходных сигналов производились при помощи цифрового запоминающего осциллографа TektronixTDS2012S. Главными особенностями данного приборами являются: обеспечение точного сбора данных в режиме реального времени во всей полосе частот, проведение анализа и выявление проблем в цепях обеспечения контроля качества на производстве и функциональной безопасности в изделии.

Исследована схема задающего генератора опорного сигнала, получены результаты моделирования с трех разных точек (1’, 2’ и 3’). В данном схемотехническом решении был применён отключаемый трансформатор, предназначенный для гальванической развязки выходного сигнала с коэффициентом трансформации 1:1.

При моделировании были исследованы пакеты ПП MultiSim от компании National Instruments, Quite Universal Circuit Simulator, и LTspice от фирмы Linear Technology [2-4]. В результате исследований были получены несколько осциллограмм и временных диаграмм выходных сигналов.

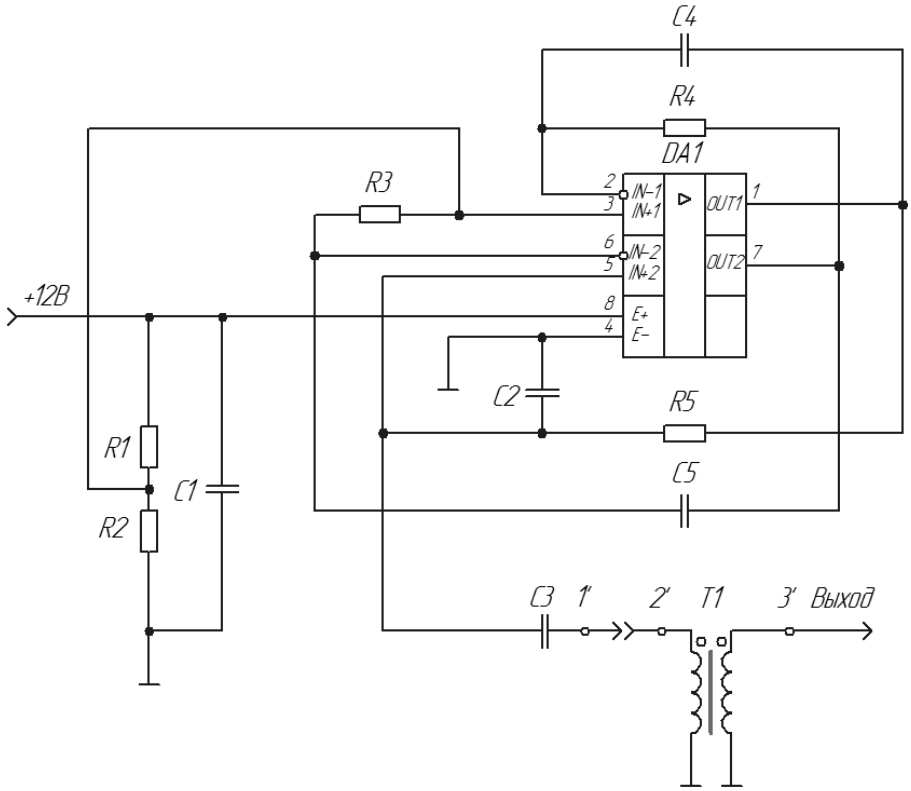

Рисунок 1. Схема электрическая генератора опорного сигнала

Вывод: LTspice имеет достаточно сложный графический интерфейс, проблемы с моделированием в реальном времени (real-time simulation), но практически идеально справляется с поставленными задачами.

Литература:

[1] Хернитер Марк Е. Multisim 7: Современная система компьютерного моделирования и анализа схем электронных устройств. (Пер. с англ.) / Пер. с англ. Осипов А.И. – М.: Издательский дом ДМК-пресс, – 2006. – 488 с.: ил.

[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 Networks, Devices and Fields. – 2008. – September. – Vol. 22, no. 4. – Pp. 297 – 319.

[4] Кузнецов В.В., Крючков Н.М. Qucs: Использование свободного ПО для моделирования электронных схем в учебном процессе/ XI конференция разработчиков свободных программ: Тезисы докладов/ Калуга, 26–28 сентября 2014 года. М.: Альт Линукс, 2014.

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

Мазин Анатолий Викторович – д-р техн. наук, заведующий кафедрой "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: mazinav@yandex.ru

Я.А. Фотина, А.Б. Лачихина

ВЕРИФИКАЦИЯ И ВАЛИДАЦИЯ ПРОГРАММНЫХ СИСТЕМ

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

В современном мире информационные технологии все более плотно внедряются в повседневную жизнь людей. Еще в 1995 г. учеными было установлено, что человек в целом за день взаимодействует с 25 устройствами, обрабатывающими информацию. Вместе с тем до 20% стоимости таких крупных систем, как автомобили, самолеты и поезда приходятся на программное обеспечение. Вследствие высокой интеграции информационных технологий во многие сферы деятельности человек вынужден все больше полагаться на надежность программных и аппаратных средств, что особенно важно в эксплуатации систем, критичных в отношении безопасности (например, атомные электростанции). Сложность программного обеспечения растет быстро, и как следствие повышается риск возникновения различного рода ошибок. Кроме того, важное значение имеет финансовая составляющая последствий этих ошибок [1].

Поэтому в настоящее время все большую значимость приобретают методы и технологии, позволяющие предотвратить возникновение всевозможных уязвимостей программных и аппаратных средств. Особую важность имеет обеспечение качества программного обеспечения, так как в современных системах с его помощью реализуется основная функциональность. К таким технологиям относятся верификация и валидация. Верификация и валидация – родственные процессы, направленные, однако, на получение разного результата.

Верификация – это проверка на соответствие программного обеспечения той технической документации, которая представлена техническим заданием, архитектурой или моделью предметной области. В общем смысле верификация обозначает соответствие предопределенным эталонным характеристикам конечного продукта. Кроме того, под верификацией понимается процесс или акт подтверждения подлинности данных. Цель верификации – обеспечение гарантий того, что промежуточное программное изделие или конечная продукция отвечает установленным требованиям. Принципом верификации является знание о том, что система поддается экспериментальной проверке. Верификация является нарастающим процессом. Она начинается с верификации требований, затем следует верификация промежуточных продукций на различных стадиях их разработки и заканчивается верификацией конечной продукции. Результатом этого процесса является вывод о соответствии или несоответствии продукта своей спецификации. Таким образом, можно сказать, что верификация отвечает на вопрос: «Строим ли мы систему правильно?» [2]

В отличие от верификации валидация представляет собой проверку на соответствие разрабатываемого программного обеспечения требованиям, предъявленным заказчиками или пользователями. Подобного рода требования не отражаются в документации, поэтому валидация – менее формализованный процесс, чем верификация. Целью валидации является доказательство того, что все требования конкретного пользователя программного продукта удовлетворены. Результат валидации – вывод о возможности применения продукта для конкретных условий. Следовательно, валидация отвечает на вопрос: «Строим ли мы правильную систему?»

Таким образом, разница между верификацией и валидацией существенна: верификация показывает, насколько технически правильно реализована программная продукция; валидация отражает степень соответствия продукта требованиям заказчика. Поэтому верификация производится всегда, а потребность в валидации может отсутствовать [3].

Если рассматривать данные понятия с позиции информационной безопасности, то можно сказать, что верификация является более значимой, чем валидация. Сама по себе верификация – сложный процесс, и в настоящее время область информационных технологий, связанная с верификацией, мало изучена. Поэтому в истории человечества существует немало примеров, свидетельствующих о том, что некачественно проведенная верификация может стать причиной человеческих жертв и материальных потерь.

Подводя итог, можно сказать, что верификация и валидация занимают важное место в сфере информационных технологий, в частности, в области информационной безопасности. В настоящее время ведутся активные разработки, направленные на совершенствование различных методов верификации и развитие новых, поэтому перспективы исследования в этой области очевидны.

Литература

[1] Лаврищева Е.М., Петрухин В.А. Методы и средства инженерии программного обеспечения: учебник. М.: МФТИ, 2006, 304 с.

[2] Рудаков И. В., Гурин Р.Е., Ребриков А.В. Верификация программного обеспечения: обзор методов и характеристик. Ежемесячный журнал. 2014. №3, ч. 2, 22-26 с.

[3] Синицын С.В., Налютин Н.Ю. Верификация программного обеспечения. М.: БИНОМ, 2008, с. 28-55.

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

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

В.А. Шавернев

ВИРУС, ШИФРУЮЩИЙ ДАННЫЕ

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

Введение. 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 де-

ло. 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 Александрович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: barus625@gmail.com

Е.А. Коваленко, Т.С. Белова, А.Н. Молчанов

ВОПРОСЫ ПРОГРАММНОЙ РЕАЛИЗАЦИИ АЛГОРИТМА ШИФРОВАНИЯ ДАННЫХ AES

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

Одним из принципов создания алгоритмов шифрования является простота, который позволяет минимизировать вероятность программных ошибок, даёт возможность анализа и уменьшает закрытость алгоритма. В тоже время возрастающие требования к криптостойкости вынуждают разработчиков использовать новые и более сложные операции для шифрования данных. В статье рассматривается симметричный алгоритм блочного шифрования AES (Advanced Encryption Standard), а также сложные для понимания этапы его программной реализации.

Принцип работы алгоритма заключается в разбиении информации, подлежащей шифрованию, на блоки фиксированной длины по 128 бит. При этом исходная информация представляет собой последовательность чисел в шестнадцатеричной системе.

Алгоритм шифрования AES представляет собой следующую последовательность действий:

1. Формирование раундовых ключей (Expand_key).
2. Сложение блока исходного текста State с ключом шифрования (Add_Cipher_key).
3. Выполнение следующих действий в цикле, каждая итерация которого называется раундом:
   - замена байтов исходного текста, используя таблицу подстановок (Subbytes);
   - циклический сдвиг данных в блоке на различные величины (ShiftRows);
   - смешивание данных в каждом столбце блока (Mix_Columns);
   - сложение данных в блоке с раундовым ключом (Add_Round_key).

Количество раундов равняется 10. В каждом раунде применяется свой раундовый ключ из списка ключей, сформированных на первом шаге. В последнем раунде операция Mix_Columns не применяется.

В процессе программной реализации данного алгоритма могут возникнуть трудности в понимании принципа работы некоторых его этапов. Наиболее сложным является этап формирования ключей.

Первый раундовый ключ формируется из ключа шифрования Cipher_key, имеющего длину 128 бит и записанного в таблицу из 16 байт. Каждый последующий раундовый ключ формируется из предыдущего. Все раундовые ключи, так же, как и Cipher_key имеют длину 128 бит.

Ячейки последнего столбца ключа, из которого формируется текущий раундовый ключ, циклически сдвигаются вверх, после чего каждый байт полу-

ченного вектора заменяется на соответствующий ему байт в таблице table_S_Box (рис. 1). После этого каждый байт вектора складывается по модулю 2 с соответствующим вектором таблицы Rcon (рис. 2), а также с вектором, представляющим собой первый столбец таблицы ключа, из которого формируется текущий. Формирование раундовых ключей показано на рисунке 3.

X \ Y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Рисунок 1. S-Box

01	02	04	08	10	20	40	80	1b	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

Рисунок 2. Rcon

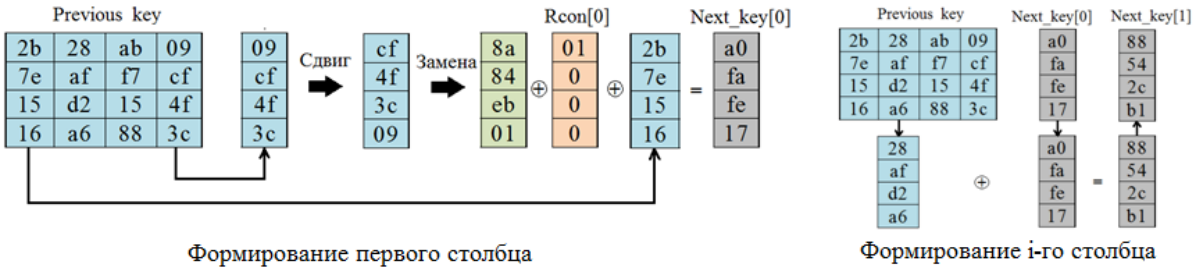

Рисунок 3. Формирование раундовых ключей

Последующие столбцы раундового ключа формируются путем сложения по модулю 2 байтов вектора, полученного на предыдущем шаге, и байтов следующего вектора ключа, из которого формируется текущий.

При сложении с Cipher_key каждый байт таблицы State складывается с соответствующим байтом таблицы Cipher_key по модулю 2. Сложение осуществляется в соответствии с формулой: $A \oplus B = (A + B) - 2 \bullet (A \& B)$.

Для формирования последовательности ключей в программной реализации создадим функцию Form_keys, которая, в свою очередь, в цикле бу-

дет использовать функцию Form_one_key, отвечающую за формирование одного ключа. Таким образом исходный код программы может быть написан в следующем виде

```
private List<string> Form_one_key(List<string> Previous_key, int
count_table)    {
    List<string> move_column = new List<string>();
        move_column = ShiftLastCell(Previous_key);
    List<string> replace_column = new List<string>();
        replace_column = ReplaceLastCell(move_column,table_S_Box);
        List<string> next_key_list = new List<string>();
        next_key_list = Add_Module2(Previous_key,replace_column,
      count_table, next_key_table)
}
```

В функцию Form_one_key передается предыдущий ключ Previous_key, необходимый для формирования ключа, который будет добавлен в next_key_list, а также счетчик count_table, отвечающий за номер вектора таблицы Rcon. С помощью функции ShiftLastCell происходит сдвиг последнего столбца матрицы Previous_key, затем происходит замена элементов этого столбца с помощью функции ReplaceLastCell. После этого к матрице Previous_key применяется функция сложения по модулю 2 Add_Module2.

Следующая сложность появляется при реализации функции Mix_Columns, которая отвечает за перемешивание байтов в столбцах блока State. При этом каждый столбец блока данных рассматривается как полином над полем GF(2^8) и умножается по модулю $x^4 + 1$ на фиксированный полином: $a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x^1 + \{02\}$

Новое значение каждого байта столбца образуется в соответствии со следующими выражениями:

$$S'_{0,y} = (\{02\} \bullet S_{0,y}) \oplus (\{03\} \bullet S_{1,y}) \oplus S_{2,y} \oplus S_{3,y}$$
$$S'_{1,y} = S_{0,y} \oplus (\{02\} \bullet S_{1,y}) \oplus (\{03\} \bullet S_{2,y}) \oplus S_{3,y}$$
$$S'_{2,y} = S_{0,y} \oplus S_{1,y} \oplus (\{02\} \bullet S_{2,y}) \oplus (\{03\} \bullet S_{3,y})$$
$$S'_{3,y} = (\{03\} \bullet S_{0,y}) \oplus S_{1,y} \oplus S_{2,y} \oplus (\{02\} \bullet S_{3,y})$$

- При умножении на {01} умножаемое не изменяет своего значения.
- Умножение на {02} производится по правилу: если умножаемое значение меньше {80}, оно сдвигается влево на 1 бит. Если же умножаемое значение больше или равно {80}, оно сначала сдвигается влево на 1 бит, а затем к результату сдвига применяется операция XOR со значением {1b}. Результат может перескочить за значение {ff}, то есть за границы одного байта. В этом случае нужно вернуть остаток от деления результата на {100}.
- Умножение на другие константы можно выразить умножением на {01} и {02}. Например, $S_{x,y} \bullet \{03\} = S_{x,y} \bullet (\{01\} \oplus \{02\}) = S_{x,y} \bullet \{01\} \oplus S_{x,y} \bullet \{02\}$.

За перемешивание байтов в каждом из столбцов блока данных будет отвечать функция MixColumn, программный код которой продемонстрирован ниже.

```
    private List<string> Mix_Column(List<long> block_long)
//Перемешивание байтов текущего столбца
    {
        List<string> mixed_data = new List<string>();
            long s0 = Sum_mod2(Sum_mod2(Mult_2(block_long[0]),
        Sum_mod2(Mult_2(block_long[1]), block_long[1])),
        Sum_mod2(block_long[2], block_long[3]));
            long s1 = Sum_mod2(Sum_mod2(block_long[0],
        Mult_2(block_long[1])), Sum_mod2(Sum_mod2(Mult_2(block_long[2]),
        block_long[2]), block_long[3]));
            long s2 = Sum_mod2(Sum_mod2(block_long[0], block_long[1]),
        Sum_mod2(Mult_2(block_long[2]),
        Sum_mod2(Mult_2(block_long[3]), block_long[3])));
            long s3 =
        Sum_mod2(Sum_mod2(Sum_mod2(Mult_2(block_long[0]),
        block_long[0]), block_long[1]), Sum_mod2(block_long[2],
        Mult_2(block_long[3])));
            mixed_data = LongToString(s0, s1, s2, s3);
            return mixed_data;
    }
private long Mult_2(long a) //умножение байта на {02}
    {
     long res;
     if (a < 128)
       res = a * 2;
     else
     {
       res = a * 2;
       res = Sum_mod2(res, 27);
       if (res > 255)
         res = res % 256;
     }
     return res;
    }
```

Для наглядности применения данного алгоритма было создано приложение, которое реализует точную последовательность действий, входящих в алгоритм. Интерфейс приложения обеспечивает удобную работу пользователя, позволяя вводить текст и ключ шифрования в формате текста. Текст ключа по нажатию кнопки «Зашифровать» преобразуется в последовательность чисел в шестнадцатеричной системе и заносится в таблицу. Также у пользователя есть возможность посмотреть таблицы, необходимые в процессе шифрования и расшифровывания в выпадающем

списке «Таблицы»: S_Box, Rcon, InvS_Box. Для расшифровки текста необходимо нажать кнопку «Расшифровать» и в соответствующем поле появится расшифрованный текст. (Рис.5)

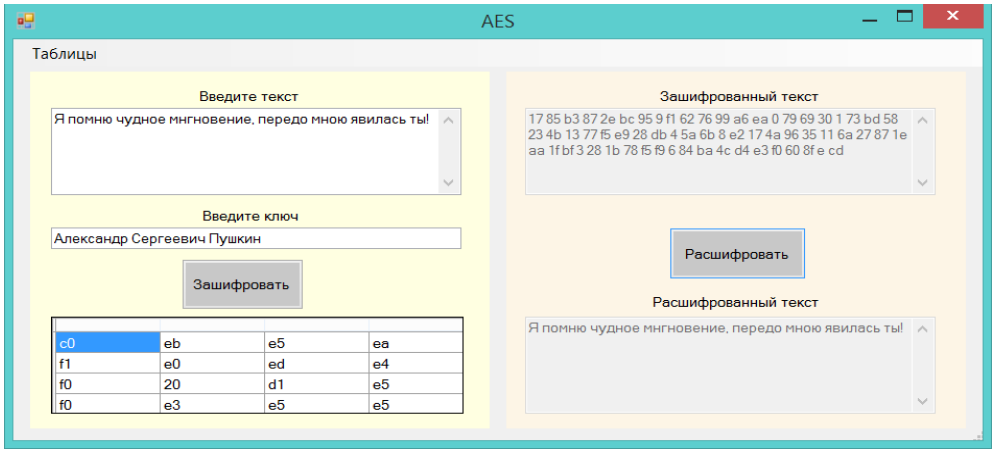

Рисунок 5. Демонстрация работы программы

В ходе проведения работы над выбранной темой был изучен алгоритм шифрования AES, рассмотрены последовательности действий, входящие в этап формирования раундовых ключей, этап шифрования и этап расшифровывания. Было создано пользовательское приложение, демонстрирующее работу данного алгоритма и реализующее точную последовательность шагов, входящих в алгоритм. Описана и продемонстрирована работа с созданным приложением. Также была освещена проблема сложности написания исходного кода программных продуктов, реализующих работу алгоритмов шифрования.

Литература

[1] *Ш. Брюс.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – Издательство: Триумф, 2012 г.

[2] *А.А. Молдовян, А.Н. Молдовян.* Криптография: скоростные шифры. – Издательство: BHV, 2014 г.

[3] *Н.А. Гатченко, А.С. Исаев, А.Д. Яковлев.* Криптографическая защита информации. Министерство образования и науки российской федерации Санкт–петербургский национальный исследовательский университет информационных технологий, механики и оптики, 2012

[4] *И.Н. Васильева*. Криптографические методы защиты информации. Учебник и практикум для академического бакалавриата. 2016

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

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

Молчанов Алексей Николаевич – ст. преп. кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: alexeymolchanov@yandex.ru

А.С. Макаров, А.Б. Лачихина

ВЫБОР ПОМЕХОУСТОЙЧИВОГО КОДА ДЛЯ СИСТЕМЫ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ ПРИ ОРГАНИЗАЦИИ СВЯЗИ С КОСМИЧЕСКИМИ АППАРАТАМИ

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

Особую роль при обеспечении информационного обмена с космическими аппаратами играет задача обеспечения достоверной и точной передачи данных. На космических аппаратах и наземной станции устанавливается радиокомплекс связи, который состоит из приемной и передающей части. При передаче цифровых данных по каналам, на которые могут воздействовать шумы, всегда существует вероятность того, что принятые данные будут содержать ошибки [1]. Для правильного взаимодействия с космическими аппаратами вся передаваемая информация (в том числе специальные команды управления) между наземной станцией и космическими аппаратами должна циркулировать без появления ошибок.

В системах связи возможны несколько стратегий борьбы с ошибками:

- обнаружение ошибок в блоках данных и автоматический запрос повторной передачи повреждённых блоков;
- обнаружение ошибок в блоках данных и стирание повреждённых блоков;
- исправление ошибок [2].

Наиболее эффективным способом борьбы с ошибками в данном случае является применение методов помехоустойчивого кодирования, которые предназначены для обнаружения и исправления возникающих ошибок без необходимости повторной передачи искаженных данных. Идея помехоустойчивого кодирования заключается в разнесении кодовых комбинаций за счет введения избыточности, при которой искажения элементов не приводят к изменению смыслового содержания сообщения. На сегодняшний день в теории кодирования существует множество кодов и методов их декодирования, различающихся корректирующей способностью, сложностью реализации и рядом других параметров [1]. Самыми распространенными группами помехоустойчивых кодов являются блоковые, сверточные и каскадные.

Основным критерием помехоустойчивого кода является его эффективность. Эффективность кода складывается из следующих компонентов:

- количество ошибок, исправляемых кодом;
- количество избыточной информации, которую необходимо добавить для обеспечения исправления определенного числа ошибок;

– техническая сложность реализации механизмов кодирования и декодирования.

В статье [3] приведен сравнительный анализ помехоустойчивых кодов. В данной статье описывается задача сравнения эффективности современных алгоритмов помехоустойчивого кодирования с кодовой скоростью 1/2 (данная скорость была выбрана в связи с тем, что в настоящее время в современных информационных системах, от увеличения избыточности кода до больших значений, а следствие, повышения надежности декодирования, акцент смещается на требования к высокой скорости передачи). Выполнялось сравнение следующих кодов: Рида – Соломона, сверточных и каскадных (турбо-кодов). Все они были примерно одной и той же избыточности. Основным ограничением являлось время декодирования пакета. Поставленная задача была решена в среде MatlabSimulink. Были разработаны модели цифровых систем связи (ЦСС) с различными кодерами в своем составе. Было проанализировано распределение серий ошибок в пакете с использованием смоделированного шумового воздействия аддитивного белого гауссовского шума [3].

Для декодирования Код Рида – Соломона, представляющего собой недвоичный циклический код, исправляющий ошибки в блоках данных, был использован алгоритм Берлекэмпа – Мэсси. Для декодирования сверточных кодов, которые являются непрерывными рекурсивными кодами (т.е. кодируемая последовательность не разделяется на блоки, а выход кодера – это свертка отклика линейной системы на входную информационную последовательность), был использован алгоритм Витерби. Для декодирования каскадных кодов (турбо-кодов), которые используют комбинацию разных алгоритмов кодирования для получения высокой эффективности кода, используется алгоритм максимума апостериорной вероятности. Все рассмотренные коды активно применяются для передачи данных в спутниковой связи [3].

По результатам проведенных исследований методов помехоустойчивого кодирования, каскадные коды имеют наименьшую вероятность битовой и пакетной ошибки. Таким образом, каскадные коды оптимально подходят для задач, в которых пакет с ошибками стирается. Но использование таких кодов ограничивает временная задержка декодирования, которая связана с тем, что отсутствует возможность раскодировать даже часть пакета, пока он не будет получен полностью (в остальных кодах такое возможно). Для тех случаев, когда пакеты с ошибками используются и одиночные ошибки более приемлемы, чем множественные, лучше подходят сверточные коды. Для случаев, когда пакеты с ошибками используются, вероятность появления множественных ошибок высока и смещается акцент в сторону повышения избыточности кода, а значит уменьшения скорости, наиболее подходящими являются коды Рида – Соломона [3].

Таким образом, при обеспечении информационного обмена с космическими аппаратами, для обеспечения помехоустойчивого кодирования циркулирующей информации, в данном случае наиболее оптимально подходит использование кодов Рида – Соломона.

Список литературы

[1] *Гринченко Н. Н., Овечкин Г. В.* Помехоустойчивое кодирование для цифровых систем связи // Известия ЮФУ. Технические науки. 2006. №15. URL: http://cyberleninka.ru/article/n/pomehoustoychivoe-kodirovanie-dlya-tsifrovyh-sistem-svyazi (дата обращения: 02.02.2017).

[2] *Морелос-Сарагоса Р.* Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / пер. с англ. В. Б. Афанасьева. – М.: Техносфера, 2006. – 320 с.

[3] *Сидоркина Ю. А., Шахтарин Б. И., Балахонов К. А.* Анализ эффективности современных помехоустойчивых кодов // Вестник МГТУ им. Н.Э. Баумана. Серия «Приборостроение». 2014. №6 (99). URL: http://cyberleninka.ru/article/n/analiz-effektivnosti-sovremennyh-pomehoustoychivyh-kodov (дата обращения: 02.02.2017).

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

М.А. Хорошилова

ВЫБОР СИСТЕМЫ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ С ПОЗИЦИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

В последнее время системы управлении базами данных (СУБД) стали неотъемлемой частью IT-инфраструктуры практически любой компании. Если раньше СУБД использовались для хранения текстовых и числовых данных, то сейчас в них хранятся данные различных форматов такие, как изображения, видеозаписи и др. Объёмы базы данных в некоторых отраслях выросли до нескольких терабайт. В связи с этим повышаются требования к надёжности, производительности и безопасности систем управления базами данных.

По данным Gartner на конец 2016 года лидирующие позиции на рынке среди СУБД занимает Microsoft SQL Server. Его доля составляет 46,8%, остальная часть рынка принадлежит Oracle и IBM DB2, относительно небольшую его часть занимают СУБД Open Source, такие как Postgre и Firebird.

Microsoft SQL Server. Microsoft SQL Server является новейшей и мощнейшей системой управления базами данных. Помимо стандартных функций, SQL Server содержит большой набор интегрированных служб по анализу данных. Доступ к данным, расположенным на SQL Server могут получить любые приложения, разработанные на .Net и VisualStudio, а также приложения пакета Microsoft Office 2007. SQL Server обеспечивает высочайшую в своём классе масштабируемость, производительность и безопасность.

Ввиду того, что на SQL Server работают критические бизнес-приложения, предприятия выдвигают очень жёсткие требования по производительности, отказоустойчивости и безопасности самой СУБД.

Таблица 1. Встроенные средства защиты данных в SQL Server

Средство	Описание
Проверка подлинности	Проверка подлинности - это процесс входа в SQL Server, в рамках которого участник запрашивает доступ путем подачи учетных данных, которые проверяет сервер. Во время проверки подлинности происходит идентификация пользователя или процесса.
Авторизация	Авторизация - это процесс определения того, к каким защищаемым ресурсам участник может получить доступ и какие операции с этими ресурсами ему разрешены.
Назначение роли сервера и роли базы данных	Безопасность на основе ролей, что позволяет назначать разрешения на доступ к данным роли или группе пользователей, а не отдельным пользователям.

Владение и разделение пользовательских схем	Отделение пользователей от схем обеспечивает дополнительную гибкость в управлении разрешениями объектов базы данных. Схема представляет собой именованный контейнер для объектов базы данных, позволяющий группировать объекты по отдельным пространствам имен.
Проверка прав доступа и разрешений	После создания объектов базы данных необходимо явно предоставить разрешения, чтобы сделать их доступными для пользователей. Каждый защищаемый объект имеет разрешения, которые могут быть предоставлены участнику с помощью инструкций разрешения.
Шифрование данных	SQL Server содержит функции шифрования и расшифровки данных с помощью сертификата и асимметричного или симметричного ключа. Все они содержатся во внутреннем хранилище сертификатов. Хранилище использует иерархию шифрования, обеспечивающую безопасность сертификатов и ключей на уровне, находящемся выше в иерархии. Эта область функций SQL Server называется секретным хранилищем.
Безопасность интеграции со средой CLR	Microsoft SQL Server обеспечивает интеграцию компонентов среды CLR платформы .NET Framework. Интеграция со средой CLR позволяет записывать хранимые процедуры, триггеры, определяемые пользователем типы, определяемые пользователем функции и потоковые возвращающие табличное значение функции, используя любой язык NET Framework. Среда CLR поддерживает модель безопасности, называемую управлением доступом для кода (CAS). В этой модели разрешения предоставляются сборкам на основе свидетельства, поставляемого кодом в метаданных. SQL Server интегрирует пользовательскую модель безопасности SQL Server с кодом модели безопасности на основе доступа среды CLR.

СУБД Oracle Database. Oracle Database - это объектно-реляционная система поддерживающая некоторые технологии, реализующие объектно-ориентированный подход, то есть обеспечивающих управление создания и использования баз данных. Программные средства Oracle поддерживают механизмы безопасности, основанные на стандартных алгоритмах защиты и встроенных методах работы с объектами для поддержания и сохранности хранимой в базе информации.

Таблица 2. Встроенные средства защиты данных в Oracle Database

Средство	Описание
Virtual Private Database (VPD)	Virtual Private Database (VPD) - средства разграничения доступа к данным на уровне строк и возможность организации работы пользователя только с виртуальной регламентированной частью данных, а не с реальной базой данных.

Oracle Advanced Security	Oracle Advanced Security - комплекс средств аутентификации и обеспечения сетевой безопасности, включающий в себя поддержку защищенных протоколов передачи данных, в том числе SSL.
Fine Grained Audit Control (FGAC)	Fine Grained Audit Control (FGAC) - инструмент подробного аудита.
Advanced Security	Advanced Security. Прозрачно шифрует все данные приложений или только определенные ряды данных, такие как номера кредитных карт, паспортные данные и другую персональную информацию. Таким образом, организации могут обеспечивать соответствие внутренним политикам и федеральным законам о защите информации. Инструмент шифрует данные в базе, а также при передаче и резервном копировании.

SQL Server – это база данных, которая уже шесть лет признается наименее уязвимой по результатам тестов на уязвимость в Национальном институте стандартов и технологий США (NIST). Нововведения SQL Server в области безопасности помогают защитить данные благодаря многоуровневому подходу к безопасности, добавляют технологию постоянного шифрования и обеспечивают безопасность на уровне строк, прозрачное шифрование данных (TDE), динамическую маскировку данных и надежный аудит.

Список литературы

[1] *Душан Петкович*. Microsoft SQL Server 2012. Руководство для начинающих. – БХВ-Петербург, 2013. – 816 с.

[2] *Александр Бондарь*. Microsoft SQL Server 2012. – БХВ-Петербург, 2013. – 608 с.

[3] *Поляков А. М*. Безопасность Oracle глазами аудитора: нападение и защита. – М.: ДМК Пресс, 2010. – 336 с.

[4] *Томас Кайт, Дарл Кун.* Oracle для профессионалов. Технологии и решения для достижения высокой производительности и эффективности. 3-е издание. – *Вильямс*, 2016. – 960 с.

[5] CNews. ИТ-зависимость: какую роль играют данные в современном бизнесе. URL: http://business.cnews.ru/articles/2016-06-16_itzavisimost_kakuyu_rol_igrayut_dannye_v_sovremennom_biznese.

Хорошилова Мария Александровна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: mary.hory@yandex.ru

Д.У. Белетова

ЗАЩИТА ДАННЫХ В СЕТЯХ WI-FI

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

Главной проблемой и задачей всех беспроводных локальных сетей является безопасность. Данные пользователя могут оказаться в руках злоумышленника, если он использует открытые точки доступа Wi-Fi дома или на рабочем месте и не использует шифрование либо VPN (Virtual Private Network – виртуальная частная сеть). Эта проблема еще тем серьезнее, что пользователь может передавать личную информацию или профессиональные данные, а сеть при этом не защищена от постороннего вторжения.

Все продукты для беспроводных локальных сетей, сертифицированные на соответствие спецификациям Wi-Fi, поставляются для работы в режиме открытого доступа с выключенными функциями безопасности. Открытый доступ или отсутствие безопасности могут быть уместны для общественных хот-спотов, таких как кофейни, университетские городки, аэропорты или другие общественные места, однако для предприятий этот вариант не подходит. Функции безопасности должны быть включены на беспроводных устройствах в процессе их установки. Некоторые компании не включают функции безопасности сетей WLAN, что значительно повышает уровень риска для таких сетей.

Базовая безопасность заключается в использовании идентификаторов сети SSID (Service Set Identifier), открытой аутентификации или аутентификации с использованием общего ключа, статических WEP-ключей и аутентификации по MAC-адресу. С помощью перечисленных опций можно настроить элементарные средства управления доступом и конфиденциальностью, однако каждый отдельный элемент такой защиты может быть взломан. Идентификатор SSID – это общее имя сети для устройств в подсистеме WLAN. Каждая беспроводная сеть имеет уникальное имя (SSID). SSID предотвращает доступ любого клиентского устройства, не имеющего SSID. По умолчанию точка доступа передает в эфир свой SSID среди своих сигналов, и даже если отключить передачу в эфир SSID, злоумышленник или хакер всё равно может обнаружить нужный SSID, используя так называемый «сниффинг» или незаметный мониторинг сети. Группа спецификаций для сетей WLAN стандарт 802.11, разработанная IEEE (англ. Institute of Electrical and Electronics Engineers – Институт инженеров электротехники и электроники), включает два средства аутентификации клиента: открытую аутентификацию и аутентификация с использованием общих ключей.

При аутентификации с использованием общих ключей точка доступа посылает на клиентское устройство тестовый текстовый пакет, который

клиент должен зашифровать правильным WEP-ключом и вернуть на точку доступа. Без правильного ключа аутентификация будет прервана и клиент не будет допущен в группу пользователей точки доступа. Аутентификация с использованием общих ключей не считается надежной, поскольку злоумышленник, получивший в свое распоряжение начальное тестовое текстовое сообщение и это же сообщение, зашифрованное WEP-ключом, может расшифровать сам WEP-ключ. При открытой аутентификации, даже если клиент проходит аутентификацию и получает доступ в группу пользователей точки доступа, использование WEP-защиты не позволяет клиенту передавать данные с этой точки доступа без правильного WEP-ключа. WEP-ключи могут состоять из 40 или 128 бит и обычно статически определяются сетевым администратором на точке доступа и каждом клиенте, передающем данные через эту точку доступа. При использовании статических WEP-ключей сетевой администратор должен потратить много времени на ввод одинаковых ключей в каждое устройство сети WLAN. Если устройство, использующее статические WEP-ключи, потеряно или украдено, обладатель устройства сможет получить доступ к сети WLAN. Администратор не сможет определить, что в сеть проник несанкционированный пользователь, до тех пор, пока не будет выявлен факт пропажи. После этого администратор должен сменить WEP-ключ на каждом устройстве, использующем тот же статический WEP-ключ, что и пропавшее устройство. В условиях сети крупного предприятия, включающей сотни или даже тысячи пользователей, это может оказаться затруднительно. Некоторые поставщики решений WLAN поддерживают аутентификацию на базе физического адреса или MAC-адреса, клиентской сетевой карты. Точка доступа позволит клиенту ассоциироваться с точкой доступа только в случае, если MAC-адрес клиента соответствует одному из адресов в таблице аутентификации, используемой точкой доступа. Однако аутентификация по MAC-адресу не является приемлемой мерой безопасности, поскольку MAC-адрес можно подделать, а сетевую карту – потерять или украсть.

Другая форма доступной на сегодняшний день базовой безопасности – это WPA или WPA2 с использованием общих ключей (Pre-Shared Key, PSK). Общий ключ проверяет пользователей с помощью пароля или кода идентификации ("фраза-пароль") как на клиентской станции, так и на точке доступа. Клиент может получить доступ к сети только в том случае, если пароль клиента соответствует паролю точки доступа. Общий ключ также предоставляет данные для генерации ключа шифрования, который используется алгоритмами TKIP или AES для каждого пакета передаваемых данных. Являясь более защищенным, чем статический WEP-ключ, общий ключ аналогичен статическому WEP-ключу в том, что хранится на клиентской станции и может быть взломан, если клиентская станция потеряна или украдена. Рекомендуется использовать сильную общую фразу-пароль,

включающую разнообразные буквы, цифры и не алфавитно-цифровые символы.

Базовая безопасность сетей WLAN, основанная на комбинации SSID, открытой аутентификации, статических WEP-ключей, MAC-аутентификации и общих ключей WPA/WPA2, является достаточной только для очень небольших компаний или тех, которые не доверяют жизненно важные данные своим сетям WLAN. Всем прочим организациям рекомендуется вкладывать средства в надежные решения безопасности сетей WLAN класса предприятия [1].

Повышенный уровень безопасности рекомендуется для тех, кому требуется безопасность и защищенность класса предприятия. Cisco Unified Wireless Network представляет собой решение безопасности повышенного уровня, полностью поддерживающее WPA и WPA2 со строительными блоками двусторонней аутентификации 802.1X и шифрования алгоритмами TKIP и AES. Cisco Unified Wireless Network включает следующие возможности:

- 802.1X для мощной двусторонней аутентификации и динамических ключей шифрования для каждого пользователя и каждой сессии;
- TKIP для расширения шифрования на базе RC4, например, хэширования ключей (для каждого пакета), проверки целостности сообщения (MIC), изменений вектора инициализации (IV) и ротации широковещательных ключей;
- AES для шифрования данных государственного уровня, максимальной защищенности;
- интеграция с Cisco Self-Defending Network и NAC;
- возможности системы предотвращения сетевых вторжений (Intrusion Prevention System, IPS) и слежения за перемещением абонента – прозрачное представление сети в реальном времени [2];

В некоторых случаях предприятиям может потребоваться всеобъемлющая безопасность для защиты бизнес-приложений. Воспользовавшись защищенным удаленным доступом, администраторы могут настроить виртуальную частную сеть (VPN) и позволить мобильным пользователям обмениваться данными с корпоративной сетью из общественных хот-спотов, например, аэропортов, отелей и конференц-залов[3]. При развертывании на предприятии решения повышенной безопасности, такое как Cisco Unified Wireless Network, использовать виртуальные частные сети в корпоративной сети WLAN становится необязательно, так как посредством указанного решения выполняются все требования к безопасности беспроводных локальных сетей. Использование VPN во внутренней сети WLAN может повлиять на производительность сети WLAN, ограничить возможности роуминга и сделать процедуру входа в сеть более сложной для пользователей [4]. Таким образом, дополнительные накладные расходы и ограничения,

связанные с наложением VPN-сети на внутреннюю сеть WLAN, не представляются необходимыми [5].

Таким образом, технология WPA2 с использованием алгоритма AES для шифрования данных обеспечит более высокий уровень защищенности беспроводной сети по сравнению с WPA, использующий RC4 с динамическими ключами. Для обеспечения высокого уровня безопасности можно воспользоваться решениями, которые полностью поддерживают WPA и WPA2 с двухсторонней аутентификацией 802.1X и шифрованием алгоритмами TKIP и AES. Если требуется защищенный удаленный обмен данными пользователям, то можно настроить виртуальную частную сеть.

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)

[5] [Электронный ресурс] Что такое аутентификация и ассоциация по протоколу IEEE* 802.11. URL: http://www.intel.ru/content/www/ru/ru/support/network-and-i-o/wireless-networking/000006508.html (дата обращения 24.11.2016)

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

И.И. Золотин

ЗАЩИТА ИНФОРМАЦИОННЫХ СИСТЕМ ПРИ ПОМОЩИ БРАНДМАУЭРА

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

В настоящее время одной из самых актуальных является проблема защиты информационных систем и сетей, в частности от НСД. Одним из самых популярных и эффективных средств решения данной проблемы являются брандмауэры. В этой работе рассматривается данный класс средств защиты информации, анализируется их роль в комплексном подходе к защите информации в современных информационных системах и сетях.

Для защиты от вторжения по сети используются средства межсетевого экранирования. Межсетевой экран (Firewall, брандмауэр) является основой безопасности и первым кольцом защиты вторжения извне [1]. Согласно документам гостехкомиссии «межсетевой экран – это локальное (однокомпонентное) или функционально- распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС. Межсетевой экран обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС на основе заданных правил, проводя таким образом разграничение доступа субъектов из одной АС к объектам другой АС. Каждое правило запрещает или разрешает передачу информации определенного вида между субъектами и объектами. Как следствие, субъекты из одной АС получают доступ только к разрешенным информационным объектам из другой АС. Интерпретация набора правил выполняется последовательностью фильтров, которые разрешают или запрещают передачу данных (пакетов) на следующий фильтр или уровень протокола».

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 [2].

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.

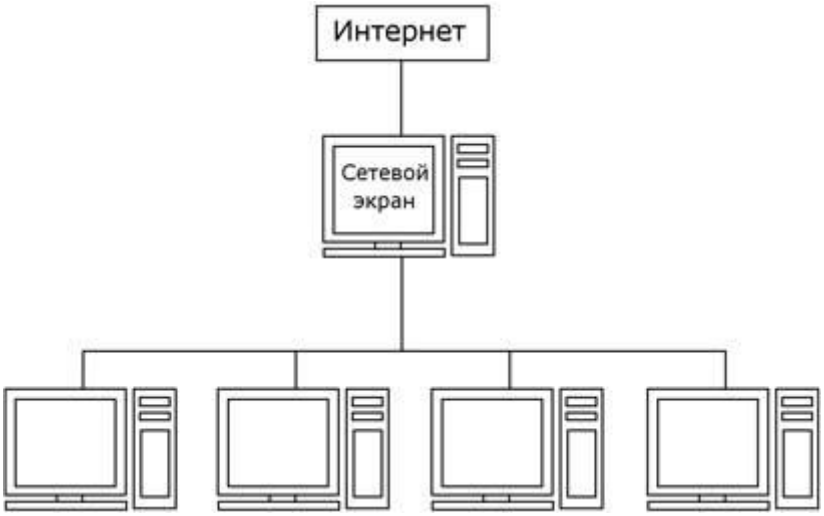

Рис. 1. Схема работы межсетевого экрана[3]

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. Сперва были разработаны простые пакетные фильтры, которые постепенно развивались в более сложные межсетевые экраны, способные анализировать информацию на нескольких сетевых уровнях [3].

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

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.

Рис. 2. Структура межсетевого экрана[1]

Дополнительно межсетевой экран может выполнять следующие функции:

– идентификация и аутентификация пользователей. 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.
– трансляция сетевых адресов; 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.

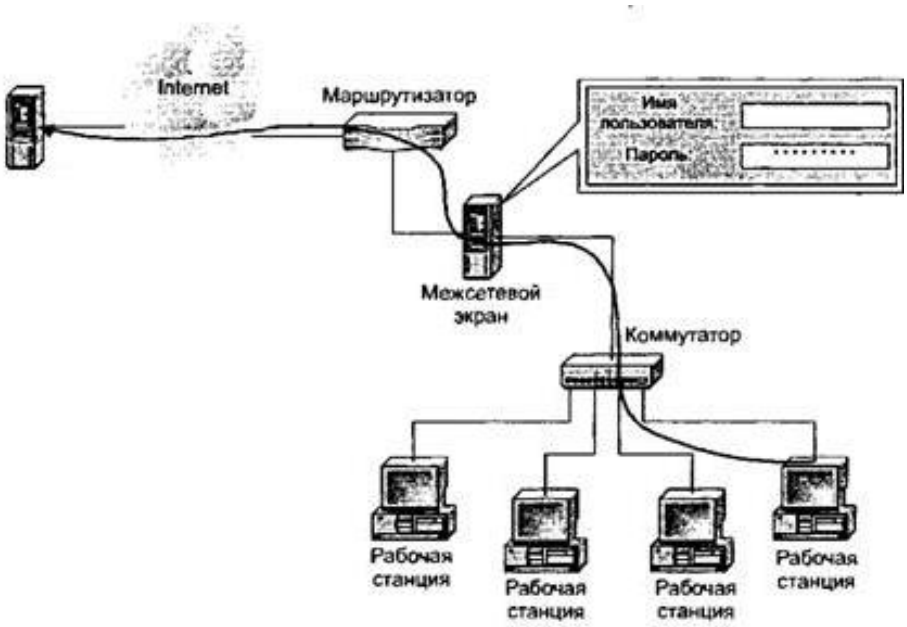

Рис. 3. Схема аутентификации пользователя с использованием межсетевого экрана [1]

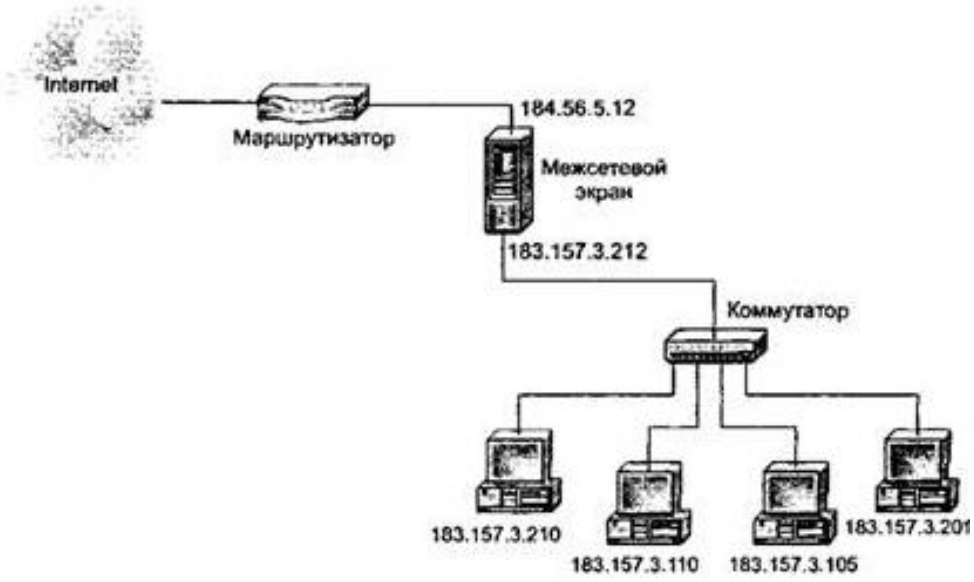

Рис. 4. Трансляция сетевых адресов [1]

– 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] Лапонина О. Р. Межсетевое экранирование. – Бином, 2014. – 343 с.

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

К.Н. Солдатов, С.М. Твердова

ИССЛЕДОВАНИЕ ИСПОЛЬЗОВАНИЯ OLAP-ТЕХНОЛОГИИ ДЛЯ АНАЛИЗА ХРАНИМЫХ ДАННЫХ БОЛЬШОГО ОБЪЕМА

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

На сегодняшний день существует множество компаний, в ходе работы которых накапливается большое количество рабочей информации. Примерами рабочей информации являются сведения о клиентах, их счетах, заказах и прочие данные, получаемые в процессе деятельности организации.

