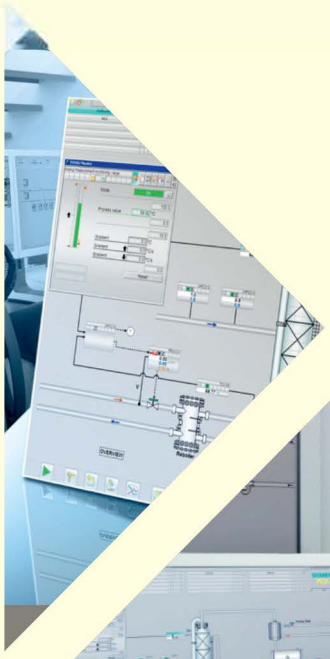
ISSN online 2658-6436

№ 3 (5)
2019



Научно-технический журнал

Автоматизация и моделирование

в проектировании и управлении

АВТОМАТИЗАЦИЯ И МОДЕЛИРОВАНИЕ в проектировании и управлении

НАУЧНО – ТЕХНИЧЕСКИЙ ЖУРНАЛ

Издается с 2018 года **№ 3(05), 2019**

Сетевое издание

Выходит 1 раз в квартал

Учредитель издания – федеральное государственное бюджетное образовательное учреждение высшего образования

«Брянский государственный технический университет» (БГТУ)

Адрес редакции:
241035, г. Брянск, бульвар 50 лет Октября, 7
тел.: (4832) 56-49-90
Адрес размещения: https://aimpu.ru
E-mail: aim-pu@mail.ru

Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).
Свидетельство о регистрации средства массовой информации Эл № ФС77-73848 от 05 октября 2018 года

ISSN online: 2658-6436

Журнал включен в специализированный референтный библиографический сервис Crossref

Журнал публикует основные результаты научных исследований по специальностям:

05.13.06 – Автоматизация и управление технологическими процессами и производствами
05.13.10 – Управление в социальных и экономических системах
05.13.12 – Системы автоматизации проектирования
05.13.18 – Математическое моделирование, численные методы и комплексы программ

AUTOMATION AND MODELING

in design and managment

SCIENTIFIC TECHNICAL JOURNAL

Issued since 2018 **№ 3(05), 2019**

Online edition

Published once a quarter

The founder of the publication –the Federal state budgetary educational institution of higher education **«Bryansk State Technical University» (BSTU)**

Address of edition 7, 50 Yearsof October Avenue, Bryansk, Russia, 241035
Tel.: (4832) 56-49-90
Accommodation address: https://aimpu.ru
E-mail: aim-pu@mail.ru

The Journal is registered by the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications of Russian Federation (ROSKOMNADZOR). Registration certificate Эл № ФС77-73848 of October 05, 2018

ISSN online: 2658-6436

Journal is included in a specialized consultant bibliographical service CrossRef

СОДЕРЖАНИЕ

Математическое моделирование, численные методы и комплексы программ

Управление в социальных и экономических системах

Автоматизация и управление технологическими процессами и производствами, системы автоматизации проектирования

CONTENTS

Mathematical modeling, numerical methods and program complexes

Management in social And economic systems

Automation and control of technological processes and production, automated design systems

УДК: 004.93'11
DOI: 10.30987/article_5d8d113d478348.62159890

Е.А. Леонов, Ю.А. Леонов, А.В. Аверченков, Ю.М. Казаков, А.С.Зуева

МЕТОД РАСПОЗНАВАНИЯ НА ИЗОБРАЖЕНИЯХ ОБЪЕКТОВ ЭЛЛИПТИЧЕСКИХ ФОРМ

В статье кратко описана методика и предложен метод для распознавания на изображениях любых объектов, которые должны иметь эллиптическую форму. Данный метод универсален и может быть применен в любых интеллектуальных системах распознавания, например, дорожных знаков с изображений видеокамер. Преимуществом предложенного метода является высокая скорость работы и стойкость к ошибкам за счет значительного уменьшения размерности исходных данных подаваемых на нейронную сеть.

Ключевые слова: *методы анализа данных; системы распознавания изображений; поиск геометрических примитивов; искусственные нейронные сети.*

E.A. Leonov, Y.A. Leonov, A.V. Averchenkov, Y.M. Kazakov, A.S. Zueva

RECOGNITION METHOD OF ELLIPTIC FORMS OBJECTS ON THE IMAGES

The article briefly describes the methodology and suggests the method for recognizing any elliptic forms objects on the images. This method is universal and can be applied in any intelligent recognition systems, for example, recognition system of the road signs from video camera images. The advantages of the proposed method are high speed and resistance to errors due to a significant reduction in the dimension of the source data supplied to the neural network.

Keywords: *data analysis methods, image recognition systems, search for geometric primitives, artificial neural networks.*

Введение

Поиск геометрических примитивов на изображениях широко используются в интеллектуальных системах распознавания изображения как промежуточная стадия получения исходных данных для последующего анализа, либо для уточнения области дальнейшего распознавания [1]. Так, например, для распознавания дорожных знаков в видео потоке более оптимальным является распознавать только изображения, находящиеся внутри объектов, имеющих геометрические формы: круга, треугольника, квадрата и пр. Также следует отметить, что на реальных изображениях данные фигуры могут быть значительно искажены в связи с углом их съемки и проекцией. Так круг будет чрезвычайно редко представлен в данном виде и почти всегда представляется в виде эллипса, границы которого достаточно сильно размыты и имеют неправильную форму.

Применение классических методик распознавания изображений, использующих сверточные и рекуррентные нейронные сети [2], а также другие сети для классификации в задачах распознавания простых геометрических примитивов крайне неэффективны и требуют значительных вычислительных ресурсов, особенно при больших размерах

изображений или поточного видео. Более правильным подходом является обработка изображения и поиск замкнутых контуров, удовлетворяющих необходимым условиям.

Поиск примитивов в изображении предлагаемым методом можно разбить на четыре основных этапа: обработка изображения и приведение его к бинарной карте, поиск контуров по бинарной карте, поиск примитивов в массиве контуров, фильтрация набора найденных примитивов.

1. Определение контуров

Так как анализ цветов изображений не производится, для ускорения работы и упрощения алгоритмов изображение переводится в оттенки серого. Далее используется уже ставший классическим алгоритм Джона Кенни (John Canny) [3]. Данный алгоритм сначала сглаживает изображение, чтобы устранить шум и находит градиент изображения, чтобы подсветить области с высокими пространственными производными. После чего алгоритм проходит по этим областям и подавляет все пиксели, которые не в максимуме (не максимальное подавление). После чего градиентный массив уменьшается гистерезисом, который используется, чтобы отследить оставшиеся пиксели, которые не были подавлены. Гистерезис использует два порога и если величина ниже первого порога, то она устанавливается в ноль (делается не краевой). Если величина выше высокого порога, она делается краевой. В том случае если нет пути от текущего пиксела к пикселю с градиентом выше второго порога, и если величина яркости пикселя находится между двумя порогами, то она устанавливается в ноль. В результате преобразований получаем бинарную карты изображений.

Далее осуществляется поиск контуров границ и при этом используется алгоритм Судзуки (Suzuki, S.) [4]. При анализе используется небольшая модификация оригинального алгоритма, использующая аппроксимацию линий для замыкания контуров. Далее выбирались только замкнутые контуры, имеющие более семи линий с заданной пропорцией общей площади контура по отношению ко всему изображению.

2. Определение эллиптических объектов

Основным этапом обработки изображения является непосредственно определение является ли замкнутый контур относительно правильным эллипсом. Для этого создается массив уникальных точек $P = \langle X, Y \rangle$, образующих контур. В данном массиве находятся минимальные и максимальные координаты точек по обеим осям:

$$X_{\min} \le \forall x \in X, \quad X_{\max} \ge \forall x \in X,$$
$$X_{\min} \le y \in Y, \quad Y_{\max} \ge \forall y \in Y.$$

Таким образом, находится прямоугольник, описывающий предполагаемый эллипс (рис. 1). Стороны прямоугольника, разделенные пополам $a = (X_{\max} - X_{\min}) / 2$ и $b = (Y_{\max} - Y_{\min}) / 2$, являются также полуосями искомого эллипса. Данное утверждение правомерно, так как началом координат всегда является верхний левый угол изображения, следовательно, все координаты положительны. Центр данного прямоугольника, при этом является центром предполагаемого эллипса.

Далее, используя стандартную формулу эллипса в декартовых координатах, и выражая большую и малую полуось через имеющиеся координаты, получаем следующую зависимость для определения любой точки эллипса:

$$\left(\frac{X_{\min} + a - x}{a}\right)^2 + \left(\frac{Y_{\min} + b - y}{b}\right)^2 = 1, \quad \forall x \in X, \quad \forall y \in Y.$$

Однако данная зависимость является уравнением, что требует жесткого выполнения условия равенства. Так как на практике контур практически никогда не может быть

рассчитан по битовой карте точно, то необходимо расширить зависимость. Предлагается сделать это двумя различными способами в зависимости от требуемой скорости алгоритма и его точности. Если требуется обеспечить наивысшую скорость работы, пожертвовав точностью (как показывает практика не значительной), то наиболее простым является создание системы неравенств, при удовлетворении которой точка, могла бы быть признана принадлежащей эллипсу.