Для принятия решений по управлению бизнес-процессами компании требуется итоговая информация, сформированная на основе рабочих данных, в виде обобщенных отчетов. Для этих целей информационная система организации может включать в себя программы анализа и генерации отчетов, отражающих актуальные агрегированные данные, их динамику, тенденцию и прочие важные показатели.

Для оперативной генерации подобных отчетов информационные системы предприятия включают в себя подсистемы бизнес-аналитики, предназначенные для комплексного анализа и обработки больших массивов рабочих данных. Указанные подсистемы могут являться собственной разработкой организации или готовыми системами (MS Analysis Services, Прогноз, Oracle и т.д.).

В основе большинства систем анализа используется OLAP- технология комплексного многомерного анализа данных. Эта технология основана на построении многомерных массивов данных – OLAP-кубов. Структура OLAP-куба предполагает наличие осей, которые содержат параметры, и ячеек, хранящих агрегированную информацию, зависящую от параметров. Конкретные значения параметров являются точками на осях и называются членами. Вдоль каждой оси данные могут быть организованы в виде иерархии, представляющей различные уровни их детализации [1].

Основными преимуществами данной технологии являются:

- высокая скорость получения результатов анализа
- возможность осуществления любого логического и статистического анализа, характерного для данного приложения, и его сохранения в доступном для конечного пользователя виде
- многомерное представление данных, включающее полную поддержку для множественных иерархий [2].

Существует ряд готовых продуктов для анализа больших наборов данных. Одним из них являются службы Analysis Services – подсистема аналитики данных, которая используется в принятии решений и бизнес-аналитике. Эта подсистема предоставляет аналитические данные, которые применяются в деловых отчетах и клиентских приложениях, таких как

Power BI, Excel, отчеты служб Reporting Services, а также других инструментах визуализации данных.

Типовой рабочий процесс для службы Analysis Services включает построение модели на основе многомерных или табличных данных, развертывание модели как базы данных в экземпляре Службы Analysis Services, обработку базы данных для загрузки в нее данных или метаданных и назначение разрешений на доступ к данным конечным пользователям. После подготовки доступ к этой многоцелевой семантической модели данных может осуществляться любым клиентским приложением, поддерживающим службы Analysis Services в качестве источника данных [3].

Российским производителем в области бизнес-аналитики является компания «Прогноз», которой принадлежит разработка Prognoz Platform 8 – BI-платформа для создания и разработки настольных, веб и мобильных приложений, объединяющая современные технологии хранилищ данных, визуализации, оперативного анализа данных (OLAP), формирования отчётности, моделирования и прогнозирования бизнес-процессов.

Для работы с источниками данных Prognoz Platform 8 использует многомерную модель: источники данных представляются в виде набора измерений и фактов. Для реализации многомерной модели применяется ROLAP-подход (Relational OLAP – реляционный OLAP), при котором структура многомерных источников данных хранится в реляционной базе данных. Сначала создаётся реляционная база данных, затем реляционные наборы данных: таблицы, представления, SQL-запросы и так далее. Затем на основе наборов данных формируются справочники. Далее создаются многомерные источники данных, измерения в которых формируются на базе справочников [4].

Существуют и другие решения, но основой для них так же является OLAP-технология. К недостаткам данной технологии можно отнести малую гибкость структуры OLAP-куба при его перестроении. Предполагается, что на этапе создании куба все параметры и иерархии известны и не будут подвергаться изменениям. Поэтому, в случае необходимости замены измерений или добавления новых, потребуется полный перерасчет данных куба, который повлечет большие затраты времени и машинных ресурсов.

В результате исследования выявлено, что многие современные организации пользуются различными средствами для бизнес-анализа, в основе которых располагается OLAP-технология, являющаяся мощным инструментом, позволяющим агрегировать информацию и оперативно формировать отчеты, требуемые для принятия управленческих решений. Однако в ряде случаев может возникнуть необходимость оперативного обновления набора осей OLAP-куба, для чего требуется достаточно высокая гибкость структуры.

Список литературы

[1] Vieira R. Professional Microsoft SQL Server 2008 Programming. – Indianapolis, Wiley, 2009. – 893 p.

[2] Введение в OLAP: часть 1. Основы OLAP. URL: http://www.olap.ru/basic/OLAP_intro1.asp (дата обращения 17.03.2017).

[3] Analysis Services. URL: https://msdn.microsoft.com/ru-ru/library/bb522607.aspx (дата обращения 20.03.2017).

[4] Справочная система Prognoz Platform 8. URL: http://help.prognoz.com/ru/help.htm#mergedProjects/Intro/capabilities/purposestructure.htm (дата обращения 20.03.2017).

Солдатов Константин Николаевич – аспирант КФ МГТУ им. Н.Э. Баумана. E-mail: Konstantin_Nikolaevich_91@mail.ru

Твердова Светлана Михайловна – канд. техн. наук, доцент кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: ivalug@rambler.ru

В.Л. Бухман, А.Н. Молчанов

КРИТЕРИИ ВЫБОРА СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

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

В любой компании информация является важнейшим ресурсом, определяющим успех и конкурентоспособность. Хищение, потеря доступности, внесение ложных данных могут привести к катастрофическим последствиям и краху компании. Поэтому любой организации необходимо организовать и обеспечить надежную защиту используемой информации. Один из методов защиты данных – средства криптографической защиты. В настоящее время перечень средств криптографической защиты очень велик, многие из таких продуктов имеют широкий функционал, часть из которого может быть избыточна или не применима в конкретных ситуациях. Даже специалистам зачастую тяжело определить, какое именно программное или аппаратное решение подходит для задач их компании. В данной статье будут рассмотрены критерии, которые нужно учитывать при выборе систем криптографической защиты информации.

Средства криптографической защиты информации (СКЗИ) – это аппаратные, программные и аппаратно-программные средства, системы и комплексы, осуществляющие криптографическое преобразование данных, предназначенные для защиты информации при ее обработке, хранении и передачи. При выборе СКЗИ для определенной системы нужно руководствоваться следующими аспектами.

Область применения. Данный фактор является одним из наиболее важных и именно он определяет на каком этапе существования информации необходима защита. Область применения различных СКЗИ может сильно отличаться: защита каналов связи, реализация защищенного документооборота, доверенное хранение, защита информации от несанкционированного доступа, идентификация и аутентификация удаленных пользователей криптографическими методами, формирование электронной цифровой подписи и др. [1]. Определение сферы применения значительно сужает спектр подходящих решений и является основой для дальнейшего анализа.

Тип реализации. На основании предыдущего критерия и системы, требующей защиты информации, производится выбор из трех типов реализации: аппаратная, программная, аппаратно-программная.

Программные СКЗИ – специализированное программное обеспечение, отдельные библиотеки или программные модули, предназначенные для шифрования информации на определенном носителе или для безопасной передачи через Интернет. Программные средства имеют широкую цено-

вую категорию от бесплатных до очень дорогих, и цена зависит от функциональности и стойкости СКЗИ.

Аппаратные СКЗИ – физические устройства, обеспечивающие шифрование, запись и передачу информации. Данному типу характерны высокая скорость, быстрая установка и высокая цена. К аппаратным средствам относят USB-шифраторы, микросхемы и аппаратные модули, совмещенные со средствами вычислительной техники или встраиваемые в автоматизированные системы, специализированные сетевые коммутаторы и маршрутизаторы для создания защищенных каналов.

Программно-аппаратные средства являются более сложными, но очень эффективными комплексами обеспечения безопасности и конфиденциальности. Они сочетают в себе взаимосвязанные программные и аппаратные блоки, поддерживающие множество современных алгоритмов шифрования, идентификацию и аутентификацию пользователей, криптографическое преобразование данных, обеспечение целостности информации. Кроме того, данный тип реализации поддерживает комплексные методы защиты: защиты целостности и конфиденциальности, при помощи использования шифрования, электронной цифровой подписи и криптографических ключей. Следовательно, программно-аппаратная реализация является наиболее действенным способом защиты информации, однако стоит учитывать и высокую стоимость данного продукта.

Поддерживаемые операционные системы. Данный показатель является очень важным для программно-реализованных продуктов, однако совершенно несущественен для чисто аппаратного решения. Несмотря на универсальность настройки программных СКЗИ не все они поддерживают большой набор операционных систем. Поэтому прежде чем приобретать определённое программное обеспечение требуется убедиться в том, что операционная система содержится в списке поддерживаемых для данной СКЗИ.

Типы файловых систем. От выбранной операционной системы непосредственно зависят типы файловых систем, с которыми она может работать. Из этого следует, что помимо определения операционной системы требуется также ориентироваться на поддерживаемые типы файловых систем и типы носителей, с которыми может взаимодействовать СКЗИ.

Системные требования. Программные СКЗИ могут иметь различные назначения и различные реализации, на основании которых составляется список системных требований данного продукта. Соответственно, рациональность использования более мощных технологий должна обуславливаться необходимостью высокого уровня конфиденциальности информации. В случае, если средства криптографической защиты информации необходимы для частного использования то, подходящим решением будет использование решений средних системных требований.

Сертификация продукта. В настоящее время, в многих странах, обладающих развитыми криптографическими технологиями, разработка СКЗИ тесно связана со сферой государственного регулирования. Государственное регулирование, как правило, включает, лицензирование деятельности, связанной с разработкой и эксплуатацией криптографических средств, сертификацию СКЗИ и стандартизацию алгоритмов криптографических преобразований. Под сертификацией подразумевается получение разработчиком СКЗИ в уполномоченных органах сертификата, подтверждающего соответствия систем шифрования и электронной цифровой подписи принятым в РФ стандартам, которые заданы ГОСТом [2]. При работе с информацией, конфиденциальность которой определяет государство, необходимо применять именно сертифицированные средства и строго регламентированные меры [3]. Однако в случае, когда мы сами определяем конфиденциальность какой-либо информации, то меры и средства по ее защиты могут несертифицированными. Соответственно, при выборе той или иной СКЗИ нужно руководствоваться степенью конфиденциальности информации, с которой предстоит работать, а также учитывать, что сертифицированная система с большей долей вероятности будет удовлетворять принятым уровням безопасности.

Реализованные криптографические алгоритмы. Современные СКЗИ могут поддерживать реализацию различные алгоритмы шифрования. Как правило криптосистемы разделают на две группы по способу шифрования: одноключевые (симметричные) и двухключевые (ассиметричные) [4].

Симметричные криптосистемы – это те системы, в которых для шифрования и расшифровывания используется один и тот же закрытый ключ. Данные системы широко применяются для сокрытия конфиденциальной информации и обладают высокой скоростью передачи данных. Множество СКЗИ реализовывают симметричные алгоритмы, содержащиеся в ГОСТ 28147-89. Для сертифицированных СКЗИ использование алгоритмов ГОСТ 28147-89 является обязательным условием [5].

Ассиметричные криптосистемы – системы шифрования, в которых генерируется два ключа, определенным способом связанным друг с другом – открытый и закрытый ключ. Открытый ключ передается по незащищенному каналу и используется для шифрования. Закрытый ключ доступен только его владельцу и предназначен для расшифровывания данных. Приведенный алгоритм обладает повышенной надежностью систем основываясь на том факте, что знание открытого ключа не позволяет по нему определить парный закрытый ключ. Данная криптосистема чаще всего предназначена для авторизации и обеспечения юридической значимости электронных документов при обмене ими между пользователями, посредством использования процедур формирования и проверки электронной цифровой

подписи в соответствии с отечественными стандартами ГОСТ Р 34.10-94, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001.

Взаимодействие с решениями другими производителей. Определенные средства криптографической защиты имеют возможность интегрирования продуктов и решений других компаний. Приведённый критерий чаще всего относиться к программным СКЗИ типа "криптобиблиотека". Данный подход значительно расширяет имеющийся функционал, однако требует знания документации продукта и определенной настройки [6].

Реализация протокола SSL/TLS. TLS – криптографический протокол, обеспечивающий аутентификацию и защиту от несанкционированного доступа, нарушения целостности передаваемых данных. Чаще всего в механизме защиты реализации протокола TLS применяются криптографические алгоритмы шифрования в соответствии с ГОСТ 28147-89, обмена ключей по алгоритму Диффи-Хеллмана, хэширования в соответствии с ГОСТ Р 34.11-94. Поддержка данного протокола в СКЗИ является полезным дополнением к функциональности продукта.

Поддержка языков. В связи с множеством различных средств криптографической защиты информации, в том числе и зарубежных производителей, можно выделить один из опциональных критериев – поддержка языков. Он не является обязательным при выборе подходящей системы, тем не менее требует определенных навыков владения иностранным языком для уверенной работы с программным обеспечением. Однако существуют СКЗИ, которые имеют возможность добавления языков, не входящих в стандартную версию продукта.

Экономическая составляющая. Экономический показатель чаще всего является основополагающим, поскольку именно он ограничивает приобретение той или иной СКЗИ. Он зависит от всех выше описанных возможностей системы: поддержка множества операционных систем, поддержка множества файловых систем, реализация различных алгоритмов, сертификация продукта, тип реализации и наличие дополнительных возможностей. Соответственно, чем больше функциональность и надежность продукта, тем выше ценовая категория.

Таким образом, определившись с критериями, стоит отметить, что многие составляющие взаимосвязаны и при выборе определённой СКЗИ изначально нужно ориентироваться на сферу применения. Впоследствии необходимо определить уровень безопасности, который требуется обеспечить. Однако стоит учитывать, что с повышение уровня безопасности также повышается цена на продукт. На сегодняшний день существует множество систем, имеющие собственные достоинства и недостатки. Из этого следует вывод, что из множества различных решений есть возможность подобрать такое, которое обеспечивало бы должный уровень безопасности за приемлемую цену.

Список литературы

[1] Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности – Утверждены руководством 8 Центра ФСБ России, 31 марта 2015 года, № 149/7/2/6-432

[2] Информационный ресурс Перечень средств защиты информации, сертифицированных ФСБ России. http://clsz.fsb.ru/certification.htm

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

[4] Информационный ресурс Журнал "Рынок ценных бумаг" http://www.rcb.ru/dep/2007-04/8318/

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

[6] Информационный ресурс Журнал "Information Security/ Информационная безопасность" #6, 2007 http://www.itsec.ru/articles2/Oborandteh/sredstva_kriptograf_zasch_inform

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

Молчанов Алексей Николаевич – ст. преп. кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: alexeymolchanov@yandex.ru

Я.А. Бланк, А.Н. Молчанов

КРИТЕРИИ ОЦЕНКИ ПРОГРАММНО-АППАРТНЫХ КОМПЛЕКСОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ПРЕДПРИЯТИЙ

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

На протяжении всей истории человечества информация была крайне важна для человека. В рамках постиндустриального общества ее значимость только усилилась. Информация стала одним из важнейших стратегических, управленческих ресурсов, наряду с материальными, человеческими и финансовыми ресурсами. Для многих предприятий владение информацией является залогом прибыли и конкурентоспособности. Отсюда хищение информации может нанести компании ощутимый вред. В связи с этим информация нуждается в соответствующей защите информации.

В 2013 Аналитическим Центром InfoWatch зарегистрировано 1143 случая утечки конфиденциальной информации, что на 22,3 % больше, чем в 2012 году (934 утечки) [1].

Компания Gemalto, мировой лидер в области цифровой безопасности, опубликовала данные индекса утечек информации Breach, согласно которому за первые 6 месяцев 2015 года было зарегистрировано 888 случаев хищения информации и пропажи более 246 миллионов записей о клиентах, медицинских карточек, банковских и личных данных за первые 6 месяцев 2016 года увеличилось на 15%. На глобальном уровне в первой половине 2016 года было зафиксировано 974 утечки, в результате которых в небезопасности оказались более 554 миллионов записей данных, по сравнению с 844 утечками и 424 миллионами скомпрометированными записями за предыдущие шесть месяцев [2].

Эти и многие другие статистические исследования показывают, что задача защиты информации не теряет свою актуальность. Однако в связи с увеличением масштаба и сложности информационных систем предприятий увеличивается количество и усложняются атаки, направленные на эти системы. Этим объясняется усложнение комплекса средств и методов, используемых для защиты информации, циркулирующей в информационной системе предприятия, - подсистемы защиты информации. Для повышения эффективности функционирования подсистем защиты информации и управления ими применяются системы обеспечения информационной безопасности. Существует множество предлагаемых на рынке решений и комплексов систем обеспечения информационной безопасности. Поэтому выбор наилучшего комплекса обеспечения информационной безопасности предприятия является особенно актуальным.

Основными характеристиками, значимыми для процесса управления информационными системами предприятия являются [3]: степень распределенности информационной системы, класс реализуемых в информационной системе технологических операций, режим работы информационной системы.

По степени распределенности информационные системы делят на локальные и распределенные. Распределенные системы широко распространены и более сложны для управления, поэтому если системы обеспечения информационной безопасности могут управлять распределенными информационными системами, то это делает ее лучше по сравнению с другими системами.

По классу реализуемых технологических операций информационные системы делят на системы с текстовыми редакторами, системы с табличными редакторами, СУБД, системы управления базами знаний, системы с графикой, мультимедиа, гипертекстом [4]. Присутствие той или иной технологической операции в информационной системе предприятия обусловлено производственной необходимостью. Поэтому чем большее количество технологических операций может контролировать система обеспечения информационной безопасности, тем более гибкой и более предпочтительной она является.

По режимам работы информационные системы делят на пакетные и диалоговые. Диалоговые информационные системы являются более распространенными, чем пакетные, так что более предпочтительным для системы обеспечения информационной безопасности является возможность управления диалоговыми информационными системами. Однако существуют информационные системы, способные функционировать как в диалоговом, так и в пакетном режиме работы. Таким образом, лучшей является система безопасности, способная управлять смешанным режимом работы информационной системы.

Основными характеристиками, влияющими на процесс обеспечения информационной безопасности, являются цели реализации атак и объекты, на которые эти атаки направленны [5].

Выделяют следующие цели реализации атак: нарушение конфиденциальности информации; нарушение целостности информации; отказ в обслуживании; фишинг; использование стандартных учетных данных производителя целевой системы; SQL-инъекции; перехват передаваемых данных. Чем на большее количество целей реализации атак сможет отреагировать система обеспечения информационной безопасности, тем больше атак смогут быть обнаружены и предотвращены.

Выделяют следующие объекты воздействия атак: рабочие станции; приложения; сервер; сетевое оборудование; система управления базами данных; удаленные клиенты. Чем большее количество объектов воздействия атак будет находиться под контролем системы обеспечения инфор-

мационной безопасности, тем меньшее количество атак на информационную систему предприятия останется незамеченными.

Обычно комплексы обеспечения безопасности информационных систем предприятий состоят из следующих подсистем: подсистема управления доступом; подсистема регистрации и учета; криптографическая подсистема; подсистема обеспечения целостности. Система обеспечения информационной безопасности, способная управлять всеми выделенными подсистемами является наилучшей.

Процесс обеспечения информационной безопасности должен быть непрерывным. Оценки состояния объекта, которые возвращает система, должны периодически актуализироваться, т.е. пересчитываться. Для систем обеспечения информационной безопасности основной оценкой состояния информационной системы предприятия являются информационные риски, которым она подвержена. Данные оценки должны постоянно пересчитываться.

Рынок решений и систем обеспечения информационной безопасности огромен. Для выявления наилучшей системы обеспечения информационной безопасности предприятия необходимо проводить многокритериальный анализ с помощью выделенных критериев.

Для проведения многокритериального анализа набор качественных критериев был преобразован в числовой вектор $K = (K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_8)$

Качественным значениям критериев были поставлены в соответствие количественные аналогично (1).

$К_3$ – управляемые режимы работы информационной системы:

$$K_3 = \begin{cases} 0, \textit{ пакетный режим} \\ 0.5, \textit{ диалоговый режим} \\ 1, \textit{ смешанный режим} \end{cases} \quad (1)$$

Для проведения анализа был сформирован наилучший вектор K^*, в котором все значения критериев соответствуют максимальным значениям. Для всех критериев это значение 1.

$$K^* = (1,1,1,1,1,1,1,1).$$

Для оценки качества системы обеспечения информационной безопасности вводится скалярная величина равная Эвклидову расстоянию между наилучшим вектором и вектором критериев, полученным для i-го оцениваемого метода:

$$K^i = (K_1^i, K_2^i, K_3^i, K_4^i, K_5^i, K_6^i, K_7^i, K_8^i),$$

рассчитываемая по формуле (2):

$$P = \sqrt{\sum_{j=1}^{8} (K_j^* - K_j^i)^2} \quad (2)$$

Система, для которой расстояние до наилучшего вектора окажется наименьшим, можно считать наилучшей системой обеспечения информационной безопасности предприятия.

Список литературы

[1] Электронный ресурс InfoWatch. URL: https://www.infowatch.ru/report2013 (Дата обращения 26.03.217)

[2] Электронный ресурс Gemalto. URL: http://www.gemalto.com/press/Pages/Gemalto-Releases-Findings-of-First-Half-2015-Breach-Level-Index.aspx (Дата обращения 26.03.217)

[3] О.Г. Инюшкина. Проектирование информационных систем (на примере методов структурного системного анализа: учебное пособие / О.Г. Инюшкина, Екатеринбург: «Форт-Диалог Исеть», 2014. 240 с.

[4] И.О. Белавин Информационные системы и их использование в профессиональной деятельности [Электронный ресурс]: учеб.-метод. пособие / И.О. Белавин ; подгот. к изд. В.Ю. Васильев. – Тверь, УМЦ Банка России, 2013. (Дата обращения 30.03.2017)

[5] Электронный ресурс Безопасник URL: http://bezopasnik.org/article/22.htm (Дата обращения 30.3.2017)

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

Молчанов Алексей Николаевич – ст. преп. кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: alexeymolchanov@yandex.ru

М.О. Швачкина

МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ КАК СРЕДСТВО ОБЕСПЕЧЕНИЯ СЕТЕВОЙ БЕЗОПАСНОСТИ

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

Социальные и экономические изменения в последние годы создали условия для широкого внедрения в России новейших информационных технологий, создания и использования информационных, телекоммуникационных систем связи и обработки информации, что 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

А.А. Кухарева

ОБЗОР СТЕГАНОГРАФИЧЕСКИХ СИСТЕМ

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

Стеганография – это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи.

В отличие от криптографии, которая скрывает содержимое секретного сообщения, стеганография скрывает сам факт его существования. Как правило, сообщение будет выглядеть как что-либо иное, например, как изображение, статья или письмо.

Преимущество стеганографии состоит в том, что сообщения не привлекают к себе внимания. Сообщения, факт шифрования которых не скрыт, вызывают подозрение и могут быть сами по себе уличающими в тех странах, в которых это запрещено. Таким образом, стеганография защищает сам факт наличия каких-либо скрытых посланий.

Классификация стеганографии

В конце 90-х годов выделилось несколько направлений стеганографии:

1) Классическая стеганография;

2) Компьютерная стеганография;

3) Цифровая стеганография.

Классическая стеганография

Симпатические чернила

Одним из наиболее распространенных методов классической стеганографии является использование симпатических (невидимых) чернил. Текст, записанный такими чернилами, проявляется только при определенных условиях (нагрев, освещение, химический проявитель и т. д.).

В настоящее время под стеганографией чаще всего понимают скрытие информации в текстовых, графических либо аудио файлах путём использования специального программного обеспечения.

Стеганографические модели – используются для общего описания стеганографических систем.

Стеганографическая система (стегосистема) – объединение методов и средств, используемых для создания скрытого канала для передачи информации.

Компьютерная стеганография

Компьютерная стеганография – направление классической стеганографии, основанное на особенностях компьютерной платформы. Примеры – стеганографическая файловая система StegFS для Linux, скрытие данных в неиспользуемых областях форматов файлов, подмена символов в названиях файлов, текстовая стеганография и т. д.

Метод скрытия информации в неиспользуемых местах гибких дисков – при использовании этого метода информация записывается в неиспользуемые части диска, к примеру, на нулевую дорожку.

Метод использования особых свойств полей форматов, которые не отображаются на экране – этот метод основан на специальных «невидимых» полях для получения сносок, указателей.

Использование особенностей файловых систем – при хранении на жестком диске файл всегда (не считая некоторых ФС, например, ReiserFS) занимает целое число кластеров (минимальных адресуемых объёмов информации).

Цифровая стеганография

Цифровая стеганография – направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов. Как правило, данные объекты являются мультимедиа-объектами и внесение искажений, которые находятся ниже порога чувствительности среднестатистического человека, не приводит к заметным изменениям этих объектов.

Алгоритмы

Все алгоритмы встраивания скрытой информации можно разделить на несколько подгрупп:

Работающие с самим цифровым сигналом, например, метод LSB.

«Впаивание» скрытой информации. В данном случае происходит наложение скрываемого изображения (звука, иногда текста) поверх оригинала. Часто используется для встраивания ЦВЗ.

По способу встраивания информации стегоалгоритмы можно разделить на линейные (аддитивные), нелинейные и другие. Алгоритмы аддитивного внедрения информации заключаются в линейной модификации исходного изображения, а её извлечение в декодере производится корелляционными методами. В нелинейных методах встраивания информации используется скалярное либо векторное квантование.

Метод LSB

LSB (Least Significant Bit, наименьший значащий бит) – суть этого метода заключается в замене последних значащих битов в контейнере (изображения, аудио или видеозаписи) на биты скрываемого сообщения. Разница между пустым и заполненным контейнерами должна быть не ощутима для органов восприятия человека. Все методы LSB являются, как правило, аддитивными.

Эхо-методы

Эхо-методы применяются в цифровой аудиостеганографии и используют неравномерные промежутки между эхо-сигналами для кодирования последовательности значений. При наложении ряда ограничений соблюдается условие незаметности для человеческого восприятия. Эхо характери-

зуется тремя параметрами: начальной амплитудой, степенью затухания, задержкой.

Фазовое кодирование

Фазовое кодирование – так же применяется в цифровой аудиостеганографии. Происходит замена исходного звукового элемента на относительную фазу, которая и является секретным сообщением. Фазовое кодирование является одним из самых эффективных методов скрытия информации.

Метод расширенного спектра

Метод встраивания сообщения заключается в том, что специальная случайная последовательность встраивается в контейнер, затем, используя согласованный фильтр, данная последовательность детектируется. Данный метод позволяет встраивать большое количество сообщений в контейнер, и они не будут создавать помехи друг другу.

Стеганография и цифровые водяные знаки

Цифровые водяные знаки (ЦВЗ) используются для защиты от копирования, сохранения авторских прав. Невидимые водяные знаки считываются специальным устройством, которое может подтвердить либо опровергнуть корректность.

ЦВЗ имеют небольшой объём, но для выполнения указанных выше требований, при их встраивании используются более сложные методы, чем для встраивания обычных заголовков или сообщений. Такие задачи выполняют специальные стегосистемы.

Кухарева Анна Александровна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: anna.a.kukhareva@gmail.com

И.С. Герасимова

ОБФУСКАЦИЯ, КАК ОДИН ИЗ МЕТОДОВ ЗАЩИТЫ ПРОГРАММНОГО КОДА

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

Проблема защиты программного обеспечения от несанкционированной модификации остается актуальной для большинства программистов, которые занимаются разработкой программного обеспечения.

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 механизма 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

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

Е.А. Коваленко, А.Б. Лачихина

ОСНОВНЫЕ МЕТОДЫ ВОССТАНОВЛЕНИЯ УТРАЧЕННЫХ ДАННЫХ

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

В современном мире проблема сохранения целостности данных занимает важнейшее место с точки зрения обеспечения информационной безопасности. Нарушение целостности данных может быть осуществлено как путем несанкционированного изменения информации с целью реализации угрозы, так и случайно. Целью данной статьи является рассмотрение основных концепций восстановления утраченных файлов.

В настоящее время существует большое количество программ для восстановления файлов и все они работают по схожим принципам. Простейший метод восстановления утерянной информации заключается в том, чтобы обратиться к резервным копиям файлов. Но это будет возможно, если таковые были созданы заранее. Если же резервное копирование не предусмотрено в системе, а нужная информация потеряна, необходимо обратиться к методам восстановления файлов.

Существуют логические и физические ошибки информационных накопителей. При логической ошибке накопитель не имеет видимых физических повреждений и опознается в системе, а проблема возникает при попытке получения доступа, записи или чтении данных. При физическом повреждении данные либо вовсе не подлежат восстановлению, либо для их восстановления требуется помощь профессионала и специально оборудованное помещение. Данные можно восстановить если неисправность заключается лишь в повреждении поверхности самого носителя. Как показывает практика, попытки неквалифицированного вмешательства в структуру накопителя влекут за собой окончательную и безвозвратную потерю данных.

Восстановить утраченные файлы позволяет принцип работы операционной системы во время удаления пользователем файлов. При удалении файла не происходит мгновенного разрушения его данных. Вместо этого вносятся некоторые изменения в информацию о файлах и папках, показывающие что файл был удален. То есть файл просто помечается как удаленный, при этом сами данные файла сохраняются до тех пор, пока это место на носителе не потребуется для записи другого файла. Если данные на носителе перезаписаны, то их не удастся восстановить ни одном из известных программных методов [1].

Существует два основных метода восстановления утраченных данных: восстановление файлов посредством анализа информации о файлах и

папках и восстановление файлов при помощи поиска файлов по сигнатурам.

Первый метод используется первым в утилитах восстановления. В начале осуществляется попытка прочитать и обработать первую копию информации о файлах и папках. Такой метод помогает при случайном удалении и ежеминутном восстановлении данных. В случае повреждения первой копии, информации о файлах и папках, утилита начинает сканирование носителя и поиск второй копии информации о файлах и папках. После сбора всей доступной информации утилита её обрабатывает и воссоздает утерянную структуру файлов и папок. В точности файловая структура может быть восстановлена лишь при несерьезных повреждениях файловой системы носителя. При сильном повреждении файловой системы восстановленные файлы будут находится в папках с присвоенными виртуальными именами.

Механизм поиска по сигнатурам файлов подразумевает считывание абсолютно всей информации с носителя, что позволяет обнаружить даже те файлы, на которые нет ссылок из файловой системы. Файловая сигнатура – это некий общий шаблон данных, он уникален для определенного типа файлов и находится в конце или в начале файла. К примеру, все файлы типа PNG начинаются с символов «‰PNG», файлы типа MP3 начинаются с «ID3». Для начала считываемая с носителя информация соотносится с сигнатурами известных типов файлов на предмет соответствия содержания найденного файла одному из пунктов базы данных форматов файлов. Если формат данных оказывается знакомым, происходит анализ заголовка файла, чтобы извлечь как можно больше информации о нем. Такой алгоритм позволяет определить точный размер файла, а это уже поможет рассчитать расположение всего файла на носителе. Недостаток данного метода заключается в том, что из-за отсутствия базе того или иного типа, файл невозможно найти [2].

Современные программы для восстановления данных используют гибридный подход к восстановлению данных, стараясь по возможности считать максимум информации из файловой системы и прибегая к сигнатурному анализу содержимого носителя только в случаях крайней необходимости – при повреждении или отсутствии файловой системы, а также для поиска файлов, удалённых длительное время назад.

В заключение необходимо отметить следующие выводы, сделанные в ходе проведения исследования:

- Состояние файлов будет зависеть от того, что вызвало их утрату, от состояния носителя до сбоя, а также от действий, которые были предприняты до начала восстановления данных.
- Не следует предпринимать попыток восстановить данные с физически неисправных носителей.

– Следует выполнять все задачи по восстановлению данных с образов носителей, чтобы оставить неизменным текущее состояние данных на носителе.

В ходе проведения работы над выбранной темой, были рассмотрены причины потери данных, изучены основные методы их восстановления. Сделаны выводы об основных принципах, которые необходимо учитывать при восстановлении утраченной информации.

Список литературы

[1] *Лачихина А.Б., Твердова С.М.* Поддержание целостности информации в базах данных корпоративных информационных систем. Вопросы радиоэлектроники. 2014. Т. 4. № 4. С. 137-146.

[2] http://datarecord.net/poleznaya-informatsiya/

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

А.Ю. Макарова, А.Н. Молчанов

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ НЕСОВЕРШЕННОЛЕТНИХ В ИНФОРМАЦИОННОЙ СРЕДЕ.

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

Согласно законодательству Российской Федерации, персональные данные (далее – ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). В настоящее время обеспечение безопасности личной информации человека является одной из основных задач. С развитием Интернет технологий, широким распространением персональных устройств (компьютеров и смартфонов) с разнообразными функциями проблема защиты личных данных людей занимает одно из первых мест [1].

При обеспечении защиты персональных данных человека в сети Интернет особое внимание следует уделить защите прав особой категории граждан – несовершеннолетних. В сети Интернет несовершеннолетний субъект является особо уязвимым, так как он в полной степени не осознает последствий совершенных действий, которые в дальнейшем могут нанести ему существенный вред. В настоящий момент в отечественном законодательстве отсутствуют какие-либо нормы, предусматривающие особенности работы по защите персональных данных несовершеннолетних граждан, в том числе в сети Интернет.

Несовершеннолетний субъект имеет право на конфиденциальность ПДн, которое признается за ним вне зависимости от возраста и способности осознать потребность неприкосновенности собственного статуса.

Таким образом, ПДн несовершеннолетних можно охарактеризовать как особый вид информации с ограниченным доступом, затрагивающий интересы лиц в возрасте до 18 лет, который отличается более узким кругом относимых к ней сведений, участием в защите ее конфиденциальности родителей или законных представителей, широким кругом полномочий в процессе обработки персональных данных государственных органов в сфере образования, социальной защиты, здравоохранения и профилактики правонарушений [2].

К ПДн несовершеннолетнего субъекта, обучающегося в каком-либо образовательном учреждении, относятся:

а) сведения, содержащиеся в свидетельстве о рождении, паспорте или ином документе, удостоверяющем личность;

б) информация, содержащаяся в личном деле несовершеннолетнего;

в) информация, содержащаяся в личном деле несовершеннолетнего, лишенного родительского попечения;

г) сведения, содержащиеся в документах воинского учета (при их наличии);

д) информация об успеваемости;

е) информация о состоянии здоровья;

ж) документ о месте проживания;

з) иные сведения, необходимые для определения отношений обучения и воспитания [2].

Помимо вышеперечисленных ПДн можно выделить специальные и биометрические персональные данные.

К специальным персональным данным относятся:

1) Информация о расовой или национальной принадлежности;
2) Информация о политических взглядах;
3) Информация о религиозных или философских убеждениях;
4) Информация о состоянии здоровья.

К биометрическим персональным данным относятся сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных [3].

Право доступа к ПДн несовершеннолетнего субъекта, обучающегося в каком-либо образовательном учреждении, имеют:

а) работники управления образования (при наличии соответствующих полномочий, установленных приказом управления образования);

б) директор образовательного учреждения;

в) секретарь образовательного учреждения;

г) главный бухгалтер образовательного учреждения;

д) заместители директора по УВР, ВР, социальный педагог, педагог-психолог;

е) классные руководители (только к ПДн несовершеннолетнего своего класса);

ж) учителя-предметники (только к ПДн обучающихся своего предмета);

з) библиотекарь;

и) медработник.

Согласно статистическим данным за последние несколько лет, в сети Интернет было выявлено более 2027 сайтов в Российской Федерации, распространяющих персональные данные детей и их родителей в открытом доступе. Сайты, разместившие информацию о детях, как правило, принадлежат школам, детским садам, интернатам, а также муниципальным образованиям и администрациям ряда субъектов Российской Федерации. Обнаруженные данные содержали списки не только самих воспитанников детских садов, учеников школ, с указанием их ФИО, даты рождения, места

проживания, а также сведения о социальном статусе родителей и их принадлежности к той или иной льготной категории граждан [4].

Следует отметить, что размещение подобной информации не соответствует цели ее обработки, так как ключевым принципом законодательства в области персональных данных, в том числе международного является принцип, согласно которому «обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных». К тому же размещение данной информации в сети Интернет квалифицируется как распространение информации неограниченному кругу лиц в публичном информационном источнике. После того, как данные о детях будут выложены в Сеть, оператор не сможет контролировать их обработку третьими лицами, эти данные могут быть скопированы, изменены и далее распространены в Сети. Они могут храниться в различных регистрах, базах, серверах из которых удалить данные будет практически невозможно. Таким образом, оператор, выложив персональные данные граждан в глобальную сеть Интернет, которые он собрал в определенных целях, уже не сможет проконтролировать и обеспечить обещанные субъекту данных условия обработки [4].

Как уже говорилось, в настоящее время в российском законодательстве отсутствуют какие-либо нормы, предусматривающие механизмы по защите персональных данных несовершеннолетних граждан в информационной среде. Несомненно, данной проблеме следует уделить особое внимание и разработать соответствующие нормативно-правовые акты.

Список литературы

[1] Федеральный закон от 27.07.2006 г. No 152–ФЗ «О персональных данных». – М.: Изд-во стандартов, 2006. – 22 с.

[2] Покаместова Е. Ю. Правовая защита конфиденциальности персональных данных несовершеннолетних: Автореферат диссертации на соискание ученой степени кандидата юридических наук. – [Электронный ресурс]. – Воронеж, 2010 – Режим доступа: http://law.edu.ru/book/book.asp?bookID=1291833.

[3] http://xn--80aalcbc2bocdadlpp9nfk.xn--d1acj3b/

[4] http://rkn.gov.ru/

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

Молчанов Алексей Николаевич – ст. преп. кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: alexeymolchanov@yandex.ru

А.А. Корнеев, А.В. Мазин

ПОВЫШЕНИЕ НАДЕЖНОСТИ И ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ВАКУУМНЫХ ЭЛЕКТРОННЫХ ПРИБОРОВ

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

К вакуумным электронным приборам относятся электрические приборы, действие которых основано на использовании потока электрических зарядов в вакууме или в среде разреженного газа. После ламп накаливания наиболее широкое распространение получили электронные лампы, к которым относятся триоды, пентоды, тетроды и другие. Они предназначены для преобразования энергии постоянного тока в энергию электрических колебаний со средней частотой $3 \cdot 10^9$ Гц.

Качество, надежностьи функциональная безопасность радиотехнического устройства во многом зависит от стабильности параметров электронной лампы и её электропитания. Поэтому продление её срока службы имеет большое значение и окупает затраты на усложнение схемы электронного изделия. Тем более, если такие компоненты используются в дорогостоящем военном оборудовании, где требуется непрерывная стабильная работа, долговечность и функциональная безопасность, а стоимость специализированных электронных ламп слишком велика.

Целью данной работы является рассмотрение возможности построения схем, обеспечивающих стабильность работы радиоламп, продление их срока службы и как следствие функциональную безопасность реализованных схем и систем.

Стабильность работы электровакуумного изделия во многом зависит от долговечности его катодов. На их долговечность, в большей степени, влияет температурный режим, то есть величина и стабильность напряжения и величина тока накала. Достаточно часто радиолампы выходят из строя из-за потери эмиссии одного или пары катодов, а также их короткого замыкания на нить подогревателя. Постоянное колебание напряжения и тока накала приводит к изменению температурного режима, из-за чего меняются эмиссионные свойства катодов.

При начальном этапе эксплуатации радиолампы её выходные параметры обеспечиваются эмиссией электронов с поверхностного слоя катодов, что достигается при пониженных величинах напряжения и тока подогревателя.

Когда срок службы электровакуумного прибора подходит к концу, необходимо увеличить величины тока накала и напряжения подогревателя для обеспечения эмиссии электронов из глубинного слоя катода.

При подаче номинального значения напряжения накала на вакуумный электронный прибор, происходит его быстрый разогрев. Данный режим негативно влияет на долговечность работы. Другими словами, появляется

температурный перепад между поверхностями внутренней и внешней частей катода. Это влечет за собой его деформацию. Поэтому, следует рассмотреть методику увеличения срока службы подобных приборов.

Чтобы сохранить их работоспособность и повысить функциональную безопасность, необходимо использовать нарастание от минимального до номинального значения напряжения, тока накала и подачу анодного напряжения только в том случае, когда электронная лампа уже разогрета до рабочей температуры. Для этого следует применить генератор опорного управляющего напряжения ступенчатой формы.Временная диаграмма при реализации данного метода представлена на рисунке 1:

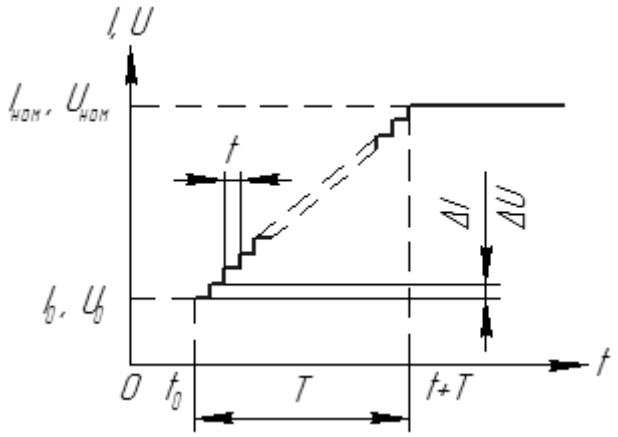

Рисунок 1. Временная диаграмма изменения тока и напряжения накала

Достоинством является возможность регулировки напряжения питания от минимального до максимального значения в процессе эксплуатации с целью компенсации потери эмиссии.

Литература:

[1] Батушев В. А. Электронные приборы: Учебник для вузов. - 2-е, перераб. и доп. - М.: Высшая школа, 1980. - 383 с.

[2] Богатырёв Е.А., Ларин В.Ю., Лякин А.Е. Энциклопедия электронных компонентов. - М.: Дрофа, 2006

[3] Денискин Ю.Д., Жигарев А.А., Смирнов Л.П. Электронные приборы. – М.: Энергия, 1980.

[4] В. Н. Дулин, Н. А. Аваев, В. П. Демин и др.; Под ред. Г. Г. Шишкина. Электронные приборы. - М.: Энергоатомиздат, 1989. - 496 с.

[5] Морозова И. Г. Физика электронных приборов. - М.: Атомиздат, 1980.

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

Мазин Анатолий Викторович – д-р техн. наук, заведующий кафедрой "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: mazinav@yandex.ru

Д.А. Мельников, С.М. Твердова

ПРЕИМУЩЕСТВА И ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

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

В современном мире, для которого характерно непрерывное развитие информационных технологий, всё чаще используется электронная документация, вместо её печатных аналогов. Это обусловлено тем, что использование электронных документов позволяет большую часть общественных отношений перевести на качественно иной уровень – уровень информационного общества, для которого характерны мобильность и экономия времени. Особое место в электронном документообороте занимает задача идентификации пользователей, решить которую призвана электронная подпись (ЭП) – наиболее удобный современный инструмент для совершения сделок в удаленном режиме и обмена юридически значимой документацией.

Идея использования ЭП нашла свое воплощение в реальной жизни – 6 апреля 2011 года был принят новый Федеральный закон «Об электронной подписи» (ФЗ-№ 63). Принятие закона было обусловлено приведением отечественного законодательства в соответствие с международными стандартами. Закон значительно расширил сферу использования электронной подписи, разрешил ее получение не только физическим, но и юридическим лицам, закрепил систему аккредитации удостоверяющих центров и др. Одним из главных новшеств стало введение нескольких видов ЭП, тогда как предыдущий Федеральный закон от 10 января 2002 года «Об электронной цифровой подписи» (утративший силу с 1 июля 2013 года) предусматривал только один ее вид. Так, согласно действующему законодательству, выделяют простую и усиленную ЭП, последняя, в свою очередь, подразделяется на неквалифицированную и квалифицированную [4, ст. 5] Усиленная квалифицированная подпись создана лицом, которое в соответствии с федеральными законами и изданными в соответствии с ними нормативными правовыми актами наделено полномочиями на создание и подписание таких документов.

Выбор того или иного вида ЭП зависит от сферы ее использования, так как действующее законодательство предъявляет требования к использованию строго определенного вида электронной подписи в разных случаях. На данный момент универсальной ЭП, разрешенной к использованию при взаимоотношениях со всеми государственными органами и во всех сферах электронного документооборота, не существует. Так, в случае об-

ращения за получением муниципальных и государственных услуг, если их содержание состоит в предоставлении справочной информации и не предусматривает выдачу документов, в большинстве случаев может использоваться простая ЭП [1].

Если простая ЭП подтверждает, что электронное сообщение отправлено конкретным лицом, то неквалифицированная ЭП позволяет подтвердить, что с момента подписания документ не менялся. Но законодательством в большинстве случаев (для сдачи налоговой отчетности, участия в электронных торгах и т. д.) предусмотрено использование усиленной квалифицированной ЭП.

Организацию юридически значимого документооборота на предприятии с использованием ЭП можно вести как внутри организации, так и между разными организациями и при этом необходимо учитывать разрешимые сферы использования каждого из видов подписей. ФЗ «Об электронной подписи» установил две презумпции. Первая из них заключается в том, что документы, подписанные усиленной квалифицированной ЭП, признаются равнозначными бумажному документу, подписанному собственноручно. Исключения предусмотрены только в тех случаях, когда закон прямо предусматривает обязательность соблюдения письменной формы документа. Обратная презумпция установлена в отношении равнозначности подписанным вручную бумажным документам простой и усиленной неквалифицированной подписей. При этом признание такой равнозначности должно быть закреплено либо в соглашении сторон, либо в федеральном законе или принятом в соответствии с ним подзаконном акте.

Тем не менее, не смотря на кажущиеся сложности использования ЭП, нормативное регулирование сферы ее использования позволяет упростить и ускорить некоторые юридически значимые действия хозяйствующих субъектов – стало возможным сдавать налоговую отчетность через интернет, участвовать в электронных торгах государственного и корпоративного заказа, получить доступ к электронным услугам ряда ведомств, совершать операции по счету и обмениваться с банком документами без визита в офис и др. То есть использование ЭП позволяет значительно сократить временные издержки, а также обеспечивает взаимодействие тех или иных структур независимо от их удаленности друг от друга.

Также, следует отметить, что лица, использующие ЭП, получают гарантию защиты от подделок документов. ЭП подделать фактически невозможно, нежели ручную. Сделки, совершенные в виртуальном пространстве, становятся безопаснее сделок реальной действительности.

Технологические же особенности ЭП определили то, что авторство документа доказать не составляет труда – владелец не может отказаться от электронной цифровой подписи, размещенной под документом, так как

для создания корректной подписи нужен закрытый ключ, который имеется лишь у хозяина подписи [3].

Таким образом, среди основных преимуществ использования ЭП следует выделить экономию времени, безопасность использования и надежность обеспечиваемых ею сделок.

На сегодняшний день нормативное регулирование сферы использования ЭП несовершенно и требует доработок, тем не менее, активное использование достижений научно-технического прогресса не должно откладываться до лучших времен. Электронная подпись – это продукт, способный решать задачи, стоящие перед хозяйствующими субъектами. Электронная подпись – это инструмент современного информационного общества, преимущество от использования, которого можно считать в качестве, пусть не конкурентного, но как минимум, вспомогательного к нему.

Наряду с преимуществами, использование ЭП может вызвать и некоторые затруднения. Если говорить об основной проблеме, препятствующая широкому использованию ЭП, то она заключается в отсутствии доверия со стороны населения инновационным, высокотехнологичным решениям задач, стоящих перед современным человеком [5]. К тому же, обеспечение электронного документооборота требует наличия определенных технических средств, минимального набора знаний, позволяющих без затруднений использовать продукт информационного общества – электронную подпись. Информация, содержащаяся в электронных документах, требует соответствующей защиты от несанкционированных изменений [2]. Кроме того, активному использованию ЭП большинства хозяйствующих субъектов препятствуют ее цена и необходимость оформления разных подписей для взаимодействия с разными госорганами и доступа к различным базам данных.

Выводы. Как показывает практика, даже при наличии названных недостатков, широкое использование информационных продуктов не заставляет долго ждать. Давний тезис «будущее за информационными технологиями» успел себя оправдать. Ведь главные преимущества от использования информационных продуктов – экономия времени, мобильность, надежность и эргономичность на сегодняшний день обеспечивают выживаемость на конкурентном рынке. Использование ЭП выражает названные преимущества. Электронная подпись – это краеугольный камень развитого электронного документооборота, интенсивного экономического развития, успешного функционирования корпоративных отношений. И широкое ее использование, следует полагать, дело самого ближайшего будущего.

Библиографический список

[1] Горовцова М. Переходим с обычной подписи на электронную: преимущества и нюансы. URL: http://www.garant.ru/article/482896/ (дата обращения 06.03.17).

[2] Пазизин С. Преимущества электронной цифровой подписи и ее отличия от собственноручной подписи. URL: http://bankir.ru/tehnologii/s/preimyschestva-elektronnoi-cifrovoi-podpis/ (дата обращения 06.03.17).

[3] Туркин Р. Электронная подпись: опыт комплексного изучения. URL: http://zakon.ru/blogs/elektronnaya_podpis_opyt_ kompleksnogo_izuchen/ (дата обращения 08.03.17).

[4] Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи.URL: http://www.consultant.ru (дата обращения 10.03.17).

[5] Шадрина Т. Роскликом пера. Визировать документы теперь можно по Интернету. URL: http://www.rg.ru/2011/04/08/sign.html#comments (дата обращения 11.03.17).

Мельников Дмитрий Алексеевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: dmitriymelnikov1407@gmail.com

Твердова Светлана Михайловна – канд. техн. наук, доцент кафедры "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: ivalug@rambler.ru

А.Ю. Макарова

ПРИЗНАКИ ФИШИНГОВЫХ РЕСУРСОВ

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

Целью данной работы является исследование характерных признаков фишинговых ресурсов в сети Интернет.

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 [1].

Анализ существующих фишинговых ресурсов позволил составить перечень их характерных признаков.

1. Сходство графического контента.

Основная задача злоумышленников при проведении фишинговой атаки – заставить пользователя поверить в аутентичность фишингового ресурса. Наиболее простым способом сделать это является заимствование графического оформления у атакуемого сайта.

Несмотря на большое количество исследований, задача определения степени сходства изображений в настоящее время не имеет универсального и эффективного решения. Объясняется это в первую очередь тем, что понятие похожести двух изображений неразрывно связано с особенностями человеческого восприятия и вследствие этого трудно формализуемо. Уверенно можно говорить лишь о факте полной идентичности изображений, которая определяется попиксельным сравнением или сравнением на основе значений некоторой хэш-функции.

Для определения похожести изображений, подвергаемых незначительной модификации, возможно использование методов, основанных на сравнении усредненных характеристик изображения, например, метода поблочного анализа цвета или метода сравнения гистограмм [2].

Более сложный метод сравнения изображений–метод SURF. Он базируется на сравнении ключевых точек, инвариантных как к геометрическим и фотометрическим преобразованиям, так и к изменению масштаба. Нахождение ключевых точек осуществляется с помощью прохода по пикселям изображения и поиска максимума гессиана – определителя матрицы, составленной из вторых частных производных (матрицы Гессе) функции яркости изображения. Реализация данного метода содержится во многих открытых библиотеках алгоритмов, например, в библиотеке openCV.

2. Сходство текстового контента.

Понятие похожести текстов также является нечетким, и, как и в предыдущем случае, с уверенностью можно заявлять лишь об их полной идентичности. Однако на практике при изменении текстового контента оригинального ресурса злоумышленники, как правило, используют стандартный набор преобразований, таких, как:

- вставка наборов случайных символов;
- произвольная вставка и удаление пробелов;
- замена символов одной кодировки на похожие по написанию символы другой кодировки;
- вставка ключевых слов на случайные позиции.

В большинстве случаев производится сравнение не самих исходных текстов, а построенных на их основе подмножеств или отпечатков этих подмножеств – значений некоторых хэш-функций. В зависимости от способов построения отпечатков методы определения похожести текстов можно разделить на два класса – синтаксические и лексические. В первом случае анализируются построенные по определенным правилам последовательности слов из текста, во втором– строятся словари ключевых слов. С точки зрения эффективности и простоты реализации оптимальными являются два метода определения близости текстового контента: метод определения индекса повторяемости и метод поиска длинных предложений.

Сложность выявления сходства контента растёт пропорционально числу защищаемых ресурсов, что серьёзно сказывается на производительности антифишинговой системы. Проверка признаков, перечисляемых далее, не требует сравнения с оригиналом.

3. Наличие ресурса в фишинговых базах.

Интернет-сообществом поддерживается большое количество баз опасных ресурсов. Одни пользователи добавляют ссылки на такие ресурсы, другие – подтверждают или опровергают их опасность. Окончательное решение принимается администрацией конкретной базы. Как правило, фишинговые ресурсы попадают в такие списки в течение нескольких суток. Данный признак является очень сильным, однако сама концепция ведения списка подразумевает постоянную его актуализацию, которая всегда отстаёт от деятельности злоумышленников.

4. Использование особенностей формата URL.

Формат URL имеет много параметров, часть из которых крайне редко применяется на практике. Зачастую злоумышленники используют более пол-

ную форму, добавляя в неё редко используемые параметры, чтобы ввести пользователя в заблуждение и убедить его в подлинности фишингового ресурса.

5. Подозрительные регистрационные данные ресурса.

К регистрационным данным можно отнести географическое положение, дату регистрации домена, имя собственника сайта или название организации-владельца. Как правило, фишинговые сайты активны в первые пять дней после их создания. В связи с этим большое значение имеет дата регистрации домена. Часто фишинговые ресурсы регистрируются в стране, отличной от той, в которой расположен оригинальный сайт, поэтому необходимо также отслеживать соответствие домена верхнего уровня реальному местонахождению сайта [3].

6. Наличие ресурса на одном IP-адресе с выявленными ранее фишинговыми ресурсами.

Расположение нескольких ресурсов на одном IP-адресе является достаточно распространенной ситуацией, поэтому целесообразно использование списков IP-адресов, на которых были замечены фишинговые ресурсы. Таким образом можно идентифицировать ресурс как потенциально опасный, если он расположен на одном IP с множеством фишинговых ресурсов.

7. Наличие изображений, содержащих в себе текст в графическом представлении.

Данный способ применяется злоумышленниками для усложнения идентификации опасного ресурса. Пользователь будет воспринимать такой объект как обычный текст, а автоматизированные антифишинговые системы– как изображения. Если контент изображений дополнительно не анализируется, система может принять неправильное решение о степени опасности ресурса [4].

8. Использование «неоправданно большого» количества скриптов

Как правило, объём исполняемого кода на странице растёт пропорционально её информативности и предоставляемой функциональности. «Неоправданно большое» количество скриптов может являться признаком недокументированных возможностей. Для определения максимально допустимого количества скриптов предлагается использовать статистические данные из выборки в конкретной предметной области.

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

К.А. Евраскина

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, РЕГИСТРИРУЮЩЕЕ НАЖАТИЯ КЛАВИШ КЛАВИАТУРЫ И МЫШИ

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

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.

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

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.

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

А.А. Нефедов

ПРОГРАММНЫЕ ПЕРЕХВАТЧИКИ

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.

Способы распространения программного перехватчика:

- 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

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

В последние годы отмечается значительный рост числа различных вредоносных программ, использующих функции программного перехватчика. 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.

Программные перехватчики осуществляют контроль над действиями программного обеспечения, 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.

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

Методы защиты от программных перехватчиков:

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

Программные перехватчики относятся к виду шпионских программ, шпионские программы могут быть как узкоспециализированными (экранные и клавиатурные шпионы) так и комплексными. Последние обычно используются для слежения за сотрудниками в офисах или в качестве дополнительных инструментов родительского контроля.

Использование перехватчиков 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). Также они могут наносить вред программному обеспечению, изменять логику легитимных программ, путем внесения коррективов в события из очереди.

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

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

Таким образом, был рассмотрен программный перехватчик событий, способы его реализации, распространения и методы защиты. В результате было установлено, что в настоящее время отмечается значительный рост вредоносных программ на основе программных перехватчиков, 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

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

Е.А. Колодкина

РАЗНОВИДНОСТИ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, РАСПРОСТРАНЕННОГО В НАСТОЯЩЕЕ ВРЕМЯ

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

Существует класс программного обеспечения, которое было изначально написано с целью уничтожения данных на чужом компьютере, похищения чужой информации, несанкционированного использования чужих ресурсов или же приобрели такие свойства вследствие каких-либо причин. Такие программы несут вредоносную нагрузку и соответственно называются вредоносными. Вредоносное ПО – программное обеспечение, наносящее какой-либо вред компьютеру, на котором она запускается или другим компьютерам в сети.

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 2016–2017 годов наибольшую активность показали четыре шифровальщика: это TeslaCrypt (почти половина атак), CTB Locker, Scatter и Cryakl.

В 2016 году появилась первая программа-вымогатель, работающая на JavaScript, получившая имя Ransom32. Использование JavaScript делает данный вымогатель кроссплатформенным, т.е. он может использоваться 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 2017 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 2017 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 2016 году. Эта цифра примерно в 2 раза превышает ущерб от всех других экономических преступлений. В январе 2017 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/2016/12/28/biggest-cybersecurity-threats-in-2017.html

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

[3] Развитие информационных угроз во втором квартале 2017 года. https://securelist.ru/analysis/malware-quarterly/29062/it-threat-evolution-in-q2-2017-statistics/

[4] https://www.anti-malware.ru/news/2017-09-22/21018

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

А.А. Колесникова

РАЗРАБОТКА МОДУЛЯ ОБЕСПЕЧЕНИЯ ДОСТУПНОСТИ ДАННЫХ

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

Жизнь современного человека тесно связана с информацией, которая, в свою очередь, хранится и обрабатывается различными базами данных. Таким образом, задача любой существующей организации заключается в обеспечении необходимого и максимально возможного уровня защиты используемых баз данных. Для построения надежной системы баз данных используются средства обеспечения целостности, доступности и конфиденциальности, каждое из которых представляет собой сложнейшую комбинацию механизмов и правил. Чтобы выполнить качественную настройку хотя бы одного их перечисленных средств, предприятию необходимо установить дорогостоящие программно-аппаратные комплексы, а также иметь высококвалифицированных специалистов для работы с ними. А, как известно, технологии не стоят на месте и стремительно развиваются, в результате чего разработчикам необходимо успевать модернизировать системы безопасности своих продуктов в целях обеспечения гарантированно надежной защиты пользовательской и другой конфиденциальной информации. С увеличением уровня сложности защитных механизмов так же возрастает число трудностей в процессе выполнения их настроек и выбора наиболее подходящего варианта для конкретного сервера.

Целью данного проекта является разработка программного модуля обеспечения доступности баз данных, позволяющего оптимизировать процессы управления БД, а также обеспечить гарантированно высокий уровень доступности данных на предприятии, решив множество проблем, возникающих при использовании традиционных методов настройки БД.

Угрозы доступности БД. Под доступностью данных понимается состояние ресурсов автоматизированной информационной системы, при котором субъекты могут беспрепятственно реализовывать свои права доступа [1].

Угрозы, нацеленные на отказ в обслуживании, приводят к снижению работоспособности автоматизированной системы, а, в худшем случае, полностью блокируют доступ к её ресурсам. Все эти угрозы можно подразделить на две большие группы: внешние и внутренние.

К основным источникам внутренних угроз можно отнести:

1. Отказ программного обеспечения в результате наличия ошибок, изменения злоумышленником алгоритма работы программы, случайного или преднамеренного повреждения исполняемых модулей.

2. Возникновение ошибок конфигурирования в сложных системах при осуществлении некорректных настроек.

3. Нарушение правил эксплуатации в результате несоблюдения установленных требований к системе.

4. Проблемы работы в системе, вызванные отсутствием подробной документации к ней или сложностями понимания интерфейса.

Основными источниками внешних угроз могут быть:

1. нарушение работы аппаратных средств;

2. перебои с электричеством;

3. воздействие сетевых атак, внедрение в систему вредоносного ПО.

Самыми распространёнными причинами, приводящими к недоступности АС, являются человеческие ошибки, так как даже малейшая оплошность администратора может привести к катастрофическим последствиям. А потому преодоление человеческого фактора с помощью увеличения числа автоматизированных процессов позволит гарантированно увеличить уровень обеспечения доступности БД.

Сложность настроек и нехватка документации для разрешения экстренных ситуаций так же влекут за собой продолжительные отказы в обслуживании БД. Эти факторы значительно затрудняют диагностирование проблем и вызывают значительные затруднения у сотрудников даже при повторных аналогичных сбоях.

Таким образом, наличие специального программного обеспечения, позволяющего как можно более надёжно обезопасить систему от угроз доступности БД, позволит предприятию комфортно и со значительно меньшими рисками вести свои дела и взаимодействовать с клиентами.

Программный модуль обеспечения доступности данных позволит реализовать защиту БД с помощью двух мощных механизмов: Зеркальное отображение баз данных и Доставка журналов. Их комбинация позволит достичь наиболее надёжной системы безопасности, не перегрузив её при этом избыточным количеством настроек.

Зеркальное отображение базы данных. При использовании этого метода, устанавливается связь, называемая сеансом зеркального отображения БД, между двумя разными экземплярами сервера, на которых размещены копии одной базы данных. Один из экземпляров сервера выступает в качестве основного, другой – в качестве зеркального. Синхронизация данного сеанса позволяет получить сервер, который способен поддерживать быструю отработку отказа без потери информации о зафиксированных транзакциях [2].

Зеркальное отображение базы данных заключается в том, что в зеркальной БД повторяются все операции изменения, удаления, вставки, и обновления, которые выполняются в основной базе. Для этого поток записей активных транзакций с максимально возможной скоростью пересылается на зеркальный сервер. Зеркальный сервер получает журнал, после чего выполняет операции по его скорейшему применению. Как только журналы будут при-

менены на зеркальном сервере, базы данных считаются синхронизированными и остаются такими до разрыва сеанса зеркального отображения [3].

В случае если происходит сбой, зеркальный сервер может начать процедуру автоматического переключения ресурсов, в этот момент следящий сервер осуществляет поддержку данного процесса - определяет доступна ли база данных основного сервера. Проблему необходимо устранять на том сервере, который в настоящий момент является зеркальным партнером, до того, как основа станет основным. Как только все процессы по устранению неполадок будут успешно завершены, начинается перемещение обратно на сервер зеркального партнера, и базы данных синхронизируются снова. После выполнения синхронизации сеанс зеркального отображения можно возобновить [3].

Доставка журналов. Доставка журналов реализуется посредством резервного копирования и восстановления. Такой подход представляет собой весьма экономичное решение и, соответственно, очень выгодное как для разработчиков, так и для пользователей. Во время функционирования рассматриваемого процесса, база данных-получателя своевременно обновляется за счет применения резервного копирования журналов транзакций через определенные и заранее установленные интервалы времени [4].

Сама процедура задания доставки журналов по продолжительности занимает несколько минут, а также проста для понимания пользователями, не являющимися экспертами в работе с SQL. Все необходимые настройки, наблюдение, инициализация, планирование и т.д. осуществляются с помощью специально разработанных мастеров.

Этапы настройки доставки журналов:

1. На первом этапе необходимо определить базу данных-источника.

2. На втором выполняется создание расписания.

3. На третьем – определение и установка возраста файлов резервной копии.

4. На четвертом осуществляется настройка файлов резервной копии как общих файловых ресурсов.

5. На пятом выполняется восстановление БД-источника.

6. На шестом требуется инициировать БД-получателя, а также указать местоположение ее файлов.

7. На седьмом осуществляются работы по настройке расписания восстановления резервных копий журналов транзакций и резервного копирования файлов, учитывая все исключения и нюансы, а также расставляя время, необходимое для выполнения каждого этапа.

В большинстве случаев результатом сбоя, как правило, является отказ основного сервера, и для того чтобы вернуть его в строй требуется выполнить следующие действия: т.к. теперь вторичная база выполняет все функции рабочей, необходимо создать ее резервную копию, далее на основном сервере осуществить восстановление этой копии, после чего требуется пе-

ренаправить клиентские приложения снова на основной сервер; затем в обязательном порядке следует удалить любые старые задания для сетевого, резервного копирования и другие. Если пользователь платформы SQL проделал перечисленные действия корректно, после он сможет осуществить настройку механизма доставки журналов заново [4].

Основные функции разрабатываемого ПО. Программный продукт должен выполнять следующие функции:

1. возможность создания основного, зеркального и следящего серверов (для работы в режиме обеспечения доступности «Зеркальное отображение данных»), а также БД-источника и БД-получателя (для работы в режиме обеспечения доступности «Доставка журналов»);
2. возможность изменения ролей баз данных вручную;
3. автоматическая настройка синхронизации между серверами, благодаря которой сервер будет способен поддерживать быструю отработку отказа без потери информации о зафиксированных транзакциях;
4. организация пересылки потока записей активных транзакций на зеркальный сервер;
5. организация получения зеркальным сервером журнала и выполнения операций в соответствии с ним;
6. возможность создания расписания восстановления резервных копий;
7. возможность определения и установки возраста файлов резервной копии;
8. возможность настройки файлов резервных копий как общих файловых ресурсов;
9. проверка отклика баз данных;
10. восстановление данных и работоспособности БД после сбоя системы;
11. возможность работы с любой базой данных корпоративной автоматизированной системы.

Список литературы

[1] *Лачихина А.Б., Петраков А.А., Москвина А.А.* Обеспечение доступности в базах данных корпоративных информационных систем с помощью средств СУБД SQL Server // Вопросы радиоэлектроники. – 2015. – № 8 (8) – С. 100-108.

[2] *Мартин Грабер*. MasteringSQL. – М.: Лори, 2007. – 672 с.

[3] *S.S. Bagui*. Learning SQL on SQL Server 2005 – Sebastopol: O'Reilly, 2006. – p.342

[4] *Алекс Кригель, Борис Трухнов.* SQL. Библия пользователя. – М.: И.Д.Вильямс, 2010. – Издание 2. – 752 с.

Колесникова Анастасия Александровна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: N.Haruka69@yandex.ru

Е.Е. Костикова

РАЗРАБОТКА МОДУЛЯ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ БАЗЫ ДАНЫХ

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

Введение. Базы данных являются основой современных информационных технологий и роль их как единого средства хранения, обработки, доступа к большим объемам информации постоянно возрастает. Формируются новые требования к СУБД, например, поддержка широкого спектра типов представляемых данных и операций над ними (включая фактографические, документальные, картинно-графические данные, пространственно-временные с обеспечением визуализации данных). Усиливаются и традиционные требования повышения объема памяти, производительности, надежности, безопасности, поддержки целостности данных, контроля избыточности, непротиворечивости данных, применения стандартов, снижения времени реакции системы и др.

Исходя из определения информационной безопасности проблема защиты систем баз данных состоит в разработке методов и средств, обеспечивающих выполнение трех взаимосвязанных компонентов: *конфиденциальности, целостности, доступности*, которые связаны не только между собой, но и со свойствами обрабатываемой информации: актуальностью, своевременностью, точностью, достоверностью. Так, под конфиденциальностью подразумевается, что санкционированным пользователям *разрешается* выполнять необходимые действия, а под целостностью – *корректность* этих действий. Утрата целостности приводит к потере доступности, фальсификации данных. Утрата конфиденциальности нарушает неприкосновенность личных данных, параметры актуальности и точности жестко связаны соответственно с параметрами своевременности и достоверности и т.д.

Для современных корпоративных информационных систем более важными аспектами информационной безопасности являются целостность и доступность данных и услуг по их обработке. Понятие целостности является одним из основополагающих понятий, как для систем баз данных, так и для систем защиты. Поддержка целостности необходима даже в однопользовательских системах.

Современные СУБД предоставляют широкий спектр средств для обеспечения и поддержания целостности хранимых и обрабатываемых данных. Чаще всего средства пишутся на специальном процедурном расширении языка SQL (например, Transact-SQL) или на некотором универсальном языке программирования с включением в его код операторов SQL в соответствии со специальными правилами такого включения. Таким об-

разом, обеспечить целостность данных может только специалист, обладающий знаниями языка Transact-SQL, и других языков программирования. Сложность выполнения проверки целостности повышается.

Целью данного проекта является разработка приложения, позволяющего обеспечить достаточную целостность данных и выполнять проверку целостности страниц и структур базы данных в СУБД MS SQL Server на заданном предприятии. Кроме того, приложение должно выполнять следующие функции:

- восстановление данных при их случайном удалении и некорректном изменении;
- проверка структур выделения места на диске для указанной базы данных;
- проверка согласованности между файлами и директориями файловой системы на уровне ссылок;
- выведение нарушений пользователей в режиме журнала (логин пользователя; несанкционированное действие). В данном случае несанкционированным действием считается любое действие, на которое не распространяется право пользователя;
- анализ зарегистрированных в базе данных пользователей (логин/пароль пользователя; компьютер входа; время входа в базу данных);
- возможность работы с любой базой данных корпоративной автоматизированной системы.

Виды целостности данных. Целостность данных можно рассматривать на разных уровнях базы данных. Чаще всего считается достаточным обеспечение сущностной, доменной, ссылочной и определяемой пользователем целостности.

Сущностная целостность определяет строку таблицы как уникальный экземпляр некоторой сущности и обеспечивает целостность столбца с идентификатором (посредством индексов, ограничений UNIQUE, PRIMARY KEY или свойств IDENTITY).

Доменная целостность гарантирует наличие в некотором столбце только допустимых значений. Можно обеспечивать доменную целостность, ограничивая тип (посредством типов данных), формат (с помощью ограничений CHECK и правил) или диапазон допустимых значений (с помощью ограничений FOREIGN KEY и CHECK, определений DEFAULT, определений NOT NULL и правил).

Ссылочная целостность обеспечивает сохранность связей между таблицами при добавлении или удалении записей. В SQL Server ссылочная целостность основана на связях между внешними и первичными ключами или между внешними и уникальными ключами (через ограничения FOREIGN KEY и CHECK) и гарантирует согласованность значений ключа в связанных таблицах. Подобная согласованность требует отсутствия ссы-

лок на несуществующие значения и согласованного изменения ссылок на ключ во всей базе данных при изменении самого ключа.

При обеспечении ссылочной целостности SQL Server предотвращает следующие действия пользователей:

- добавление записей в связанную таблицу, если нет необходимой записи в главной таблице;
- изменение значений в главной таблице, в результате которого в связанной таблице останутся «зависшие» записи;
- удаление записей из главной таблицы при наличии связанных записей во внешней таблице.

Целостность, определяемая пользователем, позволяет определять некоторые бизнес-правила, не попадающие ни в какую другую категорию целостности.

Требования к разрабатываемому программному продукту:

1. Обеспечение целостности данных посредством объектовязыка программирования C# DataRelation.

2. Выполнение проверки целостности страниц и структур базы данных в СУБД MS SQL Server посредством использования инструкций DBCC CHECKDB и DBCC CHECKTABLE.

3. Восстановление данных при их случайном удалении и некорректном изменении посредством резервных копий. Сроком хранения резервных копия установить 6 месяцев. Данные, удаленные или измененные более 6 месяцев назад, не подлежат восстановлению в данном приложении.

4. Проверка структур выделения места на диске для указанной базы данных посредством использования инструкции DBCC CHECKALLOC.

5. Проверка согласованности между файлами и директориями файловой системы на уровне ссылок. При обнаружении несогласованности остановить какие-либо действия, производимые над данными файлами, и выводить на экран приложения информационное сообщение об найденной несогласованности.

6. Выведение нарушений пользователей в режиме журнала (логин пользователя; несанкционированное действие). В данном случае несанкционированным действием считается любое действие, на которое не распространяется право пользователя. В отдельном окне при необходимом запросе необходимо выводить все права, распространяемые на любого выбранного пользователя.

7. Анализ зарегистрированных в базе данных пользователей (Собранные данные должны быть представлены в виде таблицы со следующими входящими в нее данными: логин/пароль пользователя; компьютер входа; время входа в базу данных).

8. Возможность работы с любой базой данных корпоративной автоматизированной системы.

Заключение. Исходя из вышесказанного видно, что существует множество механизмов обеспечения целостности, но использования каждого из них требует знания языков программирования и наличие опыта работы с базой данных. Таким образом, обеспечение целостности, а, значит, и безопасности базы данных становится трудоемким процессом, требующим больших организационных и временных затрат предприятия. Создание приложения, которое автоматизировало бы все эти функции, могло бы решить проблему обеспечения целостности в базе данных предприятия.

Список литературы

[1] Лачихина А.Б., Мазин А.В. Методика подготовительных работ к настройке и мониторингу баз данных. LAMBERT Academic Publishing, Германия. 2011. 72 с.

[2] Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК. 2000. 448 с.

[3] Лачихина А.Б., Мазин А.В. Методика рациональной настройки баз данных на примере системы «Аналитик». – Вестник МГТУ им. Н.Э. Баумана, сер. Приборостроение. 2010. №4 (81). С.91-103.

[4] Алекс Кригель, Борис Трухнов. SQL. Библия пользователя. 2-е издание: Вильямс, 2010. 752 с.

Костикова Екатерина Евгеньевна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: ekaterina.hmel@yandex.ru

Ю.С. Носова, А.В. Чевычелов

РЕАЛИЗАЦИЯ АЛГОРИТМОВ СОРТИРОВКИ С CUDA

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

Введение

Язык программирования CUDA был представлен в 2008 году компанией Nvidia для параллельных вычислений на устройствах, произведённых данной компанией, например, на графических процессорах (GPU). В данной статье рассматривается повышение скорости выполнения алгоритмов сортировки с помощью Nvidia и языка CUDA. Теоретически, графический процессор, поддерживающий CUDA SM 2.0, может выполнять 1024 потока за цикл, что эквивалентно 1024 ядрам ЦП при параллельном вычислении, например, простых арифметических операций. Определить, повышает ли CUDA скорость выполнения операций, можно сравнив теоретические значения с фактическими результатами.

Последовательные алгоритмы сортировки

Алгоритмы сортировки обычно используются для упорядочивания элементов в массиве. Рассматриваются пять алгоритмов последовательной сортировки с различными вычислительными сложностями, а именно: сортировка пузырьком, сортировка выбором, сортировка вставками, быстрая сортировка и сортировка Шелла.

Таблица 1. Теоретические значения сложности для алгоритмов сортировки.

Алгоритм сортировки	Лучшее время	Среднее время	Среднее время
Пузырьковая	$O(n)$	$O(n^2)$	$O(n^2)$
Вставками	$O(n)$	$O(n^2)$	$O(n^2)$
Быстрая	$O(n \log n)$	$O(n \log n)$	$O(n^2)$
Выбором	$O(n^2)$	$O(n^2)$	$O(n^2)$
Шелла	$O(n)$	$O(n^{3/2})$	$O(n^{3/2})$

В сортировке пузырьком и быстрой сортировке элементы в массиве сравниваются попарно, а перестановка элементов происходит только при необходимости. Сортировка выбором - это тип сортировки, где выбирается крайнее значение (например, максимум или минимум), после чего происходит обмен этого значения со значением первой неотсортированной ячейки, после чего данная операция повторяется, пока сортировка не будет завершена. В сортировках вставками и Шелла конечный отсортированный массив компонуется один за другим, то есть каждый элемент перемещается в нужное положение до тех пор, пока список не будет полностью отсортирован.

Алгоритмы параллельной сортировки

Программа на CUDA состоит из частей, которые по одиночке или по несколько запускаются на CPU или GPU. В CUDA часть кода, выполняемого параллельно, называется стержнем. Стержень может состоять из функций и структур, которые запускаются на GPU. Во время компиляции кода генерируется большое количество потоков. Во время работы программы часть кода выполняется на GPU, где генерируется большое количество потоков для параллельной работы. Концепция модели программирования CUDA состоит в том, чтобы генерировать тысячи потоков, которые будут выполняться в режиме Single Program Multiple Data (SPMD), параллельно, над небольшими фрагментами данных.

В данной статье используется библиотека Python с открытым исходным кодом, называемая PyCUDA.

Детали реализации

Прежде всего, многоядерная архитектура GPU очень хорошо подходит для параллельных вычислений. Все рассмотренные алгоритмы сортировки обеспечивают параллелизм на уровне данных. Другими словами, массив, подлежащий сортировке, фактически разлагается на подмассивы и при использовании многопоточного подхода каждый подмассив сортируется графическими процессорами, а результаты собираются в основной поток. Рассмотрим алгоритмы сортировки пузырьком для стандартной архитектуры и CUDA соответственно.

```
1: FOR passnum BETWEEN LengthOf(array) AND 0
2:   FOR i BETWEEN 0 AND passnum
3:     IF (array[ ith_element] > array [i+1_th_element])
4:       SWAP(array[ ith_element] WITH array [i+1_th_element
5:     ENDIF
6:   ENDFOR
7: ENDFOR
```

Рисунок 1. Псевдокод последовательной сортировки пузырьком

```
1: idx = thread_id, N = length_of(array)-1
2: FOR i = idx BETWEEN 0 AND N
3:   FOR j BETWEEN 0 AND N-1-i
4:     IF (array[ j ] > array [ j+1 ])
5:       SWAP(array[ j ] WITH array [ j+1 ])
6:     ENDIF
7:   ENDFOR
8: ENDFOR
```

Рисунок 2. Псевдокод параллельной сортировки пузырьком

В первой строке псевдокода параллельной сортировки переменная idx связана с thread_id, что означает, что при каждом запуске номер потока будет уникальным. Эта строка необходима для правильного вычисления, а также для распараллеливания кода. Тогда переменная N равна длине вход-

ного массива. Вторая строка начинается с цикла for для каждого thread_id, связанного с переменной цикла i, затем внутренний цикл выполняет итерацию индексов сравнения и перемещения для каждого прохода внешнего цикла FOR. Четвертая строка сравнивает элементы массива попарно, и если какая-либо пара находится в порядке убывания, то выполняется замена.

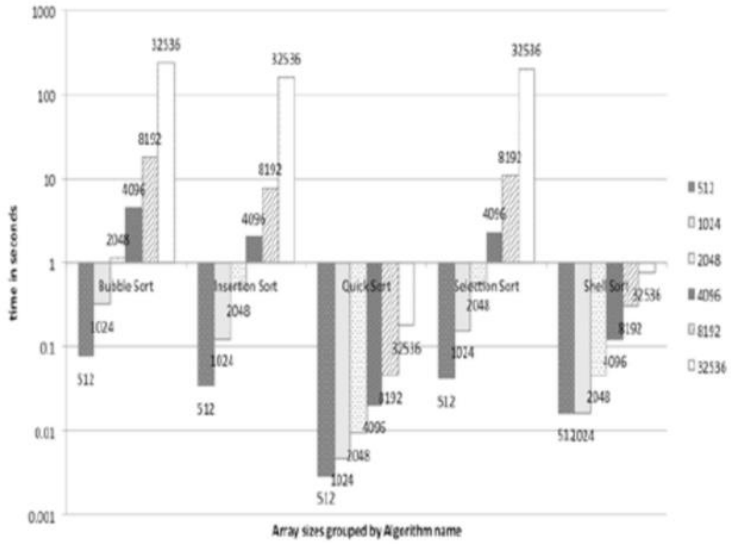

Рисунок 3. Время выполнения сортировок в последовательном коде

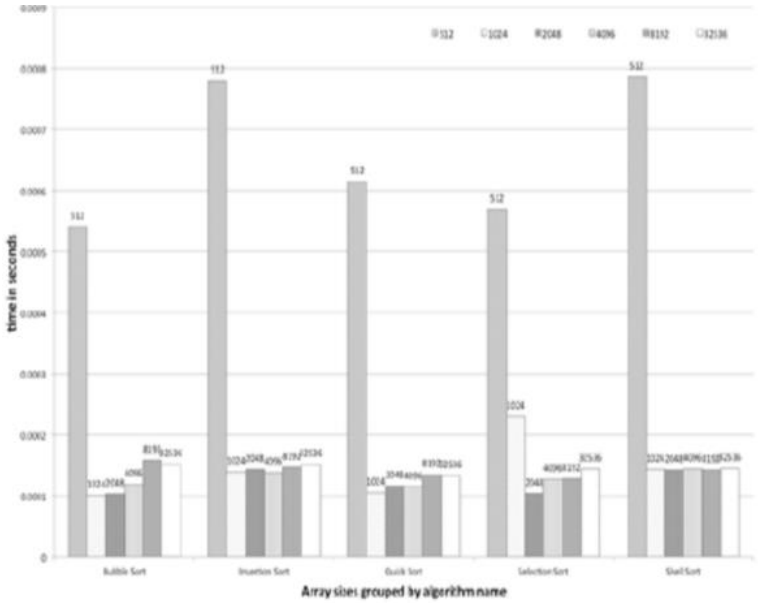

Рисунок 4. Время выполнения сортировок в параллельном коде

Исходя из диаграмм, представленных на рисунках 3 и 4, можно сделать вывод, что для наиболее эффективной работы с CUDA, размеры массивов должны быть очень большими, тогда время, затраченное на выполнение алгоритмов, будет соответствовать сложности, возникающей при использовании последовательных алгоритмов.

Заключение

Результаты, исследования, предоставленные в данной статье, показывают, что при использовании CUDA вместо последовательного кода может быть достигнуто значительное ускорение. Как показывают результаты, алгоритмы последовательной сортировки, организованные для графических процессоров, могут обеспечить высокие результаты производительности без существенного изменения последовательных кодов. Однако, чтобы получить максимальную отдачу от вычислительной мощности графического процессора, необходимо переработать алгоритмы, чтобы они соответствовали основной параллельной архитектуре графических карт (GPU).

Список используемой литературы

[1] С. Кук, CUDA Programming: Руководство разработчика по параллельным вычислениям с использованием графических процессоров (приложения Gpu Computing), 2012

[2] Пачеко П., Введение в параллельное программирование, Морган Кауфманн, 2012

[3] Н. Вильдт, Руководство CUDA, Полное руководство по программированию на GPU, Образование Pearson, 2013

[4] Дж. Эдосомван, Алгоритм сортировки, LAP Lambert Academic Publishing, 2012

[5] С. Арора, Б. Барак. Вычислительная сложность: современный подход. Ed., Cambridge University Press, 2009

Чевычелов Артем Владимирович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: artyomche9@gmail.com

Носова Юлия Сергеевна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: yuliya-nosova1996@yandex.ru

Е.И. Антипова

СИСТЕМЫ КОНТРОЛЯ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЯ

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

Современные системы информационной безопасности реализуют принцип «многоэшелонированной» защиты. Правильно установленные и настроенные средства защиты информации позволяют достаточно надёжно защититься от атак злоумышленников или вирусных эпидемий. Но, несмотря на все это, проблема внутренних нарушителей остается актуальной. Раньше, на фоне хакеров и множества компьютерных вирусов, собственные сотрудники выглядели не столь угрожающе. Но в наше время их действия, совершенные из-за некомпетентности или же, что тоже довольно часто – преднамеренности, влекут за собой реальные угрозы для компании [1].

Аналитический Центр компании InfoWatch [2] провел глобальное исследование утечек конфиденциальной информации в I полугодии 2016 г. и опубликовал следующие данные:

1. В I полугодии 2016 года в мире зафиксировано, обнародовано в СМИ и зарегистрировано Аналитическим центром InfoWatch 840 случаев утечки конфиденциальной информации, что на 16% превышает количество утечек, зарегистрированных за аналогичный период 2015 года.

2. Россия занимает второе место по количеству опубликованных утечек. Количество «российских» утечек по сравнению с 2015 годом выросло на 2% – в исследуемый период зарегистрировано 110 случаев утечки конфиденциальной информации из российских компаний и государственных организаций.

3. Во всем мире скомпрометировано более 450 млн записей, в том числе финансовые и персональные данные.

4. В 71% случаев виновными в утечке информации оказались сотрудники компаний. В 3% случаев - высшие руководители организаций.

5. К непосредственным утечкам данных относятся 83% случаев компрометации информации, 11% зафиксированных утечек сопряжены с использованием сотрудниками служебного положения для получения личной выгоды, в 5% утечек произошли вследствие превышения сотрудниками прав доступа к информации.

Всем этим объясняется рост интереса в последние десятилетия к мониторингу действий пользователя. С помощью систем контроля пользователей рабочие операции проверяются на предмет их соответствия корпоративным политикам по соблюдению нормативных требований и автоматически выводятся предупреждения, когда нарушаются политики безопасно-

сти, либо информация и технологические активы подвергаются риску несанкционированного доступа и деструктивных действий [3].

Программное обеспечение для мониторинга пользователей, как правило, включает в себя:

- мониторинг рабочего стола;
- мониторинг процессов;
- мониторинг доступа к USB;
- мониторинг интернет-активности;
- мониторинг локальных действий.

Мониторинг рабочего стола реализуется двумя способами - администратор видит всё то, что в данный момент видит пользователь, или просматривает сохранённые снимки экрана. Они могут быть использованы как вещественные доказательства нарушения трудового договора. Существует много других способов получить снимок экрана, например, программа Greenshot [4].

Мониторинг процессов отслеживает запущенные приложения, сохраняя различные параметры: время запуска, время работы, время активности на экране и т.д. Это позволяет оценить эффективность использования рабочего времени работником, отследить вирусную атаку, которая может повредить корпоративную информацию.

Большинство систем позволяет блокировать запуск определённых процессов. Может существовать функция завершения уже запущенных процессов удалённо. Существует множество вариантов получения списка процессов. Например, библиотека tlhelp32.h позволяет получить список процессов в Windows.

Мониторинг доступа к USB. Съёмные usb-носители представляют серьёзную угрозу конфиденциальной информации. Большинство систем наблюдения предоставляют возможность блокировки доступа ко всем устройствам, фильтрации устройств и журналирование использования usb-устройств. Это предотвращает как утечку информации, так и проникновение вирусов на рабочий компьютер. Часто, при разрешённом доступе, всё, что копируется на съёмный носитель, сохраняется в другом месте и может быть использовано для расследования нарушений политики компании. В Windows технически это реализуется несколькими способами:

- полное блокирование через реестр;
- полное блокирование, через запрет записи в файлов %SystemRoot%\Inf\Usbstor.pnf , %SystemRoot%\Inf\Usbstor.inf;
- частичная блокировка и фильтрация возможна через написание USB-драйвера.

Мониторинг интернет-активности. Интернет - серьёзный канал утечки конфиденциальных данных, поэтому системы контроля за действиями пользователей отслеживают многие аспекты интернет активности работника.

Мониторинг посещаемых веб-сайтов позволяет выявить нецелевое использование рабочего времени, отслеживать поисковые запросы сотрудника (из них можно отследить - ищет ли он другие вакансии или не относящуюся к работе информацию). Сохраняются Url, заголовки посещённых страниц, время их посещения. Некоторыми системами реализуется возможность наблюдения в режиме реального времени за открытыми сайтами [4].

Социальные сети. Помимо не целевой траты рабочего времени на социальные сети, через них может утекать конфиденциальная информация. Поэтому система может сохранять набор данных: просматриваемые профили, переписки, а также отправляемые туда фотографии.

IM. Чтобы предотвратить или потом доказать утечку информации, перехватываются и сохраняются сообщения большинства популярных IM-протоколов и мессенджеров (ICQ, Skype). Это делается как программными средствами, так и через анализ трафика, проходящего через шлюз.

Мониторинг электронной почты. Для этого ведётся полное журналирование всех сообщений электронной почты. Чаще всего это делается путём перехвата сообщений локального почтового клиента, однако возможен и перехват сообщений, отправляемых через web-клиент. Технически, такой вид мониторинга может быть реализован двумя способами:

1. Перехват непосредственно сетевого трафика программно или аппаратно. Это работает до тех пор, пока не используется защищенное интернет соединение, например, SSL.

2. Перехват содержания web-форм, полей ввода и прочего. При таком методе наблюдения скрыть передаваемое сообщение практически невозможно.

Мониторинг локальных действий. Основные локальные действия пользователя тоже контролируются.

Мониторинг клавиатуры. Система записывает все нажимаемые клавиши, включая системные (CTRL, SHIFT, ALT, CAPS LOCK), кроме этого могут быть записаны название окна, в которое производился ввод, язык раскладки и т.д. Это позволяет контролировать использование конфиденциальной информации, восстанавливать забытые пароли [5]. Для Windows кейлоггеры создаются с помощью так называемых хуков, когда между нажатием клавиши и отправкой сообщения окну о факте нажатия, вклинивается сторонняя функция, которая отмечает факт нажатия клавиши. В unix-подобных системах, использующих X-сервер, кейлогеры реализуются по средствам функции XQueryKeymap из библиотеки Xlib.

Буфер обмена. Система сохраняет всё, что было скопировано в буфер обмена, и почти всегда, сопутствующую информацию. Это позволяет предотвратить потерю информации, даёт возможность обнаружить разглашение конфиденциальной информации. Windows предоставляет стандартную функцию для этих целей SetClipboardViewer, для Linux это делается через Xlib. Так же есть платформонезависимые средства управления буфером обмена, например, Qt.

Запоминаются все действия с файлами: копирование, удаление, редактирование, и программа, через которое действие совершено. Это позволяет установить, какие файлы использовал сотрудник для своей работы, и выявить вирусную атаку. Для Windows программно это реализуется подменой стандартных функций чтения/записи файла в соответствующих динамических библиотеках (DLL). В Linux этого можно достичь, перехватывая системные вызовы.

Печать файлов. Через принтер может утечь конфиденциальная информация, достаточно распечатать важный документ и вынести с предприятия, поэтому сохраняются названия печатаемых файлов, времени и даты печати. Также печатаемые файлы могут сохраняться, как в виде исходного файла, так и в виде графического файла. В Windows для таких целей предусмотрен Print Spooler API [5], позволяющий управлять очередью печати. Для Linux теневое копирование файлов печати реализуется с помощью CUPS.

Подведем некоторые итоги данного исследования.

Защита безопасности – актуальная тема, включающая несколько направлений. Пользователь, как главное действующее лицо корпоративной информационной системы, может умышленно или неумышленно нанести ущерб безопасности данным. Следовательно, мониторинг действий пользователя является важной частью комплексной системы безопасности компьютерных систем. Применение специальных программных средств может поднять на новый качественный уровень систему комплексной безопасности предприятия.

Список литературы

[1] Горбачевская, Е.Н., Краснов, С.А. Анализ структуры системы информационной безопасности предприятия с централизованной авторизацией пользователей // Вестник Волжского университета имени В.Н. Татищева. - №4(22). - С. 63-74.

[2] Глобальное исследование утечек конфиденциальной информации в I полугодии 2016 года. URL: http://www.infowatch.ru/report2016_half

[3] Жадаев, А.Г. Как защитить компьютер на 100%. – СПб.: Питер, 2014. – 304 с.

[4] Эминов, Б.Ф., Эминов, Ф.И. Безопасное управление ресурсами и пользователями в корпоративных информационных сетях: Учебное пособие. - Казань: Новое знание, 2007. – 80 с.

[5] Система контроля действий пользователя. URL: https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8F_%D0%B4%D0%B5%D0%B9%D1%81%D1%82%D0%B2%D0%B8%D0%B9_%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8F

Антипова Евгения Игоревна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: antipova.evgenia93@gmail.com

А.А. Гапутина, И.С. Скубаева

СПОСОБЫ ЗАЩИТЫ ВИДЕОДАННЫХ

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

В связи с распространением цифрового медиаконтента, глобальное использование высокоскоростного Интернета, локальных вычислительных сетей, беспроводных сетевых технологий делает проблему защиты видеоданных еще более актуальной. Существуют многочисленные способы передачи видеоинформации (видеоконференции, видеосвязь, видеонаблюдение, цифровое наземное, кабельное и спутниковое ТВ), которые не могут быть конфиденциальны без применения средств защиты.

Способ защиты видеоданных выбирается в зависимости от области их применения. Выбор актуальных методов влияет на построение надежной системы защиты.

Можно выделить следующие группы методов защиты видеоданных:

1. Криптографические методы
2. Стеганографические методы
3. Методы, использующие робастные хэш-функции
4. Гибридные методы

Методы защиты видеоданных.

Суть криптографии (с древнегреческого - "тайнопись") заключается в том, что текст, который необходимо зашифровать (открытый текст) подвергается некоторому преобразованию с использованием секретного ключа, в результате получается закрытый текст, непонятный никому, кроме обладателя ключа.

Для преобразования обычно используются алгоритм и устройство шифрования. Процесс преобразования осуществляется с помощью изменяемого ключа, позволяющего каждый раз получать оригинальное представление информации при использовании одного и того же алгоритма или устройства. Наличие ключа позволяет просто, быстро и однозначно расшифровать текст. Но даже при известном алгоритме и неизвестном ключе, расшифровать текст может быть практически невозможно.

Отличительной особенностью криптографических методов является использование «хрупких» аутентификаторов, применяющихся к безизбыточным данным. Если хотя бы один бит заверяемых данных будет искажен вследствие ошибок в канале связи, то данный фрагмент не пройдет проверку. Данное условие создает ограничение в использовании.

Другой подход к защите видеоданных – это использование технологий стеганографии, а именно технологий цифровых водяных знаков (ЦВЗ).

Основные проблемы данного метода:

1. Ограничение на объем информации

2. Возможные визуальные искажений видеоданных

3. Недостаточная чувствительность к искажениям.

Подходом к решению проблем криптографических методов является применение вместо криптографических хэш-функций робастных. Данный класс хэш-функций формирует аутентификатор на основе изображения и конфиденциальной ключевой информации. Робастные хэш-функции имеют низкую чувствительность к случайным искажениям и значительную к преднамеренным. Основная проблема робастных хэш-функций: недостаточная теоретическая проработка критериев выявления искажений.

Хеширование - преобразование данных произвольной длины в строку фиксированной длины. Такие преобразования также называются хеш-функциями или функциями свёртки, данные – прообразом, а результаты преобразования - хешем, хеш-кодом, хеш-образом, цифровым отпечатком.

Так как равенство значений хеш-функции $h(x) = h(y)$ на двух различных значениях x, y, $x \neq y$ – это коллизия, то к хеш-функции должны применятся следующие свойства:

- для конкретно заданного значения $h(x)$ становится невозможным подобрать значение аргумента x. Обычно хеш-функции, отнесенные к этому свойству, называют стойкими в сильном смысле, либо стойкими в смысле обращения;
- для конкретно заданного аргумента x становится невозможным подобрать другой аргумент y, который удовлетворяет равенству $h(x) = h(y)$. Данные хеш-функции называют стойкими в слабом смысле или стойкими в смысле вычисления коллизий.

Значение хеш-функции называют имитовставкой, кодом аутентификации данных (Data Authentication Code) или кодом проверки подлинности сообщений (Message Authentication Code) только в том случае, когда значение хеш-функции будет зависеть от закрытого ключа, а не только от прообраза.

Алгоритм организации защиты видеоданных:

1. Реализуется сжатие группы кадров кодеком H.264.

2. Получают некий набор целочисленных квантованных коэффициентов DC и AC от блоков 4x4 и 16x16.

3. По полученному набору определяется криптографический хэш-код, посредством функции SHA длиной 160 бит.