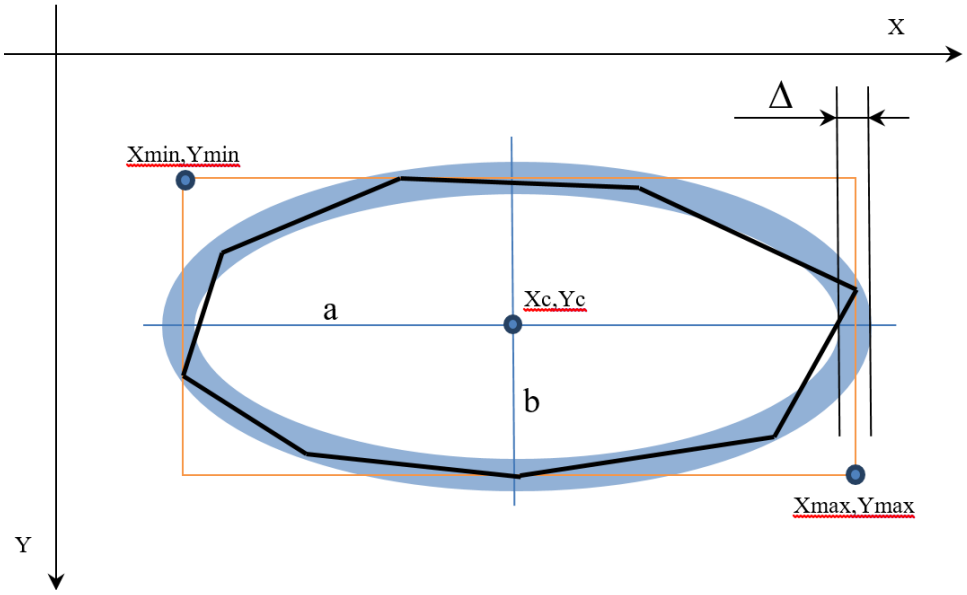


Рис. 1. Схема с основными параметрами эллипса

Введем допуск на искажение формы эллипса Δ = max (a, b,) / 12 , характеризующий расстояние до математической границы

$$\begin{cases} \left(\frac{X_{\min}+a-x}{a+\Delta/2}\right)^2+\left(\frac{Y_{\min}+b-y}{b+\Delta/2}\right)^2<1 \\ \left(\frac{X_{\min}+a-x}{a-\Delta/2}\right)^2+\left(\frac{Y_{\min}+b-y}{b-\Delta/2}\right)^2>1 \end{cases}$$

Описанная система неравенств определяет принадлежит ли точка p = {x, y} массива P эллипсу с границами в крайних точках и толщиной контура Δ в 12 раз меньшей, чем наибольшая ось эллипса.

Проверяем все точки исследуемого контура на выполнение системы неравенств. В случае если каждая точка, образующая контур удовлетворяет системе неравенств, считаем контур эллипсом с полуосями a и b и центром в точке {$X_{\min}$ + a, $Y_{\min}$ + b}. В случае, если a = b ± Δ/2, эллипс считаем окружностью с радиусом r = (a + b) / 2 и с центром в той же точке.

Определение условий съемки и реконструкция возможной окружности по эллипсу являются отдельной задачей и данной статье не рассматриваются, но для ее решения исходными данными могут быть как изменение найденного эллипса в последовательности кадров (съемка в движении), так и по статическим изображениям ориентируясь на других искажениях и артефактах изображения.

В случае если необходимо обеспечить большую точность определения, то для этого можно использовать обыкновенный полносвязный многослойный персептрон всего с тремя входами и двумя выходами. На вход можно подавать количество вершин в анализируемом контуре, средневзвешенное отклонение от центра между эллипсами минимума и максимума

$$\delta = \left(\frac{X_{\min} + a - x}{a - \Delta/2} \right)^2 + \left(\frac{Y_{\min} + b - y}{b - \Delta/2} \right)^2$$

и дельту между размерами полуосей $|a - b|$, так как практика показывает, что размер вылета за норму найденных точек контура зависит от пропорций эллипса.

Заключение

Предлагаемый метод хорошо себя зарекомендовал при решении различных практических задач, таких как поиск знаков на фотографиях [5], обнаружение окружностей на диаграммах и схемах [6], поиск границ овалов лиц и др. Основным достоинством метода является его чрезвычайная простота реализации, а также высокая скорость работы, что позволяет применять его не только на современных стационарных компьютерах, но и мобильных устройствах с низкой вычислительной мощностью. При корректном использовании для изображений имеющих четкие контрастные границы эллиптических объектов и имеющие незначительный угол наклона к границам изображения, метод имеет приемлемо низкое количество ошибок и может эффективно применяться на предварительных стадиях распознавания изображений.

Список литературы:

1. Prasad, D.K. Geometric primitive feature extraction – concepts, algorithms, and applications [Ph.D. thesis] / D.K. Prasad. – Singapore: School of Computer Engineering, Nanyang Technological University, 2012. – pp. 333.
2. Liang, M. Recurrent convolutional neural network for object recognition / X. Hu, M. Liang // 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). – Boston, MA, USA: IEEE, 2015. – pp. 3367-3375.
3. Canny, J.F. A computational approach to edge detection / J.F. Canny // Readings in computer vision: issues, problems, principles, and paradigms. – San Francisco, CA, USA: Morgan Kaufmann Publishers Inc, 1987. – pp. 184-203.
4. Suzuki, S. Topological structural analysis of digitized binary images by border following / S. Suzuki, K. Be // Computer Vision, Graphics and Image Processing. – Amsterdam: Elsevier, 1985. – № 30 (1). – pp. 32-46.
5. Dataset [Электронный ресурс]: German Traffic Sign Benchmarks. Режим доступа: http://benchmark.ini.rub.de/?section=gtsrb&subsection=dataset#Downloads
6. Леонов, Е.А. Формализация процесса мониторинга информации в сети Интернет при создании предметно-ориентированных хранилищ данных: дис. … канд. техн. наук: 05.13.01: защищена 28.12.11 [Место защиты: Волгоградский государственный технический университет, Волгоград] / Леонов Евгений Алексеевич. – Брянск: Брянский государственный технических университет, 2012. – 198 с.

References:

1. Prasad, D.K. Geometric primitive feature extraction – concepts, algorithms, and applications [Ph.D. thesis] / D.K. Prasad. – Singapore: School of Computer Engineering, Nanyang Technological University, 2012. – pp. 333.
2. Liang, M. Recurrent convolutional neural network for object recognition / X. Hu, M. Liang // 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). – Boston, MA, USA: IEEE, 2015. – pp. 3367-3375.
3. Canny, J.F. A computational approach to edge detection / J.F. Canny // Readings in computer vision: issues, problems, principles, and paradigms. – San Francisco, CA, USA: Morgan Kaufmann Publishers Inc, 1987. – pp. 184-203.
4 Suzuki, S. Topological structural analysis of digitized binary images by border following / S. Suzuki, K. Be // Computer Vision, Graphics and Image Processing. – Amsterdam: Elsevier, 1985. – № 30 (1). – pp. 32-46.
5. Dataset [Electronic resource]: German Traffic Sign Benchmarks. Access mode: http://benchmark.ini.rub.de/?section=gtsrb&subsection=dataset#Downloads.
6. Leonov, E.A. Formalization of the information monitoring on the Internet process in creating domain-specific data warehouses: PhD in Engineering Sciences thesis: 05.13.01: defended 28.12.11 [Volgograd State Technical Univercity, Volgograd] / Leonov Evgeny Alekseevich. – Bryansk: Bryansk State Technical Univercity, 2012. – 198 p.

Статья поступила в редколлегию 10.06.19.
Рецензент: д.т.н., доцент,
Брянский государственный технический университет
Захарова А.А.
Статья принята к публикации 28.06.19.

Сведения об авторах

Леонов Евгений Алексеевич
Кандидат технических наук,
Доцент каф. «Компьютерные технологии и системы»
ФГБОУ ВО «Брянский государственный технический университет»
тел.: 8-952-960-60-01
E-mail: johnleonov@gmail.com

Леонов Юрий Алексеевич
Кандидат технических наук, доцент,
Доцент каф. «Компьютерные технологии и системы»
ФГБОУ ВО «Брянский государственный технический университет»
тел.: 8-952-960-60-03
E-mail: yorleon@yandex.ru

Аверченков Андрей Владимирович
Доктор технических наук, доцент,
Профессор каф. «Компьютерные технологии и системы»
ФГБОУ ВО «Брянский государственный технический университет»
тел.: 8-903-868-58-55
E-mail: mahar@mail.ru

Казаков Юрий Михайлович
Кандидат технических наук, доцент,
Доцент каф. «Компьютерные технологии и системы»
ФГБОУ ВО «Брянский государственный технический университет»
тел.: 8-953-283-92-42
E-mail: kym2000@yandex.ru

Зуева Анастасия Сергеевна
Студент специальности «Информационно-аналитические системы безопасности»
ФГБОУ ВО «Брянский государственный технический университет»
тел.: 8-980-309-50-60
E-mail: nastermaster@yandex.ru

Information about authors:

Leonov Evgeny Alekseevich
Candidate of Technical Sciences,
Associate Professor of the department «Computer technologies and systems»
FSBEI HE «Bryansk State Technical University»
tel.: 8-952-960-60-01
E-mail: johnleonov@gmail.com

Leonov Yuri Alekseevich
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the department «Computer technologies and systems»
FSBEI HE «Bryansk State Technical University»
tel.: 8-952-960-60-03
E-mail: yorleon@yandex.ru

Averchenkov Andrey Vladimirovich
Doctor of Technical Sciences, Associate Professor,
Professor of the department «Computer technologies and systems»
FSBEI HE «Bryansk State Technical University»
tel.: 8-903-868-58-55
E-mail: mahar@mail.ru

Kazakov Yuri Mikhailovich
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the department «Computer technologies and systems»
FSBEI HE «Bryansk State Technical University»
tel.: 8-953-283-92-42
E-mail: kym2000@yandex.ru

Zueva Anastasia Sergeevna
Student of specialty «Information and analytical systems of security»
FSBEI HE «Bryansk State Technical University»
tel.: 8-980-309-50-60
E-mail: nastermaster@yandex.ru

УДК: 004.056
DOI: 10.30987/article_5d8d113d6e9f18.01574772

М.Ю. Рытов, И.В. Луценко, П.С. Цвинкайло

РАЗРАБОТКА ПОЛИТИКИ БЕЗОПАСНОСТИ НА МАЛОМ ПРЕДПРИЯТИИ С ПОМОЩЬЮ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

В статье рассматривает поиск оптимальной политики безопасности информационной системы малого предприятия с помощью модели полного перекрытия. С помощью реализованной автоматизированной модели можно быстро и качественно найти нужный набор барьеров защиты за определенные затраты.