4. Данный хэш-код подтверждается электронной цифровой подписью.

5. Эта подпись посылается в виде потока зашифрованного сигнала как дополнительная информация об улучшении (Supplemental Enhancement Information).

После принятия данных реализуются следующие шаги:

1. Производится декодирование группы кадров, а также извлечение набора проверочных коэффициентов.

2. По полученной группе кадров осуществляется расчет хэш-кода посредством все той же функции SHA.

3. Анализируется ЭЦП дешифрованная, и решается, прошла ли группа кадров проверку или нет.

Можно сделать вывод, что на сегодняшний день существует несколько методов защиты видеоданных, обладающих своими преимуществами и недостатками.

Литература:

[1] Грибунин В.Г. Цифровая стеганография / Грибунин, В.Г., Оков И.Н., Туринцев И.В. // Солон-Пресс. -2002. -Научное издание, -с. 235

[2] Оков И.Н. О требуемой пропускной способности каналов передачи аутентифицированных сообщений в безусловно стойких системах. Проблемы информационной безопасности. Компьютерные системы. 2000. №3(7), с. 78-64.

[3] Шаньгин В. Информационная безопасность. Litres, 2017. С. 233-235

[4] Шнайер Б. Прикладная криптография / Брюс Шнайер // "Триумф". -2002. -Научное издание, -параграф 16.9

Гапутина Алина Александровна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: alina.gaputina@mail.ru

Скубаева Ирина Сергеевна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: russia071@yandex.ru

И.Б. Парамонов, А.В. Мазин

СПОСОБЫ ОБЕСПЕЧЕНИЯ ВЫСОКИХ ПОКАЗАТЕЛЕЙ НАДЕЖНОСТИ АППАРАТУРЫ

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

При разработке изделий, обеспечивающих безопасность объектов, в частности средств защиты информации, одной из значимых задач, требующей решения и проработки является обеспечение заданных показателей надежности (ПН) при эксплуатации.

В рамках данной статьи будем использовать понятия безотказности, т.е. свойства объекта непрерывно сохранять работоспособное состояние в течение некоторого времени или наработки [1], и долговечности – способности объекта не достигать в течение достаточно длительного времени предельного состояния, т.е. такого состояния, при котором дальнейшее использование объекта по назначению становится невозможным или нецелесообразным, несмотря на наличие установленной системы технического обслуживания и ремонта [2].

Особое место среди средств защиты занимают устройства (рис. 1), осуществляющие защищенную передачу данных с целью посылки команд управления.

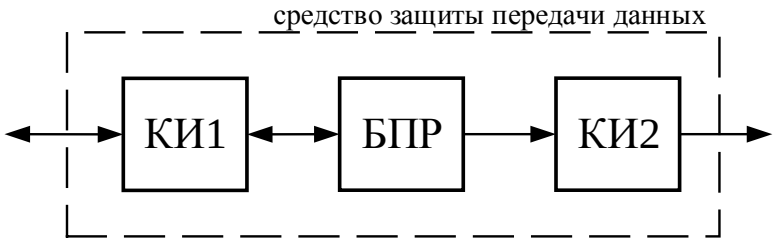

Рис. 1. Общая структура средства защиты передачи данных

Применение методик расчета показателей надежности, установленных в государственных стандартах, а также используемых в современных отечественных автоматизированных системах расчета надежности показало, что достижение высоких показателей надежности аппаратуры зачастую невозможно без управления режимом её работы. Путем непосредственного расчета показателей надежности с использованием автоматизированной системы обеспечения надежности и качества аппаратуры «АСОНИКА» рассмотрим взаимосвязь показателей надежности с управлением режимами работы аппаратуры.

Согласно рис. 1 средство защиты передачи данных включает:

1) Контроллер интерфейса 1 (КИ1);

2) Блок принятия решения (БПР);

3) Контроллер интерфейса 2 (КИ2).

Для расчета показателей надежности вышеуказанной системы зададим численные значения показателей безотказности и долговечности.

Пусть заданная вероятность безотказной работы устройства принимает значение:

$$P(t_{б.р.}) = 0{,}999995,$$

где $t_{б.р.}$ – наработка, в пределах которой вероятность безотказной работы изделия не ниже заданной [3].

Средняя наработка до отказа:

$$T_{ср} = 150000 \text{ ч}$$

В качестве предельного состояния устройства установим отказ в передаче данных.

Вероятность безотказной работы средства защиты, построенного в соответствии со структурой, показанной на рис. 1 (экспоненциальная модель) [2]:

$$P(t_{б.р.}) = e^{-\Lambda_{РЭА} \cdot t_{б.р.}}, \quad (1)$$

где $\Lambda_{РЭА}$ – суммарная интенсивность отказов аппаратуры (постоянная) [4].

$$\Lambda_{РЭА} = K_a \cdot \sum_{j=1}^{m} \sum_{i=1}^{n} \lambda_{эij}, \quad (2)$$

где K_a – коэффициент качества производства аппаратуры; $\lambda_{эij}$ – эксплуатационная интенсивность отказов *i*-го типа изделий *j*-ой группы; *n* – количество изделий j-ой группы; *m* – количество групп изделий.

Средняя наработка до отказа

$$T_{ср} = \frac{1}{\Lambda_{РЭА}}. \quad (3)$$

Значения эксплуатационной интенсивности отказов большинства групп электрорадиоизделий (ЭРИ) рассчитываются по математической модели, имеющей вид:

$$\lambda_э = \lambda_б \times \prod_{i=1}^{n} K_i. \quad (4)$$

где $\lambda_б$ – базовая интенсивность отказов типа ЭРИ, рассчитанная по результатам испытаний ЭРИ на безотказность, долговечность, ресурс; K_i – коэффициенты, учитывающие изменения эксплуатационной интенсивности отказов в зависимости от различных факторов (устанавливаются для каждой группы ЭРИ); *n* – число учитываемых факторов.

Примерный перечень элементов (с их базовыми интенсивностями отказов) средства защиты информации, имеющего структуру согласно рис. 1, для расчета приведем в таблице 1.

Таблица 1. Примерный перечень элементов устройства защиты

Наименование	**Кол-во**	**Базовая интенсивность отказов, $\lambda_б \cdot 10^7$, 1/ч**
Резонатор кварцевый РК319-Д-8,000 М	1	0,2600
Конденсаторы		
К53-68-"С"-10 В-10 мкФ±20%	1	0,6400
К10-17-4в-Н90-0,22 мкФ	4	0,2070
К10-17-4в-М47-33 пФ±20%-2	1	0,2070
К10-17-4в-Н90-0,1 мкФ	3	0,2070
К10-17-4в-М47-33 пФ±20%-2	1	0,2070
К10-17-4в-Н90-0,1 мкФ	4	0,2070
Микросхемы		
5559ИН4У	2	0,4300
1158ЕН3,3ВХ	1	0,2800
1986ВЕ92У	1	0,2300
1636РР2БУ	1	0,1800
Резисторы		
Р1-12-0,125-100 кОм±5%-М	1	0,0600
Р1-12-0,125-10 кОм±5%-М	1	0,0600
Р1-12-0,125-510 Ом±5%-М	4	0,0600
Р1-12-0,125-10 кОм±5%-М	14	0,0600
Диоды		
2Д212А/СО	2	0,9100
2Д522Б	1	0,9100
Соединители		
Вилка РРС5-19-1-1-В	1	0,0190
Вилка РРС5-19-1-2-В	1	0,0190

Результаты расчета в автоматизированной системе обеспечения надежности и качества аппаратуры «АСОНИКА» сведем в таблицу 2.

Таблица 2. Результаты расчета показателей надежности устройства защиты со структурой согласно рис. 1.

Параметр	**Значение**
Температура окружающей среды, °С	Плюс 55
Расчетная интенсивность отказов: 1/ч	$29{,}8971 \cdot 10^{-7}$
Вероятность безотказной работы за время работы 150000 ч	0.7442

Очевидно, что для значения средней наработки до отказа $T_{ср}$ = 150000 ч при построении устройства в соответствии со структурой, показанной на

рис. 1, и непрерывном режиме работы вероятность безотказной работы $P(t_{б.р.})$ = 0,999995 не достижима.

Для достижения заданной величины вероятности безотказной работы $P(t_{б.р.})$ введем двойное резервирование всех блоков средства защиты, а также сеансность работы изделия.

Структура средства защиты передачи данных при двойном резервировании блоков показана на рис. 2.

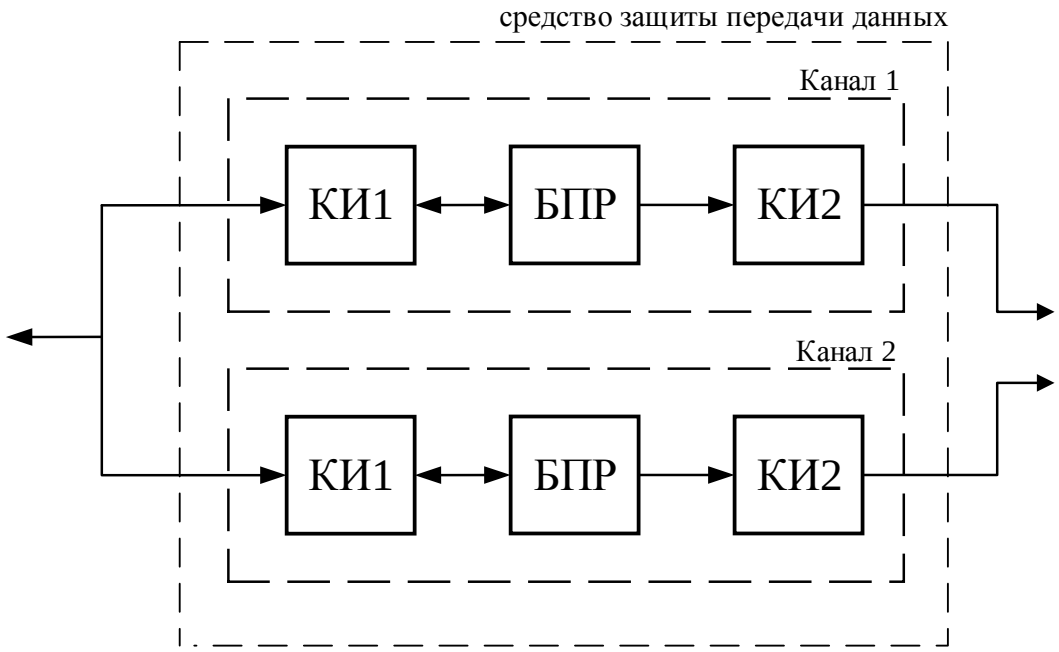

Рис. 2. Структура средства защиты передачи данных при двойном резервировании блоков

Вероятность безотказной работы устройства защиты при таком построении будет вычисляться по следующей формуле:

$$P(t_{б.р.}) = 1 - \left[1 - P_0(t_{б.р.})\right]^2, \quad (5)$$

где $P_0(t_{б.р.})$ – вероятность безотказной работы одного канала.

При использовании сеансности работы устройства суммарное время работы устройства за время $T_{ср}$ будет вычисляться как:

$$T = \frac{t_c \cdot k_c}{60} \cdot T_{ср}, \quad (6)$$

где t_c – время сеанса связи АС, мин; k_c – количество сеансов связи за 1 час наработки.

Зависимость значения вероятности безотказной работы от времени сеансной работы средства защиты покажем на рис. 3.

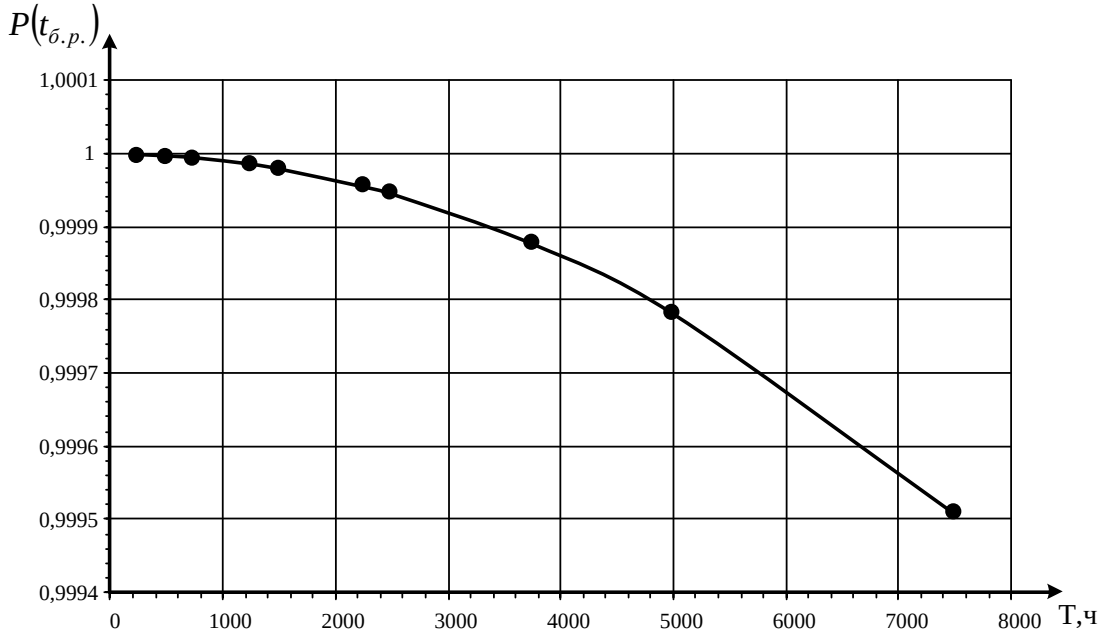

Рис. 3. График зависимости вероятности безотказной работы от времени сеансной работы средства защиты информации

Используя зависимость, полученную в результате расчетов показателей надежности средства защиты информации, можно сделать вывод о том, что для повышения отказоустойчивости подобного рода устройств, т.е. повышения их надежности, целесообразно, во-первых, введение резервирования, полного или частичного, а, во-вторых, использовать режимы работы изделий, позволяющие задействовать блоки аппаратуры в течение небольшого промежутка времени, т.е. использовать сеансную работу устройств с заданной (целесообразной в данных условиях эксплуатации) скважностью.

Список литературы

[1] ГОСТ 27.002-89. Надежность в технике. Основные понятия. Термины и определения.

[2] *В.В. Клюев, В.В. Болотин, Ф.Р. Соснин* и др. Машиностроение. Энциклопедия. Надежность машин. Т. IV-3. – М.: Машиностроение. 2003. – 592 с.

[3] ГОСТ 27.003-90. Надежность в технике. Состав и общие правила задания требований по надежности.

[4] Надёжность электрорадиоизделий. Справочник. 22 ЦНИИИ МО РФ. 2006.

Парамонов Илья Борисович – аспирант КФ МГТУ им. Н.Э. Баумана. E-mail: piborisovich@gmail.com

Мазин Анатолий Викторович – д-р техн. наук, заведующий кафедрой "Информационная безопасность автоматизированных систем" КФ МГТУ им. Н.Э. Баумана. E-mail: mazinav@yandex.ru

Е.Ю. Шестопалов, А.Б. Лачихина

СРАВНИТЕЛЬНЫЙ АНАЛИЗ БАНКОВСКИХ КАРТ

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

Современный мир невозможно представить без банковских карт. На них перечисляют зарплату, ими удобно оплачивать покупки, они позволяют легко и быстро делать денежные переводы, брать кредиты и многое другое. Банковские карты стали постоянным спутником многих людей, которые зачастую хранят на них значительные суммы денег. Это, безусловно, вызывает большой интерес преступников.

В связи с этим в данной сфере остро стоит вопрос безопасности [1].

Сегодня в платежной сфере используется три вида карт:

– карты с магнитной полосой;
– чип-карты;
– бесконтактные карты.

Первыми появились карты с магнитной полосой. Помимо идентификационного номера карты, срока её действия, фамилии и имени держателя и других данных, нанесенных непосредственно на них, в три магнитные дорожки карты заносится и другая информация. В первой и второй хранятся данные, используемые для защиты операций по карте, её порядковый номер, дублируется информация, нанесенная на карту. Третья дорожка содержит номер карты, код страны, срок действия, географическое использование карты, тип счета. Первая и вторая дорожки не перезаписываются, третья может использоваться для хранения данных по выполняемой операции.

Данные карты оказались недостаточно надёжными. Ограниченная емкость магнитной полосы не позволяет использовать многоступенчатые механизмы защиты. Злоумышленник может считать информацию с карты, приложив к ней устройство для чтения. Кроме того, срок эксплуатации магнитной полосы мал [2].

Следующим типом банковских карт стали микропроцессорные карты. Они являются настоящими микро-ЭВМ, содержащими центральный процессор, память программ и память данных. Специальное программное обеспечение в полном объеме позволяет поддерживать множество систем защиты, таких как защищенные кодом владельца и кодом пользователя области памяти, блокировка карты после сделанных подряд неверных попыток ввести код, использование алгоритмов шифрования.

Чип-карты обладают высокой защищенностью и надежностью. Злоумышленник не сможет считать данные дистанционно. Срок их действия достаточно большой, так как микросхема с хранящимися на ней данными не подвержена разрушению. Однако наличие физических контактов чипа,

подверженных износу, является слабым местом микропроцессорных карт [3].

Бесконтактные карты появились самыми последними. В основе дистанционного взаимодействия карты и считывающего устройства лежат принципы электромагнитной индукции и резонанса. При попадании карты в переменное магнитное поле в антенне, находящейся в ней, возникает электрический ток, который питает чип, производящий все необходимые операции для выполнения платежа. Ответные данные посылаются через ту же антенну посредством магнитных полей.

Такие карты позволяют увеличить скорость обработки операций и снизить их себестоимость. Из-за отсутствия механического контакта карты и терминала обеспечивается более низкий уровень их физического износа, что повышает надёжность. За счет наличия чипа обеспечивается безопасность операций, характерная для операций по микропроцессорным картам [2].

В таблице 1 приведены характеристики карт по следующим критериям:

- безопасность;
- срок службы;
- скорость выполнения платежа.

Таблица 1. Характеристики разных типов банковских карт

Критерий сравнения	Комментарий
Карты с магнитной полосой	
Безопасность	Не обеспечивают достаточной безопасности: данные могут быть считаны с небольшого расстояния, малый объем памяти не позволяет использовать достаточный набор средств защиты
Срок службы	1-2 года
Скорость выполнения платежа	Средняя
Микропроцессорные карты	
Безопасность	Обеспечивают высокую безопасность: имеют микропроцессор, защищенные разделы памяти и специальное программное обеспечение
Срок службы	3-5 лет
Скорость выполнения платежа	Низкая
Бесконтактные карты	
Безопасность	Обеспечивают высокую безопасность: имеют микропроцессор, защищенные разделы памяти и специальное программное обеспечение
Срок службы	3-5 лет
Скорость выполнения платежа	Высокая

Исходя из всего вышеперечисленного, ясно, что карты с магнитной полосой не удовлетворяют требованиям, предъявляемым к современным банковским картам. Они устарели. Микропроцессорные карты наиболее распространены, так как надежны и безопасны. Однако сейчас банки проявляют всё больший интерес к бесконтактным картам, которые безопасны, надежны и удобны в использовании.

Список литературы

[1] Мошенничество в платежной сфере [Электронный ресурс]: бизнес-энциклопедия/ *Л. Лямин* [и др.]. – Электрон. текстовые данные. – М.: ЦИПСиР, 2016. – 352 с. – Режим доступа: http://www.iprbookshop.ru/41953.html. – ЭБС «IPRbooks»

[2] *Голдовский И.М.* Банковские микропроцессорные карты [Электронный ресурс]/ Голдовский И.М.– Электрон. текстовые данные. – М.: ЦИПСиР, 2010. – 686 с.– Режим доступа: http://www.iprbookshop.ru/9026. – ЭБС «IPRbooks»

[3] *Патрик Гелль* Чип-карты. Устройство и применение в практических конструкциях [Электронный ресурс]/ Патрик Гелль– Электрон. текстовые данные. – М.: ДМК Пресс, 2007. – 176 с.– Режим доступа: http://www.iprbookshop.ru/7723.html. – ЭБС «IPRbooks»

Шестопалов Егор Юрьевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: shestopalovegor@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

УДК 004.056.5

С.С Щеголихин, А.В. Чевычелов

СТЕГАНОГРАФИЯ В СИСТЕМАХ ВИДЕОКОНФЕРЕНЦИЙ

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

Введение

Развитие компьютерной стеганографии связано, в первую очередь, с ростом популярности общения посредством сети интернет. Стеганографические методы призваны скрывать зашифрованные сообщения в “безобидных” данных таким образом, чтобы третье лицо не могло их обнаружить, или даже доказать факт передачи зашифрованных данных, в связи с этим довольно распространено сокрытие информации в цифровых изображениях, аудиофайлах и фоновых шумах телефонных звонков.

Системы видеоконференцсвязи

В видеоконференциях используются алгоритмы сжатия, чтобы обеспечить приемлемое качество видео даже в системах с низкой скоростью передачи данных, таких как ISDN. Обычно алгоритмы сжатия допускают потери данных, что означает, что восстановленное изображение не идентично оригиналу. Видеоконференция, используемая для реализации стенографической системы, представленной в этой статье, работает на стандарте H.261. Это самый распространенный стандарт сжатия в видеоконференциях и рекомендован Международным союзом телекоммуникаций (ITU). Для встраивания данных требуется носитель, который позволяет незаметно модифицировать данные. Типичными примерами такого носителя являются шум и помехи в сигнале. Алгоритмы сжатия применяются для уменьшения шума и помех, таким образом, чем лучше сигнал сжимается, тем сложнее встроить данные.

Дискретное косинусное преобразование

Для реализации стеганографических алгоритмов в системе с видеоконференцией, изображения преобразуются, теряя информацию, не влияющую на восприятие данных человеком. Такое квантование устраняет незначительные части изображения. Для того, чтобы восстановить основные части изображения, преобразование должно быть обратимым. Многие цифровые системы видеоконференцсвязи, например, основанные на стандартах H.261, M-JPEG, MPEG, используют двумерное дискретное косинусное преобразование (DCT), преобразующее изображение 8 × 8 пикселей с 64 значениями яркости F (0,0) ... F (7,7) в 64 значения (так называемые коэффициенты DCT) f (0,0) ... f (7,7) согласно уравнению $f(k,n) = \frac{C(k)}{2}\frac{C(n)}{2}\sum_{x=0}^{7}\sum_{y=0}^{7}F(x,y)\cos\left(\frac{\pi(2x+1)k}{16}\right)cos(\frac{\pi(2y+1)n}{16})$

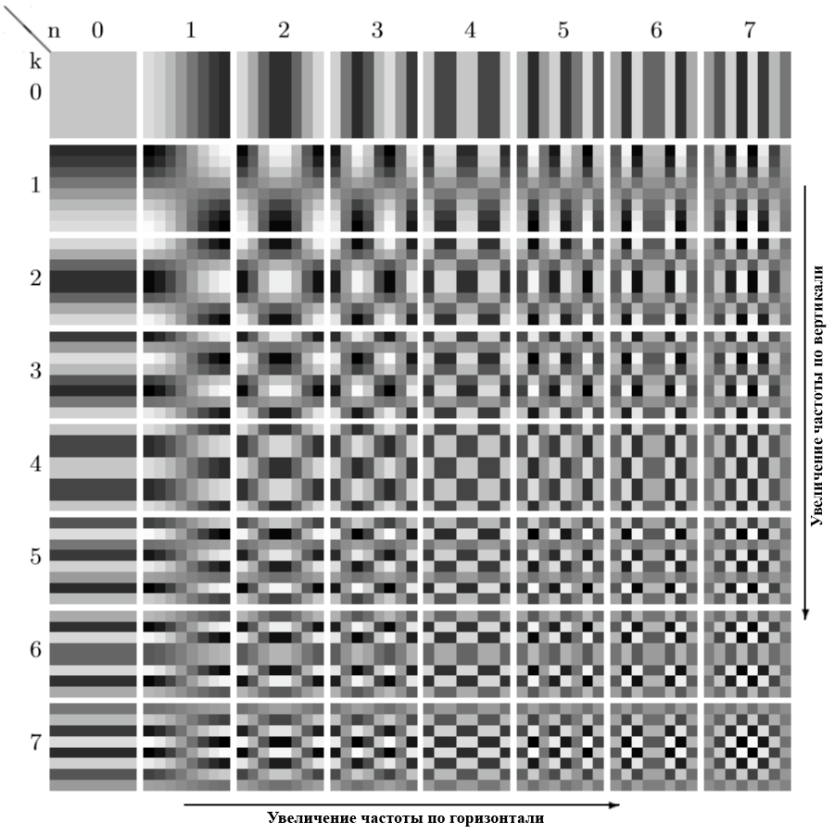

Рисунок1. DCT на основе изображения $B_{k,n}$

Преобразование не приводит к значительным потерям (имеют место только ошибки при округлении). Повторное изменение изображение является результатом обратного преобразования коэффициентов DCT согласно уравнению

$$F(x,y) = \frac{C(k)}{2}\frac{C(n)}{2}\sum_{x=0}^{7}\sum_{y=0}^{7} f(k,n)\cos\left(\frac{\pi(2x+1)k}{16}\right)cos(\frac{\pi(2y+1)n}{16}).$$

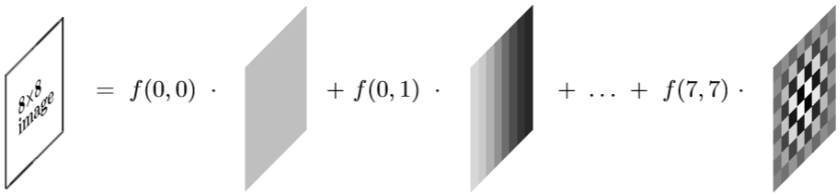

Рисунок 2. Разбиение изображения 8×8 на 64 части.

Его также можно рассматривать как линейную комбинацию коэффициентов DCT: $F(x,y) = \sum_{x=0}^{7}\sum_{y=0}^{7} f(k,n)B_{k,n}(x,y)$, где $B_{k,n}$ – базовые изображения DCT.

Заключение

Благодаря сжатию, используемому в видеоконференциях, наименее значимые биты становятся более важными, поэтому каждый бит сжатого сигнала вносит существенный вклад в изображение. Обнаружение полной

замены этих битов возможно, однако можно изменить только часть носителя, что сделает невозможным обнаружение этих изменений без непосредственного сравнения с оригиналом. Для этого используются специальные функции устройств ввода, таких как камера или сканер. Результат проведения анализа устройств ввода показывает свободные пространства, разрешающие внедренные данные. Стеганографические методы имитируют особенности камеры, поэтому эти изменения не вызывают подозрений у возможного злоумышленника. Данный алгоритм воспроизводит эти эффекты искусственно, и сигнал изменяется необратимо. Прямое сравнение с оригиналом позволяет дифференцировать, но, в силу своего анатомического строения, наблюдатель не может заметить разницы между исходным и модифицированным сигналом. Кроме того, отправитель просто передает измененные кадры. Таким образом, может быть внедрено секретное сообщение. Небольшая горизонтальная дефазировка незаметна.

Список используемой литературы

[1] Быков С.Ф. Алгоритм сжатия JPEG с позиции компьютерной стеганографии. Защита информации. Конфидент 2000 №3.

[2] Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: ”СОЛОН-Пресс”, 2002.

[3] Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. - М.: Кудиц-образ, 2003. - 240 с.

[4] Кнут Д. Искусство программирования. Том 2. Получисленные алгоритмы. - М. Вильямс. - 2003. - 400 с.

[5] Оков И.Н. О требуемой пропускной способности каналов передачи аутентифицированных сообщений в безусловных стойких системах. Проблемы информационной безопасности. Компьютерные системы. 2000. №3(7), с. 78-64.

[6] Тимофеев П.А. Принципы защиты информации в компьютерных системах. Конфидент. Защита информации. 1998, № 3, с. 72.

[7] Anderson R. Stretching the Limits of Steganography. Information Hiding, Springer Lecture Notes in Computer Science. 1996. Vol.1174. P. 39-48.

[8] Collberg C., Thomborson C. Watermarking, Tamper-Proofing, and Obfuscation – Tools for Software Protection. Department of Computer Science University of Arizona, 2000.

Чевычелов Артем Владимирович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: artyomche9@gmail.com

Щеголихин Сергей Станиславович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: sergey.schegolihin@gmail.com

И.А. Мальцев, М.К. Савкин

ТОПОЛОГИЯ СВЁРТОЧНОЙ НЕЙРОННОЙ СЕТИ

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

Свёрточная нейронная сеть – специальная архитектура искусственных нейронных сетей, использующая 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. 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.

Принцип работы. 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. 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.

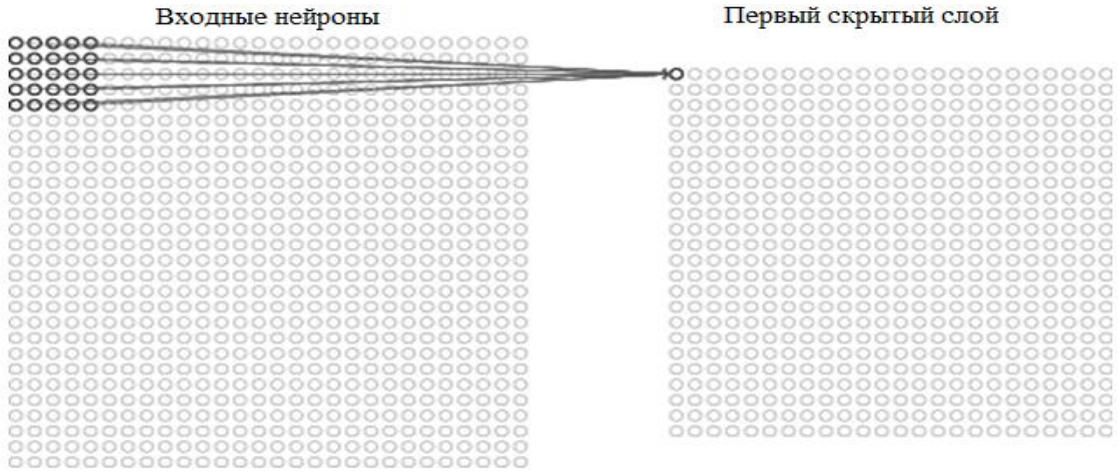

Рис. 1. Свёртка исходного изображения

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

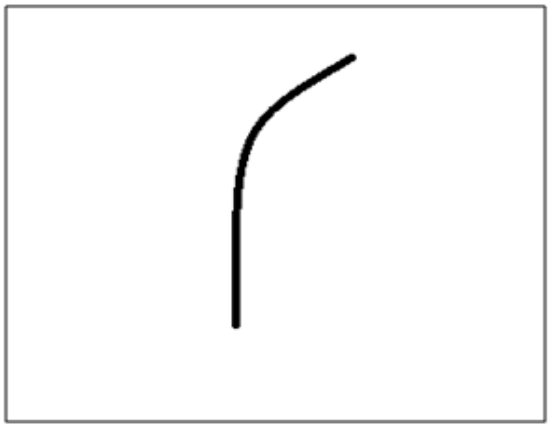

Рис. 2. Ядро свёртки

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).

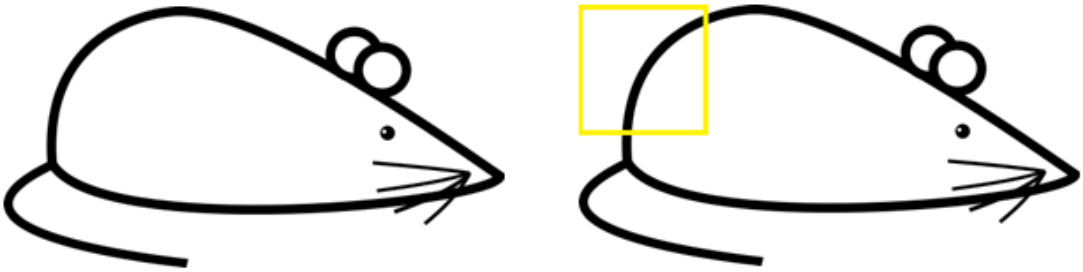

Рис. 3. Исходное изображение

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. 4. 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. 5. 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 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.

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

СЕКЦИЯ 14.

ДИНАМИКА, ПРОЧНОСТЬ И НАДЕЖНОСТЬ ПОДЪЕМНО-ТРАНСПОРТНЫХ, СТРОИТЕЛЬНЫХ, ДОРОЖНЫХ МАШИН И ОБОРУДОВАНИЯ

А.С. Болтнева, С.Л. Заярный

АНАЛИЗ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ТЕОРИИ ГРАФОВ К ИССЛЕДОВАНИЯМ СТРУКТУРЫ И ПОКАЗАТЕЛЕЙ ЭКСПЛУАТАЦИОННО-ТЕХНИЧЕСКИХ ХАРАКТЕРИСТИК МЕТАЛЛОКОНСТРУКЦИИ ПУТЕВОЙ МАШИНЫ

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

При незначительной начальной информации о структуре системы, когда учитываются лишь наличие и направление связи, удобно использовать аппарат теории графов.

Теория графов - раздел математики, который исследует свойство разных геометрических схем (графов – абстрактная модель исследуемой структуры), образованных множеством точек и соединительных линий. При структурном анализе систем элементам ставят в соответствие вершины графа, а связям - ребра (вершинный граф).

Проведем структурный анализ металлоконструкции рамы выправочно-подбивочно-рихтовочной машины ВПРС 600 представленной на рис. 1. Обозначим элементы рамы вершинами графа – позиции: 1, 2, 3, а связи между элементами рамы (сварочное и болтовое соединения) – ребрами графа [1].

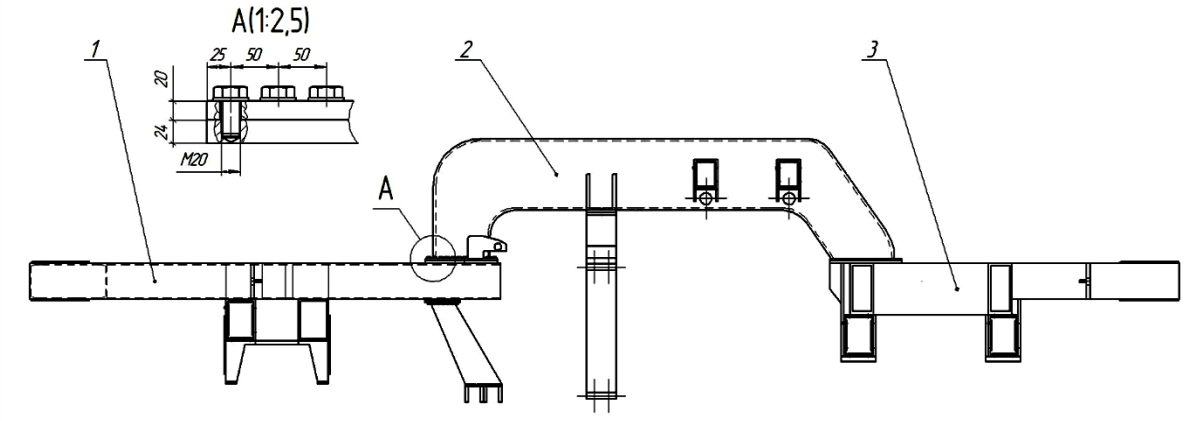

Рис.1. Рама выправочно-подбивочно-рихтовочной машины ВПРС 600
1 – левая секция; 2 – центральная секция; 3 – правая секция

Под сложностью структуры будем понимается большой набор элементов структуры и нетривиальность связей между ними. Сложные структуры обладают особым свойством иерархичности, т.е. элементы (или связи между элементами) структуры упорядочены по времени их появления. В начальный момент структура представляет собой “несложный” граф. В следующий момент времени появляются элементы, имеющие связи, как

между собой, так и с элементами структуры, возникшими в предыдущий момент времени, причем количество новых элементов и связей оптимизировано в зависимости от среды, где строится структура – условия эксплуатации. Рост структуры продолжается до тех пор, пока этого требует среда.

Расчет показателей эксплуатационно-технические характеристик (ЭТХ) системы и, в частности, ее безотказности или готовности, существенно зависит, от описывающей систему модели [2]. Такая модель может быть представлена как сеть, т. е. граф, ребрами которого являются элементы системы, а вершинами – места соединения элементов (рис. 2.). Вероятности безотказной работы обозначаются как P_{ij}, где i, j – номера соединенных соответствующим элементу ребром вершин. Они равны вероятности безотказной работы элементов, если элементы системы невосстанавливаемые. Примерами таких сетей могут служить металлоконструкции инженерных сооружений, их разъемные и неразъемные соединения, разъемные и неразъемные соединения тягового привода машин и т. п [3].

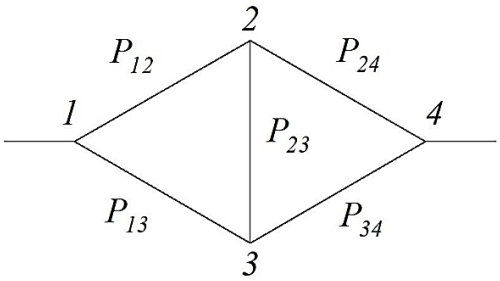

Рис. 2. Модель структурно сложной системы надежности

Использование для формализации описания объекта проектирования графа определенного вида – неориентированного и ориентированного, гипер- и ультраграфа позволяет:

- разрабатывать модели, адекватные в смысле полноты и правильности отображения информации, которая требуется для решения задачи;
- получать формальную постановку задач анализа и синтеза объектов проектирования, ориентирующую исследователя на выбор операций и метода преобразования модели исходного описания в модель результата.

Для расчета показателей ЭТХ структурно сложных систем используются методы прямого перебора и разложения относительно особого элемента

Метод перебора состояний – универсальный метод анализа систем. При пользовании им полагают, что, отказы отдельных элементов не улучшают состояние системы.

Если критерий отказа системы определен, то все множество состояний системы и ее модели делят на два подмножества: работоспособных со-

стояний *R* и неработоспособных состояний *G*. Для каждого из работоспособных состояний определяют вероятность безотказной работы или коэффициент готовности

$$P_{сист} = \sum_{i \in R} P_i, \qquad (1)$$

где P_i – вероятность пребывания системы в *i-м* работоспособном состоянии. Для перебора состояний системы строят таблицу ее возможных состояний.

Метод разложения относительно особого элемента, по сравнению с методом перебора состояний, позволяет существенно сократить число вычислительных операций. Его суть заключается в том, что сетевая модель (граф) системы сводится к параллельно-последовательной структуре, для чего в процессе анализа выбирают один, так называемый «особый» элемент, относительно которого делают два предположения:

1. элемент отказал и соответствующее ребро в графе отсутствует;

2. элемент безотказен с вероятностью, равной единице, и вершины, соединенные этим ребром, стягиваются в одну точку, т. е. соединяются между собой перемычкой без элемента.

Метод основан на известной в математической логике теореме о разложении функции логики по любому аргументу. Применительно к задачам анализа надежности двухполюсных систем эта теорема выглядит следующим образом:

$$P_{сист} = P_{ij} P_{P_{ij}=1} + Q_{ij} P_{P_{ij}=0}, \qquad (2)$$

где $P_{сист}$ – вероятность того, что система находится в работоспособном состоянии; P_{ij}, Q_{ij} – соответственно вероятность безотказной работы и вероятность отказа особого элемента, моделируемого ребром ij; $P_{ij}=1$ – вероятность связности графа при стягивании вершин i и j в одну вершину; $P_{ij}=0$ – вероятность связности графа с отсутствующим ребром между вершинами i и j.

Рассмотренные методы расчета показателей ЭТХ структурно сложных систем могут быть применены далеко не всегда. Поэтому на практике иногда пользуются методами интервального оценивания показателей ЭТХ (надежности, готовности), т. е. методами определения верхней и нижней границ вероятности пребывания системы в работоспособном состоянии.

Готовность ЭТХ выступает в виде целевой функции или ограничения при решении оптимизационных эксплуатационных задач. Она может описываться моделями в виде графов перехода систем из состояния в состояние.

Одним из наиболее широко распространенных методов оценки границ работоспособного состояния структурно сложных систем является метод минимальных путей и минимальных сечений.

Минимальным путем B называют множество ребер графа, обеспечивающее его связность и подобранное таким образом, что при удалении любого ребра из этого множества связность графа нарушается (если все остальные ребра графа, не принадлежащие данному множеству, уже удалены).

Минимальным сечением C называют множество ребер графа, одновременное удаление которых приводит к нарушению связности. Восстановление любого одного ребра минимального сечения приводит к восстановлению связности.

Очевидно, что в модели любой системы можно найти несколько *(M)* минимальных путей и некоторое число (*S)* минимальных сечений. И если существует хотя бы один минимальный путь или хотя бы по одному ребру каждого минимального сечения, то модель системы – граф – является связным, а сама система – работоспособной.

Техническая система (ТС) многократного применения, к которым можно отнести металлоконструкцию крана, работает сеансами, между которыми она может находиться в состоянии ожидания применения.

Переход из режима ожидания в режим непосредственного использования осуществляется или непосредственно по команде, поступление которой следует считать равновероятным в любой момент интервала времени эксплуатации системы или в соответствии с планом применения ТС в заранее запланированный момент времени.

Параметры потоков переходов из состояния в состояние проставлены на соответствующих ребрах графа на рис. 3. В этой модели оперативная готовность ТС будет определяться вероятностью ее пребывания в первом состоянии P_1 – состоянии исправности и выполнения задачи. Готовность можно характеризовать вероятностью P_2 пребывания во втором состоянии, когда ТС исправна и готова к выполнению задачи.

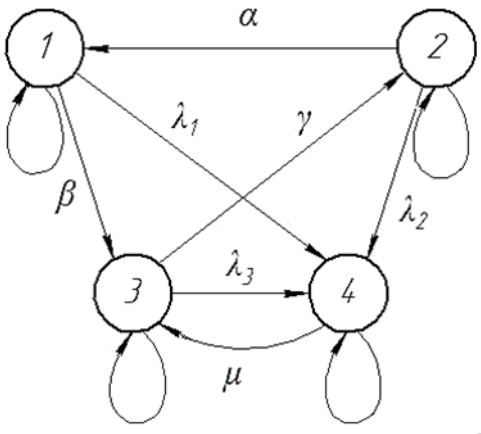

Рис. 3. Граф перехода из состояния в состояние ТС многократного применения

Для моделей, описываемых дифференциальными уравнениями и подобными им, существует стационарный режим, для которого при $t \to \infty$:

$$\frac{dP_i}{dt} = 0; \;\; P_i(t) = P_i = const. \qquad (3)$$

В этом случае система дифференциальных уравнений переходит в систему алгебраических уравнений для стационарного режима функционирования марковской модели. Решение уравнений позволяют исследовать влияние соотношений параметров потоков переходов на готовность и оперативную готовность такой системы и определить пути повышения указанных показателей.

Рассмотренные методы расчета и анализа эксплуатационно-технических характеристик металлоконструкции путевой машины, с использованием теории графов, показывают их эффективность при анализе сложных технических систем, и позволяют, повышая уровень детализации определять точные взаимосвязи между элементами.

Список литературы

[1] Путевые машины: Учебник для вузов ж.д. транспорта/Соломонов С.А., Попович М.В. Бугаенко В.М. и др. Под ред. С.А. Соломонова. — М.: Желдориздат, 2000. – 756 с.

[2] Обеспечение надежности сложных технических систем / Дорохов А.Н., Керножицкий В.А., Миронов А.Н., Шестопалов О.Л. – СПб.: Лань. – 2011. – 352 с.

[3] Овчинников В. А. Графы в задачах анализа и синтеза структур сложных систем. / В. А.Овчинников. – М.: Изд-во МГТУ им. Н. Э. Баумана, 2014. – 423 с. Ил.

Болтнева Анна Сергеевна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: annrash1994@yandex.ru

Заярный Сергей Леонидович – канд. техн. наук, доцент кафедры "Детали машин и подъемно-транспортное оборудование" КФ МГТУ им. Н.Э. Баумана. E-mail: texnakon@yandex.ru

М.А. Качан, Н.М. Борискина, Е.А. Витушкина

АНАЛИЗ ТРАНСПОРТИРОВАНИЯ МАТЕРИАЛЬНОЙ ТОЧКИ В ВИБРАЦИОННЫХ КОНВЕЙЕРАХ

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

В предыдущих исследованиях рассмотрены условия транспортирования частиц в качающихся конвейерах с учетом дополнительных силовых факторов, т.е. воздействие воздушных потоков, направленных вдоль и перпендикулярно вибрирующей плоскости. В настоящей работе дополнительное силовое поле образуется за счет аэродинамических сил F_x и F_y, направление которых совпадает с направлением скоростей воздушных потоков V_x и V_y. Дополнительное силовое поле обеспечивает осуществление разделения частиц различной плотности, размеров с транспортированием разделенных смесей в противоположные направления.

Для дальнейшего рассмотрения действия сил введем подвижную систему координат XOY, жестко связанную с колеблющейся плоскостью и систему неподвижных осей координат ξ, O_1, η, параллельных подвижным осям. Проекции ξ и η перемещения плоскости на оси неподвижной системы координат будут:

$$\xi = A\cos\beta\sin\omega t$$

$$\eta = A\sin\beta\sin\omega t$$

где A – амплитуда, ω – частота колебаний плоскости, β – угол наклона вибрации. (Рис. 1).

В работах [1], [3] рассмотрено движение по вибрирующей плоскости материальной точки. Опишем движение материальной частицы с учетом влияния сил сопротивления F_x^c и F_y^c воздушного потока, в котором она перемещается с собственной скоростью *V*. Поведение частицы определяется системой воздействующих на нее сил: сила тяжести, сила сухого трения *F*, нормальная реакция *N*, силы сопротивления от действия вертикального и горизонтального потоков F_x и F_y и силы сопротивления F_x^c и F_y^c, пропорциональные квадрату собственной скорости *V*. В настоящей работе рассмотрено движение частицы по вибрирующей поверхности с учетом сил сопротивления F_x^c и F_y^c, определяемых по формулам [2]:

$$F_x^c = C_x(R_E)\frac{\pi d^2}{4}\rho\cdot\frac{\xi^2}{2},\ F_y^c = C_y(R_E)\frac{\pi d^2}{4}\rho\cdot\frac{\eta^2}{2},$$

где ρ - плотность воздуха, d – диаметр частицы, C_x, C_y - коэффициенты аэродинамического сопротивления, являющиеся функцией числа Рейнольдса. Число Рейнольдса определяем по формуле:

$$R_E = \frac{V \cdot d}{\nu},$$

где ν - кинематическая вязкость воздуха.