Ключевые слова: *оптимальный набор, комплексная защита информации, малое предприятия, моделирование.*

M. Yu. Rytov, I. V. Lutsenko, P. S. Svincolo

SECURITY POLICY DEVELOPMENT FOR SMALL BUSINESS USING AN AUTOMATED SYSTEM

The article considers the search for the optimal security policy of the information system of a small enterprise using the model of complete overlap. With the help of the implemented automated model, you can quickly and efficiently find the right set of protection barriers at a certain cost.

Keywords: *optimal set, complex information protection, small enterprise, modeling.*

Введение

С развитием новых информационных технологий и появление доступных мощных компьютеров позволило малому бизнесу их использовать в безнес-процессе. Также появилась необходимость в повышение уровня защиты в связи с развитием хранения и обработки информации. Так постепенно защита экономической информации становится обязательной: разрабатываются возможные документы по защите информации, формируются рекомендации по защите информации, даже проводиться федеральный закон о защите информации, который рассматривает проблемы защиты информации и задачи защиты информации, а также решают некоторые уникальные вопросы защиты информации.

Следует, что угрозы защиты информации сделала средства обеспечением информационной безопасности одной из обязательных элементов информационной системы.

Под информационной безопасностью Российской Федерации(информационной системы) подразумевается техника защита информации от преднамеренного или случайного несанкционированного доступа и нанесения тем, самым вред нормальному процессу документооборорота и обмена данными в системе, а также хищения, модификации и уничтожения информации [1*].

Вопрос защиты информации на малом предприятии решаются для того, чтобы изолировать нормально работоспособную информационную систему от несанкционированных управляющих воздействий и доступа посторонних лиц или программ к данным с целью хищения.

Успешная реализованная угроза на информационную система малого предприятии может привести временной остановки и финансовым потерям. Процесс реализации угрозы за последние года усовершенствовался. Для реализации уже не нужно специализированные знания, а требуется приобрести специализированное обеспечение которое по нажатию кнопки может обойди все барьеры защиты информации. Можно выделить распространенные меры защиты информации на малом предприятии: антивирусная защита, регулярное

обновление программного обеспечения и также тонкая настройка политики безопасности в информационной системы.

Процесс проектирование системы защиты информации трудоемкий. Для того чтобы спроектировать нужно нанимать в штат специалиста. Выход из такой сложной ситуации приходиться находить специалистам, которые смогут выполнять ряд задач других сотрудников. Для того, чтобы настроить всю информационную систему предприятия, необходимо иметь в штате инженера-программиста, который сможет проанализировать информационные потоки, и на основе анализа построить систему и внедрить на предприятие, а также в дальнейшем ее сопровождать при возникновении проблем.

1. Описание модели

Автоматизированные системы используют различные модели. Наиболее подходящей моделью для проектировании автоматизированной системы можно использовать модель “Клементса - Хофмана”. Данная модель позволяет найти оптимальный набор средств защиты информации (рис.1).

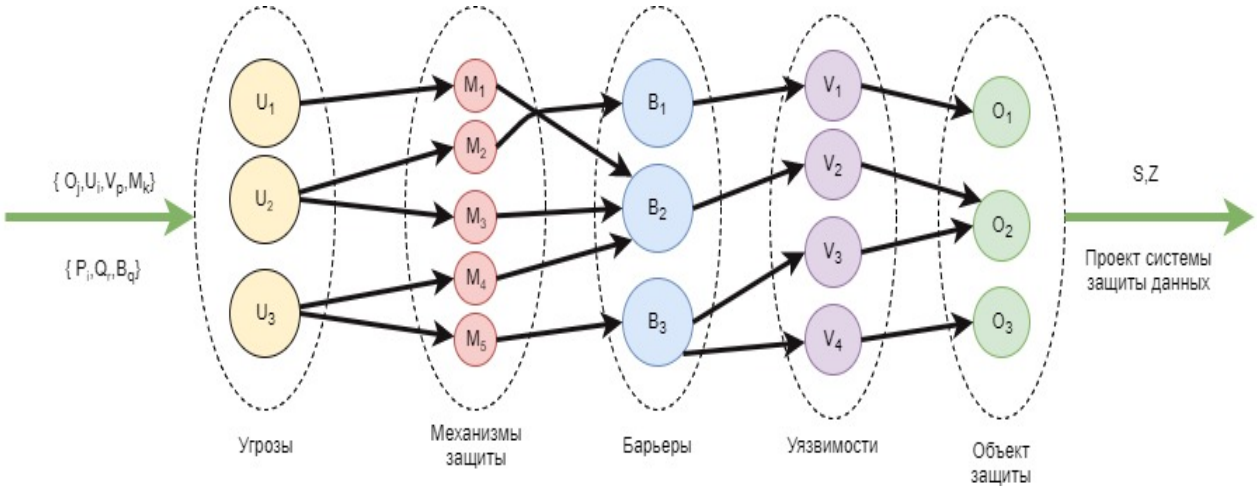


Рис. 1. Модель системы полного перекрытия (модель Клементса – Хофмана)

Модель проста в использовании, можно рассчитать защищённость барьеров системы, рассчитать экономические затраты при проектировании системы защиты информации, а самое главное определить оптимальный вариант построения системы безопасности.

Таким образом, процесс защиты информации представляет собой кортеж:

$$S = \{O, U, M, V, B\}, \quad (1)$$

Где O - множество защищаемых объектов;

U - множество возможных угроз;

M - множество средств защиты;

V - множество уязвимых мест в системе защиты информации;

B - множество барьеров.

Чтобы получить доступ, злоумышленнику необходимо выполнить ряд этапов и процессов, которые можно свести к трем условиям разведывательного контакта злоумышленника с источником информации:

- поиск ценной информации ($P_{пр}$ - пространственный фактор);
- размещение программно-аппаратных средств для получения информации на удалении от источника, при котором гарантируется приемлемое отношение сигнал/шум на входе средства ($P_{эн}$ - энергетический фактор);
- совпадение времени проявления демаскирующих признаков объекта защиты

или передачи информации и работы средства добывания ($P_{вр}$ - временный фактор).

Угрозы выполняются одновременно при трех условиях, а общая вероятность равна произведению:

$$P = P_{пр} \cdot P_{эн} \cdot P_{вр}, \tag{2}$$

Аппарат нечетких множеств позволяет производить простейшие операции непосредственно со значениями лингвистических переменных без промежуточного перевода их в числовые значения.

Принцип обобщения Заде может найти функцию принадлежности нечеткого числа, советующего значению четкой функции от нечетких аргументов

$$\mu\overline{y} = f(x_1, x_2, ..., x_n) \to (\mu\overline{x}(x_i))$$
$$x_i \in \sup(\overline{x_i}), i = \overline{1,n} \tag{3}$$

Требуется в таких условиях найти нечеткое число

$$\tilde{p} = \tilde{p}_{пр} \cdot \tilde{p}_{эн} \cdot \tilde{p}_{вр} \tag{4}$$

Дефазификация вероятности проявления угрозы определяем по формуле:

$$p = \frac{\sum_{i=1}^{k} U_i \cdot \mu_A(U_i)}{\sum_{i=1}^{k} \mu_A(U_i)}. \tag{5}$$

Прочность барьера системы защиты информации характеризуется величиной остаточного риска $Risk_i$, связанного с возможностью осуществления угрозы u_i в отношении объекта o_j, при использовании барьера b_q. Определяется по формуле :

$$Risk_i = P_i \cdot Q_j \cdot (1 - B_q), i = \overline{1,m}, j = \overline{1,n}, q = \overline{1, m \times n};, \tag{6}$$

Где P_i - вероятность появления угрозы u_i,

Q_i - величина ущерба при удачном осуществлении угрозы u_i в отношении защищаемого объекта o_j. Величина ущерба рассчитывается в условных единицах,

B_q- степень сопротивления барьера, величина характеризует вероятность его преодоления.

По формуле можно определить величину защищенности всей системы:

$$S = \frac{1}{\sum_{(\forall b_q \in B)} (P_i \cdot Q_j \cdot (1 - B_q))},$$
$$P_i \in (0,1), B_q \in [0,1). \tag{7}$$

2. Структура автоматизированной системы, составные модули

Созданы универсальные алгоритмы в виде модулей, входящие в состав системы. Структурно-функциональная модель проектирования системы защиты информации представлена на рис. 2.

Задача моделирования защиты информации состоит в объективном описании объектов защиты, с помощью которых будет происходить процесс защиты. Защищаемый объект в модели (данные, сервер базы данных и т.д.) должен быть представлен на схеме системы защиты информации в виде некоторой структуры.

Свойствами этой структуры являются наиболее важные характеристики объекта, такие как перебор пароля, открытые порты в сервисе, установление антивирусного ПО и т.д. В моделирование объектов защиты так же входит: источник угрозы, описание основных моментов, где возможно произвести атаку для несанкционированного получения данных, описание с указанием характеристик существующих барьеров на путях проникновения за пределы защиты. На основе полученных данных происходит иерархическое построение модели объекта защиты.