Силы сопротивления зависят от формы и размеров тела, плотности среды и пропорциональны квадрату скорости. Коэффициент сопротивления, в свою очередь, является практической функцией, представленной в виде известной кривой Рейлея [2]. При движении частицы в воздушном потоке с переменной скоростью, что имеет место при колебательном процессе, коэффициент сопротивления будет переменной величиной. Точное аналитическое выражение зависимости коэффициента от параметров движения, в данном исследовании не представляется возможным. При малых углах на основе гипотезы стационарности [1], [2] коэффициент сопротивления определяют по наибольшей скорости колебательного процесса:

$$V_{\max} = A\omega.$$

На основании гипотезы стационарности, коэффициенты сопротивления C_x и C_y в формулах F_x^c и F_y^c - будем считать постоянными, определяемыми по величине проекции максимальной скорости $A\omega$. При таких предположениях дифференциальные уравнения движения частицы в абсолютных координатах с учетом силы тяжести, сил сопротивления и силы инерции ($m\ddot{\xi}$, $m\ddot{\eta}$) имеют вид:

$$\begin{cases} m\ddot{\xi} = -\text{sign}(\dot{\xi})F_x^c - F_x - mg\sin\alpha \\ m\ddot{\eta} = -\text{sign}(\dot{\eta})F_y^c + F_y - mg\cos\alpha \end{cases}, \quad (1)$$

где α – угол наклона плоскости:

Уравнение (1) будем интегрировать отдельно для каждого участка траектории. Разделив уравнение (1) на массу, можно записать для участков 0-1 или 0-3.

$$\begin{cases} \ddot{\xi} = -\dfrac{F_x^c}{m} - g\sin\alpha - \dfrac{F_x}{m} \\ \ddot{\eta} = -\dfrac{F_y^c}{m} - g\cos\alpha + \dfrac{F_y}{m} \end{cases}, \quad (2)$$

Приведем уравнение (2) к виду, удобному для интегрирования:

$$\frac{d\dot{\xi}}{dt} = -a_1^2\dot{\xi}^2 - b_1^2, \quad (3)$$

$$\frac{d\dot{\eta}}{dt} = -a_2^2\dot{\eta}^2 - b_2^2, \quad (4)$$

где

$$a_1^2 = \frac{3C_x(\dot{\xi})\rho}{4\rho_ч d_ч}, \tag{5}$$

$$a_2^2 = \frac{3C_x(\dot{\eta})\rho}{4\rho_ч d_ч}, \tag{6}$$

$$b_1^2 = g\sin\alpha + \frac{3C_x\rho v_x^2}{4\rho_ч d_ч}, \tag{7}$$

$$b_2^2 = g\cos\alpha - \frac{3C_x\rho v_y^2}{4\rho_ч d_ч}, \tag{8}$$

Интегрируя эти уравнения и решая, относительно скоростей, для определения постоянной интегрирования используем начальные условия при t=0; $\dot{\xi} = \dot{\xi}_0$; $\dot{\eta} = \dot{\eta}_0$.

Обозначим φ_1 и φ_2 :

$$\varphi_1 = \operatorname{arctg}\frac{a_1}{b_1}\cdot\dot{\xi}_0;$$

$$\varphi_2 = \operatorname{arctg}\frac{a_2}{b_2}\cdot\dot{\eta}_0$$

Имеем:

$$\dot{\xi} = \frac{b_1}{a}\operatorname{tg}(\varphi_1 - a_1 b_1 t), \tag{9}.$$

$$\dot{\eta} = \frac{b_2}{a_2}\operatorname{tg}(\varphi_2 - a_2 b_2 t), \tag{10}$$

Так как отрицательным значениям скорости соответствует другой участок траектории. На участке 0-1 конец интервала наступает при $\dot{\eta} = 0$ (Рис. 1), в этом случае из уравнения (10) можно найти время перехода t_1:

$$\frac{b_2}{a_2}\operatorname{tg}(\varphi_2 - a_2 b_2 t_1) = 0.$$

Так как необходимо знать ближайший корень, то для конца участка 0-1 можно записать

$$t_1 = \frac{\operatorname{arctg}\frac{a_2}{b_2}\cdot\dot{\eta}_0}{a_2 b_2} = \frac{\varphi_2}{a_2 b_2}, \tag{11}$$

Проведя аналогичные рассуждения для конца участка 0-3, найдем время перехода к участку 3-4, исходя из того, что конец интервала наступает при $\dot{\xi} = 0$

$$t_2 = \frac{\operatorname{arctg}\frac{a_1}{b_1}\cdot\dot{\xi}_0}{a_1 b_1} = \frac{\varphi_1}{a_1 b_1}, \tag{12}$$

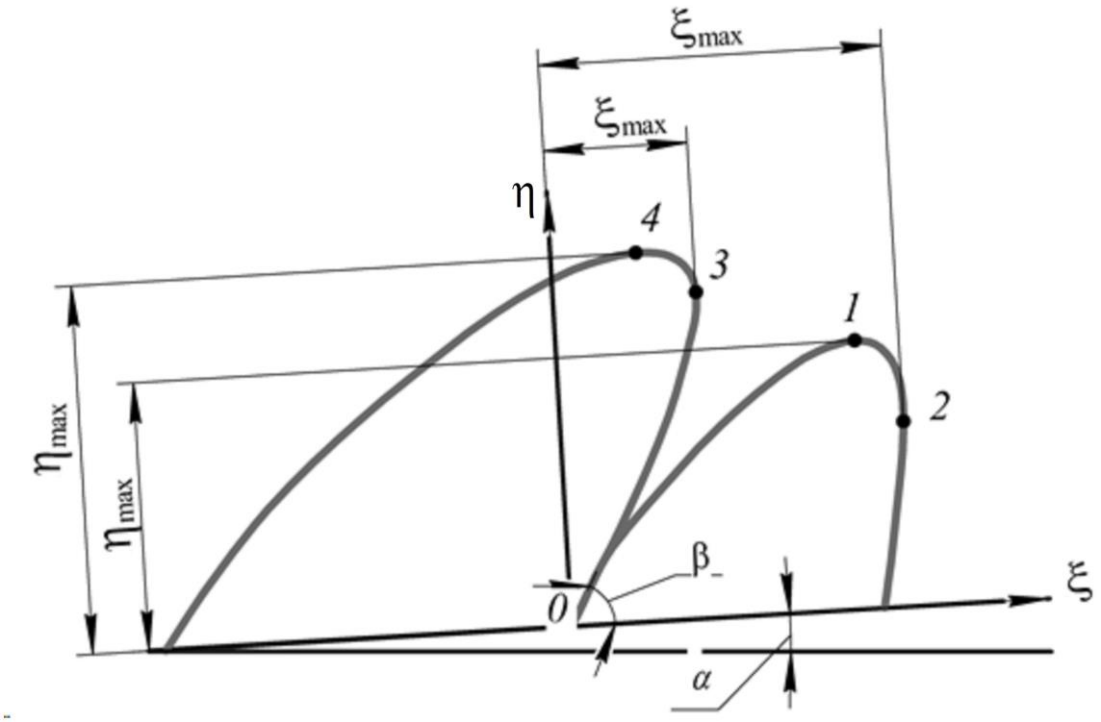

Рис.1. Траектории движения частиц

Интегрируя уравнения (9) и (10) найдем уравнения траектории движения на участке 0-1 и 0-3.

Постоянную интегрирования найдем из следующих граничных условий, т.е. начальных t=0; $\xi = 0$.

$$\xi = \frac{1}{a_1^2} \ln \frac{\cos(\varphi_1 - t a_1 b_1)}{\cos \varphi_1}, \tag{13}$$

$$\eta = \frac{1}{a_2^2} \ln \frac{\cos(\varphi_2 - a_2 b_2 t)}{\cos \varphi_2}. \tag{14}$$

Из уравнения (14) можно найти максимальную координату движения частицы по вертикали η_{max} с учетом t_1 из (11) для участка 0-1.

$$\eta_{max} = -\frac{1}{a_2^2} \ln \cos(\operatorname{arctg} \frac{a_2}{b_2} \dot{\eta}_0)$$

Для участка 0-3 с учетом t_2 (12) максимальное положительное значение координаты движения частицы по горизонтали найдем из (13):

$$\xi_{max} = -\frac{1}{a_1^2} \ln \cos \varphi_1$$

Дифференциальные уравнения движения частицы на участке 1-2 имеют следующий вид:

$$m\ddot{\xi} = -F_x^c - F_x - mg \sin \alpha, \tag{15}$$

$$m\ddot{\eta} = -F_y^c + F_y - mg \cos \alpha \tag{16}$$

Проводя аналогичные преобразования, приводим уравнения (15), к виду, удобному для интегрирования и получим уравнение аналогично уравнению (1). Поэтому уравнение движения частицы (13) будет справедливым на участке 1-2.

Для вертикальной составляющей, уравнение (16) приводим к виду, удобному для интегрирования и окончательно получим траекторию перемещения в следующем виде:

$$\xi = \frac{1}{a_1^2} \ln \frac{\cos(\varphi_1 - t a_1 b_1)}{\cos \varphi_1}, \tag{17}$$

$$\eta = \frac{1}{a_2^2} \ln \frac{1}{\mathrm{ch}[(t - t_1) a_2 b_2] \cos \varphi_2}, \tag{18}$$

Уравнения (17) и (18) справедливы для участка 1-2, конец которого наступает при $\dot{\xi} = 0$.

Проводя на участке 3-4 аналогичные рассуждения, получим уравнение движения материальной точки. Траектория движения частицы с учетом сил сопротивления, пропорциональных квадрату собственной скорости движения частицы показаны на рис. 1.

Проведенные исследования подтверждают предположения о существенном влиянии дополнительного силового поля на движение частиц.

В работе создана математическая модель, описывающая процесс движения частицы на наклонной плоскости под воздействием сложной системы нагружения.

Список литературы

[1] Блехман И.И., Джанелидзе Г.Ю. Вибрационное перемещение. – М.: Изд-во Наука, 1964. –412 с.

[2] Горлин С.Н. Экспериментальная аэромеханика. – М: Изд-во Высшая школа 1970. – 423с.

[3] Шубин А.А., Борискина З.М., Барышникова О.О. Математическое моделирование перемещений в качающихся конвейерах. Известия Тульского государственного университета. \Технические науки. Вып. 7. Ч.2. Тула: Изд-во ТулГУ. 2015. С.128-136.

Качан Максим Аркадьевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: red-blade@yandex.ru

Витушкина Евгения Алексеевна – ст. преп. КФ МГТУ им. Н.Э. Баумана. E-mail: k3kf@yandex.ru

Борискина Надежда Михайловна – канд. техн. наук, доцент кафедры "Детали машин и подъемно-транспортное оборудование" КФ МГТУ им. Н.Э. Баумана. E-mail: k3kf@yandex.ru

С.Л. Заярный, А.А. Голосов

АСПЕКТЫ ПРИМЕНЕНИЯ НЕКОТОРЫХ КОМПОЗИТНЫХ МАТЕРИАЛОВ В ИНЖЕНЕРНЫХ СООРУЖЕНИЯХ

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

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. Их прочность, при этом 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 стержней с тонкостенным сечением [2].

Рассмотрим 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)

Технология производства. Рассмотрение технологии производства и технико-экономических показателей 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] URL: http://www.meto.ru/firma.htm (31.03.2017).

[4] URL: http://www.eurograte.ru (31.03.2017).

Заярный Сергей Леонидович – канд. техн. наук, доцент кафедры "Детали машин и подъемно-транспортное оборудование" 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

М.В. Потапов, А.А. Шубин

ВАРИАНТЫ МОДЕРНИЗАНИЦИИ МОБИЛЬНОЙ ЖЕЛЕЗНОДОРОЖНОЙ ТЕЛЕЖКИ

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

Текущее содержание и ремонт пути являются обязательным условием эффективной работы железнодорожного транспорта. Текущее содержание пути осуществляется круглогодично и на всей сети железных дорог, включая участки, находящиеся в ремонте. Основной объем работ по содержанию пути выполняют с использованием разных механизированных путевых инструментов, которые облегчают труд путейцев и многократно увеличивают его производительность. Одной из таких работ является уплотнение балласта под шпалами, которая выполняется электрошпалоподбойкой [1].

Электрошпалоподбойка представляет собой вибратор ненаправленного действия. Корпус шпалоподбойки приводится в состояние вынужденных колебаний с частотой, соответствующей частоте вращения дебаланса. Таким образом, вращательное движение превращается в колебательное. Колебания корпуса шпалоподбойки сообщаются рабочему подбивочному полотну, которое в свою очередь передает их балласту. В месте подбивки на уплотняемый балласт кроме вибраций действует периодические ударные импульсы с частотой, кратной частоте вращения дебаланса. Вибрация корпуса шпалоподбойки передается также на ручки, а, следовательно, и монтеру пути. Учитывая, что вес электрошпалоподбойки 19 кг и монтеру приходится поднимать и опускать ее в процессе работы не менее 5 раз в минуту, а также переносить ее на значительные расстояния, можно сделать вывод: данный инструмент наименее технологичен с точки зрения воздействия на рабочего. Работа подбойщика очень трудоемка, не мобильна и не эргономична, что обусловлено многими факторами:

- Необходимость переноса инструмента и питающей его станции на большие расстояния;
- Создания больших усилий на рукояти шпалоподбойки для внедрения внутрь балласта подбивочного полотна;
- Вибрация ручек шпалоподбойки, вызывающая различные болезни у монтера.

В связи с этим актуальным является проведение работ, направленных на облегчение и повышение производительности работы монтера пути, которую можно разделить на следующие этапы:

- Повышение мобильности;
- Повышение производительности;
- Уменьшение физических нагрузок;
- Уменьшение вибраций на ручках.

В настоящей работе рассматриваются пути снижения физических нагрузок, которые могут быть обеспечены за счет снижения массы инструмента или применения дополнительных механизмов. Снижение массы электрошпалоподбойки имеет неоднозначный результат – с одной стороны облегчает работу при подъеме инструмента, но при заглублении придется прикладывать большее усилие. Конструктивные особенности инструмента и его работы не позволяют снизить его массу без снижения его надежности. Снижение физических нагрузок за счет использования дополнительных механизмов рассмотрено в работе [2]. Предложена конструкция несамоходной тележки (рис. 1), которая состоит из двух рам 1 с катками 2, соединенных балкой 3, установленных на опорах 4, на которой с помощью ползуна 5 закреплена неподвижная стойка. На неподвижной стойке установлена поворотная опора 6, к которой шарнирно крепятся тяги 7. К тягам через карданы крепится плита 8, служащая для установки шпалоподбойки. Вес шпалоподбойки компенсируется пружиной 9 [2].

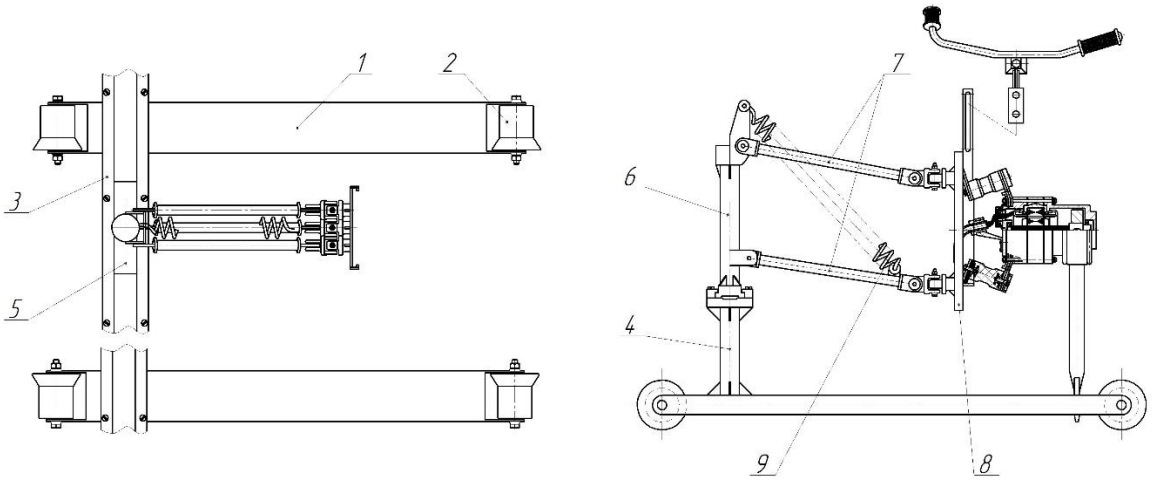

Рис. 1 Железнодорожная тележка для механизированного путевого инструмента

Предложенная конструкция тележки позволяет повысить эффективность работ, выполняемых электрошпалоподбойкой.

Некоторые элементы конструкции тележки требуют доработки с целью повышения их надежности, в первую очередь это относится к узлу поперечного перемещения основной опоры.

Механизм передвижения опоры 6 представляет собой ползун 5 и элемент балки 3, которые образуют между собой открытую пару трения скольжения. В связи с этим при работе тележки поверхности трения не защищены от попадания пыли и грязи, что приведет к увеличению коэффициента трения, повышенному износу трущихся пар, заклиниванию механизма передвижения и, как следствие, увеличению силы прикладываемой монтером при передвижении опоры.

В связи с вышесказанным в качестве механизма передвижения предлагается использовать каретки, в которых подвижные элементы образуют пары трения качения (рис. 2).

Рис. 2 Каретки:
а – роликовая с ребордами; б – шариковая; в – роликовая

В каретке, изображенной на рис. 2б в качестве тел качения используют шарики, поэтому в ней возникают наименьшие силы трения. Недостатком этого варианта является возможность попадания, в полевых условиях, грязи и влаги в подвижный узел, что может привести к увеличению сил сопротивления движению, вплоть до заклинивания.

В конструкциях, приведенных на рис. 2а и 2в каретка перемещается и удерживается на направляющих с помощью роликов, при этом в конструкции рис. 2а ролики имеют реборды, исключающие, размыкание узла при воздействии опрокидывающего момента. Это позволяет сделать вывод, что применение данной конструкции каретки наиболее предпочтительно в узле поперечного передвижения железнодорожной тележки.

Шарнирно-рычажная система, состоящая из тяг, компенсирующей пружины и плиты, служит для удержания шпалоподбойки и подводу ее к месту работы. Тяги образуют параллелограммный механизм (рис. 1), поэтому перемещение подбойки в вертикальной плоскости плоскопараллельное, то есть монтер не имеет возможности изменить угол ее наклона. Для обеспечения этой возможности предлагается уйти от параллелограммного механизма, и использовать вместо него механизм, изображенный на рис. 3.

Применение мобильной железнодорожной тележки позволит существенно снизить нагрузки, прикладываемые монтером пути. Предложенное усовершенствование конструкции отдельных узлов тележки позволит повысить ее надежность и снизить усилия необходимые для ее эксплуатации.

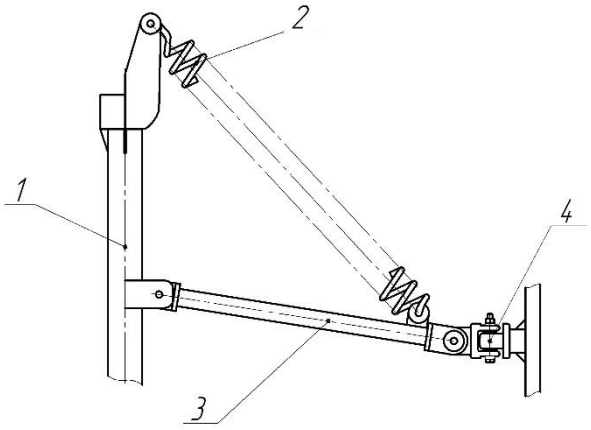

Рис. 3 Шарнирно-рычажная система:
1 – поворотная опора; 2 – компенсирующая пружина; 3 – тяга; 4 – кардан

Список литературы

[1] Сухих Р. Д., Бугаенко В. М., Огарь Ю. С., Ермаков В. Д., Пиковский И. М., Пронченко А. В. Путевые механизмы и инструменты. Сухих Р. Д; под общей ред. Р. Д. Сухих. – М.: УМК МПС, 2002, 428 с.

[2] Шубин А.А., Витчук П.В., Фадеев В.В. Повышение эффективности работы вибрационной шпалоподбойки. *Научный альманах*, 2015, №11-3, с. 462-466.

Потапов Михаил Витальевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: michail.potapov109@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

Я.В. Губанов, Д.В. Демьянов, С.Л. Заярный

ИССЛЕДОВАНИЕ КОНТАКТНЫХ ВЗАИМОДЕЙСТВИЙ В СТЫКЕ СОЕДИНЕНИЙ ЭЛЕМЕНТОВ МЕТАЛЛОКОНСТРУКЦИЙ ПРИ ИХ СТАТИЧЕСКОМ НАГРУЖЕНИИ

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

Фрикционные соединения на высокопрочных болтах (рис.1) по характеру передачи усилий принципиально отличаются от других типов разъемных и неразъемных соединений. Усилия в них передаются только силами трения, возникающими на контактных поверхностях вследствие большого предварительного натяжения болтов. В исходном состоянии (без нагрузки) поверхности соединяемых деталей находятся в контакте. После приложения внешней рабочей нагрузки на соединение, в том числе и предварительного натяжения высокопрочных болтов, на отдельных участках контактных поверхностей происходит частичный сдвиг деталей. Кроме того, местами возможен отрыв соединяемых элементов друг от друга, т. е. выход из контакта.

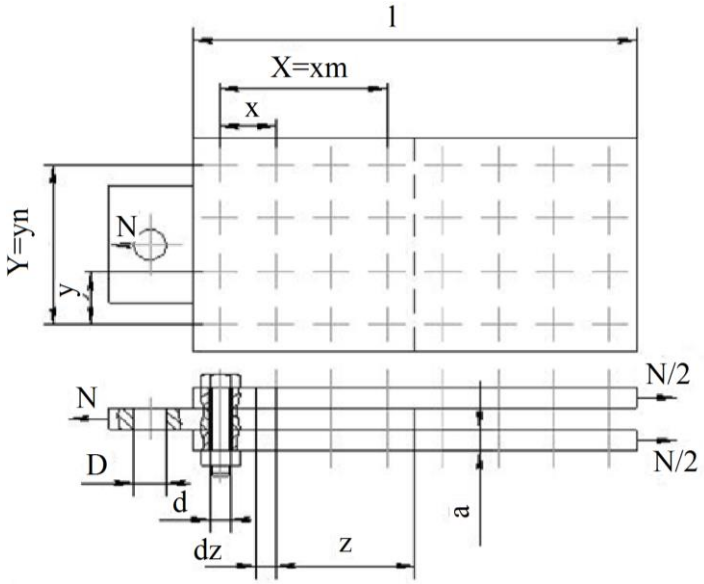

Рис. 1 Схема нагружения болтовых соединений с зазором сдвигающими силами

Работа таких соединений под нагрузкой характеризуется изменением предварительного натяжения высокопрочных болтов. В зависимости от напряженно-деформированного состояния натяжение болтов может либо увеличиваться, либо уменьшаться. Это происходит за счет поперечных деформаций пакета (эффекта Пуассона). Иначе говоря, при растяжении толщина соединяемы элементов уменьшается, что вызывает ослабление пред-

варительного натяжения болтов, и как следствие, уменьшение сил трения. При сжатии имеет место обратное явление.

Процесс передачи усилий в соединении деталей может протекать при различных условиях деформирования стыка [1], [2]. Оценка работы соединений с учетом характера перемещений в стыке имеет важное значение для изделий машиностроения, в которых под действием динамических знакопеременных нагрузок возможно развитие на контактируемых поверхностях явлений фреттинг-коррозии.

Несущая способность соединений под действием переменных нагрузок определяется условиями его контактных взаимодействий. При этом контактный слой (КС), рассматривается как третье тело, обладающее особыми механическими свойствами [1]. Свойства контактного слоя в значительной степени определяется характеристиками сопрягаемой поверхности, важнейшими из которых является шероховатость. С целью получения объективных характеристик нами были проведены измерения шероховатости, результаты которых представлены на рис. 2.

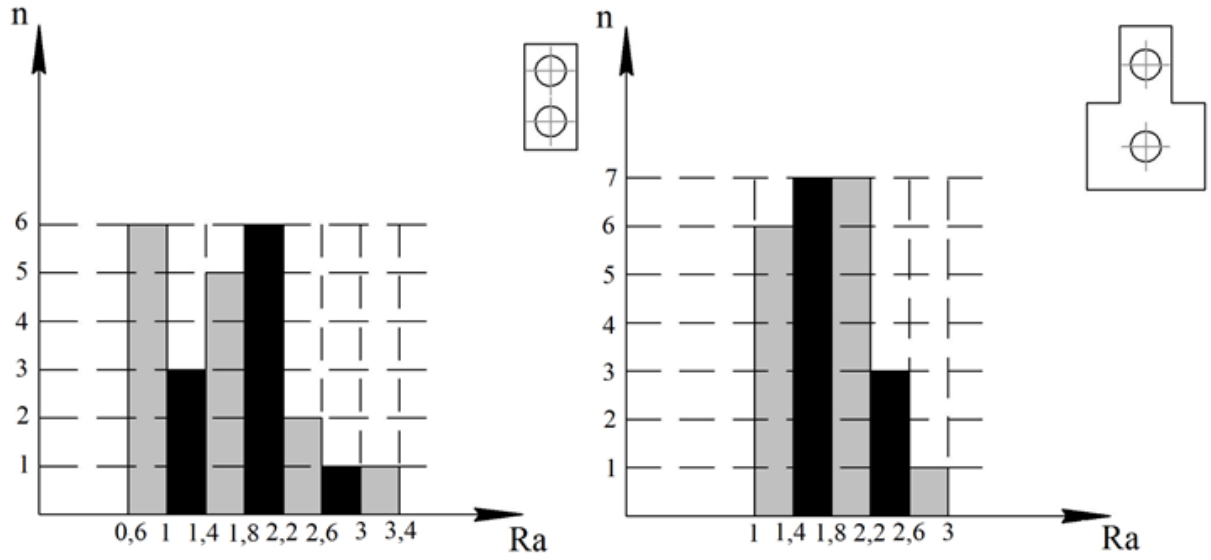

Рис. 2 Гистограммы распределения значений шероховатости образцов

Перед тем как приступить к созданию расчетных моделей приведем краткое описание эксперимента и его результатов. Испытания статической нагрузкой предполагается проводить на образцах, представляющих собой стыки двух листов, перекрытых парными накладками с болтами из стали 40Х (см. рис. 3). Образцы отличаются друг от друга расположением болтов в соединении и степенью ослабления поперечного сечения стыкуемых листов по первому ряду высокопрочных болтов.

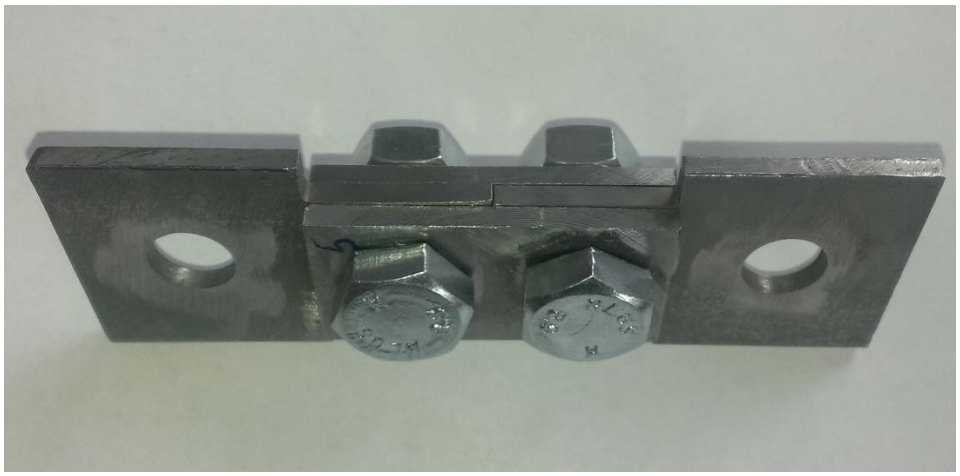

Рис. 3 Испытательный образец

Испытания проводятся на разрывной машине МИ40КУ (рис. 4), которая используется совместно с компьютером и обеспечивает построение диаграмм зависимости силы от деформации на дисплее.

Рис. 4 Стенд МИ40КУ с испытательным образцом

Площадь поперечного сечения листов брутто у всех образцов одинаковая. Контактные поверхности обработаны металлическим фрезерованием. Предварительное натяжение болтов определяется их контролируемой затяжкой.

В представленных материалах рассмотрена сущность проблемы, связанная с определением контактных взаимодействий в стыке соединений элементов металлоконструкций при их статическом нагружении. Проведена оценка шероховатости сопрягаемых поверхностей изготовленных образцов.

Список литературы

[1] Левина З. М., Решетов Д.Н. Контактная жесткость машин. – М: Машиностроение, 1971.

[2] Крагельский И.В. Трение и износ. – М: Машиностроение,1978. – 480с.

Губанов Яков Викторович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: klg.vision@gmail.com

Демьянов Дмитрий Владимирович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: finesven103@gmail.com

Заярный Сергей Леонидович – канд. техн. наук, доцент кафедры "Детали машин и подъемно-транспортное оборудование" КФ МГТУ им. Н.Э. Баумана. E-mail: texnakon@yandex.ru

Н.И. Байко, С.Л. Заярный

ИССЛЕДОВАНИЕ ПОКАЗАТЕЛЕЙ ГОТОВНОСТИ СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМ НА ПРИМЕРЕ ПУТЕВОЙ МАШИНЫ.

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

Готовность – это свойство объекта выполнять заданные функции в любой момент времени. Если у объекта два состояния, работоспособное и неработоспособное, готовность есть свойство объекта быть работоспособным в произвольный момент времени или наработки. В этом случае готовность определяется безотказностью и ремонтопригодностью объекта. Если объект является обслуживаемым, то готовность его определяется безотказностью и эксплуатационной технологичностью.

Коэффициент готовности $K_Г(t)$ – это вероятность того, что техническая система окажется в работоспособном состоянии в произвольный момент времени t, кроме планируемых периодов, в течение которых ее применение по назначению не предусматривается.

Коэффициент готовности – это комплексный показатель надежности технической системы (ТС), характеризующий ее безотказность и ремонтопригодность. В общем случае $K_Г(t)$ неизвестен. Определить его можно для систем, описываемых моделями в виде графов перехода систем из состояния в состояние.

Коэффициент готовности – это показатель, определяющий состояние ТС в некоторый конкретный момент времени t. На интервале времени $[0,\infty]$ его значение изменяется от 1 до предельного постоянного значения

$$K_Г(\infty) = \frac{\bar{T}}{\bar{T} + \bar{\theta}}.$$

Предельное значение $K_Г(\infty)$ достигается в установившемся режиме работы ТС, когда переходные процессы, связанные с вводом в эксплуатацию, и период приработки в ней завершены. Поэтому предельное значение $K_Г(\infty)$ строго применимо лишь для систем непрерывного использования, у которых влияние переходных процессов, связанных с вводом в эксплуатацию, закончилось.

В качестве примера использования показателей готовности для оценки технического состояния сложной технической системы, рассмотрим путевую машину для работ по текущему содержанию путей промышленных предприятий [2].

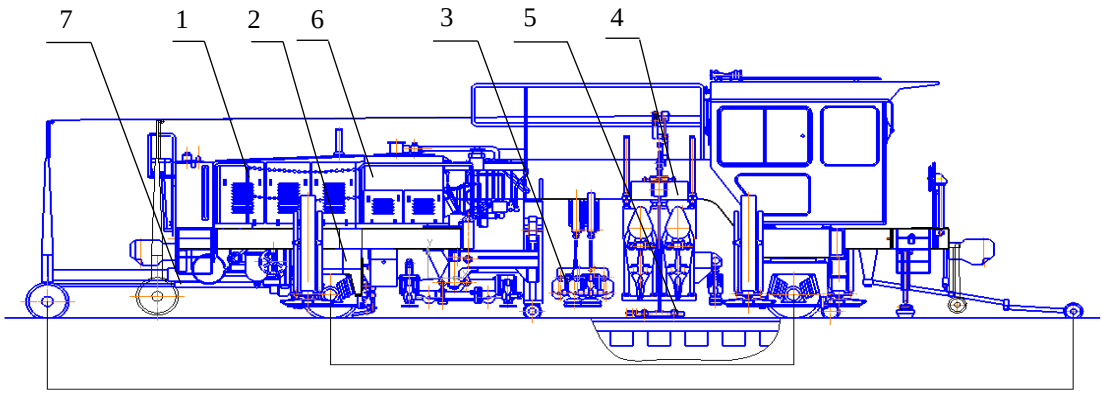

Рис. 1. Путевая машина ВПРС-1200
1 - энергетическая установка, 2 - трансмиссия, 3 - система выправки,
4 - подбивочная система, 5 - контрольно-измерительная система,
6 - система пожаротушения, 7 - гидросистема.

Путевая машина как сложная техническая система имеет большое количество подсистем (узлов и агрегатов). Условно подсистемы можно разделить на: системы обеспечивающие выполнение рабочих операций при ее движении в транспортном режиме (оперативная готовность); системы многократного применения (подбивочная система, система выправки и контрольно-измерительная система); дежурные технические системы (система пожаротушения); нерезервированные системы (все системы машины за исключением гидравлической системы, в которой имеется ручной насос для аварийного приведения машины в транспортное положение); нерезервированные системы с независимой работой ее подсистем (так в нашем случае, возможно раздельное выполнение измерения и выправки или выполнение только подбивки или только измерения); нерезервированные системы с зависимой работой ее подсистем (в нашем случае, все подсистемы за исключением подсистемы пожаротушения).

Для оценки готовности перечисленных систем в зависимости от особенностей их работы могут быть использованы расчетные соотношения, приведенные ниже.

Так коэффициент оперативной готовности – вероятность того, что техническая система окажется в работоспособном состоянии в произвольный момент времени, кроме планируемых периодов, в течение которых ее применение по назначению не предусматривается и, начиная с этого момента, будет работать безотказно в течение заданного интервала времени. Он позволяет оценить работоспособность ТС как в момент времени t (событие А), так и ее работоспособность в течение времени τ после момента t (событие Б) [1]. Коэффициент оперативной готовности – комплексный показатель для оценки восстанавливаемых систем. Он необходим для оценки вероятности выполнения целевой задачи и определяется соотношением:

$$P(t,t+\tau) = P(t)P(t+\frac{\tau}{t}) = K_{OГ}(t,\tau). \qquad (1)$$

Техническая система многократного применения работает сеансами, между которыми она может находиться в некотором произвольном состоянии ожидания применения.

Переход из режима ожидания в режим непосредственного использования осуществляется или непосредственно по команде, поступление которой следует считать равновероятным в любой момент интервала времени эксплуатации системы $[0,T]$, или в соответствии с планом применения ТС в заранее запланированный момент времени.

В первом случае естественно требование к готовности системы, чтобы она, находясь в режиме ожидания, оказалась работоспособной в любой произвольный момент времени t интервала $[0,T]$, и безотказно проработала в интервале $[t,t+\tau]$, где τ – время выполнения целевой задачи. Вероятность совместного выполнения этих двух условий – коэффициент оперативной готовности (1).

Во втором случае необходимо учитывать процесс подготовки ТС, что приводит к более сложным, по сравнению с рассмотренными, моделям определения готовности.

Дежурная техническая система – система однократного или многократного применения, у которой длительность подготовки к использованию по назначению за счет заблаговременного выполнения большинства операций подготовки сведена к минимуму и которая переводится в режим применения по назначению практически мгновенно.

Для поддержания дежурной ТС в работоспособном состоянии она периодически, через интервалы времени T_0, подвергается техническому обслуживанию (ТО), заключающемуся в контроле состояния ТС, выполнении профилактических мероприятий и в восстановлении системы при обнаружении неисправности.

Если длительность технического обслуживания намного меньше его периода, т. е. $Q_{обсл} \square T_0$, то можно сделать допущение о том, что обслуживание выполняется мгновенно и $Q_{обсл} = 0$. Поскольку длительность простоя ТС, вызванного обслуживанием, не учитывается, то в качестве показателя готовности дежурной ТС можно избрать коэффициент готовности. В этом случае необходимо учитывать, что ТС периодически подвергается техническому обслуживанию и, следовательно, значение $K_Г$ зависит от периода обслуживания

$$K_Г(t) = \frac{\bar{T}(T_0)}{\bar{T}(T_0) + \bar{\theta}(T_0)},$$

где $\bar{T}(T_0), \bar{\theta}(T_0)$ – математические ожидания соответственно временных интервалов нахождения ТС в работоспособном состоянии и ее восстановления (нахождения ТС в состоянии отказа), зависящие от периодичности обслуживания.

Многие из рассмотренных методик определения коэффициента готовности ТС предполагают наличие информации о показателях безотказности и ремонтопригодности. Если мы имеем дело с достаточно простой ТС, то такая информация известна не всегда, а в случае сложной технической системы, состоящей из нескольких подсистем, такой информации не бывает практически никогда. Коэффициент готовности нерезервированной системы может быть вычислен, если известны показатели надежности входящих в систему отдельных подсистем [1].

Структурная схема надежности нерезервированной системы представляет собой последовательное соединение n подсистем.

Если подсистемы работают независимо друг от друга, то при отказе одной из них только она и выключается для выполнения ремонта.

Пусть для каждой подсистемы известны средние значения наработки и длительности восстановления. Тогда коэффициент готовности каждой подсистемы

$$K_{\Gamma i} = \frac{\bar{T}_i}{\bar{T}_i + \bar{\theta}_i}.$$

При независимой работе подсистем вероятность работоспособности системы в целом зависит от вероятности нахождения в работоспособном состоянии каждой подсистемы:

$$K_{\Gamma} = \prod_{i=1}^{n} K_{\Gamma i} = \prod_{i=1}^{n} \frac{\bar{T}_i}{\bar{T}_i + \bar{\theta}_i}. \text{ [1]}$$

Анализ этого выражения показывает, что коэффициент готовности системы, во-первых, не может быть выше коэффициента готовности наименее готовой подсистемы, во-вторых, увеличивается с ростом средней наработки и уменьшается с увеличением среднего времени восстановления каждой из подсистем.

В случае если система состоит из n подсистем, то при отказе любой из них вся система может переходить в неработоспособное состояние и функционирование всех подсистем прекращается. Например, отказ энергетической установки (рис.1.) приведет к отказу всех систем путевой машины. Наработка на отказ каждой из подсистем распределена по экспоненциальному закону

$$\omega_i(t) = h_i e^{-h_i t} = \frac{1}{\bar{T}_i} e^{-t/\bar{T}_i}.$$

Коэффициент готовности системы

$$K_{\Gamma сист} = \frac{\bar{T}_{сист}}{\bar{T}_{сист} + \bar{\theta}_{сист}}. \text{ [1]}$$

Следовательно, для вычисления $K_{Гсист}$ необходимо определить средние времена нахождения системы в работоспособном состоянии и состоянии простоя.

Выводы: проведенный анализ состава путевой машины и взаимодействия ее узлов и агрегатов позволил установить расчетные зависимости для определения коэффициентов готовности в зависимости от специфики их использования.

Список литературы

[1] Дорохов А.Н., Керножицкий В.А., Миронов А.Н., Шестопалова О.Л. Обеспечение надежности сложных технических систем: Учебник – СПб.: Издательство «Лань»,2011-352с.: ил.-(Учебники для вузов. Специальная литература)

[2] М.В. Попович, В.М. Бугаенко, Б.Г. Волковойнов и др. Под ред. М.В. Поповича, В.М. Бугаенко. Путевые машины: Учебник для вузов ж.-д. транс. – М.: Желдориздат, 2007. – с.

Байко Наталия Игоревна – студент КФ МГТУ им. Н.Э. Баумана. E-mail: natalia.bajko@yandex.ru

Заярный Сергей Леонидович – канд. техн. наук, доцент кафедры "Детали машин и подъемно-транспортное оборудование" КФ МГТУ им. Н.Э. Баумана. E-mail: texnakon@yandex.ru

Н.В. Трухов, В.А. Раевский

КОНКРЕТИЗАЦИЯ ЛИНИИ РАВНОГО ВЫБЕГА КАНАТА ШАРНИРНЫХ СТРЕЛОВЫХ СИСТЕМ ПОРТАЛЬНЫХ КРАНОВ

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

Погрузочно-разгрузочные работы являются наиболее распространенными при осуществлении производственной деятельности любой организации. Для организации такого вида работ применяют самые разнообразные грузоподъемные машины. При выполнении широко спектра операций, таких как перевалка штучных грузов при помощи грузового крюка, работы с тяжелыми грузами, обработки навалочных грузов при помощи грейфера, работы с магнитом, обработки контейнеров при помощи спредера, рекомендуется использовать портальные краны.

Портальный кран – полноповоротный стреловой кран, поворотная часть которого установлена на портале, передвигающемся по рельсам, проложенным на земле или эстакаде [1]. Ключевое место в проектировании крана такого типа занимает синтез стрелового устройства.

Шарнирно-сочлененные стрелы (ШСС) используются на кранах, как правило, большой грузоподъемности, обеспечивают горизонтальность перемещения конца хобота и груза благодаря свойствам четырехугольника позволяют перемещать крупногабаритные грузы. В портовых грузоподъемных машинах применяют шарнирно-сочлененные стрелы с жесткой оттяжкой, выполненной в виде решетчатой или коробчатой балки, и шарнирно-сочлененные стрелы с гибкой канатной оттяжкой.

При проектировании ШСС важную роль играет выбег грузового каната[2], который представляет собой разность длины ветви каната стрелового устройства в наиболее удаленном положении и длины каната, при котором стрела с хоботом, при обеспечении кинематической схемой «наиболее» горизонтального перемещения груза, находятся в ближайшем положении относительно точки закрепления стрелы. Математически выбег грузового каната $Ukan(\varphi)$ для случая расположения обводного блока в шарнире стрела-хобот можно определить следующим образом (рис. 1):

$$Ukan(\varphi) = Lkan - Lka(\varphi), \qquad (1)$$

где $Lkan$ - длина ветви каната $КС_m$, $Lka(\varphi)$ - длина ветви каната $КС_k$.

Геометрическое место точек К, обеспечивающее при постоянных для заданных условий параметрах одинаковый выбег каната $Ukan(\varphi)$, называют линией равного выбега каната [2].

Наиболее часто рассматриваемая схема анализа ШСС подразумевает совмещение линия равного выбега каната и биссектрисы угла треугольни-

ка KC_mC_k в пределах выделенной зоны [2], причем возможно продление ее, если нижний шарнир стрелы расположен выше кабины.

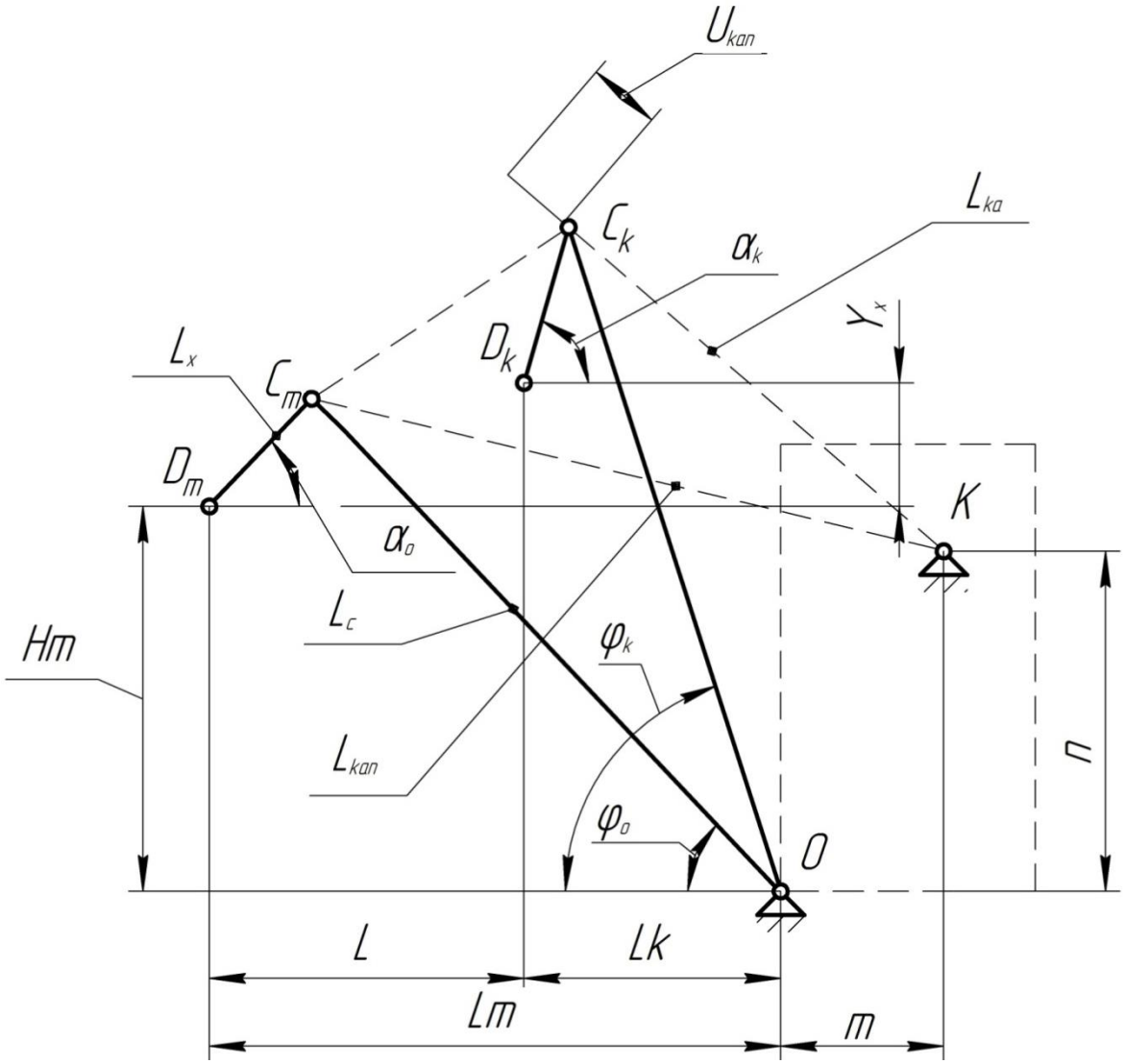

Рис. 1. Кинематическая схема стрелового механизма при расположении обводного блока в шарнире стрела – хобот

В литературе нет подтверждения факта совпадения линии равного выбега грузового каната и биссектрисы треугольника KC_mC_k [2]. Проверить данный тезис можно, применив аппарат аналитической геометрии.

Уравнения биссектрис углов между прямыми $A_1x + B_1y + C_1 = 0$ и $A_2x + B_2y + C_2 = 0$ [3]:

$$\frac{A_1x + B_1y + C_1}{\sqrt{A_1^2 + B_1^2}} = \pm\frac{A_2x + B_2y + C_2}{\sqrt{A_2^2 + B_2^2}}. \qquad (2)$$

В данном случае найдем уравнение биссектрисы угла, образованного линиями KE_m и KE_k (рис. 2).