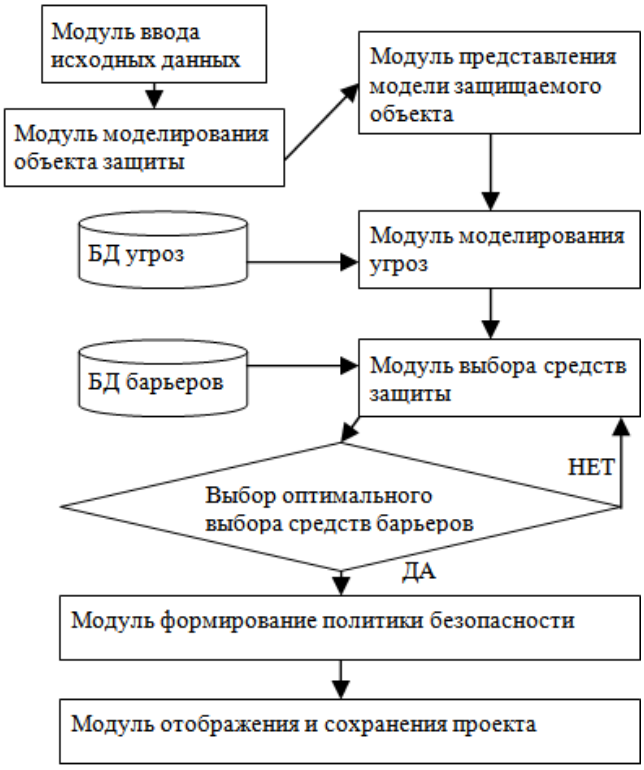


Рис. 2. Структурная схема системы защиты информации

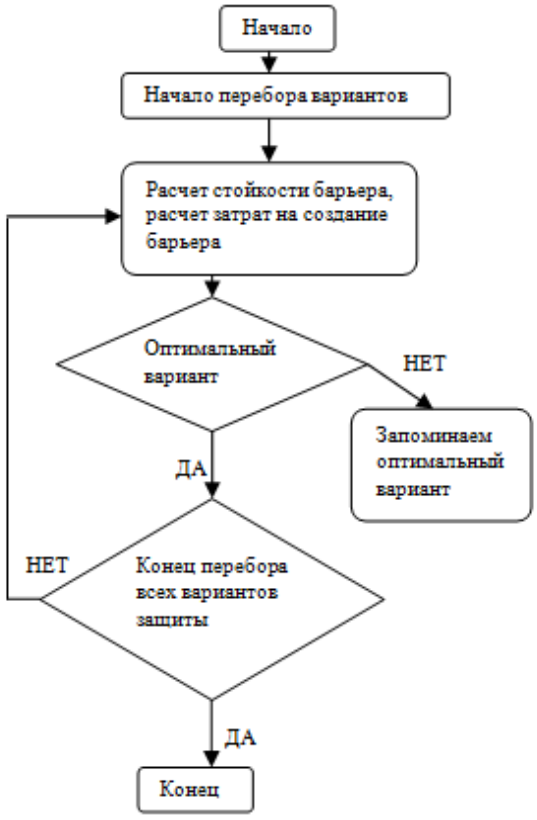


Рис. 3. Модуль перебора вариантов защиты

После создания модели защищаемого объекта происходит построение системы его защиты. Согласно принципам системного подхода, каждый элемент в программном

комплексе строится отдельным модулем, что позволяет динамически расширять возможности системы [2, с. 28].

В системе защиты информации основополагающим является программно-аппаратные средства защиты. Разработанные модули (рис. 3), позволяющие оценить и категорировать данные в соответствии в них определенных условий (в качестве таких условий выступают стойкость барьера, его цена и т.д.). Оценка основных элементов барьеров защиты таких как: персональный межсетевой экран, антивирусная программа, электронная цифровая подпись позволяют оценить их устойчивость к взломам, в случае нехватки стойкости предложить варианты по их замене или модернизации. Данные меры позволяют защитить максимально данные и увеличить время необходимое для злоумышленника, чтобы реализовать несанкционированный доступ. Данный запас позволяет системе проинформировать администратора, что был реализован несанкционированный доступ, и отреагировать, вычислив место нахождения, для задержания злоумышленника [1, с. 45].

3. Процесс проектирования

В ходе разработки *web*-сайта реализованы следующие списки:

1. Список угроз в БД.
2. Список источников угроз.
3. Список защищаемых объектов.
4. Список барьеров защиты в БД.
5. Список последствий от реализации угроз.

Открыв список угроз в БД (рис. 4) открывается окно, в котором представлены названия угроз и список действий, таких как: изменить, удалить и добавить запись. Все эти кнопки говорят сами за себя. Кнопка «Удалить» вызывает функцию, которая удалит тот элемент, напротив которого будет располагаться данная кнопка.

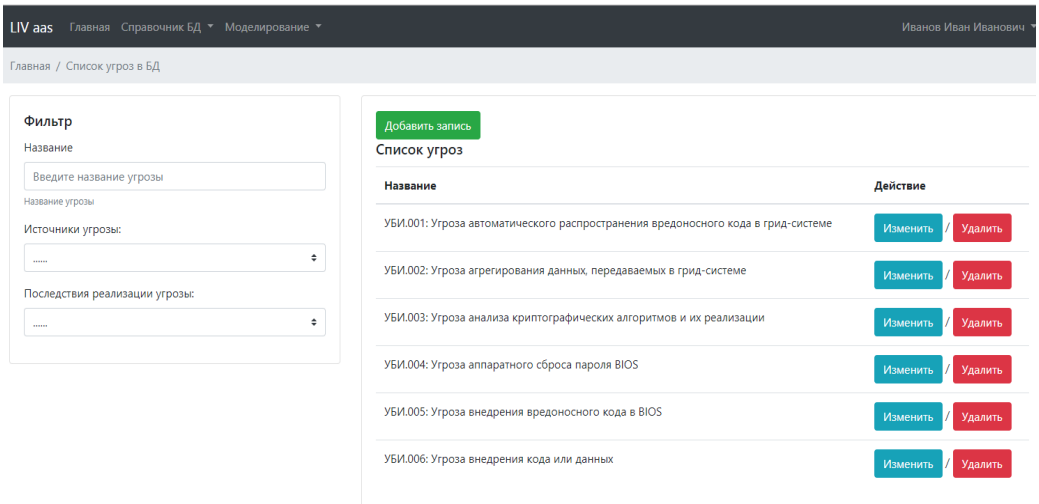


Рис.4. Список угроз в БД

При нажатии на кнопку «Изменить» открывается окно управления данными (рис. 5), где можно увидеть *ID* угрозы, описание угрозы, ее источники, и последствия, а также можно изменить эти поля, введя другое название или описание, также выбрав один или несколько пунктов в полях: «Источники угроз» и «Последствия реализации угрозы», затем нажать кнопку «Сохранить».

В окне «Список защищаемых объектов» (рис. 6) представлены названия объектов и список действий над этими объектами: «Добавить запись», «Изменить» и «Удалить».

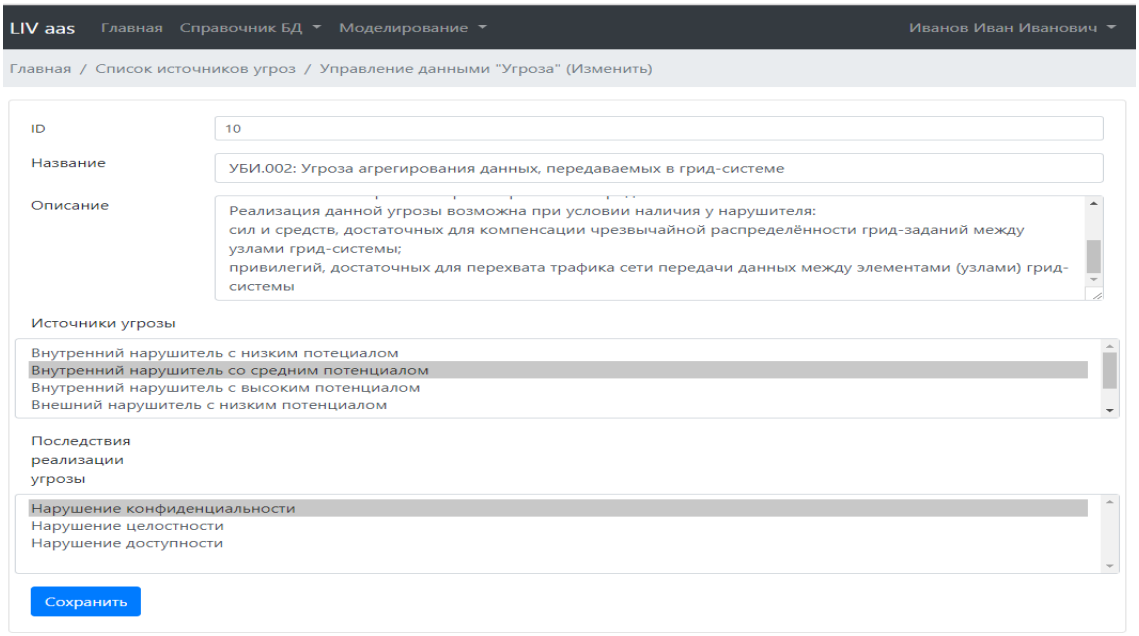


Рис. 5. Управление данными «Угроза»

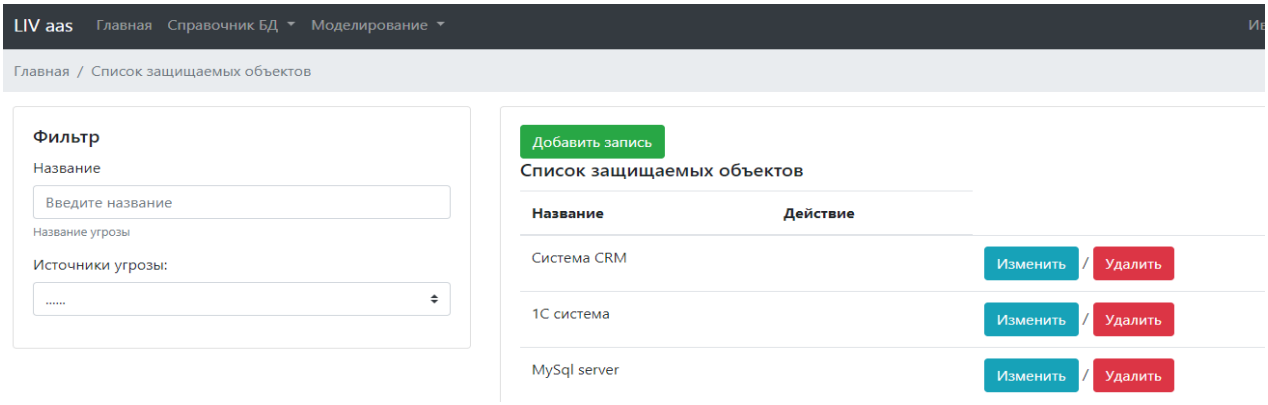


Рис. 6. Список защищаемых объектов

На странице списков барьеров защиты базы данных (рис. 7), также приведены названия барьеров и список действий, среди которых есть кнопка «Стойкость», которая позволяет просмотреть стойкость каждого барьера и внести изменения в случаях, когда данные неверны, либо потеряли свою актуальность.