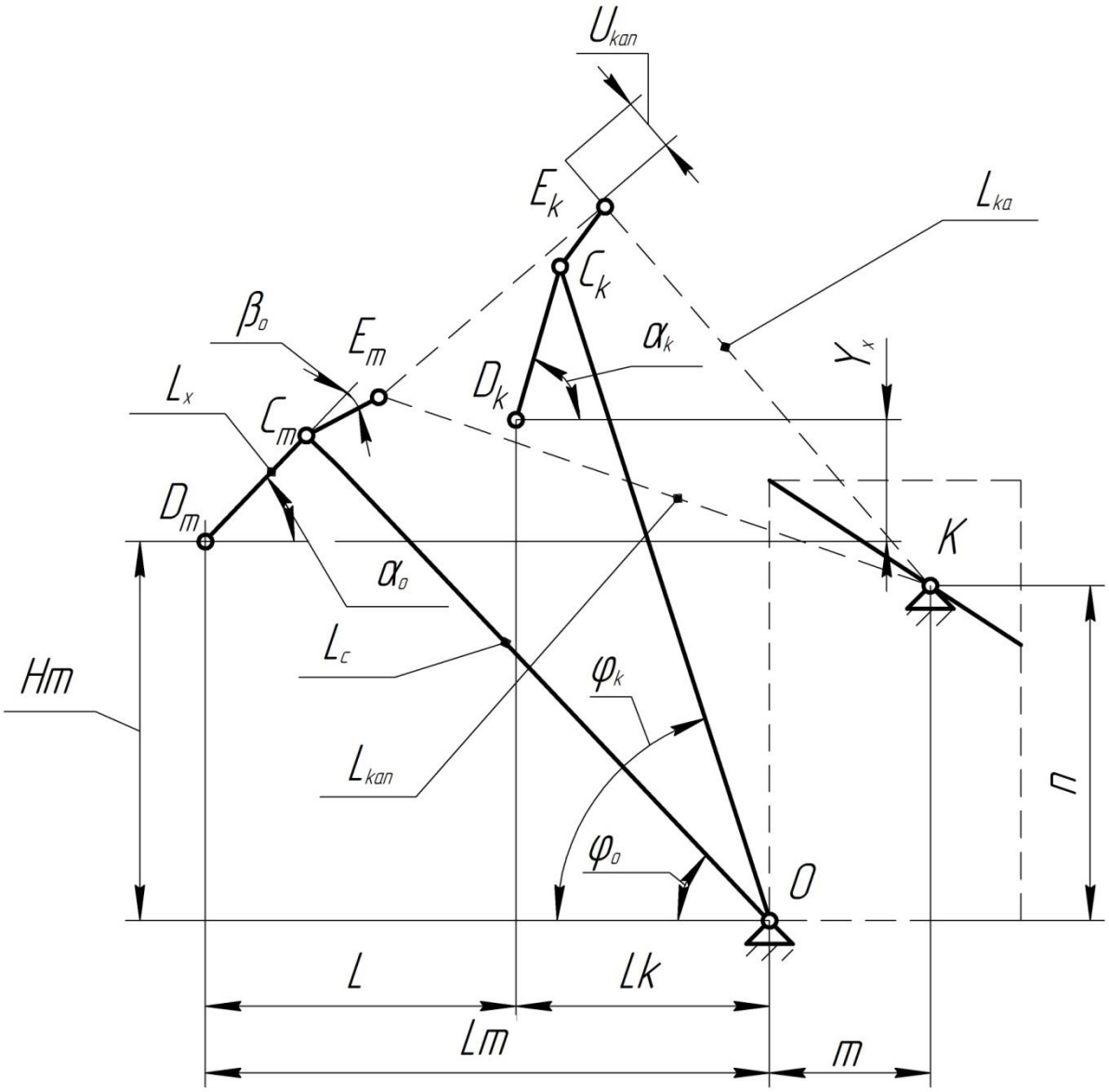

Рис. 2. Кинематическая схема стрелового механизма при расположение обводного блока в произвольном положении под углом β_0 к продолжению линии переднего плеча хобота

В общем виде уравнение прямой имеет вид: $y = kx + b$. Подстановкой координат известных точек K, E_k, E_m в данную зависимость определим коэффициенты k и b:

$$\begin{aligned} & Hm + Lx \cdot \sin(\alpha 0) + Le \cdot \sin(\alpha 0 - \beta 0) - n = \\ & = k_1 \cdot (Lm + m - Lx \cdot \cos(\alpha 0) - Le \cdot \cos(\alpha 0 - \beta 0)) + b_1, \\ & Hm + Lx \cdot \sin(\alpha k) + Le \cdot \sin(\alpha k - \beta 0) + \frac{Ukan}{pk} - n = \\ & = k_2 \cdot (Lm + m - L - Lx \cdot \cos(\alpha k) - Le \cdot \cos(\alpha k - \beta 0)) + b_2, \end{aligned} \quad (3)$$

где Hm - ордината конца хобота, Lx - длина хобота, Le - длина от оси Е блока до оси С блока, m и n – координаты точки, из которой выходит ли-

ния равного выбега каната, Lm - абсцисса конца хобота, L - длина рабочей зоны ШСС, $\alpha 0$ - угол наклона хобота к горизонтали при максимальном вылете, αk - угол наклона хобота к горизонтали при минимальном вылете, $\beta 0$ - угол наклона переднего плеча хобота, $Ukan$ - выбег каната, pk - кратность полиспаста.

При этом в точке К рассматриваемые линии пересекаются, из чего следует

$$\begin{cases} Hm + Lx \cdot \sin(\alpha 0) + Le \cdot \sin(\alpha 0 - \beta 0) - n = \\ = k_1 \cdot (Lm + m - Lx \cdot \cos(\alpha 0) - Le \cdot \cos(\alpha 0 - \beta 0)) + b_1 \\ n = k_1 m + b_1, \end{cases}$$

$$\begin{cases} Hm + Lx \cdot \sin(\alpha k) + Le \cdot \sin(\alpha k - \beta 0) + \dfrac{Ukan}{pk} - n = \\ = k_2 \cdot (Lm + m - L - Lx \cdot \cos(\alpha k) - Le \cdot \cos(\alpha k - \beta 0)) + b_2 \\ n = k_2 m + b_2. \end{cases} \quad (4)$$

Из полученных систем можно найти коэффициенты $k_{1,2}$ и $b_{1,2}$.

В данном случае: $k_1 m - n + b_1 = 0$ и $k_2 m - n + b_2 = 0$. Тогда уравнение биссектрисы примет вид:

$$\frac{k_1 m - n + b_1}{\sqrt{k^2{}_1 + 1}} = \pm \frac{k_2 m - n + b_2}{\sqrt{k^2{}_2 + 1}}. \quad (5)$$

Подставляя коэффициенты $k_{1,2}$ и $b_{1,2}$, найденные выше, можно проверить линию равного выбега грузового канта на предмет совпадения с биссектрисой угла, образованного линиями KE_m и KE_k.

Список литературы

[1] *Петухов П. З., Ксюнин Г. П., Серлин Л. Г.* Специальные краны – М: Машиностроение, 1985. – 248 с.

[2] *Стрелов В. И.* Расчет шарнирных стреловых систем портальных кранов (аналитический метод кинематического синтеза). – Калуга: Облиздат, 1998. – 188 с., ил.

[3] *Соболь Б.В., Мишняков Н.Т., Поркшеян В.М.* Практикум по высшей математике. Изд. 3-е. – Ростов н/Д: Феникс, 2006. – 640 с.

Трухов Николай Викторович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: 184ch24701@gmail.com

Раевский Владимир Алексеевич – канд. техн. наук, доцент кафедры "Детали машин и подъемно-транспортное оборудование" КФ МГТУ им. Н.Э. Баумана. E-mail: var-77@mail.ru

А.И. Усачев, П.В. Витчук

КОНСТРУКЦИЯ СТЕНДА ДЛЯ ИМИТАЦИИ АВАРИЙНОЙ ОСТАНОВКИ ЛИФТА

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

Ловители лифта предназначены для удержания кабины (противовеса) на направляющих при превышении скорости кабины (противовеса), независимо от причины, вызвавшей это превышение, например, обрыва тяговых канатов. При этом пассажиры в процессе торможения могут подвергаться значительным ускорениям замедления, вплоть до 50 м/с^2 [6]. Это обуславливает актуальность изучения вопросов взаимодействия рабочих поверхностей ловителя и направляющей.

Приведенные в отечественных и зарубежных литературных источниках методики расчета лифтовых ловителей [1-5] содержат значительное число допущений и различных коэффициентов (в том числе эмпирических), имеющих существенный разброс. Поэтому результаты расчета даже в рамках одной методики могут отличаться в несколько раз в зависимости от выбранных допущений и коэффициентов и в десятки раз при использовании разных методик.

По сути, в достаточной мере проработанной является лишь методика расчета геометрических параметров клиновых ловителей резкого торможения, которая может быть выполнена двумя способами. Первый базируется на экспериментальных данных, накопленных в большом количестве в научно-исследовательских центрах СССР, в первую очередь, ВНИИПТМАШ. Второй (аналитический) способ разработан в МГСУ (МИСИ) на основе изучения следов пластической деформации рабочей поверхности направляющей зубом ловителя [1].

Оба этих способа являются не учитывают условия смазывания и имеют ограничения по применимости для ловителей и направляющих, изготовленных из материалов и имеющих конструкцию отличных от исследованных. Последний факт особенно важен в современных условиях, когда разрабатываются большое число материалов, имеющих лучшие физико-механические свойства по сравнению с используемыми.

Неучет контактного взаимодействия ловителя с направляющей может привести к аварийной ситуации. Например, из практики эксплуатации лифтов известны случаи несрабатывания ловителей плавного торможения при смене смазочного материала направляющей.

Процесс взаимодействия рабочих поверхностей ловителя и направляющей также оказывает существенное влияние на напряженно-деформированное состояние направляющих, так как в них возникают значительные по своей величине напряжения при срабатывании ловителей.

Следует отметить важность исследования процесса взаимодействия рабочих поверхностей ловителя и направляющей для разработки математических (динамических) моделей лифтов, так как существующие модели,

представленные в большом объеме в отечественной и зарубежной литературе, практически не учитывают этот процесс.

На основании вышесказанного очевидна необходимость проведения значительного числа экспериментальных испытаний работы ловителей.

Можно выделить основные направления совершенствования методов расчета и испытаний ловителей:

1. Совершенствование существующих расчетных методик на основе дополнения их зависимостями, учитывающими контактное взаимодействие ловителей и направляющих.

2. Совершенствование методов испытаний ловителей, результатом которых должно стать не только принятие решения «да» или «нет» о работоспособности ловителей, а количественное выражение (например, в виде цифр, таблиц или графиков) резервов безопасности работы ловителей.

Решение указанных задач невозможно без проведения соответствующих экспериментальных исследований, имитирующих различные случаи свободного падения кабины.

С учетом этого факта, а также на основе анализа некоторых существующих экспериментальных установок и устройств предлагается лабораторный стенд (рис 1.).

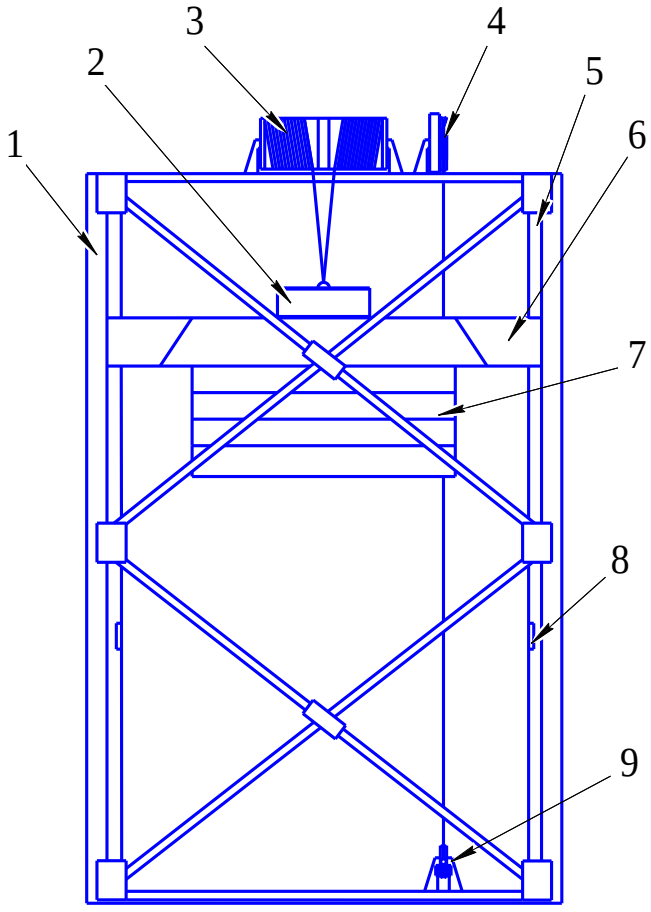

Рис.1. Эскиз установки для испытания ловителей

1 – рама; 2 – магнитное грузозахватное устройство; 3 – лебедка; 4 – ограничитель скорости; 5 – направляющие; 6 – главная балка; 7 – груз; 8 – тензодатчики; 9 – обводной блок.

Предлагаемый стенд работает следующим образом. Привод (лебедка) поднимает главную балку с установленными на ней ловителями и грузом до необходимой высоты, затем выключается магнитное грузозахватное устройство и происходит падение балки. Настроенный ограничитель скорости срабатывает, воздействуя своим канатом на тягу, приводящую в действие ловители. Происходит заклинивание. В зоне заклинивания устанавливаются тензодатчики и акселерометры для измерения параметров торможения и усилий воздействия на направляющую.

Предлагаемый стенд позволяет исследовать разнообразные конструкции ловителей с имитацией свободного падения кабины в условиях, приближенным к реальным условиям эксплуатации.

Список литературы

[1] Лифты. Учебник для вузов /под общей ред. Д.П.Волкова. М.: Изд-во АСВ,1999. 480 с.

[2] Лифты / Г.К. Корнеев [и др.]/ М.: Машгиз, 1958. 567 с.

[3] Яновски Л. Проектирование механического оборудования лифтов. Третье изд-е: -М.: Издательство АСВ, 2005. 336 с.

[4] Витчук П.В., Шубин А.А., Потапов Д.В.Зависимость ускорения замедления кабины от параметров клина ловителя // Известия ТулГУ. Технические науки. Вып. 7. Тула: Изд-во ТулГУ, 2013. С. 171-177.

[5] Мкуната Т., Кохара Х. и др. Самый быстрый лифт в мире Лифт, 2005. №4. С. 53-56.

[6] Федосеев В.Н., Гончаров Г.К. Безопасная экпслуатация лифтов. Справочное пособие / М.: Строиздат, 1987. 256 с.

Усачев Александр Игоревич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: alexandr_igorevi4@mail.ru

Витчук Павел Владимирович – канд. техн. наук, доцент кафедры "Детали машин и подъемно-транспортное оборудование" КФ МГТУ им. Н.Э. Баумана. E-mail: zzzventor@ya.ru

К.С. Малахов, Н.П. Сибилев

МОТОР-КОЛЕСО

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

Электропривод является наиболее распространенной технической системой, где электрическая энергия преобразуется в механическую, которая необходима для осуществления технологических процессов.

Важная роль принадлежит электроприводу в создании энергосберегающих технологий. Многие технологические процессы связаны с большими затратами электрической энергии, однако не всегда эти затраты оправданы.

Первые схемы сборки привода включают: электродвигатель, муфту, редуктор и исполнительный механизм. Данные схемы имеет достаточно большие габаритные размеры, низкий КПД, большие экономические затраты на проектирование и изготовление редуктора. Со временем был изобретен мотор-редуктор, что уменьшило габаритные размеры, вырос показатель КПД, но все так же присутствовал редуктор. С появлением доступных технических средств для регулирования скорости асинхронных двигателей стали применять регулируемые электроприводы на основе таких двигателей. Регулирование скорости рабочих органов машины является необходимым условием работы многих машин и механизмов. [1]

Известны приводы где электродвигатель воздействует непосредственно на колеса, что явилось следующим вариантом совершенствования электропривода и получило название мотор-колесо. Электродвигатель соединяют с рабочим органом машины либо непосредственно, либо через редуктор или другую кинематическую передачу. Для высокоточных механизмов и машин, работающих в динамичных режимах, стремятся исключить механические передачи между валом двигателя и рабочим органом. Такие электроприводы называют безредукторными.

Мотор-колесо – агрегат, объединяющий колесо и встроенные в него тяговый электродвигатель, силовую передачу и тормозную систему (таким образом, каждое мотор-колесо имеет индивидуальный привод). Устанавливается, как правило, в подвешенном к раме кронштейне (в случае, когда колесо не является управляемым) либо в установленном в поворотной цапфе подшипника (в случае, когда колесо является одновременно ведущим и управляемым). Питается энергией от двигателя внутреннего сгорания через электромеханическую трансмиссию (преимущественно на автомобильной технике, главным образом тяжёлой), от контактной сети (на троллейбусах и троллейвозах) или от аккумулятора (либо, в качестве дополнительного источника энергии, на автомобильной технике с двигателем внутреннего сгорания, такой как гибридные автомобили, или троллейбусы). Может функционировать в двух режимах – тяговом и генераторном. В тяговом режиме вращение передаётся с вала якоря электродвигателя, работающего в двигательном режиме, через редуктор к внутреннему зубчатому

венцу ведущего колеса; в генераторном режиме, используемом для электрического торможения, электродвигатель переходит в генераторный режим работы, а электроэнергия преобразуется в тепло на тормозном реостате (реостатное напряжение) либо возвращается в электрическую сеть или применяется для зарядки аккумуляторов (рекуперативное торможение) [2].

Мотор-колесо нашел свое применение в лифтовом оборудовании, и безредукторных лебедках переменного тока.Прогресс в разработке систем регулирования скорости с применением переменного тока привел к появлению на лифтовом рынке безредукторных лебедок с приводом переменного тока.

Рассмотрим, чертеж безредукторной лебедки CG 90 изготовленной компанией ALBERTO SASSI SpA приведенный на рис. 1, продольный разрез лебедки представлен на рис. 2.

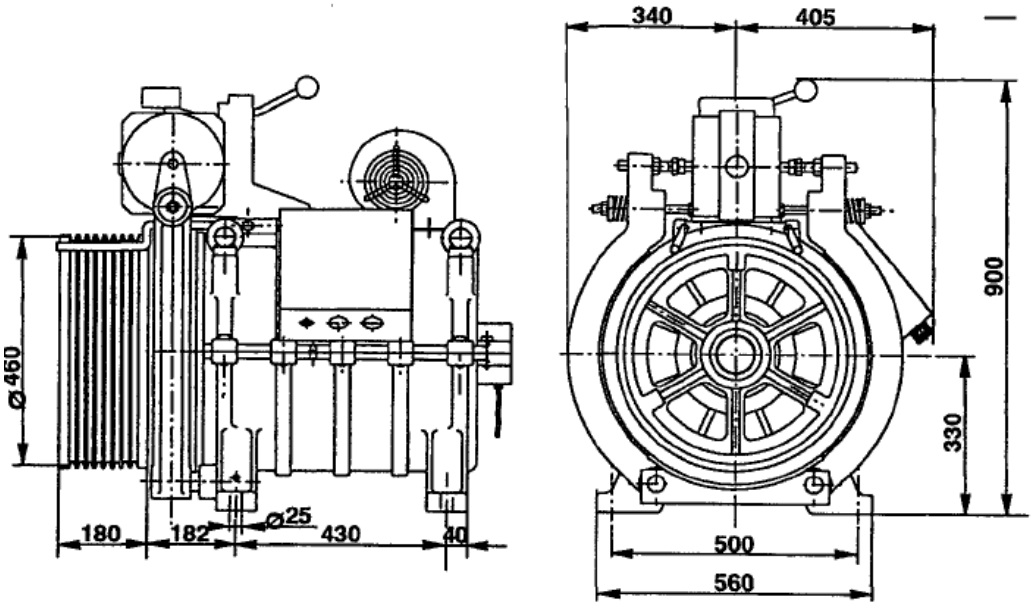

Рис. 1 Схема безредукторной лебедки CG 90 (Alberto Sassi SpA)

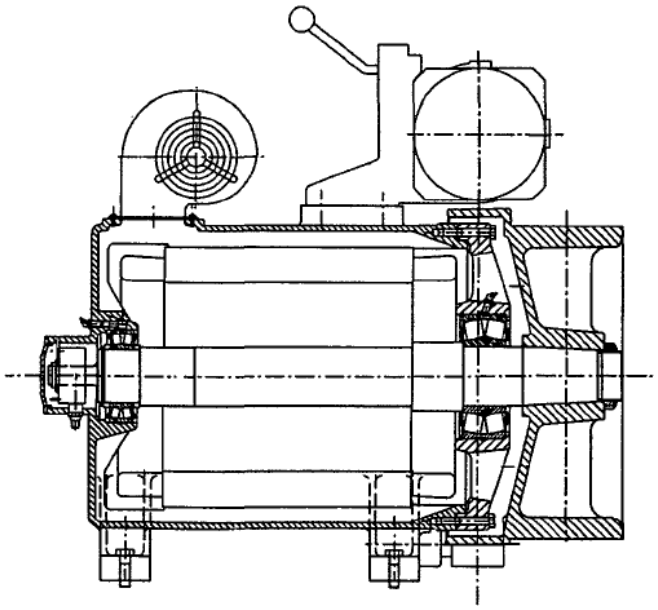

Рис. 2 Продольный разрез безредукторной лебедки CG 90

Безредукторная лебедка имеет небольшие размеры и очень компактная. Она поддерживает максимальную радиальную нагрузку на шкив 7000 кг при номинальном вращающем моменте 900 Н м.

Она спроектирована для номинальной нагрузки 1000 кг или 1275 кг, соответственно, и для скорости кабины 1,6, 2,0, 2,5 и 3,0 м/с.

Диаметры тяговых шкивов 410, 460 или 520 мм для номинальной нагрузки 1000 кг, но только 410 мм для номинальной нагрузки 1275 кг.

Шкив может иметь максимум 9 ручьев при номинальных диаметрах каната 10, 11 или 12 мм, или максимум 8 ручьев при номинальном диаметре 13 мм.

Асинхронный двигатель переменного тока с восемью полюсами контролируется частотным преобразователем с обратной связью по скорости и току для достижения совершенной диаграммы скорости и комфорта поездки.

Цифровой генератор импульсов имеет общую ось с валом двигателя (см. рис. 2) и защищен против механического повреждения колпаком, соединенным с корпусом двигателя.

Двигатель оборудован вспомогательным вентилятором 230В переменного тока (однофазный) высокой объемной производительности, что дало возможность увеличить число пусков двигателя в час до 240.

Терморезисторы тепловой защиты в обмотке двигателя дают возможность постоянно проверять температуру обмотки посредством контроллера лифта.

Вал поддерживается двумя самоустанавливающимися роликовыми подшипниками.

Шкив отлит вместе с тормозным шкивом и установлен консольно.

Тормоз - стандартной конструкции с внешним нажатием, он выключается двумя электромагнитами постоянного тока.

Для контроля зазора между тормозными башмаками и шкивом могут быть установлены микроконтакты [3].

Подводя итог, отдельно выделяя мотор-колесо, имеется ряд преимуществ, по сравнению с другим приводом. Малые экономические затраты, небольшие габаритные размеры, малый вес.

Список литературы

[1] Электрический привод: учебник для студ. высш. учеб. заведений/ Г.Б. Онищенко. – М.: Издательский центр «Академия», 2006. – 288с.

[2] Мотор-колесо // Политехнический словарь / А. Ю. Ишлинский (гл. ред.) и др. – 3-е изд., перераб. и доп. – М.: Советская энциклопедия, 1989. – С. 543. – 656 с.

[3] Яновски Л.Проектирование механического оборудования лифтов. Третье издание: - М.: Монография. Издательство АСВ, 2005, - 336 с.

Малахов Константин Сергеевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: malakhov.kostia@yandex.ru

Сибилев Николай Пантелеевич – канд. техн. наук, доцент кафедры "Детали машин и подъемно-транспортное оборудование" КФ МГТУ им. Н.Э. Баумана. E-mail: nikolaysibilev2@gmail.com

А.С. Исаченко, В.А. Ермоленко

ОГРАНИЧИТЕЛЬ ГРУЗОПОДЪЕМНОСТИ МОСТОВОГО КРАНА

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

Цель нашей работы – ограничение грузоподъемности крюковых грузоподъемных кранов.

Рассмотрены многие конструкции крановых весов и ограничителей грузоподъемности.

Известно, что большинство отказов с попыткой поднять груз, превышающую номинальную массу. Крановые весы – специализированный промышленный инструмент для измерения веса штучного груза, контейнерных единиц, перемещаемых краном. Точность базирования крановых весов составляет тысячная килограмма. Главным их недостатком является то что нельзя узнать массу груза, не подняв его.

Тензодатчик представляет собой основание с закрепленным на нем тензочувствительным элементом. Принцип измерения деформаций с помощью тензопреобразователя состоит в том, что при деформации детали на которую он закреплен изменяется активное сопротивление тензорезистора [1].

Широкое применение получила мостовая схема состоящая их тензореисторов, показанная на рис.1. Тензорезисторы R_1 и R_4 обладают одним знаком тензочувствительности, а R_2 и R_3 - противоположным. Общую точку резисторов R_2 и R_4 можно объединить с выводом подложки интегральной микросхемы тензопреобразователя.

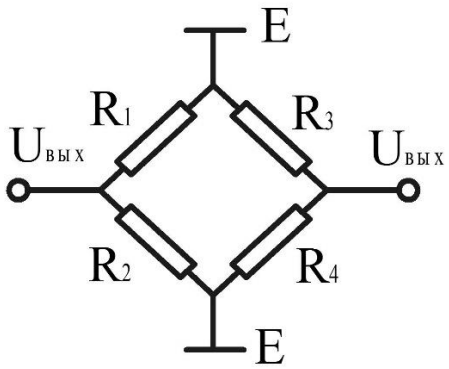

Рис. 1. Мостовая схема, подключенная тензопреобразователем
R_1, R_2, R_3, R_4 – переменное сопротивление резистора
E – потенциал

Характеристика мостовой схемы тензопреобразователя представляет собой зависимость выходного $U_{вых}$ от приложенного к детали усилия,

для двух значений температуры T_0 и T_1 определяют следующие параметры: начальный разбаланс U_0 - выходное напряжение при нулевом усилии (q=0) и температуре T_0. Разбаланс вызван технологическим разбросом номиналов тензорезисторов, полученных в результате расстояния при рассеянии параметров технологического процесса, а также начальной деформацией детали.

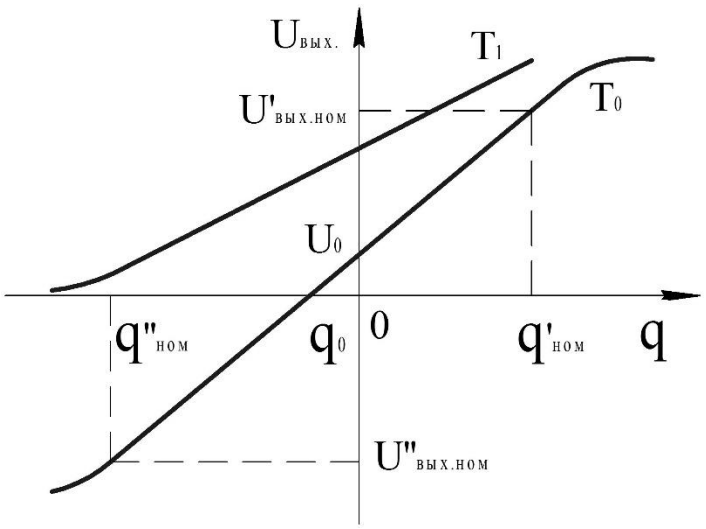

Рис. 2. Характеристика интегрального тензопреобразователя

Диапазон линейного преобразования Δq – область усилий для которых выходной сигнал мостовой схемы $U_{вых}$ линейно (с высокой степенью точности) зависит от усилия q:

$$\Delta q = q'_{ном} - q''_{ном} \quad (1)$$

где $q'_{ном}$; $q''_{ном}$ – номинальные диапазоны линейного преобразования положительного и отрицательного избыточных усилий, соответственно.

Тензопреобразователи имеют различные линейные диапазоны, которые изменяются в очень широких пределах от килопаскаля до гигапаскалей. Нелинейность характеристики определяется несколькими причинами, которые условно можно разбить на три категории: нелинейность преобразования усилия в механические напряжения; нелинейность пьезорезисторного эффекта; нелинейность измерительной электрической схемы [2].

В ограничителе нагрузки грузоподъемного крана, содержащем тензопреобразователь, установленный между упорным подшипником и поверхностью траверсы, управляющее устройство, соединенное с мостовой схемой с помощью беспроводного канала передачи данных, на основе микроконтроллера с возможностью формирования предупреждающих сигналов, для предотвращения перегрузки крана.

Поставленная задача решается за счет того, что элемент тензодатчика (рис 3) размещен между упорным подшипником и поверхностью траверсы.

Рис. 3. Тензодатчик мембранного типа

Реализуем силовоспринимающий элемент датчика нагрузки в виде упругого элемента, а чувствительный элемент в виде тензорезисторного, преобразователя деформации упругого элемента.

Оснащение датчика нагрузки автономным источником питания (гальванической батареи или аккумулятором, снабженным устройством подзарядки от внешнего источника питания), устройством для контроля его разряда, подключенным к микроконтроллеру или встроенным в него, с возможностью передачи соответствующего сигнала в управляющее устройство.

Реализация датчика, находящегося под упорным подшипником или под гайкой крюка, обеспечивает простоту монтажа, замены и ремонта. Достигается максимально возможная точность работы ограничителя грузоподъемности, поскольку в этом случае датчик нагрузки обеспечивает прямое измерение силы тяжести груза с крюком.

Ограничитель нагрузки грузоподъемного крана, при помощи тензодатчика, и управляющего устройства, соединенное с датчиком нагрузки с помощью беспроводной передачи данных, направленных на предотвращение превышения измерения нагрузки крана ее предельно допустимой величины, датчик расположен под упорным подшипником крюка.

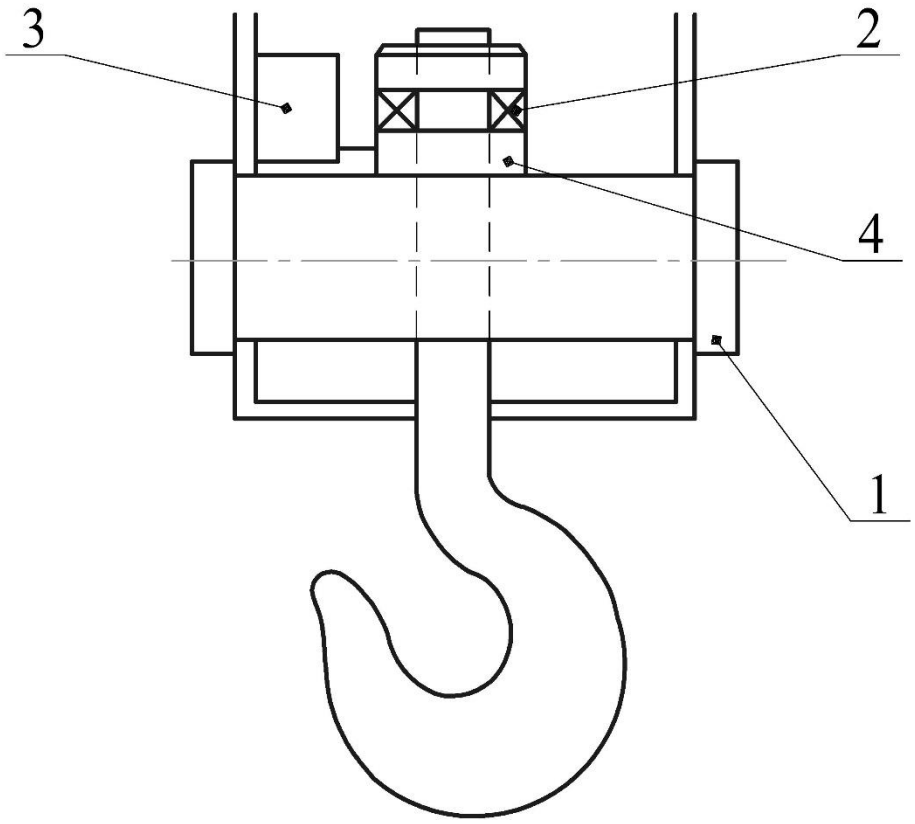

Рис. 4. Измерительная крюковая подвеска
1 – траверса; 2 – упорный подшипник; 3 – радиопередатчик;
4 – тензодатчик мембранного типа

Список литературы

[1] Крановые весы для взвешивания крупнотоннажных контейнеров. Патент РФ 2406680. Класс МПК: B66C13/16. Автор: Ададуров С.Е.; патентообладатель: Открытое акционерное общество "Российские железные дороги". Опубл. 20.12.2010.

[2] Весы для заливочного крана. Патент РФ 2306533. Класс МПК: G01G19/06. Автор: Сергеев А.И.; патентообладатель: Закрытое акционерное общество "ЭТАЛОН ВЕСПРОМ". Опубл. 20.09.2007.

Исаченко Алексей Сергеевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: privet.drugi@yandex.ru

Ермоленко Владимир Алексеевич – канд. техн. наук, доцент кафедры "Детали машин и подъемно-транспортное оборудование" КФ МГТУ им. Н.Э. Баумана. E-mail: tvermolenko@rambler.ru

Н.С. Гладышев, А.А. Шубин, С.Л. Заярный

ОЦЕНКА ЭФФЕКТИВНОСТИ ВИБРОВОЗБУДИТЕЛЕЙ ДЛЯ ГРОХОТОВ ЩЕБНЕОЧИСТИТЕЛЬНЫХ МАШИН

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

Для очистки балластной призмы используются различные путевые щебнеочистительные машины. Вне зависимости от их технических характеристик и конструктивного исполнения одним из основных рабочих органов этих машин являются грохоты, производящие очистку щебня механическим способом [1].

Одним из способов обеспечивающих колебания грохота, является использование дебалансного вибровозбудителя [2], принципиальная схема которого представлена на рис. 1.

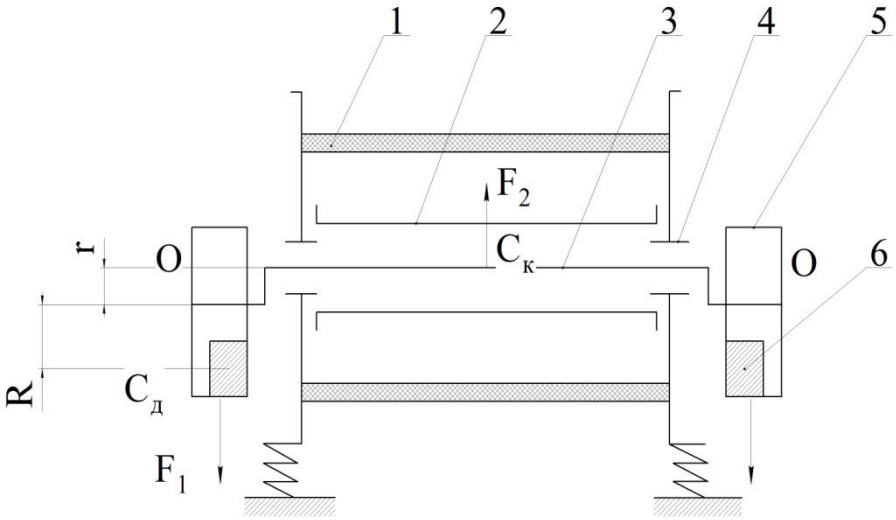

Рис. 1 Принципиальная схема действия дебалансного вибратора:
1 – грохот, 2 – труба, 3 – вал, 4 – опорный узел, 5 – шкив, 6 – дебалансный груз

Достоинствами дебалансного вибровозбудителя колебаний являются широкий диапазон, в котором можно задать частоту генерируемых вибраций, (в пределах 0,01–1000 Гц), удобство плавного или ступенчатого регулирования частоты вибрации, низкая чувствительность к изменениям внешних воздействий, простых средствах согласования совместной работы двух или нескольких вибровозбудителей на одном исполнительном органе машины.

К недостаткам дебалансных вибровозбудителей можно отнести: сравнительно небольшой ресурс, трудность независимого регулирования частоты и амплитуды вынуждающей силы.

Эти недостатки частично устраняются в гидравлических вибровозбудителях, принципиальные схемы которых представлены на рис. 2.

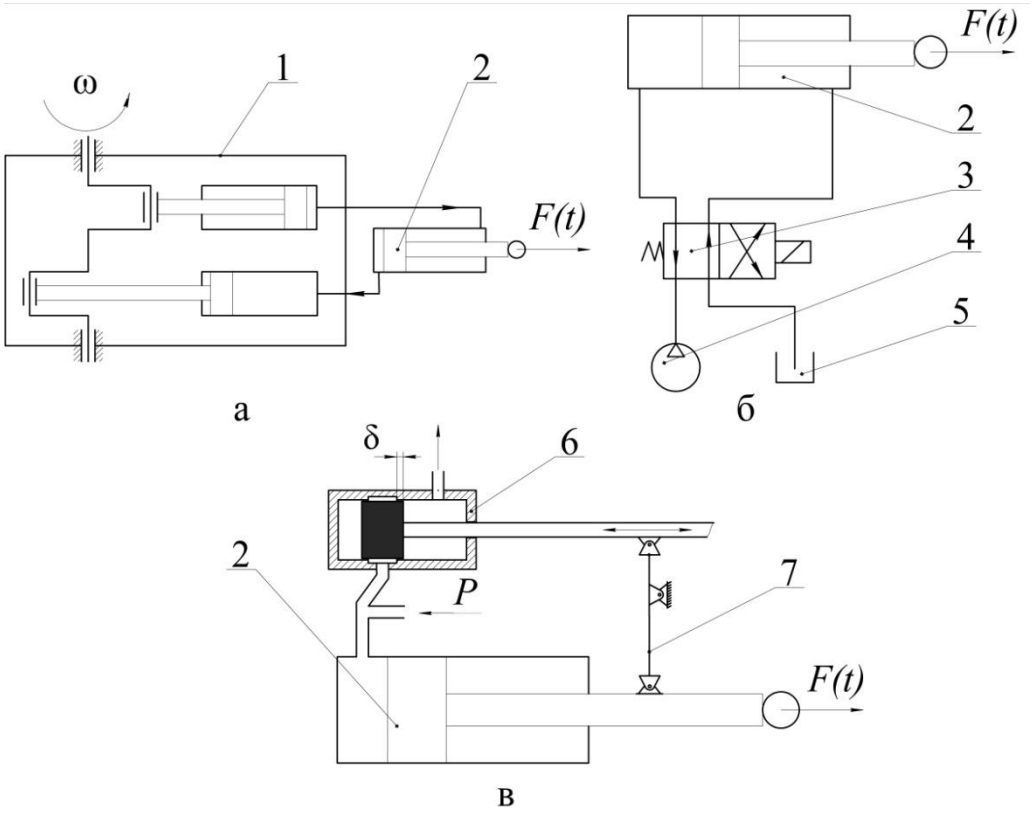

Рис. 2. Принципиальные схемы гидравлических вибровозбудителей:
а) с объемным регулированием; б) с дроссельным регулированием;
в) с дроссельным регулированием и обратной механической связью;
1 – плунжерный насос; 2 – приводной гидроцилиндр;
3 – гидравлическое распределительное устройство; 4 – насос; 5 – бак;
6 – золотниковый распределитель; 7 – обратная связь

Исполнительным элементом рассматриваемых схем вибровозбудителей является приводной гидроцилиндр, формирующий периодическое рабочее усилие $F(t)$. Приводной гидроцилиндр устанавливается на опорной раме путевой щебнеочистительной машины, а его шток соединен с опорными кронштейнами грохота. При этом возвратно-поступательные перемещения грохота обеспечиваются посредством пульсирующего потока рабочей жидкости в полости приводного гидроцилиндра. Пульсация потока рабочей жидкости обеспечивается: объемным регулированием с использованием плунжерного насоса (рис. 2а); дроссельным регулированием с использование гидравлического распределительного устройства (рис. 2б); дроссельным регулированием с использованием механической обратной связи (рис. 2в).

В гидравлических вибровозбудителях с дроссельным регулированием и обратной механической связью поршневая полость исполнительного гидроцилиндра подключена к магистрали постоянного давления P, а его шток, посредством обратной механической связи, соединен с золотниковый распределителем. Наличие зоны нечувствительности δ в золотниковом распределителе обеспечивает пульсацию рабочей жидкости в поршне-

вой полости исполнительного гидроцилиндра в режиме автоколебательного процесса, тем самым обеспечивает непрерывность его возвратно-поступательного движения [3].

Эффективным вариантом возбуждения колебаний короба могут служить трубчатые пружины. Такие пружины совмещают в себе функции гидравлического вибровозбудителя и стабилизирующей опоры (рис. 3а). Меняя расположение этих опор можно добиться различных траекторий колебания короба.

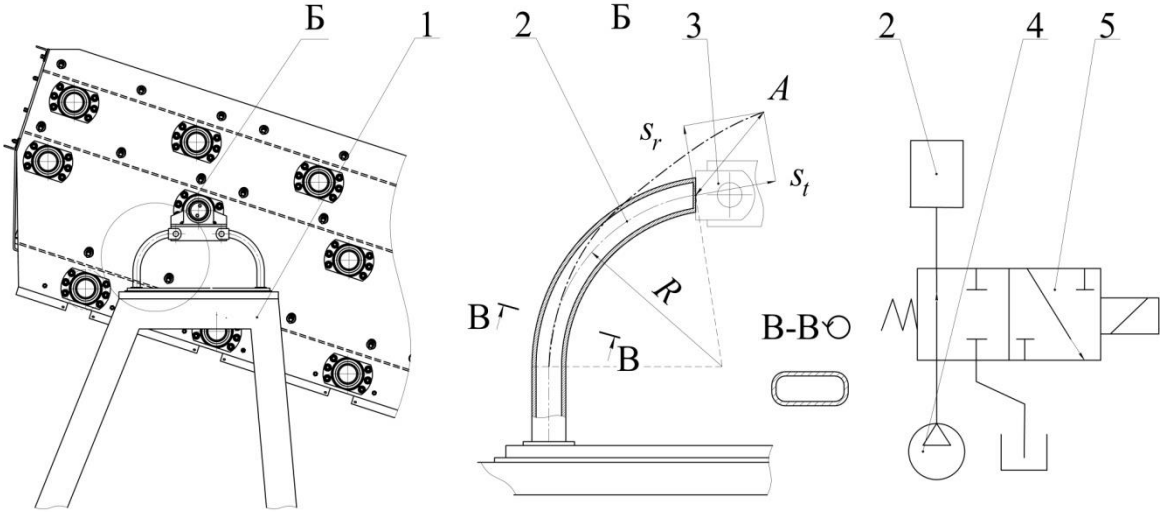

Рис. 3. Принцип действия трубчатой пружины:
а) колебания, совершаемые трубчатой пружиной; б) принципиальная схема работы трубчатой пружины: 1 – опорная рама; 2 – трубчатая пружина; 3 – шарнир; 4 – гидронасос; 5 – гидравлическое распределительное устройство

При подаче импульса давления пружина распрямляется. При оттоке жидкости конец пружины возвращается в исходное состояние. Грохот соединенной шарнирно с пружинами совершает колебания, создаваемые разницей между двумя конечными состояниями пружин с амплитудой A.

$$A = \sqrt{s_\rho^2 + s_t^2} = \frac{\Delta\gamma}{\gamma} R\Gamma, \qquad (1)$$

где s_r и s_t – перемещения пружины в радиальном направление и направление касательном к оси пружины, мм; $\frac{\Delta\gamma}{\gamma}$ – относительный угол изменение кривизны оси пружины и линейное перемещение ее конца, рад.; R – радиус кривизны, мм; Γ – коэффициент [4].

Применение трубчатых пружин позволяет в процессе работы изменять амплитудно–частотные характеристики, с помощью управляющего гидравлического распределительного устройств (рис. 3б) и, следовательно, подстраивать процесс грохочения под параметры (размер частиц, степень загрязнения и д. р.) очищаемого материала. При наличии обратной связи

можно реализовать частоты колебаний близкие к резонансным, что существенно снизит энергозатраты на процесс грохочения.

Рассмотренные варианты вибровозбудителей и их сравнительный анализ позволяют выявить перспективные направления исследований, направленные на повышение эффективности очистных модулей щебнеочистительных машин.

Список литературы

[1] Путевые машины, применяемые в ОАО «РЖД» Конструкция, теория и расчет. [Электронный ресурс] // Региональный Центр Инновационных Технологий [сайт]. URL: http://rcit.su/techinfo33.html (дата обращения: 05.03.2017).

[2] Гончаревич И.Ф. Вибрация – нестандартный путь. - М.: Наука, 1986. 209с.

[3] Денцов Н.Н. Динамика вибрационного грохота на комбинационном параметрическом резонансе // дисс. ... канд. техн. наук. Нижний Новгород, 2015 г.

[4] Пономарев С. Д., Андреева Л. Е. Расчет упругих элементов машин и приборов. - М.: Машиностроение, 1980. 326 с, ил.

Гладышев Никита Станиславович – студент КФ МГТУ им. Н.Э. Баумана. E-mail: naik14@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

Заярный Сергей Леонидович – канд. техн. наук, доцент кафедры "Детали машин и подъемно-транспортное оборудование" КФ МГТУ им. Н.Э. Баумана. E-mail: texnakon@yandex.ru

Г.Ю. Дедов, А.А. Шубин

ПЕРСПЕКТИВА ИСПОЛЬЗОВАНИЯ ГИБКОЙ ОБОЛОЧКИ В ПРИВОДАХ ЛЕНТОЧНЫХ КОНВЕЙЕРОВ

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

Ленточные конвейеры являются наиболее распространенным средством непрерывного транспортирования различных насыпных и штучных грузов в промышленности, строительстве, сельском хозяйстве и других областях народного хозяйства. Основой конвейера является бесконечная вертикальнозамкнутая гибкая лента [1].

Тяговое усилие передается приводным барабаном ленте посредством силы трения, создаваемой на поверхностях их фрикционного контакта. Очевидно, что сила трения должна быть достаточна для реализации необходимого тягового усилия, то есть не меньше суммы сил сопротивлений, возникающих при работе конвейера. При несоблюдении этого условия происходит скольжение ленты относительно вращающегося барабана (буксование), при котором тяговое усилие ленте не передается и барабан нагревается до температуры, при которой может произойти загорание ленты.

Совершенствование конструкции приводного барабана и увеличение его тяговой способности является актуальной задачей при создании конвейеров большой протяженности, транспортирующих крупнокусковые грузы. Важным моментом в работе конвейера является его пуск. При резком включении конвейера из-за значительных сил инерции возможно пробуксовывание привода, то есть сила сцепления ленты с поверхностью барабана равна или меньше суммарной силы сопротивлению движению. В этом случае в современных конструкциях конвейеров предусмотрен плавный пуск за счет изменения частоты вращения приводного барабана.

Повышение тяговой способности приводного барабана возможно нанесением рифления на его рабочую поверхность, футеровки его поверхности специальными материалами с повышенным коэффициентом трения, использование выдвижных элементов [2] и т.д.

Особого внимания заслуживает предложенная конструкция барабана [3] в которой в полость, образованную обечайкой, установлены опорные элементы, выполненные в виде сот. Обечайка, выполненная из листа небольшой толщины, может под действием ленты деформироваться, образуя многогранник со скругленными гранями (рис.1). Это благоприятно сказывается на сцеплении барабана с лентой, и тяговая способность барабана возрастает.

К недостаткам данной конструкции можно отнести циклическое деформирование обечайки, что при наличии жестких ребер опорных элемен-

тов будет приводить к ее усталостному преждевременному выходу из строя.