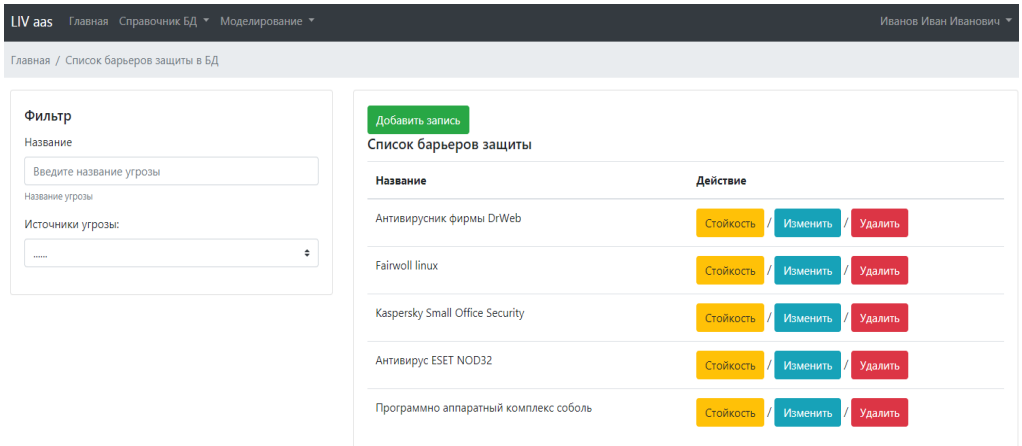


Рис. 7. Список барьеров защиты в БД

Нажав на кнопку «Стойкость» переходим в окно «Стойкость угрозам» (рис. 8), где указано:

1. Название барьера.
2. Название угрозы.
3. Стойкость барьера против данной угрозы.

Где также можно изменить поля в случаях, когда данные неверны, либо потеряли свою актуальность.

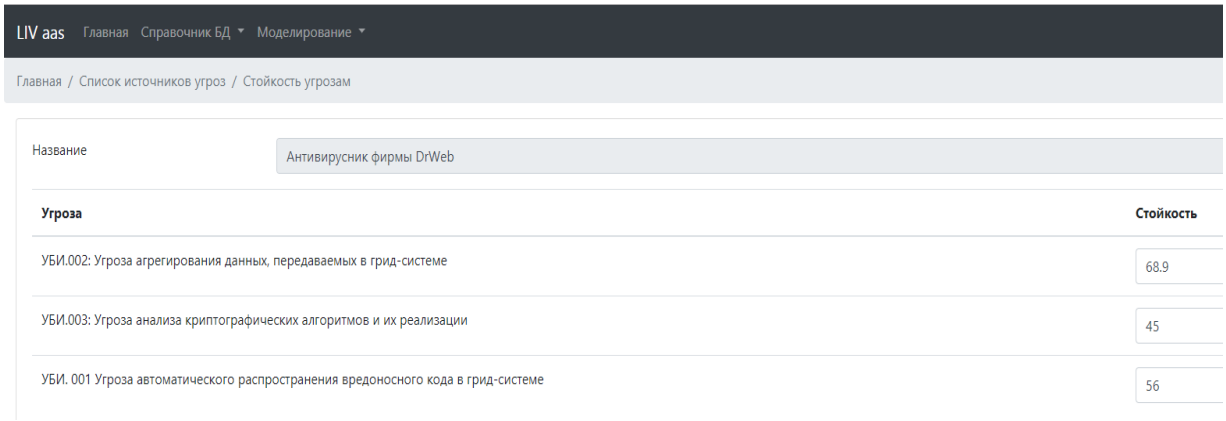


Рис. 8. Стойкость угрозам

Выбрав пункт «Моделирование» пользователю необходимо выбрать объекты, которые необходимо защитить, как показано ниже (рис. 9).

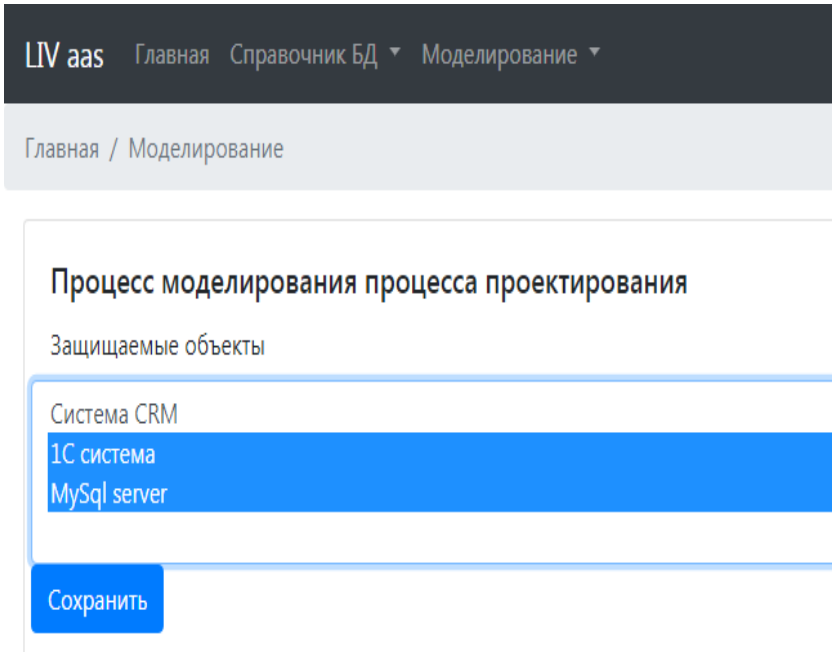


Рис. 9. Моделирование

После чего, обработав данные, пользователю предоставляется результат (рис. 10), в котором описаны: наименования защищаемых объектов, наименования угроз, которым подвержены объекты и варианты барьеров, которые можно противопоставить данным угрозам с описанием затрат и стойкости.

Результат моделирования

Защищаемые объекты- 1С система
MySql server

Угрозы- УБИ.002: Угроза агрегирования данных, передаваемых в грид-системе
УБИ.003: Угроза анализа криптографических алгоритмов и их реализации
УБИ.004: Угроза аппаратного сброса пароля BIOS
УБИ.005: Угроза внедрения вредоносного кода в BIOS
УБИ.006: Угроза внедрения кода или данных
УБИ. 001 Угроза автоматического распространения вредоносного кода в грид-системе

Результат

Вариант	Барьеры	Стойкость	Затраты
1	Fairwoll linux Kaspersky Small Office Security Антивирус ESET NOD32 Программно аппаратный комплекс соболь	61	598 USD
2	Антивирусник фирмы DrWeb Kaspersky Small Office Security Антивирус ESET NOD32 Программно аппаратный комплекс соболь	13	1948 USD
3	Антивирусник фирмы DrWeb Fairwoll linux Антивирус ESET NOD32 Программно аппаратный комплекс соболь	77	1579 USD

Рис. 10. Полученный результат моделирования

Заключение

Автоматизированная система позволила ускорить и увеличить качество защиты информации на малом предприятии в несколько раз, а (рис.11) также позволила сократить расходы на закупку только нужного перечня оборудования и его настройки для защиты информации. Благодаря нахождению оптимального варианта, автоматически время на проектирование комплексной системы защиты сократилось в 5 раз, уменьшилось появление ошибок при проектировании, а также закупка оборудование сократилась на 30 процентов.

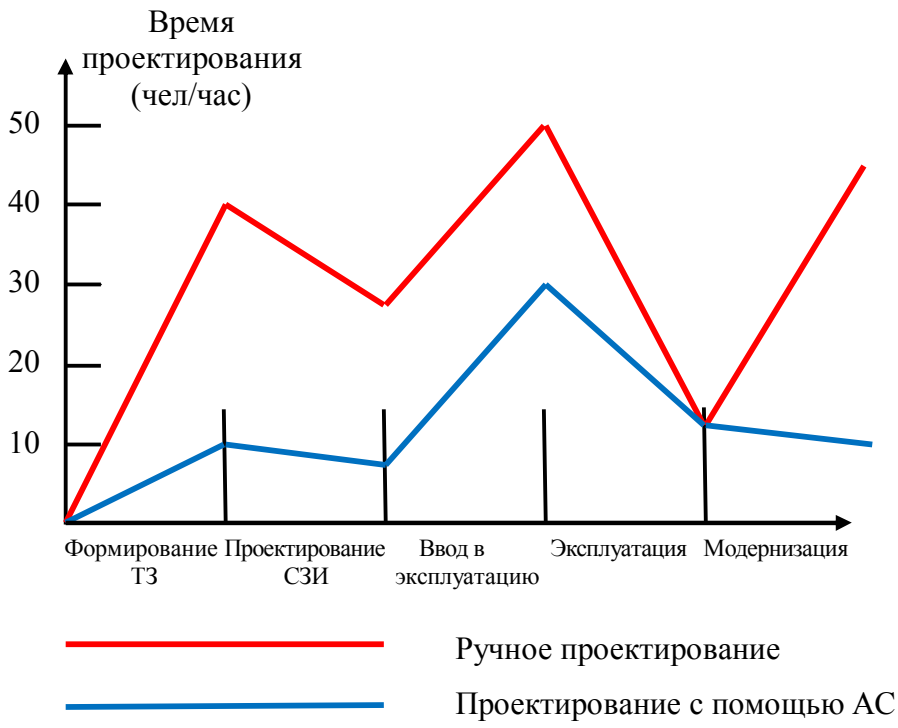


Рис. 11. Сравнительный анализ время проектирования с помощью системы или ручным методом

В результате работы для проектирования программного обеспечения была выбрана модель полного перекрытия, которая позволяет находить оптимальный вариант средств защиты информации. В конечном результате выдается перечень различных политик безопасности с общей стойкостью угроз и затрат на реализацию. Предложенные политики безопасности позволяют существенно сэкономить время на выборе необходимой. С помощью данного сайта малым предприятиям не нужно обращаться к дорогостоящим специалистам, ведь поиск оптимальной политики безопасности станет быстрым и удобным.