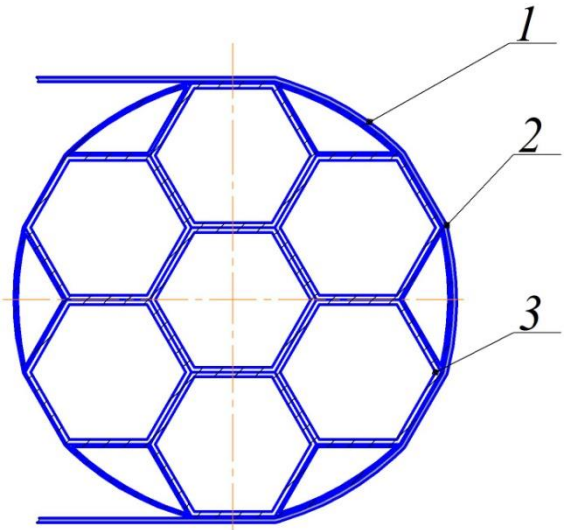

Рис.1 Схема передачи тягового усилия барабаном с жесткими элементами:
1 – лента конвейера, 2 – места перегиба, 3 – опорные жесткие элементы

В развитие данной конструкции предлагается соты выполнять из полимерных материалов, что позволит исключить, за счет деформирования сот, перегибы ленты, а при возрастании тягового усилия поверхность контакта ленты с обечайкой за счет деформации последней приобретает форму эллипса (рис.2).

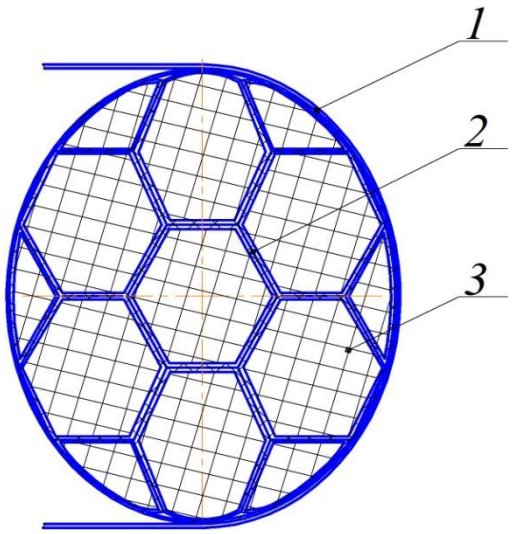

Рис.2 Схема передачи тягового усилия барабаном с эластичными элементами:
1 – лента конвейера, 2 – опорные эластичные элементы, 3 - заполнитель

Недостатком данной конструкции является необходимость для разных тяговых усилий использовать различные материалы опорных сотовых эле-

ментов различной жесткости или варьировать их толщину. Унифицировать конструкцию барабана для различных тяговых усилий позволит заполнение его ячеек полимерным материалом с различным модулем упругости.

Предлагаемая конструкция приводного барабана позволит не только увеличить тяговую способность привода в момент пуска, но и за счет гибкой оболочки эффективно реагировать на изменяющиеся условия работы конвейера. Применение сотовой конструкции в сочетании с заполнением сот гелем с различными свойствами позволит унифицировать конструкцию барабана для конвейеров с различными тяговыми характеристиками.

Список литературы

[1] Конвейеры: Справочник/ Р.А. Волков, А.Н.Гнутов, В.К. Дьячков идр. Под общей ред. Ю.А. Пертена. - Л.: Машиностроение, Ленингр. отдние, 1984. - 367с., с ил.

[2] Р. З. Гофман, С. И. Альберт, С. И. Насатин, А. П. Савченко, Э. Е. Андреев, И. Б. Тепер, И. Г. Орлова, Г. А. Желяско, М. Х. Корик и А. В. Каплунский. *Приводной барабан ленточного конвейера*. Пат. 1640062. СССР, 1989, бюл. №13, 5 с.

[3] О.Н. Алешин, И.А. Подопригора, В.П. Дунаев, А.В. Лагерев и Л.И.Блейшмидт. *Барабан подъемно-транспортной машины*. Пат. 1490043. СССР, 1981, бюл. №24, 3 с.

Дедов Григорий Юрьевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: Dedov.gr@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

Е.Ю. Володин, Т.В. Гаах

ПОДБОР РАЦИОНАЛЬНОЙ СХЕМЫ МЕХАНИЗАЦИИ ДЛЯ ПРОИЗВОДСТВА ВЫСОКОКАЧЕСТВЕННОГО ЩЕБНЯ

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

Щебень – один из самых распространённых продуктов переработки нерудных строительных материалов. Объемы производства щебня в мире превышают 3 млр.м^3 год. Современные технологии производства бетонов, асфальтобетонов и дорожных покрытий предъявляют все более высокие требования к качеству щебня.

Щебень применяемый в дорожном строительстве можно разделить на 3 группы:

- щебень для строительства оснований дорожных одежд (фракций 5-20, 20-40, 40-70, 0-40, 0-70 мм.);
- щебень для нижних слоев покрытий (фракций 5-20, 20-40 мм.);
- щебень для верхних слоев покрытий для асфальтобетонных смесей типа А и поверхностной обработки (крупностью щебня от 5 до 20 мм) с содержанием зерен пластинчатой (лещадной) и игловатой формы не более 15% (ГОСТ 8267-93), который принято называть «кубовидным».

За последние годы увеличился спрос на щебень кубовидной формы, потребность в котором в данное время удовлетворяется только на 30-40 %.

Асфальтобетонные смеси с содержанием щебня кубовидной формы имеют лучшую уплотняемость и обладают большей механической прочностью. Содержание же чрезмерного количества зерен лещадной формы (20-40% и более) приводит к образованию поверхностей, не покрытых битумом, что в последствии приводит к разрушению асфальтобетонного покрытия при проникновении воды и действии попеременного замораживания и оттаивания [1].

При производстве щебня кубовидной формы учитываются текстурно-структурные особенности исходной породы, используемое оборудование и технология производства.

Для получения щебня обычно применяют дробилки ударного действия, которые имеют повышенный выход отсева и дороги в эксплуатации. Форма производимого щебня близка к кубовидной, но иногда происходит обламывание краев зерен, поэтому форма щебня оказывается окатой. Кроме того, изначально камень будут раздавливать дробилки других типов (валковые, щековые) для получения необходимого размера кусков, что приводит к многостадийности и удорожанию производства.

Упростить технологическую схему производства (привести к двухстадийной схеме) и одновременно повысить качество получаемого щебня, возможно, используя конусную инерционную дробилку [2].

Отличительной особенностью дробилок конусных инерционных дробилок от эксцентриковых заключается в том, что привод дробящего конуса осуществляется от вибратора дебалансного типа, что позволяет увеличить дробящую силу и исключить зависимость силы от свойств перерабатываемого материала [3]. Сравнительная характеристика дробилок представлена в таблице 1.

Таблица 1. Сравнительная характеристика дробилок

Технология	Стандартная конусная дробилка	Роторная молотковая дробилка	Роторная центробежная дробилка	Конусная инерционная дробилка
Обеспечиваемая лещадность, %	25–40	10–20	5–15	10–15
Степень дробления	2,5–4	4–6	2–3	4–10
Диапазон крупности, мм питание	80	100	40–60	60–270
Диапазон крупности, мм готовый материал	25	20	20	15–60
Выход отсева (-5мм)	низкий	высокий	высокий	средний
Удельная металлоемкость	средняя	низкая	низкая	высокая
Удельная энергоемкость	низкая	высокая	средняя	низкая

Предлагается схема производства щебня (рисунок 1) главным агрегатом которой является конусная инерционная дробилка КИД-1200М [4] и подобрано рациональное оборудование для проектирование технологической линии (таблица 2).

Таблица 2. Подбор основного оборудования

Характеристика	Щековая дробилка СМД-510 [5]	Дробилка КИД-1200М [4]	Грохот ГИС-53 [5]	Грохот ГИС-42 [5]	Конвейер СМД-151-60 [5]
Производительность, $м^3/ч$	60	75	160	100	
Размер куска исходного материала, мм	500	80	200		
Масса, т	27,1	29,4	4,2	2,8	3,3
Ширина разгрузочной щели, мм	75	30			
Мощность приводов, кВт	75	200	15	11	7,5
Число ярусов сит			3	2	
Максимально допустимый вес объемно-насыпной массы, $т/м^3$			1,8	1,8	
Угол наклона просеивающей поверхности, град			10-20	10-20	
Высота разгрузки, мм					4,6
Ширина лент, мм					650
Количество оборудования	2	1	1	1	9

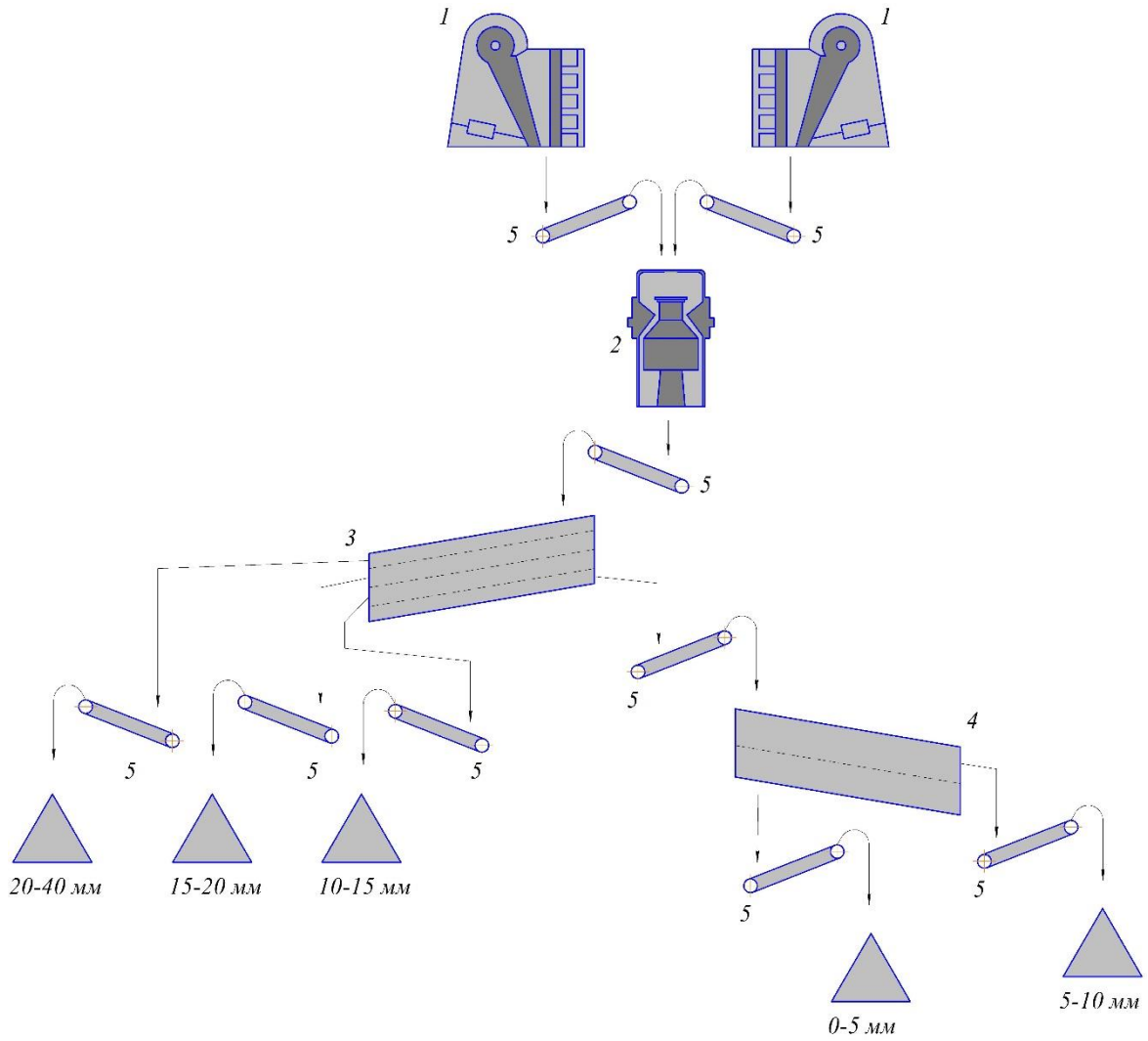

Рис 1. Схема механизации для производства
высококачественного щебня

Введение технологических схем производства с применением дробилок КИД-1200М позволяют получить кубовидный щебень в широком диапазоне крупности, минимизировать число стадий дробления, снизить энегозатраты и повысить производительность труда более чем на 20% [6].

Список литературы

[1] Гущин А.И., Косян Г.А., Артамонов В.А., Козин А.Ю., Кушка В.Н. Реальность производства щебня I группы по форме зерна. Строительные материалы, №2, 2002 г., с. 4–5.

[2] Вайсберг Л.А., Зарогатский Л.П. Новое поколение щековых и конусных дробилок. Строительные и дорожные машины, 2000 г., №7 с. 16–21.

[3] Рыков В.Ф. Спиридонов П.А. Установка с дробилкой КИД-1200М для производства щебня из гравия в ООО «Промстройинвест». Строительные материалы», №6, 2006 г. 21 с.

[4] Конусные инерционные дробилки. URL: http://mtspb.com/konusnie_inertsionnie_drobilki_kid/kid1200.html (дата обращения 20.03.2017).

[5] Продукция. URL: http://drobmash.ru/ru/oborudovanie (дата обращения 20.03.2017).

[6] Вайсберг Л.А., Шулояков А.Д., Спиридонов П.А. Сокращение стадиальности дробления – оптимальный путь снижения себестоимости высококачественного щебня. Строительные материалы, 2002 г., №11. с. 7–9.

Володин Егор Юрьевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: gaakh.tatyana@yandex.ru

Гаах Татьяна Владимировна – ассистент кафедры "Детали машин и подъемно-транспортное оборудование" КФ МГТУ им. Н.Э. Баумана. E-mail: gaakh.tatyana@yandex.ru

В.А. Ермоленко, М.А. Степанцов

ПРИМЕНЕНИЕ НАКЛОННОГО РОТОРА ЭКСКАВАТОРА ДЛЯ СЕЛЕКТИВНОЙ ВЫЕМКИ СТРОИТЕЛЬНОГО МАТЕРИАЛА

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

При добыче строительных материалов возникает необходимость селективной выемки. Полезное ископаемое отделяют от пустой породы одноковшовым экскаватором с одновременным подъёмом ковша и поворотом экскаватора [1].

Существующие роторные экскаваторы не имеют возможности изменить угол наклона оси вращения ротора, т.е. ось всегда горизонтальна.

В предложенной нами конструкции роторного экскаватора ось вращения ротора может быть наклонена от нуля до угла α, равного углу наклона верхнего опорно-поворотного устройства при повороте роторного экскаватора вокруг наклонного опорно-поворотного устройства на угол от нуля до 90° относительно исходного положения (рис. 1). При выемке полезного ископаемого наклонным ротором наезд на забой в нужном направлении возможен за счет манёвра ходовым устройством, например, шагающего, колесного или гусеничного типа. В случае разработки наклонно залегающих пластов полезного ископаемого наклон оси ротора позволяет повысить эффективность селективной выемки.

В случае применения роторного траншеекопателя, кюветообразующий или насыпеобразующий машины с наклонной осью ротора можно сформировать нужный угол откоса траншеи, кювета или насыпи, чтобы исключить обрушение откоса и столкновение ковша с твердыми включениями. При наклонном роторе твердые включения можно разрабатывать методом обхода по контуру твердого включения, при этом возможно снижение динамических нагрузок на машину и оператора, в частности, уменьшить вибрацию кабины.

Известно устройство для подъёма стрелы экскаватора, которое включает в себя лебедку подъёма стрелы [2, с.212]. Наличие барабана, канатов и блоков лебедки усложняет конструкцию. Канаты и блоки требуют частых осмотров и замены. Наклон оси вращения ротора невозможен.

Известно устройство, позволяющее наклонять верхнюю поворотную платформу относительно нижней неповоротной платформы экскаватора [3]. Оно содержит звенья между телами качения, которые могут поднимать с помощью гидроцилиндров ролики, расположенные с одной из сторон платформы. Это позволяет горизонтировать положение экскаватора, установленного на наклонном основании, и расширить технологические возможности экскаватора (регулировать угол наклона верхнего строения экс-

каватора). В этой конструкции также не предусмотрен наклон оси вращения ротора.

Предлагаемый нами роторный экскаватор (рис. 1) имеет горизонтальное и наклонное опорно-поворотные устройства, причем горизонтальное опорно-поворотное устройство расположено непосредственно на неповоротной части, а наклонное опорно-поворотное устройство расположено сверху горизонтального опорно-поворотного устройства, при этом центр нижней окружности верхнего опорно-поворотного устройства находится на оси вращения нижнего опорно-поворотного устройства, а верхнее строение расположено на наклонном опорно-поворотном устройстве.

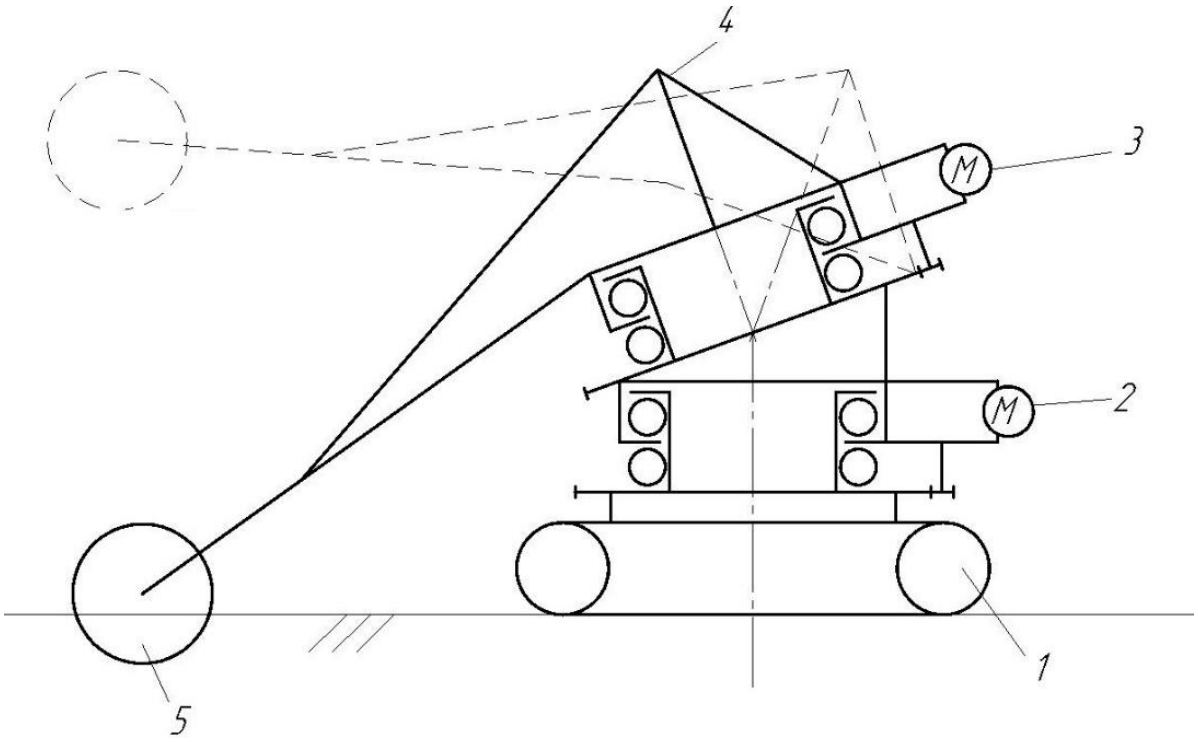

Рис. 1. Роторный экскаватор:
1 - неповоротная часть, 2 - горизонтальное опорно-поворотного устройство,
3 - наклонное опорно-поворотное устройств, 4 - верхнее строение, 5 - ротор.

Роторный экскаватор работает следующим образом. Для подъёма ротора 5 на максимально возможную высоту без поворота верхнего строения 4 вращают одновременно нижнее опорно-поворотное устройство 2 и наклонное опорно-поворотное устройство 3 в противоположные стороны и прекращают вращение после того, как будет завершен подъём ротора 5.

Для поворота верхнего строения 4 без изменения высоты подъёма ротора 5 вращают только горизонтальное опорно-поворотное устройство 2. Для совмещения операций подъёма ротора 5 и поворота верхнего строения 4 вращают одновременно оба опорно-поворотных устройства 2 и 3 в одну сторону.

Предлагаемый нами роторный экскаватор имеет более значительный угол наклона верхнего строения 4 относительно неповоротной части 1, имеет более простую конструкцию за счет того, что исключены силовые цилиндры или канатные механизмы подъёма. Исключается замена расходных материалов: гидроцилиндров, гидрожидкости или канатов. Горизонтальное и наклонное опорно-поворотные устройства 2; 3 унифицированы (взаимозаменяемы и однотипны), их обслуживание упрощается, т.е. повышается надёжность роторного экскаватора. Возможен наклон оси вращения ротора и осуществление селективной выемки.

Список литературы

[1]. *Владимиров В.М., Трофимов В.К.* Повышение производительности карьерных многоковшовых экскаваторов. М.: Недра, 1980. – 312с.
[2]. *Подэрни Р.Ю.* Горные машины и комплексы для открытых работ: Учебное пособие / Подэрни Р.Ю. – М.: Издательство МГГУ, 2001. – 422с.
[3]. А.С. 1258957 СССР, МПК Е 02 F 9/12. Опорно-поворотное устройство / *А.М.Будовой, Д.В.Булавин, Ю.Н.Матвеев* // Бюл. – 1986. – № 35.

Ермоленко Владимир Алексеевич – канд. техн. наук, доцент кафедры "Детали машин и подъемно-транспортное оборудование" КФ МГТУ им. Н.Э. Баумана. E-mail: tvermolenko@rambler.ru

Степанцов Михаил Анатольевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: stepantsov-ma@yandex.ru

А.А. Голиков, В.А. Ермоленко

РАСЧЕТ КОЛОННЫ ПОРТАЛЬНОГО КРАНА

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

Портальный кран проектируется нами для строительства набережной и перегрузочных работ с крюком и грейфером в речном порту. Наиболее сложными являются конструкция и расчет опорно-поворотного устройства портального крана, в частности его колонны.

Механизм поворота располагается на поворотной платформе. Он выполняется с зубчатым венцом. Зацепление может быть внутренним и внешним. Внешнее зацепление более удобно с точки зрения обслуживания и ремонта. При больших мощностях ставят два механизма поворота. Это позволяет применять унифицированные узлы для кранов разной мощности [1, с.178] Нарезка крупногабаритного зубчатого венца является проблематичной.

Цель расчета – уменьшение диаметра зубчатого венца и габаритов колонны.

Полагаем, что противовес уравновешивает стрелу и половину груза с грейфером. Тогда изгибающий момент, действующий на колонну (рис.1) составит:

$$\mathrm{M_и} = F_\mathrm{н} \cdot \mathrm{H} = \frac{m \cdot g \cdot L}{2 \cdot \mathrm{H}}, \qquad (1)$$

где g = 9,81 м/с^2 – ускорение свободного падения; L = 32 м – вылет стрелы; H = 3 м – расстояние между радиальными опорами (радиальным подшипником и катком).

Масса на конце стрелы

$$m = m_\mathrm{г} + m_\mathrm{гзу} = 8 + 4 = 12 \text{ т},$$

где $m_\mathrm{г}$ = 8 т – масса груза; $m_\mathrm{гзу}$ = 4 т – масса грузозахватного устройства

По формуле (1) получим:

$$\mathrm{M_и} = \frac{12 \cdot 9{,}81 \cdot 10^4 \cdot 32}{2 \cdot 3} = 62{,}8 \cdot 10^4 \text{ Нм}.$$

Момент сопротивления колонны, выполненной в виде тонкостенного квадрата в зоне нагрузки со стороны катков

$$W_\mathrm{и} = \frac{4}{3} \cdot \mathrm{B}^2 \cdot \delta = \text{ м}^3, \qquad (2)$$

где B = 1 м – сторона квадрата; δ =0,015 м – толщина стенки квадрата; 4/3 – справочный коэффициент [4, с. 40].

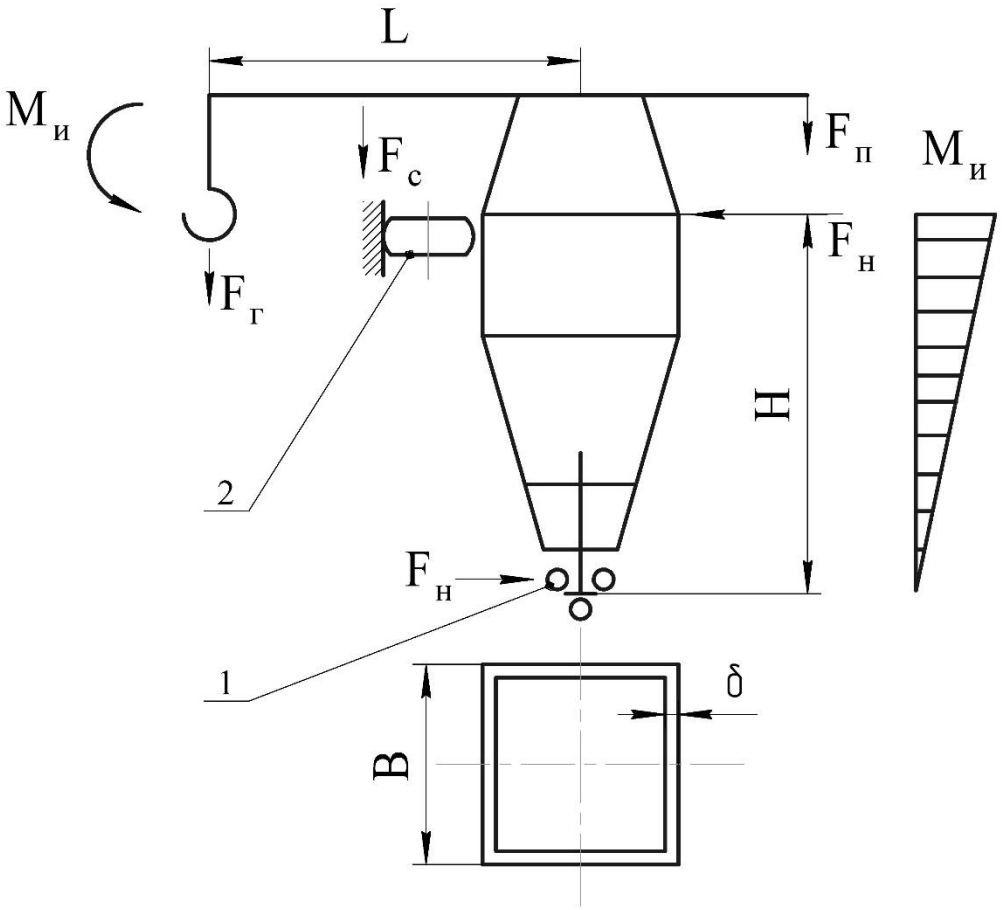

Рис.1 Схема нагрузок на колонну
1 – радиальный подшипник; 2 – каток

По формуле (2) получим:

$$W_{\text{и}} = \frac{4 \cdot 1^2 \cdot 0{,}015}{3} = 0{,}02 \text{ м}^3.$$

Напряжение изгиба

$$\sigma_{\text{и}} = \frac{\text{М}_{\text{и}}}{W_{\text{и}}}. \qquad (3)$$

По формуле (3) получим:

$$\sigma_{\text{и}} = \frac{62{,}8 \cdot 10^4}{0{,}02} = 31{,}4 \cdot 10^6 \text{ Па}.$$

Допускаемое напряжение изгиба

$$[\sigma_{\text{и}}] = \frac{\sigma_{\text{т}}}{\text{К}_{\text{б}} \cdot \text{К}_{\text{д}}}, \qquad (4)$$

где $\sigma_{\text{т}}$=$245 \cdot 10^6$ Па – допускаемое нормальное напряжение для стали Ст 3 сп [5]; $\text{К}_{\text{б}}$=1,5 – коэффициент безопасности [2, с.114]; $\text{К}_{\text{д}} = 2$ – коэффициент динамической нагрузки.

По формуле (4) получим:

$$[\sigma_{\text{и}}] = \frac{245 \cdot 10^6}{1{,}5 \cdot 2} = 81{,}6 \cdot 10^6 \text{ Па},$$

Условие прочности колонны

$$\sigma_{\text{и}} = 31{,}4 \cdot 10^6 \text{ Па} < [\sigma_{\text{и}}] = 81{,}6 \cdot 10^6 \text{ Па}.$$

Очевидно, что колонна имеет достаточную прочность, т.к. условие прочности выполняется.

Сила давления на один каток верхнего опорно-поворотного устройства

$$F_1 = \frac{F_{\text{н}}}{z_1 \cdot \cos\alpha}, \qquad (5)$$

где α– угол между катками; z_1–число катков с одной стороны верхнего опорно-поворотного устройства.

Угол между катками

$$\alpha = \frac{360°}{z}.$$

Получим:

$$\alpha = \frac{360°}{4} = 45\ °.$$

По формуле (5) получим:

$$F_1 = \frac{12 \cdot 10^4}{4 \cdot \cos 45°} = 4{,}24 \cdot 10^4 \text{ Н}.$$

Выбираем катки диаметром $d = 0{,}25$ м с допускаемой нагрузкой до $5 \cdot 10^4$ Н [3, с.76], диаметр окружности качения катков $D = 2$ м определен из рис.2. Зубчатое колесо имеет внутренний посадочный диаметр также равный диаметру окружности качения катков.

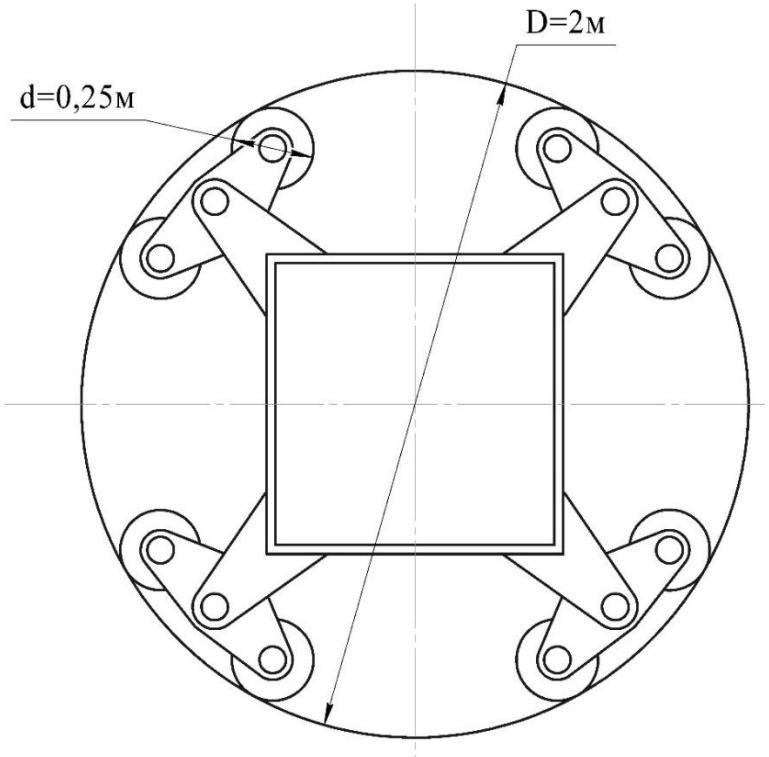

Рис. 2 Схема верхнего опорно-поворотного устройства

Таким образом, получены минимально возможные размеры зубчатого колеса, колонны и катков опорно-поворотного устройства портального крана.

Список литературы

[1] Кобзев А.П., Кобзев Р.А. Специальные краны: учебное пособие / А.П. Кобзев, Р.А. Кобзев. – Старый Оскол: ТНТ, 2014 – 472 с.

[2] Александров М. П. Грузоподъемные машины: Учебник для вузов. – М.: Издательство МГТУ им. Н. Э. Баумана – Высшая школа, 2000. – 552 с.

[3] Ермоленко В.А. Расчет механизмов грузоподъемных машин: учебное пособие / В.А. Ермоленко. – М.: Изд-во МГТУ им. Н. Э. Баумана, 2013. – 92 с.

[4] Анурьев В.И. Справочник конструктора-машиностроителя: В 3 т. Т. 1. – 8-е изд., перераб. и доп. Под ред. И.Н. Жестковой. – М.: Машиностроение, 2001 – 920 с.: ил.

[5] Официальный сайт стальные металлоконструкции гран-строй: http://gran-stroi.ru/stal-St3sp-GOST-380-2005.php (дата обращения 26.03.2017)

Голиков Антон Аркадьевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: ant1363.golikov@yandex.ru

Ермоленко Владимир Алексеевич – канд. техн. наук, доцент кафедры "Детали машин и подъемно-транспортное оборудование" КФ МГТУ им. Н.Э. Баумана. E-mail: tvermolenko@rambler.ru

А.А. Логвинов, Г.Ю. Грачев, С.Л. Заярный

РАСЧЕТНАЯ МОДЕЛЬ ДЛЯ ОПРЕДЕЛЕНИЯ НАПРЯЖЕННО-ДЕФОРМИРОВАННОГО СОСТОЯНИЯ АРМИРУЮЩИХ ЭЛЕМЕНТОВ РАСТЯНУТОГО КОМПОЗИТНОГО СТЕРЖНЯ

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

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 армирующими элементами 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) [1].

В качестве базовой расчетной модели использована модель композитного стержня, предложенная в работе [2]. В рамках решаемой задачи варьируемыми факторами являются параметры армирующих элементов: приведенный модуль упругости при растяжении; предел текучести материала; площадь поперечного сечения армирующего элемента. Приведенные модули упругости армирующих элементов являются случайными величинами, изменяющимися в установленных пределах и подчиняющимися нормальному закону распределения. Случайный характер изменения приведенного модуля упругости определяется как свойствами материала, так и особенностями технологического процесса формирования композитного стержня. Предел текучести материала, площадь поперечного сечения являются детерминированными величинами.

Растягивающее усилие является детерминированной величиной и изменятся дискретно по i уровням

$$N_i = k_i \sum_{j=1}^{n} \sigma_{ek} A_j, \qquad (1)$$

где σ_{ek}, A_j - предел текучести материала и площадь поперечного сечения j-й армирующего элемента; k_i -коэффициент запаса по нагрузке i-го уровня [2].

Диаграмма напряженно-деформированного состояния в координатах σ, ε, при упругопластическом деформировании армирующего элемента,

представлена на рис.1. На каждом расчетном цикле, соответствующем различной нагрузке, для j-го армирующего элемента проверяется условие $\sigma_j \geq \sigma_{ek}$. Справедливость этого соотношения определяет приближенную картину напряженно-деформированного состояния армирующих элементов при их деформировании за пределами упругости. При этом нелинейный участок 1 диаграммы σ, ε, аппроксимируется линейным участком 2. Такая аппроксимация, с некоторым допущением, характеризует упруго-пластического деформирования (без упрочнения) армирующего элемента. По результатам статистического моделирования строятся гистограммы и определяется изменение напряжений за пределом текучести при упруго-пластинчатом деформировании армирующих элементов для различных уровней детерминированной нагрузки (рис. 1).

Расчетная модель, составленная согласно рассмотренного алгоритма, в виде блок-схемы [3], представлена на рис. 2,3. Код программы расчета, составлена на языке Fortran [4], представлен на рис. 4,5.

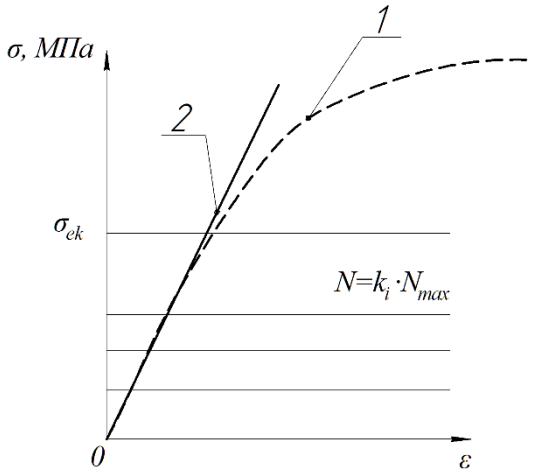

Рис. 1. График зависимости механического напряжения от относительного удлинения

В данной расчетной модели отношение относительно удлинения к напряжению является линейным (линия 2) (рис. 1.), по зависимости упругого деформирования, исключая поведение материала при пластическом деформировании (линия 1) (рис. 1.). Тем самым получая напряжения, при которых в следствии упруго-пластинчатого деформирования осуществляется перераспределение нагрузок между армирующими элементами. Изменение характеристики ε в расчетах не учитывается, деформации армирующих элементов остаются. Определяется уровень напряжений для дальнейшего расчета.

Вывод: приведенная расчетная модель и разработанная программа позволили производить моделирование напряженно-деформированного

состояния растянутого композитного стержня при упруго-пластинчатом деформировании армирующих элементов.

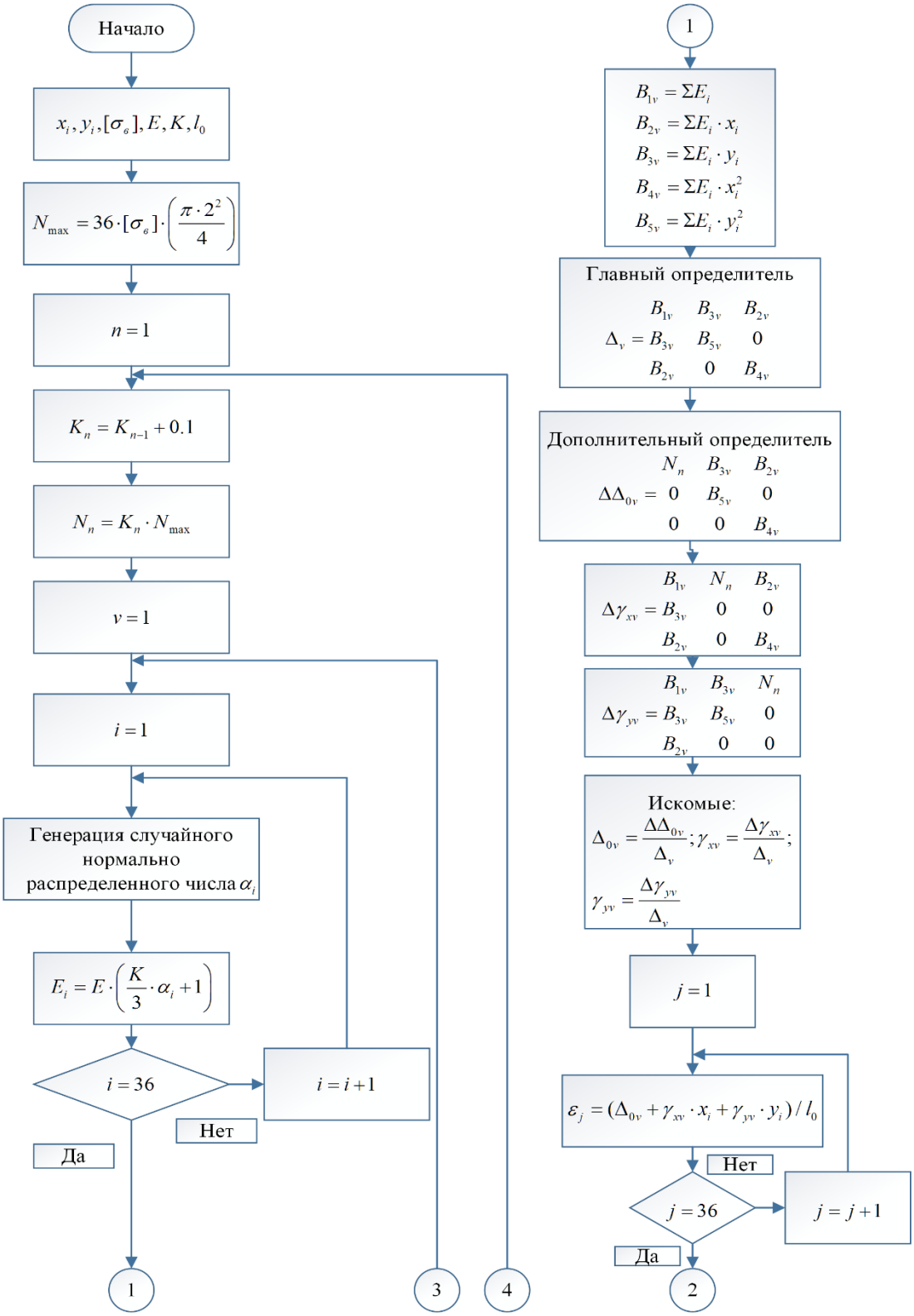

Рис. 2. Блок-схема расчетной модели

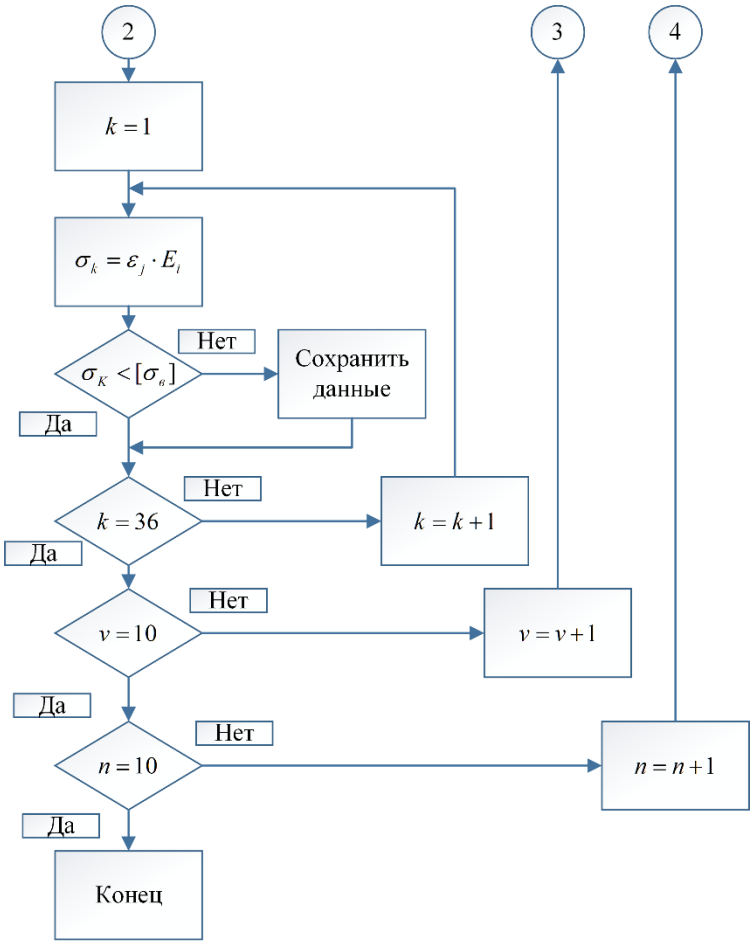

Рис. 3. Блок-схема расчетной модели (продолжение)

```
program sterzen
  real, dimension(36)::x
  data x/20,19.6962,18.7939,17.3205,15.3209,12.8558,10,6.8404,3.473,0,-3.4730,-6.8404,-10,-12.8558,-
15.3209,-17.3205,-18.7939,-19.6962,-20,-19.6962,-18.7939,-17.3205,-15.3209,-12.8558,-10,-6.8404,-
3.473,0,3.4730,6.8404,10,12.8558,15.3209,17.3205,18.7939,19.6962/
  real, dimension(36)::y
  data y/
0,3.4730,6.8404,10,12.8558,15.3209,17.3205,18.7939,19.6962,20,19.6962,18.7939,17.3205,15.3029,12.8558,10,6.
8404,3.4730,0,-3.4730,-6.8404,-10,-12.8558,-15.3209,-17.3205,-18.7939,-19.6962,-20,-19.6962,-18.7939,-
17.3205,-15.3209,-12.8558,-10,-6.8404,-3.4730/
  real, dimension(36)::Ei
  real, dimension(36)::Fj
  real, dimension(36)::Qk
  real, dimension(9)::Dv
  real, dimension(9)::Ddv
  real, dimension(9)::Dgx
  real, dimension(9)::Dgy
real, dimension(9)::pv1
  real :: Nmax, p, a,k=2.5, kn=0, E=1*10**5, L0=1000, Nn, s, B1, ADv, ADdv,ADgx,ADgy,D0v,Gx,Gy, Qb=240
  integer :: n=0
integer*2 :: s1, s2, tm(4)
real*4 r
real*8 :: Mean=0, Sigma=1 ! Требуемые средняя и стандартное отклонение.
integer, parameter :: m=10000 ! объем выборки
Nmax=36*(3.14*2**2/4)*Qb
call TIME(tm)
s1=tm(3)
s2=tm(4)
    a=1
1    kn=kn+0.1
    Nn=kn*Nmax
    a=a+1
    print *, 'Nn=', Nn
    do v=1,10
2  do i=1,36
   do j=1,m
    ! начало вычисления нормальной величины
```

Рис. 4. Код программы

```
      s=0.0
      do ki=1,12
          call randu(s1,s2,r)
          s=s+r
      end do
      s=(s-6.0)*Sigma+Mean
      ! конец вычисления нормальной величины
     end do
     p=E*((k/3)*s+1)
     Ei(i)=p
     end do
          B1=sum(Ei*((3.14*2**2)/4)/L0)
          B2=sum(Ei*x*((3.14*2**2)/4)/L0)
          B3=sum(Ei*y*((3.14*2**2)/4)/L0)
          B4=sum(Ei*x**2*((3.14*2**2)/4)/L0)
          B5=sum(Ei*y**2*((3.14*2**2)/4)/L0)
Dv=(/B1,B3,B2,B3,B5,0,B2,0,B4/)
Ddv=(/Nn,B3,B2,0,B5,0,0,0,B4/)
Dgx=(/B1,Nn,B2,B3,0,0,B2,0,B4/)
Dgy=(/B1,B3,Nn,B3,B5,0,B2,0,0/)
ADv=B1*B5*B4+0+0-B2*B5*B2-B3*B4-0
ADdv=Nn*B5*B4
ADgx=-NN*B3*B4
ADgy=-B2*B5*Nn
D0v=ADdv/ADv
Gx=ADgx/ADv
Gy=ADgy/ADv
do i=1,36
    Fj=(D0v+Gx*x+Gy*y)/L0
    Qk=Fj*Ei
                end do
          do i=1,36
    if (Qk(i)>Qb) then
    n=n+1
    pv=n
    print *, 'Q(i)=', Qk(i)
    end if
    end do
    print *, 'n=', n
    pv1=pv/36*100
               n=0
    end do
    pv=sum(pv1)/10
     print *,'veroyatnost otkaza', pv, '%'
         pause
         3   if (a<=10) then
go to 1
              end if
print *, 'konec programmi'
     PAUSE
END
```

Рис. 5. Код программы (продолжение)

Список литературы

[1] Феодосьев В. И. Сопротивление материалов: Учеб. Для вузов. - 10-е изд., перераб. И доп. - М.: Изд-во МГТУ им. Н. Э. Баумана, 1999. - 592 с..

[2] Заярный С.Л., Логвинов А.А. Определение надежности растянутого композитного стержня методом статистического моделирования – 201с. 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.

[3] Иванов Г.С. Основы программирования: Учебник для вузов. - 2-е изд., перераб. и доп. - М.: Изд-во МГТУ им. Н.Э. Баумана, 2002. ~ 416 с.

[4] Бартеньев О. В. Современный Фортран. - 3-е изд., доп. и перераб. – М.: ДИАЛОГ- МИФИ, 2000. - 449 с.

Логвинов Александр Андреевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: paradoksme@yandex.ru

Грачев Георгий Юрьевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: goshangrachev@gmail.com

Заярный Сергей Леонидович – канд. техн. наук, доцент кафедры "Детали машин и подъемно-транспортное оборудование" КФ МГТУ им. Н.Э. Баумана. E-mail: texnakon@yandex.ru

А.А. Логвинов, Г.Ю. Грачев, С.Л. Заярный

РАСЧЕТНАЯ МОДЕЛЬ ДЛЯ ОПРЕДЕЛЕНИЯ НАПРЯЖЕННО-ДЕФОРМИРОВАННОГО СОСТОЯНИЯ РАСТЯНУТОГО КОМПОЗИТНОГО СТЕРЖНЯ МЕТОДОМ ЖИВУЧЕСТИ ПРИ УСЛОВИИ ХРУПКОГО РАЗРУШЕНИЯ АРМИРУЮЩИХ ЭЛЕМЕНТОВ

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

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).

Армирующие элементы в данной модели подвергаются хрупкому разрушению. Так как не учитывается пластинчатое деформирование остается линейная зависимость, то есть упругое деформирование (рис. 1.), что характерно для хрупкого материала. Когда напряжение превышает определенный уровень можно считать элемент отказавшим, далее в системе он не учитывается.

В расчетной модели варьируемы факторами, являются параметры армирующей нити. Растягивающее усилие N_n является случайной величиной с математическим ожиданием β-го уровня $\bar{N}_\beta$. На каждом расчетном цикле i проверяется условие $\sigma \geq k \cdot \sigma_{ek}$, где $k = \frac{\sigma}{\sigma_{ek}}$, по результатам расчетов модели для определение надежности растянутого композитного стержня при упруго-пластинчатом деформировании армирующих элементов настоящего сборника. Справедливость (несправедливость) этого соотношения устанавливает факт разрушения (не разрушения) j-ой армирующей нити. В случае если на расчетном цикле i установлено, что $\sigma_{j=k} \geq \sigma_{ek}$, то на цикле $i+1$ расчет композитного стержня повторяется без изменения варьируемых параметров при условии $E_i = 0$.

При этом если на расчетном цикле $i+1$ установлено $\sigma_j \leq \sigma_{ek}$, то расчет на цикле $i+2$ повторяется как и для цикла i. Если на расчетном цикле $i+1$ установлено $\sigma_{j=k} \geq \sigma_{ek}$, то расчет на цикле $i+2$ повторяется с изменением варьируемых параметров при условии $E_i = 0$.

Отказ по условию прочности композитного стержня согласно модели потери несущей способности (разрушение) композитного стержня определяется условием $\sigma_j \geq \sigma_{ek}$, при хрупком разрушении всех армирующих нитей (рис. 1) [1].

По результатам статистического моделирования строится график зависимости количества циклов до полного разрушения от уровня нагрузки (рис. 2) и определяется вероятность отказа композитного стержня для различных уровней детерминированной нагрузки для N_n.

Расчетная модель представлена в виде блок-схемы (рис. 3, 4) [2]. Программа составлена на языке Fortran (рис. 5, 6) [3].

Вывод: приведенная расчетная модель и разработанная программа позволили производить моделирование напряженно-деформированного состояния растянутого композитного стержня методом живучести при условии хрупкого разрушения армирующих элементов.

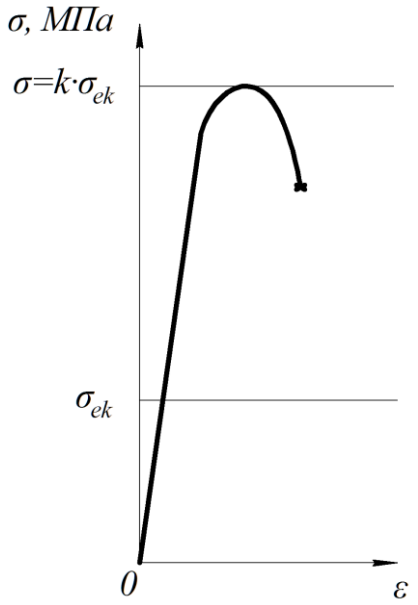

Рис. 1. Хрупкое разрушение армирующей нити

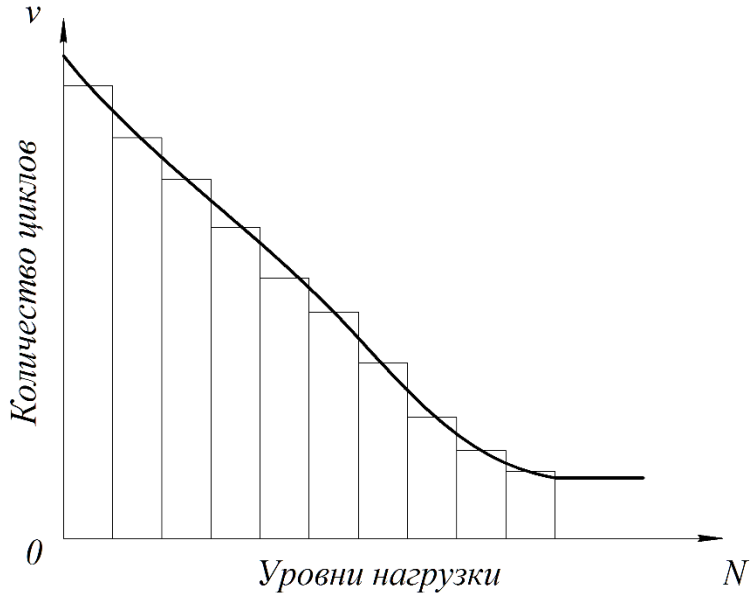

Рис. 2. График полного разрушения от уровня нагрузки

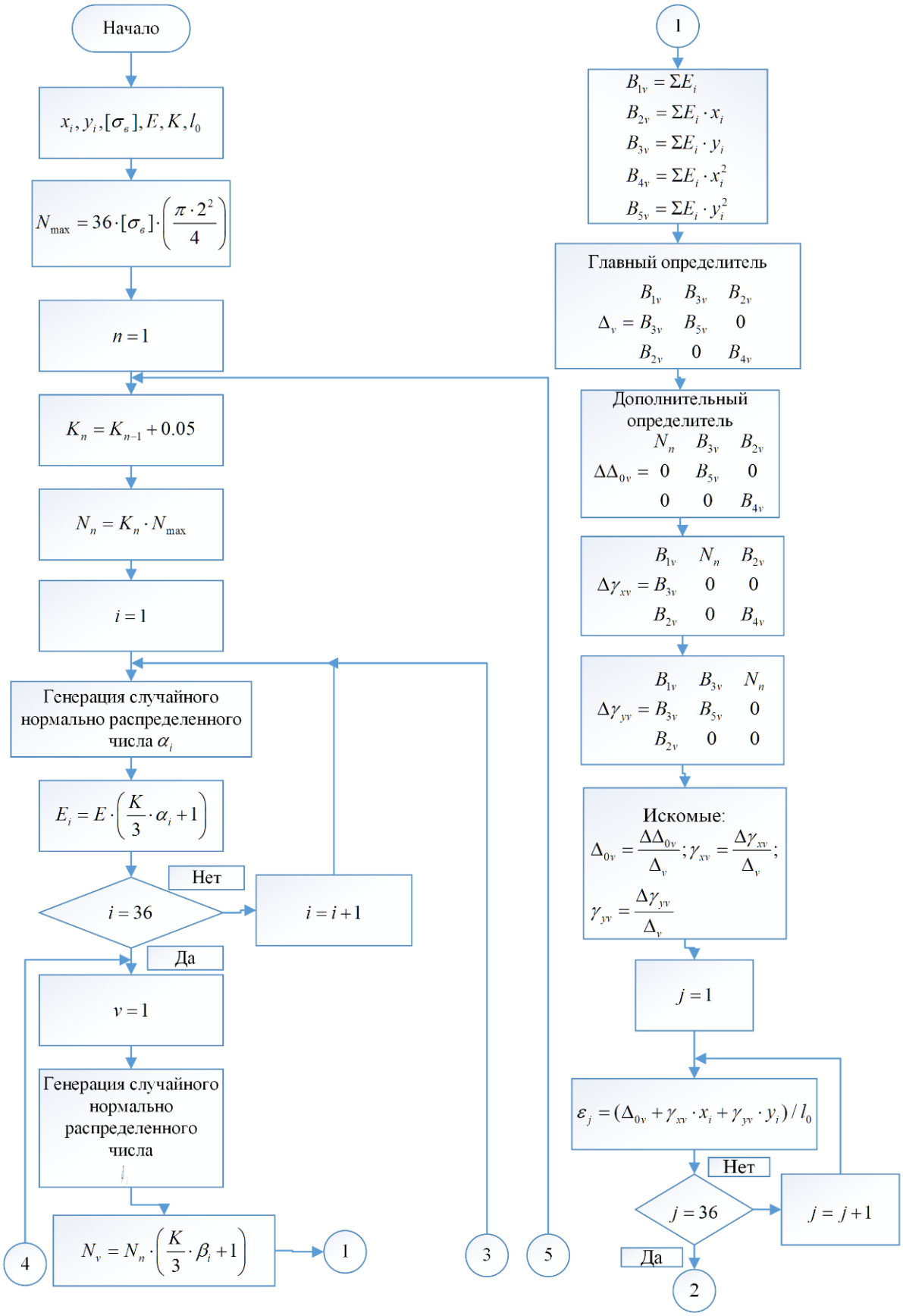

Рис. 3. Блок-схема модели живучести

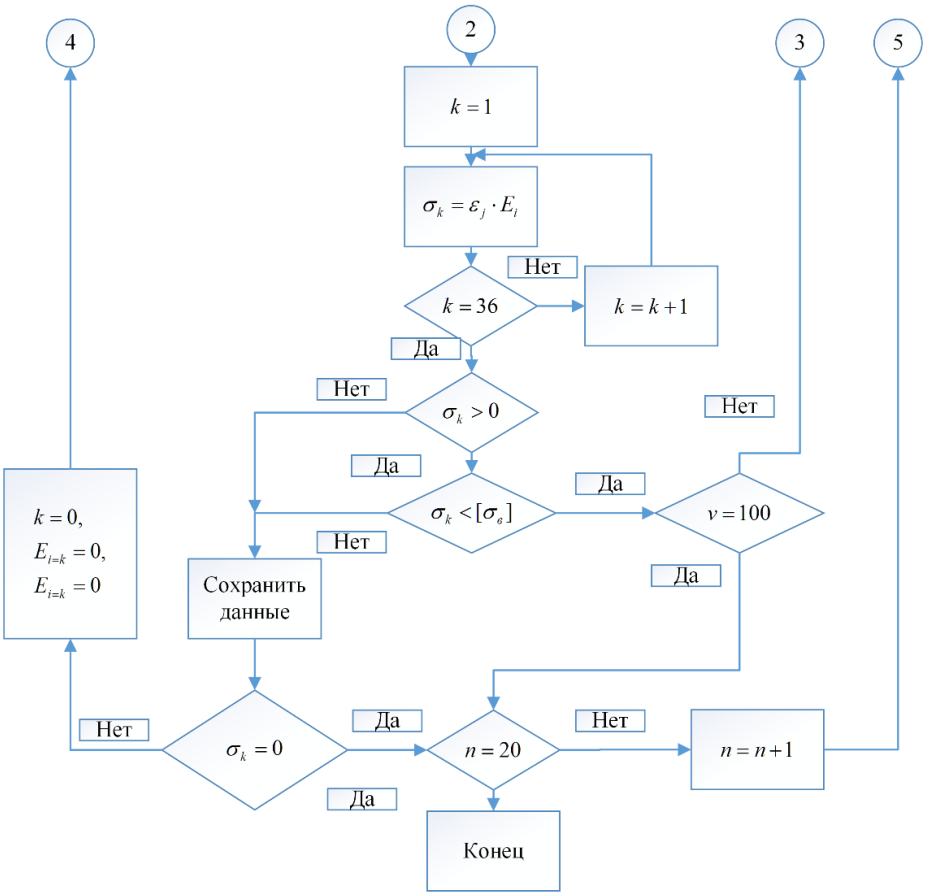

Рис. 4. Блок-схема модели живучести (продолжение)

```
program sterzen
  real, dimension(36)::x
  data x/20,19.6962,18.7939,17.3205,15.3209,12.8558,10,6.8404,3.473,0,-3.4730,-6.8404,-10,-12.8558,-15.3209,-
17.3205,-18.7939,-19.6962,-20,-19.6962,-18.7939,-17.3205,-15.3209,-12.8558,-10,-6.8404,-
3.473,0,3.4730,6.8404,10,12.8558,15.3209,17.3205,18.7939,19.6962/
  real, dimension(36)::y
  data y/
0,3.4730,6.8404,10,12.8558,15.3209,17.3205,18.7939,19.6962,20,19.6962,18.7939,17.3205,15.3029,12.8558,10,6.8404,
3.4730,0,-3.4730,-6.8404,-10,-12.8558,-15.3209,-17.3205,-18.7939,-19.6962,-20,-19.6962,-18.7939,-17.3205,-
15.3209,-12.8558,-10,-6.8404,-3.4730/
  real, dimension(36)::Ei
  real, dimension(36)::Fj
  real, dimension(36)::Qk
real, dimension(9)::Dv
real, dimension(9)::Ddv
real, dimension(9)::Dgx
  real, dimension(9)::Dgy
  real :: Nmax, p, a,k=0.5, kn=0.65, E=1*10**5, L0=1000, s,Nn,Nv, B1, ADv, ADdv,ADgx,ADgy,D0v,Gx,Gy, Qb=240,
w=0, Ky=1
integer :: n=0
integer*2 :: s1, s2, tm(4)
real*4 r
real*8 :: Mean=0, Sigma=1 ! Требуемые средняя и стандартное отклонение.
integer, parameter :: m=10000 ! объем выборки
Nmax=36*(3.14*2**2/4)*Qb
do a=1,7
        kn=kn+0.05
    Nn=kn*Nmax
call TIME(tm)
s1=tm(3)
s2=tm(4)
n=0
w=0
        print *, 'Nn=', Nn
   do i=1,36
   do j=1,m
    ! начало вычисления нормальной величины
    s=0.0
    do ki=1,12
        call randu(s1,s2,r)
        s=s+r
    end do
    s=(s-6.0)*Sigma+Mean
    ! конец вычисления нормальной величины
```

Рис. 5. Код программы

```
   end do
   p=E*((k/3)*s+1)
   Ei(i)=p
   end do
do while (n<36)
           do j=1,m
    ! начало вычисления нормальной величины
    s=0
    do ki=1,12
        call randu(s1,s2,r)
        s=s+r
    end do
    s=(s-6)*Sigma+Mean
    ! конец вычисления нормальной величины
   end do
 Nv=Nn*((k/3)*s+1)
 print *, 'Nv=', Nv
        B1=sum(Ei*((3.14*2**2)/4)/L0)
        B2=sum(Ei*x*((3.14*2**2)/4)/L0)
        B3=sum(Ei*y*((3.14*2**2)/4)/L0)
        B4=sum(Ei*x**2*((3.14*2**2)/4)/L0)
        B5=sum(Ei*y**2*((3.14*2**2)/4)/L0)
Dv=(/B1,B3,B2,B3,B5,0,B2,0,B4/)
Ddv=(/Nn,B3,B2,0,B5,0,0,0,B4/)
Dgx=(/B1,Nn,B2,B3,0,0,B2,0,B4/)
Dgy=(/B1,B3,Nn,B3,B5,0,B2,0,0/)
ADv=B1*B5*B4+0+0-B2*B5*B2-B3*B4*B3-0
ADdv=Nv*B5*B4
ADgx=-Nv*B3*B4
ADgy=-B2*B5*Nv
D0v=ADdv/ADv
Gx=ADgx/ADv
Gy=ADgy/ADv
w=w+1
    do i=1,36
    Fj=(D0v+Gx*x+Gy*y)/L0
    Qk=Fj*Ei
    end do
 Qb=Qb*Ky
 do i=1,36
if (Qk(i)>Qb)  then
   Ei(i)=0
   n=n+1
end if
if (Qk(i)<0)  then
   Ei(i)=0
   n=n+1
end if
 end do
   end do
3  print *, 'chislo ciklov=', w
   pause
               end do
        PAUSE
END
```

Рис. 6. Код программы (продолжение)

Список литературы

[1] Заярный С.Л., Логвинов А.А. Определение надежности растянутого композитного стержня методом статистического моделирования – 201с. 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.

[2] Иванов Г.С. Основы программирования: Учебник для вузов. - 2-е изд., перераб. и доп. - М.: Изд-во МГТУ им. Н.Э. Баумана, 2002. ~ 416 с.

[3] Бартеньев О. В. Современный Фортран. - 3-е изд., доп. и перераб. – М.: ДИАЛОГ- МИФИ, 2000. - 449 с.

Логвинов Александр Андреевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: paradoksme@yandex.ru

Грачев Георгий Юрьевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: goshangrachev@gmail.com

Заярный Сергей Леонидович – канд. техн. наук, доцент кафедры "Детали машин и подъемно-транспортное оборудование" КФ МГТУ им. Н.Э. Баумана. E-mail: texnakon@yandex.ru

А.А. Логвинов, Г.Ю. Грачев, С.Л. Заярный

РЕЗУЛЬТАТЫ РАСЧЕТОВ ПО РАСЧЕТНОЙ МОДЕЛИ ДЛЯ ОПРЕДЕЛЕНИЯ НАПРЯЖЕННО-ДЕФОРМИРОВАННОГО СОСТОЯНИЯ АРМИРУЮЩИХ ЭЛЕМЕНТОВ РАСТЯНУТОГО КОМПОЗИТНОГО СТЕРЖНЯ

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

В расчете композитного стержня на несущую способность главным критерием является установление условий, при которых армирующие элементы теряют свою прочность. Следует понимать при каких нагрузках конструкция станет отказывать [1].

Для избегания критический условий на практике, используется расчетно-аналитический метод, дающий возможность определить характер зависимости результатов от изменения факторов.

В данной расчетной модели отношение относительного удлинения к напряжению является линейным (линия 2) (рис. 1), по зависимости упругого деформирования, исключая поведение материала при пластическом деформировании (линия 1) (рис. 1). Тем самым получая напряжения, при которых в следствии упруго-пластинчатого деформирования осуществляется перераспределение нагрузок между армирующими элементами. Изменение характеристики ε в расчетах не учитывается, деформации армирующих элементов остаются. Определяется уровень напряжений для дальнейшего расчета [2].

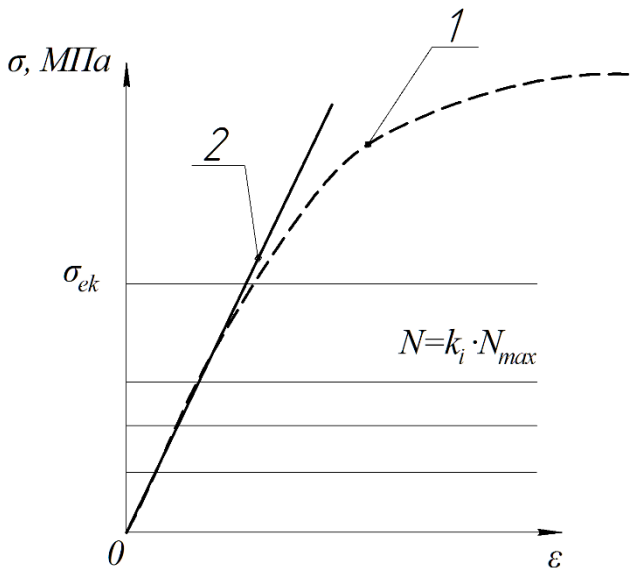

Рис. 1. График зависимости механического напряжения от относительного удлинения

На рис. 2 и 3 представлены результаты расчетов по модели для определения надежности растянутого композитного стержня при упруго-пластинчатом деформировании армирующих элементов настоящего сборника.

Где σ - напряжения превышающие предел текучести, V - выборка модулей упругости (при каждой новой выборке изменяется прочность стержня), n - число отказавших армирующих элементов.

Проведя анализ полученных данных, возможно определить отношение $k = \frac{\sigma}{\sigma_{ek}}$ для расчетов последующей модели. Получим: $k = \frac{\sigma}{\sigma_{ek}} = \frac{264}{240} = 1.1$ [3].

Вывод: полученные результаты позволили получить коэффициент увеличения напряжений при упруго-пластинчатом деформировании для расчетов нагружения стержня до его отказа.

$$N=0.9 \cdot N_{max} = 24416\ H$$

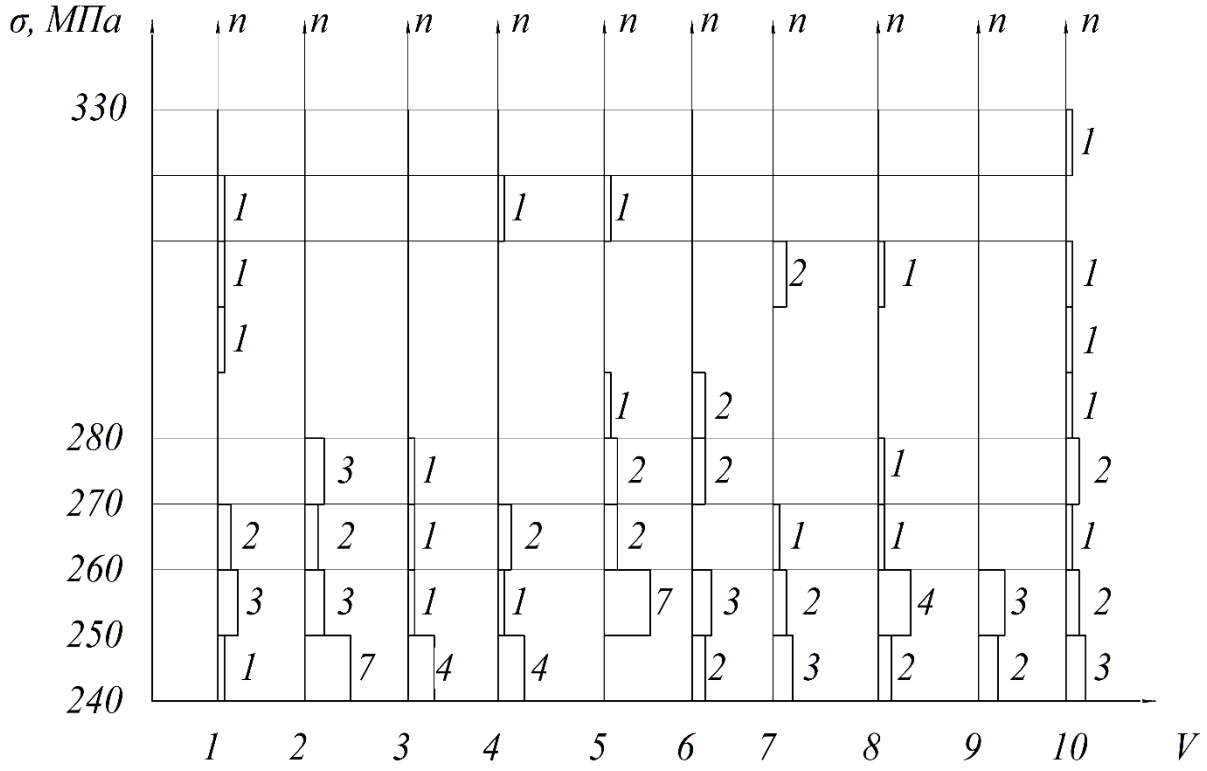

Рис. 2. Результаты отказов при нагрузке N=24416 Н

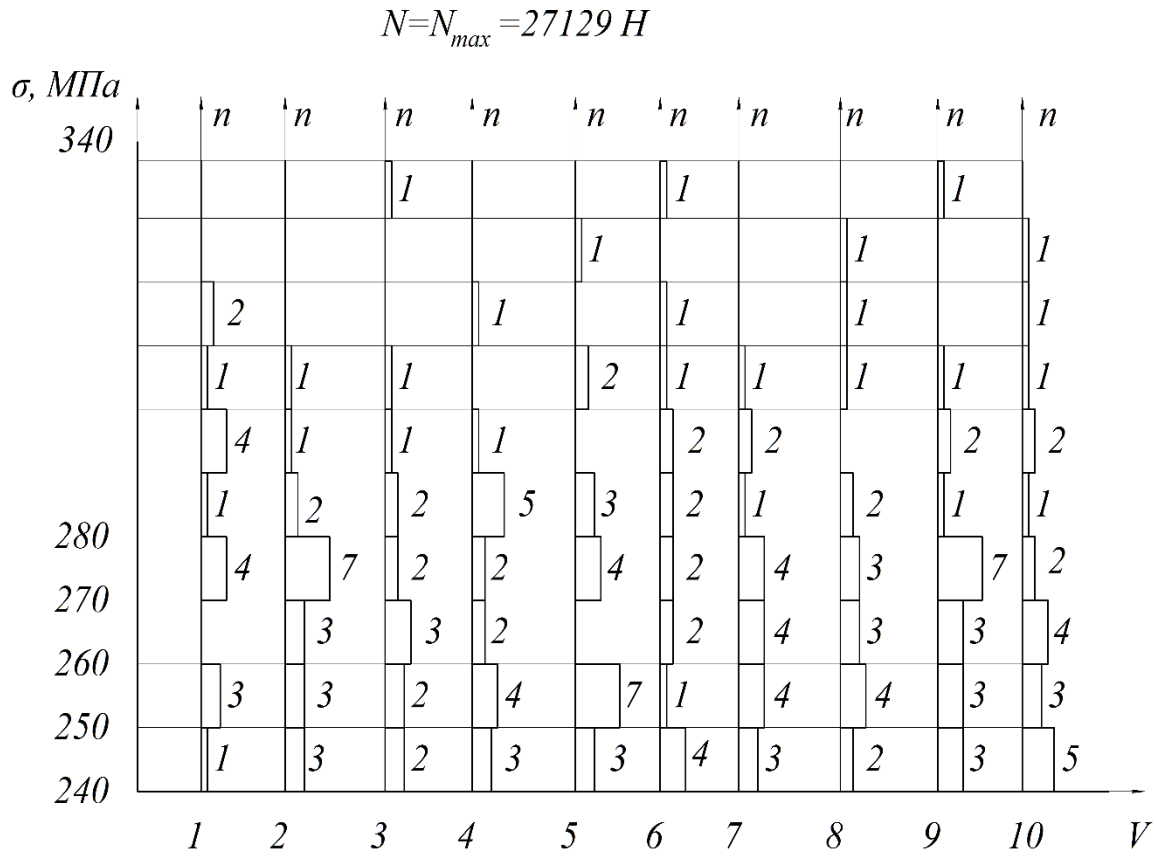

Рис. 3. Результаты отказов при нагрузке N=27129 Н

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] 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..

[3] Бартеньев О. В. Современный Фортран. - 3-е изд., доп. и перераб. – М.: ДИАЛОГ- МИФИ, 2000. - 449 с.

Логвинов Александр Андреевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: paradoksme@yandex.ru

Грачев Георгий Юрьевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: goshangrachev@gmail.com

Заярный Сергей Леонидович – канд. техн. наук, доцент кафедры "Детали машин и подъемно-транспортное оборудование" КФ МГТУ им. Н.Э. Баумана. E-mail: texnakon@yandex.ru

А.А. Логвинов, Г.Ю. Грачев, С.Л. Заярный

РЕЗУЛЬТАТЫ РАСЧЕТОВ ПО РАСЧЕТНОЙ МОДЕЛИ ДЛЯ ОПРЕДЕЛЕНИЯ НАПРЯЖЕННО-ДЕФОРМИРОВАННОГО СОСТОЯНИЯ РАСТЯНУТОГО КОМПОЗИТНОГО СТЕРЖНЯ МЕТОДОМ ЖИВУЧЕСТИ ПРИ УСЛОВИИ ХРУПКОГО РАЗРУШЕНИЯ АРМИРУЮЩИХ ЭЛЕМЕНТОВ

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

В расчете композитного стержня на несущую способность главным критерием является установление условий, при которых армирующие элементы теряют свою прочность. Следует понимать при каких нагрузках конструкция станет отказывать [1].

Для избегания критический условий на практике, используется расчетно-аналитический метод, дающий возможность определить характер зависимости результатов от изменения факторов.

В данном расчете приведены результаты надежности растянутого композитного стержня методом живучести при условии хрупкого разрушения армирующих элементов.

При напряжениях, превышающих предел текучести было выявлено за сколько циклов разрушится стержень (рис. 1). Рассматривается случай, когда рвутся армирующие элементы друг за другом. Модель классического пучка: при разрушении одного элемента нагрузка передается на элементы, которые находятся вблизи от отказавшего, передача нагрузки происходит пока не откажет стержень [2].

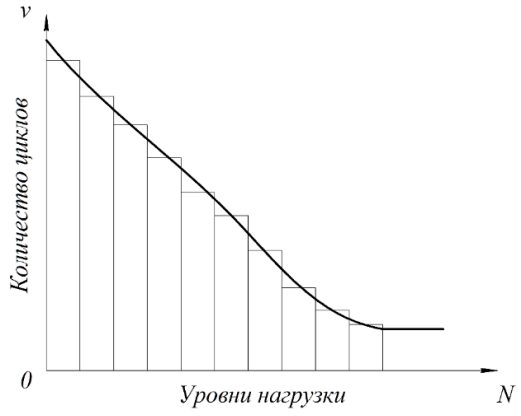

Рис. 1. График полного разрушения от уровня нагрузки

Результаты расчетов:

Нагрузка является нормально распределенной величиной для каждого нового цикла она изменяется в диапазоне.

Для нагрузки $N_n = 18990H$, $N_v = (12459...23801)H$ число циклов до полного разрушения составило $V = 21$.

Для нагрузки $N_n = 20347H$, $N_v = (17626...24386)H$ число циклов до полного разрушения составило $V = 8$.

Для нагрузки $N_n = 21703H$, $N_v = (20340...30136)H$ число циклов до полного разрушения составило $V = 3$, так как нагрузка ушла далеко от средней величины число циклов резко сократилось.

Для нагрузки $N_n = 23060H$, $N_v = (18184...25167)H$ число циклов до полного разрушения составило $V = 7$.

Для нагрузки $N_n = 24416H$, $N_v = (19058...31002)H$ число циклов до полного разрушения составило $V = 2$.

Для нагрузки $N_n = 25773H$, $N_v = (20839...25911)H$ число циклов до полного разрушения составило $V = 4$.

Для нагрузки $N_n = N_{\max} = 27129H$, $N_v = (20353...27129)H$ число циклов до полного разрушения составило $V = 3$ [3].

Результаты представлены на рис. 2.

Вывод: результаты позволили получить наглядное представление об состоянии напряженно-деформированного растянутого композитного стержня методом живучести при условии хрупкого разрушения армирующих элементов.

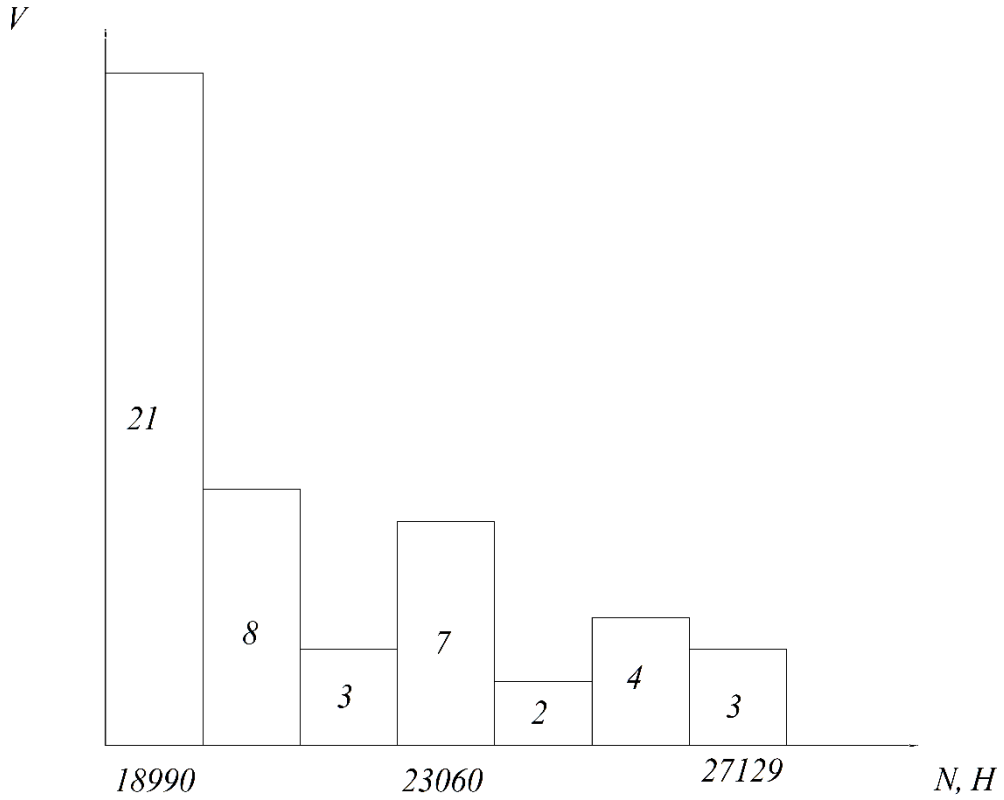

Рис. 2. График зависимости циклов до полного разрушения от уровня нагрузки

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] 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..

[3] Бартеньев О. В. Современный Фортран. - 3-е изд., доп. и перераб. – М.: ДИАЛОГ- МИФИ, 2000. - 449 с.

Логвинов Александр Андреевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: paradoksme@yandex.ru

Грачев Георгий Юрьевич – студент КФ МГТУ им. Н.Э. Баумана. E-mail: goshangrachev@gmail.com

Заярный Сергей Леонидович – канд. техн. наук, доцент кафедры "Детали машин и подъемно-транспортное оборудование" КФ МГТУ им. Н.Э. Баумана. E-mail: texnakon@yandex.ru

М.А. Качан, А.А. Шубин

ЭКСПЕРИМЕНТАЛЬНОЕ ОПРЕДЕЛЕНИЕ ОПТИМАЛЬНОЙ ТЕМПЕРАТУРЫ РЕЗАНИЯ С ПОМОЩЬЮ СРЕЗНЫХ ТЕРМОПАР

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

На данный момент весьма актуальной проблемой эксплуатации подъемных кранов являются повреждения и износ их ходовых частей. В частности, при интенсивной работе механизма передвижения имеет место сильный износ 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. Нагрузки, которым подвергается каждый участок поверхности катания колеса, особенно во время начала движения и при остановке, 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.

Изношенный профиль поверхности катания колес характеризуется переменной величиной припуска на обработку, а также изменением физико-механических свойств металла вдоль обрабатываемой поверхности. Влияние этих факторов крайне пагубно сказываться на режущем инструменте, вследствие чего технологический процесс имеет ряд особенностей.

Одним из основных критериев, характеризующих обрабатываемость материала, является скорость резания, допускаемая режущим инструментом при определенной стойкости и других постоянных параметрах. В настоящее время для определения обрабатываемости используются различные методы, которые, тем не менее, несовершенны, а использование их ограничено. Их основными недостатками являются большая продолжительность во времени, а также низкая точность. С целью разрешения дан-

ных проблем был проведен ряд экспериментальных исследований, в ходе которых была установлена такая зависимость между скоростью резания и остаточными напряжениями на обработанной поверхности, что максимум остаточных сжимающих напряжений соответствует оптимальной скорости резания (Рис. 1) Это позволило разработать способ определения оптимальной скорости резания для колесных сталей.

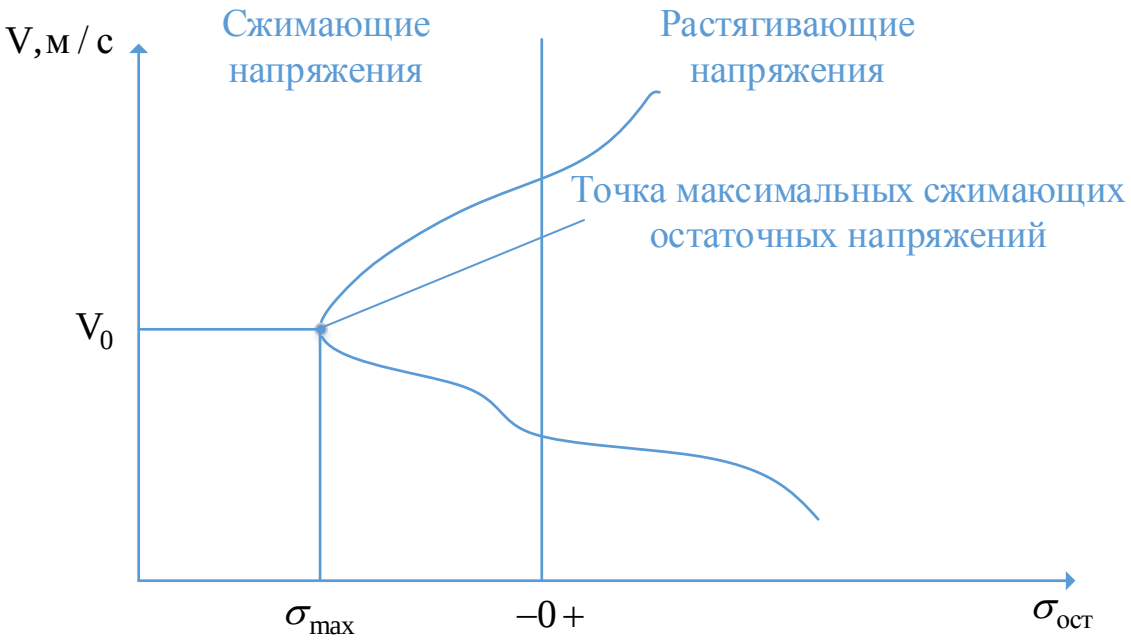

Рис. 1 Определение оптимальной скорости резания по остаточным напряжениям

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. Для проведения исследований была создана экспериментальная установка (Рис.2). Величина остаточных напряжений определялась электромагнитным прибором ЭРИОН-1Б. Анализ результатов проводился с помощью цифрового осциллографа, а также видеографического самописца. Кроме того, была предусмотрена возможность снимать приблизительные показания температуры в зоне резания с помощью искусственной хромель-алюмелевой термопары, расположенной непосредственно в резце. Однако, такое расположение термопары не позволило объективно оценить фактическую температуру резания.

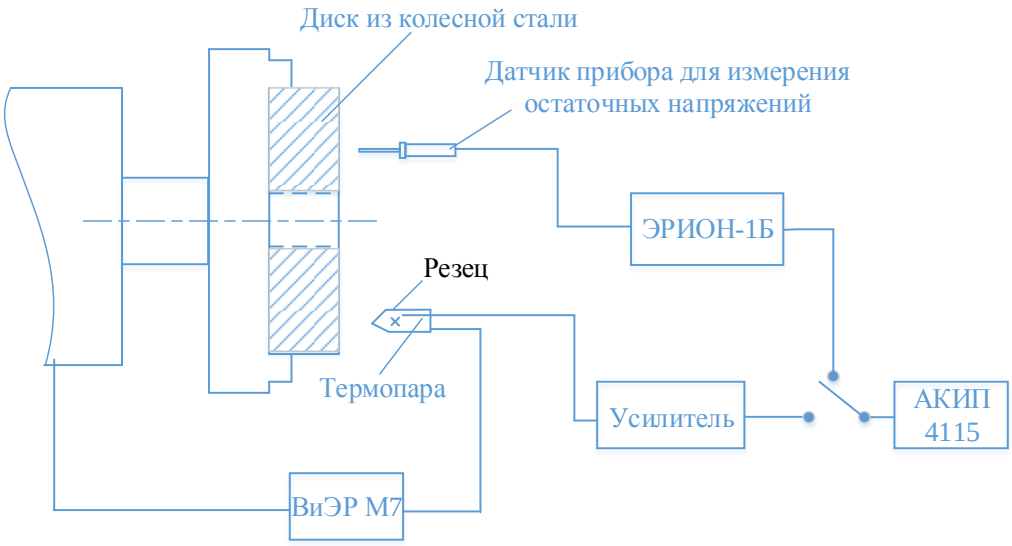

Рис. 2 Схема экспериментальной установки для определения оптимальной скорости резания

Основной задачей оптимизации процесса резания для повышения стойкости инструмента представляет собой использование таких режимов, при которых износ инструмента был бы сведен к минимуму. В результате большого числа экспериментальных исследований, температур в зоне резания, было установлено, что для каждой пары обрабатываемый материал - инструментальный материал существует так называемая оптимальная температура резания [3]. При этой температуре, износ инструмента минимален, на обрабатываемой поверхности реализуются максимальные сжимающие напряжения, а сила резания стабилизирована на минимальном значении. Из этого следует, что критерием оптимизации технологического процесса может также служить температура в зоне резания. Изменяя значение этой температуры в определенном диапазоне за счет регулировки подачи или скорости резания, можно считать процесс обработки оптимальным, что создает предпосылки для разработки адаптивной системы управления процессом резания. Для создания подобных систем, необходимо знать абсолютное значение оптимальной температуры резания для конкретной пары обрабатываемый материал – инструментальный материал.

Для экспериментального определения оптимальной температуры резания при обработке колесных сталей был предложен 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 резец – диск для дальнейшего сравнения результатов [4].

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. В процессе резания, рабочие элементы термопары срезаются.

Особенностью срезной термопары является то, что ее спай выполнен на некоторое расстояние, а не в виде шарика как в искусственной термопаре. Срезные термопары перед установкой тарируют при различной величине спая. Экспериментальное определение оптимальной температуры резания и соответствующее ей значение термо-ЭДС естественной термопары производится на установке (Рис. 3) Значения термо-ЭДС срезных термопар фиксируется с помощью цифрового осциллографа АКИП 4115, а естественной – с помощью видеографического самописца ВиЭР – М7

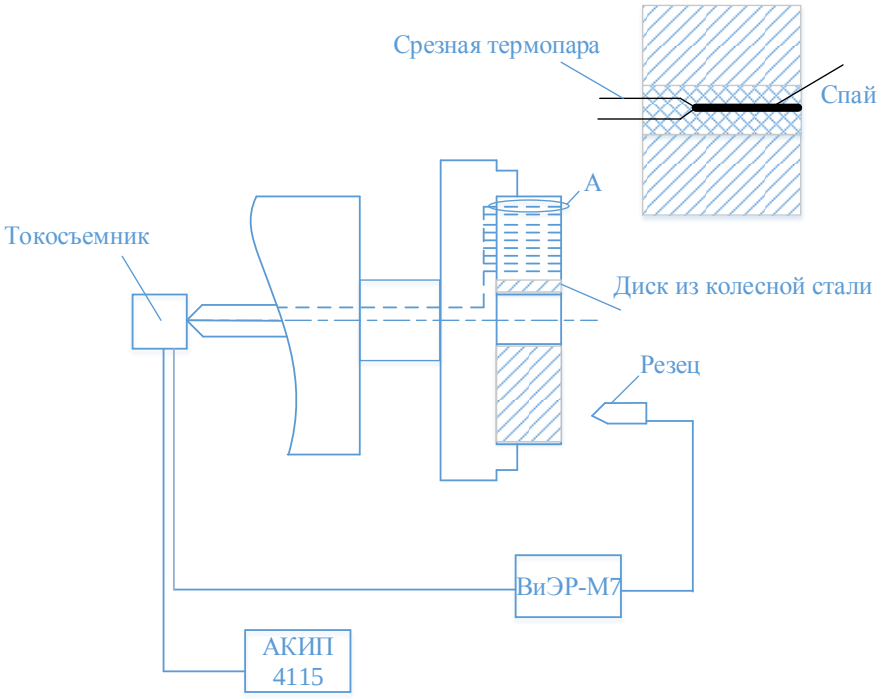

Рис. 3 Схема установки для определения оптимальной температуры резания

После проведения эксперимента, при помощи прибора ЭРИОН – 1Б определялась точка с максимальными сжимающими остаточными напряжениями. По результатам исследований строились графики зависимости значений температуры, полученных при помощи естественной и срезной термопар соответственно, а также зависимости остаточных напряжений от расстояния по радиусу диска. По значению максимальных сжимающих остаточных напряжений графически определялось абсолютное значение оптимальной температуры резания как показано на рис. 4.

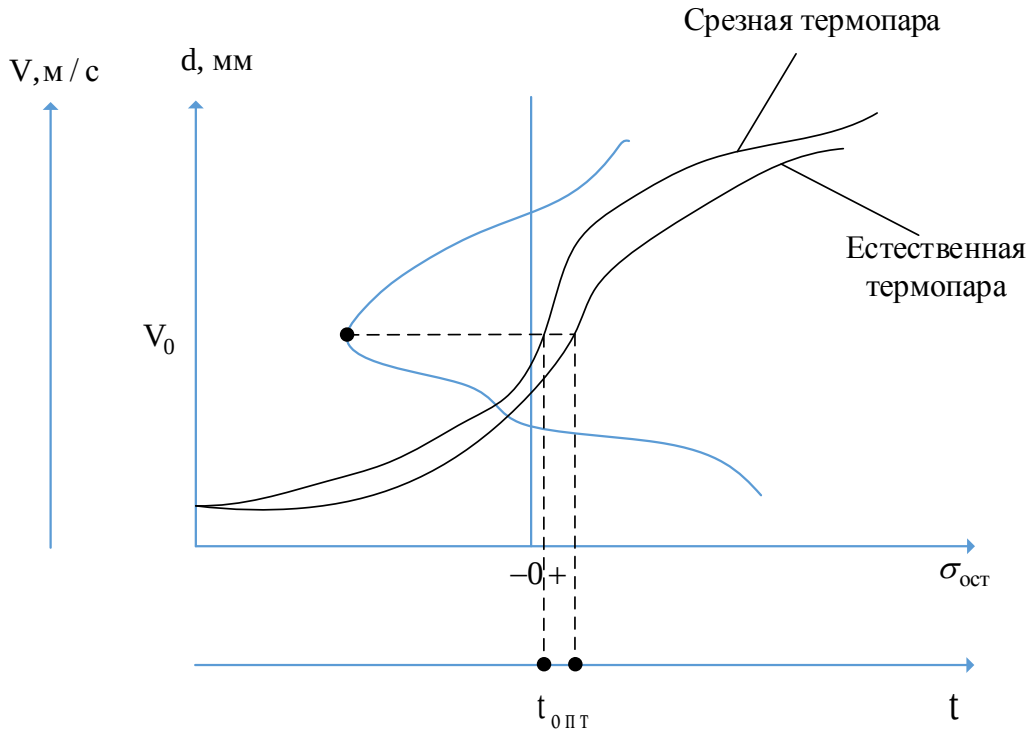

Рис. 4 Графический способ определения оптимальной температуры резания

Зная значение оптимальной температуры резания и соответствующее ей значение термо – ЭДС естественной термопары, можно реализовать систему адаптивного управления, поддерживающее это значение в определенном диапазоне.

В результате исследований был предложен принципиально новый способ экспериментального определения оптимальной температуры резания с использованием срезных термопар, что в перспективе позволит реализовать адаптивные системы управления процессами резания по температурному критерию.

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.

[4] Качан М.А., Шубин А.А. Оптимизация процесса восстановления профиля поверхности катания колес кранов. Всероссийская научно – техническая конференция 2016. Калуга, 15 – 17 ноября 2016 г., КФ МГТУ им. Н.Э. Баумана. – Калуга: МГТУ им. Н.Э. Баумана, 2016, с 204 - 207

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

СОДЕРЖАНИЕ

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

Материалы
Региональной 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 20.04.2017.
Формат 60x90/16. Печать офсетная. Бумага офсетная. Гарнитура «Таймс».
Печ. л. 15,25. Усл. п. л. 14,18. Заказ № 70

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