Разработанный программный продукт способен эффективно производить вычисления по нахождению оптимальной стоимости и стойкости барьеров. В перспективе планируется расширить функционал сайта для работы с более сложными информационными системами.

Список литературы:

1. Алаухов С.Ф. Вопросы создания систем информационной безопасности для крупных промышленных объектов / С.Ф. Алаухов, В.Я. Коцеруба // Системы безопасности. – 2011. – № 41. – С. 93.
2. Аверченков В.И. Организационная защита информации / В.И. Аверченков, М.Ю. Рытов. – Брянск: Изд-во БГТУ, 2015. – 184 с. – (Серия «Организация и технология защиты информации»).
3. Алаухов С.Ф. Вопросы создания систем информационной безопасности для крупных промышленных объектов / С.Ф. Алаухов, В.Я. Коцеруба // Системы безопасности. – 2011. – № 41. – С. 93.
4 Анин Б.Ю. Защита компьютерной информации / Б.Ю. Анин. – СПб.: БХВ-Петербург, 2010.
5. Баранова Е.К. Моделирование системы защиты информации. Практикум: учеб. пособие / Е.К. Баранова, А.В. Бабаш. – М.: РИОР: ИНФРА-М, 2016. – 224 с.
6. Драгунова Е. В., Митев П. К. Моделирование бизнес-процесса выбора инвестиционного поведения предприятия // Молодой ученый. — 2010. — №10. — С. 35-38. — URL https://moluch.ru/archive/21/2103/ (дата обращения: 10.01.2019).
7. Луценко И.В. Способы и приемы оценки защищенности данных малого предприятия / И.В. Луценко, М.Ю. Рытов // Информационные системы и технологии. – 2018. - №3(107). – с. 125.
8. Мельников, В.П. Информационная безопасность и защита информации. / В.П.Мельников, С.А.Клейменов, А.М.Петраков // 3-е изд., стер. - М.: Академия, 2008. — 336 с.
9. Рытов М.Ю. Использование специализированной САПР для проектирования комплексных систем защиты информации / М.Ю. Рытов, И.В. Луценко, М.А. Луценко // Инновационные, информационные и коммуникационные технологии. – Москва. Ассоциация выпускников и сотрудников ВВИА им проф. Жуковского, 2018. – 652 с.

References:

1. Alukov S. F. the creation of information security systems for large industrial facilities / S. F. Alahov, V. J. Kotseruba // security System. - 2011. - №41. - P. 93.
2. Averchenkov V. I. Organizational information security / V. I. Averchenkov, M. Yu. Rytov. - Bryansk: Publishing house of BSTU, 2015. - 184 p. - (Series "Organization and technology of information security").
3. Alukov S. F. the creation of information security systems for large industrial facilities / S. F. Alahov, V. J. Kotseruba // security System. - 2011. - №41. - P. 93.
4. Anin B.Y. Protection of computer information systems / B. Y. Anin. – SPb.: BHV-Petersburg, 2010.
5. Baranova E. K. Modeling of information security system. Workshop: studies. posobie / E. K. Baranova, A. V. Babash. – M.: RIOR: INFRA-M, 2016. - 224 p.
6. Dragunova E. V., Mitev p. K. Modeling of business process of the choice of investment behavior of the enterprise. Young scientist. - 2010. - №10. - P. 35-38. URL https://moluch.ru/archive/21/2103/ (accessed: 10.01.2019).
7. Lutsenko I. V. Methods and techniques for assessing the data security of a small enterprise / I. V. Lutsenko, M. Yu. Rytov / / Information systems and technologies. - 2018. - №3 (107). - p. 125.
8. Melnikov, V. P. Information security and information protection. / V. P. Melnikov, S. A. Kleimenov, A. M. Petrakov // 3rd ed., erased. - Moscow: Academy, 2008. - 336 p.
9. Rytov M. Yu. The use of specialized CAD for the design of complex information security systems / M. Yu. Rytov, I. V. Lutsenko, M. A. Lutsenko / / Innovative, information and communication technologies. – Moscow. The alumni Association staff and vvia Zhukovsky them prof, 2018. - 652 p.

Статья поступила в редколлегию 03.04.19.
Рецензент: д.т.н., доцент,
Брянский государственный технический университет
Аверченков А.В.
Статья принята к публикации 30.04.19.

Сведения об авторах:

Рытов Михаил Юрьевич
кандидат технических наук, доцент,
заведующий кафедрой «Системы информационной безопасности» Брянского государственного технического университета.
Тел.: +79103300237
E-mail: rmy@tu-bryansk.ru

Луценко Игорь Владимирович
аспирант кафедры «Системы информационной безопасности» Брянского государственного технического университета.
Тел.: +79206025080
E-mail: EROPA@LIVE.RU

Цвинкайло Петр Станиславович
Старший преподаватель кафедры «АТПиП» в Рыбницком Филиале ПГУ им Т.Г.Шевченко
Тел.: +79206025080
E-mail: human033@gmail.com

Information about authors:

Rytov Mikhail Yurevich
Candidate of Technical Sciences, Associate Professor,
Head of the department
«Information security systems»,
Bryansk state technical university
Phone: +79103300237
E-mail: rmy@tu-bryansk.ru

Lutsenko Igor Vladimirovich
Post-graduate student of the department «Information security systems», Bryansk state technical university
Phone: +79206025080
E-mail: eropa@live.ru

Ciencia Peter Stanislavovich
Senior lecturer of the department "ATEP" in Rybnitsa Branch of PSU of T. G. Shevchenko
Phone: +79206025080
E-mail: human033@gmail.com

УДК: 004.7
DOI: 10.30987/article_5d8d113d968333.98732766

М.Ю. Рытов, Р.Ю.Калашников

ПРИМЕНЕНИЕ МЕТОДОЛОГИИ STRIDE ДЛЯ ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПРОГРАММНО-ОПРЕДЕЛЯЕМЫХ СЕТЕЙ

В статье рассматривается применение модели угроз STRIDE к общим концепциям SDN. Выявлены основные недостатки безопасности в современных концепциях программно-определяемых сетей. По результатам анализа предложена основа для разработки безопасной архитектуры SDN.

Ключевые слова: *оценка рисков, программно-определяемая сеть, информационная безопасность.*

M.Yu. Rytov, R.Yu. Kalashnikov

APPLICATION OF STRIDE METHODOLOGY FOR DETERMINING CURRENT SECURITY THREATS FOR PROGRAM-DEFINED NETWORKS

In this paper, STRIDE threat model is applied to the generic SDN concepts. The current security flaws in modern concepts of software-defined networks are discussed. As a result of the analysis the basis for developing a secure SDN architecture is presented.

Keywords: *risk assessment, software-defined networks, information security.*

Введение

Основная идея программно-определяемых сетей (SDN) состоит в том, чтобы отделить данные и плоскость управления от сетевых компонентов и перенести функциональность плоскости управления на отдельные контроллеры SDN. Эта концепция связана с фундаментальными изменениями, касающимися управления сетью.

Одним их основных направлений развития концепции является применение SDN в сетях магистральной инфраструктуры интернета. Эта потенциальная область применения придает безопасности в SDN первостепенное значение.

Протокол Open Flow, несмотря на наличие альтернатив, является де-факто стандартным интерфейсом между платформой управления на основе SDN и плоскостью данных. Поддержкой, развитием, а также поиском потенциальных уязвимостей в реализациях протокола занимается организация Open Networking Foundation (ONF). Тем не менее, производители сетевого оборудования зачастую пренебрегают вопросами безопасности SDN в пользу функциональности и функциональной совместимости, которые являются важными преимуществами и, таким образом, обычно имеют приоритет над улучшениями безопасности в отношении разработки микропрограмм и программного обеспечения.

При рассмотрении вопроса о развертывании технологии SDN организациям рекомендуется проводить анализ рисков и выгод, состоящий из величины потенциальных потерь и вероятности возникновения таких потерь. Для оценки рисков необходимо определить угрозы. Microsoft STRIDE - методика определения актуальных угроз информационных систем, и поэтому она пригодна для оценки безопасности SDN. Данная методика включает в себя оценку рисков информационной безопасности по следующим категориям: спуфинг, модификация, отказ от авторства, разглашение, отказ в обслуживании и повышение привилегий. Данная статья посвящена декомпозиции концепции SDN на основные элементы (плоскость данных, плоскость управления и протокол Open Flow) и применению анализа STRIDE к этим компонентам.

1. Определение актуальных угроз в сетях SDN

SDN переносит управление всей сетью в единую автономную программную систему. Результатом этого является возможность гибкой настройки и управления сетью, но в то же время повышается зависимость от единого узла управления. Следовательно, архитектура может таить в себе непредвиденные риски. Повышенное внимание к программному обеспечению, программируемости и открытым интерфейсам может открыть для злоумышленника несколько новых векторов атаки. Кроме того, центральный контроллер является основной целью для DoS-атак, так как работа всей сети зависит от одного устройства. Поскольку влияние скомпрометированных устройств значительно возрастает, разработка устройств SDN должна подвергаться постоянному анализу угроз.

Модель угроз STRIDE (табл. 1) используется для анализа недостатков и возможных уязвимостей концепции. Для построения структуры исследуемой SDN, в статье использованы стандартные описания [1], [2] и конфигурации сети по умолчанию.

Таблица 1 – Перечень угроз в методологии STRIDE

Угроза	Описание
Спуфинг	Позволяет злоумышленникам скрыть или подделать их личность. Данный тип атак становится возможным ввиду отсутствия надлежащей аутентификации.
Модификация	Позволяет злоумышленникам поставить под угрозу целостность передаваемых или хранимых данных.
Отказ от авторства	Позволяет пользователям в системе отречься от своих действий или обвинить в них других. Системы мониторинга и журналы действий при этом не способны корректно идентифицировать злоумышленника.
Разглашение информации	Эксплуатация этой уязвимости может привести к раскрытию значимой информации или паролей. Она также часто коррелирует с атаками подмены и модификации.
Отказ в обслуживании	Устройства могут подвергаться атаке, которая делает службу или систему временно непригодными для клиентов или пользователей. Этот метод оказывает значительное финансовое влияние и поэтому является одной из наиболее распространенных угроз.
Повышение привилегий	Эта уязвимость часто возникает из-за отсутствия контроля доступа. Простой пользователь или клиент может повысить свои полномочия в системе, что дает им возможность свободного доступа к ограниченным или классифицированным активам.

A. Спуфинг

Несмотря на то, что злоумышленнику приходится использовать для реализации атаки спуфинга в SDN те же методы, что и в обычных сетях, реализация атаки может иметь более негативные последствия. SDN представляет два новых компонента сети - контроллер и приложения. Они имеют корневое значение для безопасности сети и поэтому становятся главной целью атаки. Программируемость и программные интерфейсы потенциально скрывают множество уязвимостей. Кроме того, виртуализация физических сетевых устройств, таких как коммутаторы и контроллер, снижает барьер для атаки.

Традиционные протоколы аутентификации могут служить контрмерой. Однако исследования механизмов безопасности демонстрируют, что их может быть недостаточно для защиты контроллеров и коммутаторов [3]. Важность контроллера в SDN делает спуфинг значительной угрозой, в большей степени, чем в обычных сетях. Даже если предположить, что поток данных в сети защищен, попытки спуфинга все же возможны. Таким образом, в данном анализе спуфинг считается базовой уязвимостью, которая делает возможным эксплуатацию прочих уязвимостей модели STRIDE.

B. Модификация

Атака модификации имеет схожий со спуфингом принцип реализации. Риск несанкционированного доступа при этом не усугубляется, если меры аутентификации осуществляются должным образом и сеть физически защищена. Тем не менее, плоскость управления открывает несколько новых векторов атаки. Логика маршрутизации в SDNне распределена, и коммутаторы зависят от единственного объекта, поддерживающего представление сети. Если база данных маршрутизации скомпрометирована, вся сеть подвергается риску. Контроллер должен правильно идентифицировать модифицированную и конфликтующую информацию так же, как и обнаруживать попытки спуфинга.

C. Отказ от авторства

Угроза отказа от авторства для SDN не имеет существенных отличий, ввиду поддержки основных криптографических протоколов. [1]. Кроме того, котроллер предоставляет возможность централизованного обзора сети, что дает больше возможностей для отслеживания несанкционированных попыток подключения и скрытых устройств [2]. В данном анализе STRIDE проблемы отказа от авторства в Open Flow в основном являются результатом модификации информации или халатной реализации, при которой не реализованы механизмы аутентификации.

D. Раскрытие информации

Сетевые компоненты в SDN предоставляют возможности для сбора данных. Гибкая и программируемая природа сети Open Flow увеличивает риск раскрытия информации, поскольку отдельные устройства могут быть быстро перенастроены для перенаправления трафика по обходным путям. Разница во времени отклика помогает злоумышленникам воссоздавать схему сети без необходимости доступа к какому-либо устройству. В SDN несколько элементов хранят информацию обо всей сети в таблицах потоков и базах данных виртуализации. Эта информация может быть раскрыта с помощью удаленных запросов или получения доступа к серверу. Хотя пользовательские данные могут быть защищены с помощью TLS, базовая SDN не предоставляет достаточных методов для сокрытия информации об общей структуре сети.

E. Отказ в обслуживании

SDN в значительной степени увеличивает риск отказа в обслуживании в сети. Узлы сети лишаются независимости работы в пользу гибкости и простоты настройки. Однако, если контроллер выходит из строя, то вся сеть теряет работоспособность. Программируемый и программно-ориентированный подход вводит новые векторы атак и увеличивает риск ошибок, которые могут привести к сбоям в работе сети. Кроме того, низкая отказоустойчивость системы расширяет спектр возможных атак.

Тем не менее, SDN может предоставить несколько возможностей для динамического смягчения последствий атак отказа в обслуживании. Приложения могут изолировать скомпрометированные хосты, если они будут своевременно выявлены. Трафик можно быстро перенаправить во избежание перегрузок. Датчик пропускной способности Open Flow способен автоматически ограничивать поток входящих данных, что приводит к динамической и быстрой защите уязвимых участков сети. [1] Постоянный и централизованный мониторинг сети контроллера может быстро выявить аномальное поведение. Эти возможности, однако, основаны на предположении, что контроллер использует необходимые защитные инструменты. Open Flow не включает эти возможности по умолчанию. Для обеспечения надежной защиты от атак и масштабируемости необходимо наличие нескольких контроллеров, либо одного распределенного контроллера.

F. Повышение привилегий

На текущем этапе развития SDN существует проблема определения потенциальных рисков в сетях разделяемых сервисов. На сегодняшний день не существует достаточно крупных коммерческих разработок, по которым можно было бы судить об эффективности конкретных проектных решений. Кроме того, пока нет доступных механизмов для совместного использования ресурсов контроллера несколькими пользователями сети. Исходя из этого, можно сделать вывод, что авторизация и политики разграничения доступа являются краеугольным камнем при развертывании крупномасштабной программно-определяемой сети.

2. Предлагаемые меры противодействия основным угрозам в SDN

Анализ угроз по методологии STRIDE демонстрируют, что SDN в сочетании с механизмами защиты обычных сетей нельзя считать безопасной. Традиционные меры безопасности, такие как шифрование, межсетевые экраны или системы обнаружения вторжений (IDS), должны быть адаптированы к дизайну программно-определяемой сети. Таким образом, в данной статье модель STRIDE используется, чтобы наметить реальную архитектуру безопасности, которая объединяет традиционные и специфичные решения защиты. Проект может быть использован для оценки потенциала безопасности будущих SDN, а также для формулирования минимально необходимых требований безопасности для более крупных программно-определяемых сетей.

Для выбора средств и методов, позволяющих снизить риски реализации угроз

безопасности в SDN, была проведена консультация с соответствующей литературой, проанализированы передовые решения в области безопасности, и определены требования и варианты дизайна, которые предусматривают комплексные механизмы защиты сети. Кроме того, приняты во внимание рекомендации ONF, определяющие необходимые средства безопасности для протокола Open Flow [2]. Они включают обязательное использование протоколов безопасности, введение уникальной идентификации и четкое определение границ доверия и безопасности. Таблица 2 суммирует проблемы и решения, определенные в данной статье. В результате в данной работе предлагается модель защищенной сети, использующий принципы, содержащиеся в технической спецификации ONF [1], а также текущие предложения по безопасности.

Первым и абсолютным условием в защищенной системе является использование механизмов аутентификации и проверки целостности для любого узла сети, поскольку этот функционал игнорируются в текущих стандартных разработках. Любой обмен данными между приложениями, контроллерами и коммутаторами должен проходить взаимную аутентификацию, а конфиденциальные сообщения, такие как отчеты о топологии и сообщения о модификации, должны проверяться на целостность. База данных самого контроллера должна быть подписана, чтобы гарантировать использование целостность данных. Канал управления может быть развернут вне сети либо физически, либо виртуально в конфигурациях VLAN.

Для того, чтобы избежать зависимости от одного устройства, в сети должны быть развернуты как минимум два независимых контроллера. Они могут координировать или принимать на себя управление соседними сетями, в случае если один из контроллеров выходит из строя. Подключение коммутаторов к нескольким логически децентрализованным контроллерам может предотвратить негативные последствия в случае компрометации одного из контроллеров. Контроллеры при этом могут обмениваются данными напрямую или косвенно через распределенную сетевую базу данных.

Плоскость управления должна находиться в защищенной зоне, аналогично важным базам данных в обычной сети. Только аутентифицированные хосты, являющиеся частью физически и логически защищенного домена, должны иметь доступ к настройке серверов. Любой трафик, не являющийся сообщением Open Flow, должен фильтруется с помощью встроенных межсетевых экранов.

Удаленные приложения и хосты, пытающиеся получить доступ к серверной зоне, следует проверять на основе местоположения и идентификации с использованием AAA-серверов и алгоритмов управления. Они также должны быть ограничены в правах, наборе действий и доступе к карте сети. Компоненты безопасности и чувствительные к задержке приложения могут быть запущены непосредственно на управляющем сервере, но должны выполняются в отдельном процессе и пространстве памяти. Приложения с более высокими привилегиями должны иметь возможность отменять действия более низкого уровня, а приложения администратора должны обладать полными правами конфигурации.

Управляющие приложения должны отслеживать и протоколировать действия узлов сети и приложений. Поскольку контроллеры являются незаменимыми, они могут быть защищены с помощью систем обнаружения вторжений или межсетевого экрана с хранением состояния. Так, например, для быстрого выявления атак во всей сети коммутаторы могут зеркалировать трафик на серверы обнаружения вторжений. Они сообщают результаты анализа контроллеру, который быстро перенастраивает сеть, чтобы изолировать скомпрометированные участки. Кроме того, контроллер может идентифицировать подозрительное поведение сети на основе шаблонов пакетов. О любых событиях и аномалиях в сети следует сообщать управляющему приложению или системе управления информацией и событиями безопасности (SIEM).

Как правило, рекомендуется блокировать доступ к сети из сетей с более низким уровнем безопасности и разделять сеть на сегменты с различным уровнем защищённости при помощи межсетевых экранов.

Обеспечение бесперебойной работы при установке обновлений безопасности может быть достигнуто при помощи использования технологии Hot Swap [5] или обновления путем замены единичных модулей.

Таблица 2. Угрозы и уязвимости SDN в соответствии с моделью STRIDE

УгрозаSDN	Уязвимость	Возможноерешение
Спуфинг	Возможность аутентифицироваться в качестве контроллера, коммутатора или приложения ввиду отсутствия средств защиты или ошибок в ПО.	Внедрение обязательных процедур аутентификации в рабочих операциях.
Модификация	Злоумышленник может перезаписать политики контроллера. Перехват и модификация управляющих сообщений Open Flow может иметь значительные негативные последствия для конфигурации сети.	Внедрение механизмов контроля доступа и проверки целостности на северном и южном интерфейсах SDN. Важные действия выполняются после верификации несколькими независимыми элементами управления.
Отказ от авторства	Отсутствие мониторинга состояния коммутаторов и управляющего программного обеспечения может открыть возможности для выполнения скрытых операций.	Уникальная идентификация элементов SDN. Механизмы журналирования и отслеживания должны выполняться автоматически и должны быть защищены.
Раскрытие информации	Централизованное хранение информации упрощает сбор данных о структуре сети. Кроме того, компрометация серверного ПО может привести к раскрытию учетных данных и сетевой базы данных.	Перемещение коммуникаций SDN на отдельные защищенные каналы. Контроллер и хранилище данных о состоянии сети при этом должны быть удалены из сети передачи данных.
Отказ в обслуживании	Функциональность коммутаторов зависит от единого контроллера и канала управления, который подвержен множеству возможных атак, таких как флуд, эксплойты, а также ошибки в ПО. Таблицы коммутации при этом ограничены и быстро переполняются.	Развертывание контроллера в сочетании с механизмами обнаружения вторжений; использование механизмов восстановления и избыточности сетевых узлов.
Повышение привилегий	Контроллеры SDN, к которым имеет доступ множество пользователей, в случае компрометации могут раскрыть информацию о соседних сетях. Кроме того, поскольку не существует различий в приоритетах команд приложений, вредоносные клиентские приложения могут взять на себя все полномочия контроллера.	К общим ресурсам должны применяться строгие механизмы контроля доступа на основе ролей, в то время как доверие к операциям клиентов должно быть минимальным. Программное обеспечение должно подвергаться регулярным проверкам во время разработки.

Заключение

Программно-определяемые сети являются развивающейся концепцией для сетей дата-центров и сетей доступа к магистральной инфраструктуре интернета. Поэтому безопасность становится важным аспектом, который в настоящее время рассматривается как научным сообществом, так и производителями оборудования.

Тем не менее, более тщательный анализ безопасности на текущем этапе развития SDN, показывает широкий спектр специфичных для SDN угроз, адекватных мер противодействия которым ещё не выработано. Некоторые из них по своей природе связаны с принципами проектирования SDN, например, контроллеры являются потенциально главными объектами атаки; другие наследуются от базовой инфраструктуры, как, например, подверженность спуфингу. Основываясь на результатах этого анализа, в данной статье определены основные угрозы и предложены решения, позволяющие разработать защищенную архитектуру SDN.Также подчеркнута роль контроля подлинности и целостности для узлов сети и сообщений управляющего протокола, которыми они обмениваются. Ключевым элементом предложенной модели является обеспечение того, чтобы меры безопасности не только предотвращали, но и обнаруживали попытки и успешные атаки на компоненты SDN. Стоит также отметить, что для обеспечения безопасности управляющей связи все еще необходимо полагаться на устоявшиеся традиционные концепции, такие как внеполосное управление

или, по крайней мере, отдельные VLAN управления. Кроме того, решения для противодействия атакам на переполнение таблицы потоков, например, в результате DoS-атак, на сегодняшний день не разработаны.

Список литературы:

1. Техническая спецификация Open Flow Switch Specification 1.5.1, Open Networking Foundation, 2015.
2. Техническая спецификация Threat Analysis for the SDN Architecture 1.0, Open Networking Foundation, 2016.
3. S. Scott-Hayward, S. Natarajan, S. Sezer, A survey of security in software defined networks// IEEE Communications Surveys and Tutorials, 2015, с. 1.
4. J. Francois and O. Festor. Anomaly Traceback using Software Defined Networking // International Workshop on Information Forensics and Security, 2014.
5. L. Vanbever, J. Reich, T. Benson, N. Foster, J. Rexford, HotSwap: Correct and Efficient Controller Upgrades for Software-defined Networks // Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, 2013, с. 133-138.

References:

1. Technical specification:OpenFlow Switch Specification 1.5.1, Open Networking Foundation, 2015.
2. Technical specification: Threat Analysis for the SDN Architecture 1.0, Open Networking Foundation, 2016.
3. S. Scott-Hayward, S. Natarajan, S. Sezer, A survey of security in software defined networks// IEEE Communications Surveys and Tutorials, 2015, с. 1.;
4. J. Francois and O. Festor. Anomaly Traceback using Software Defined Networking // International Workshop on Information Forensics and Security, 2014.
5 L. Vanbever, J. Reich, T. Benson, N. Foster, J. Rexford, HotSwap: Correct and Efficient Controller Upgrades for Software-defined Networks // Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, 2013, с. 133-138.

Статья поступила в редколлегию 06.05.19.
Рецензент:
д.т.н., доцент,
Брянский государственный
технический университет
Спасенников В.В.
Статья принята к публикации 20.05.19.

Сведения об авторах:

Рытов Михаил Юрьевич
кандидат технических наук, доцент,
заведующий кафедрой «Системы информационной безопасности» Брянского государственного технического университета.
Тел.: +79103300237
E-mail: rmy@tu-bryansk.ru

Калашников Руслан Юрьевич
аспирант кафедры «Системы информационной безопасности» Брянского государственного технического университета.
Тел.: +79206025080
E-mail: human033@gmail.com

Information about authors:

Rytov Mikhail Yurevich
Candidate of Technical Sciences, Associate Professor,
Head of the department
«Information security systems»,
Bryansk state technical university
Phone: +79103300237
E-mail: rmy@tu-bryansk.ru

Kalashnikov Ruslan Yurevich
post-graduate student of the department «Information security systems»,
Bryansk state technical university
Phone: +79206025080
E-mail: human033@gmail.com

УДК: 004.4
DOI: 10.30987/article_5d8d113db17c32.68186730

А.В. Аверченков, Е.Э. Аверченкова, Ф.Ю. Лозбинев

ОСНОВНЫЕ ТРУДНОСТИ И НАПРАВЛЕНИЯ ОСВОЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РФ НА СРЕДНЕ- И ДОЛГОСРОЧНУЮ ПЕРСПЕКТИВУ

Новые ориентиры цифровой экономики требуют внедрения новых информационных технологий в повседневную практику государственного управления. Рассмотрены основные правовые рамки государственного развития цифрового общества в средне- и долгосрочной перспективе на примере Национального проекта «Цифровая экономика». Показано, что обеспечение достаточного уровня регионального государственного управления в условиях информационных трансформаций возможно в рамках Федерального проекта "Цифровое государственное управление". Обучение и переподготовка кадров в области информационных технологий является важнейшим условием успешной реализации идеи информатизации российского общества, оно реализуется мероприятиями Федерального проекта "Кадры для цифровой экономики".

Ключевые слова: *информационные технологии, национальные проекты, государственное управление.*

A.V. Averchenkov, E.E. Averchenkova, F.Yu. Lozbinev

BASIC DIFFICULTIES AND DIRECTIONS OF DEVELOPMENT OF INFORMATION TECHNOLOGIES IN THE RUSSIAN FEDERATION FOR THE MIDDLE AND LONG-TERM PROSPECTS

New benchmarks of the digital economy require the introduction of new information technologies into the daily practice of public administration. The main legal frameworks of the state development of the digital society in the medium and long term are considered on the example of the National Project "Digital Economy". It is shown that the provision of a sufficient level of regional government in the conditions of information transformations is possible within the framework of the Federal Project "Digital Public Administration". Training and retraining of personnel in the field of information technologies is the most important condition for the successful implementation of the idea of informatization of Russian society, it is implemented by the measures of the Federal project "Personnel for the digital economy".

Keywords: *information technology, national projects, public administration.*

Введение

Перед нашей страной встала уже теперь осознанная необходимость прорывного технологического развития прежде всего в области информационных технологий и, в частности, искусственного интеллекта. Одним из главных вызовов современности, сформированных в Стратегии научно-технологического развития Российской Федерации, является "исчерпание возможностей экономического роста России, основанного на экстенсивной эксплуатации сырьевых ресурсов, на фоне формирования цифровой экономики и появления ограниченной группы стран-лидеров, обладающих новыми производственными технологиями и ориентированных на использование возобновляемых ресурсов" [1].

На сегодняшний день в РФ сформированы основные правовые рамки государственного развития цифрового общества. Это Национальная программа «Цифровая экономика

Российской Федерации», направленная на реализацию Стратегии развития информационного общества в Российской Федерации на 2017-2030 гг. [2]. Эти документы форсируют развитие цифровых технологий и искусственного интеллекта, в том числе и их использование в различных секторах российской экономики. Основное их целеполагание – это повышение эффективности функционирования самого государства и повышению качества жизни его граждан.

1. Постановка проблемы

В прогнозе социально-экономического развития Российской Федерации на 2018 год и на плановый период 2019 и 2020 годов особое внимание уделено такому направлению, как информационные технологии. Так, основным постулатом является то, что «создание экосистемы "цифровой" экономики Российской Федерации путем эффективного развития рынков и отраслей (сфер деятельности), в которой big data позволят выйти на новый уровень экономического развития» [3].

Информация Министерства экономического развития РФ, описывающая тренды в сфере информационных технологий определяет некоторую отрицательную тенденцию, связанную со снижением динамики значений рынка информационных технологий в 2016 г. в сравнении с прошлыми значениями (например, отмечается сокращение на 6% от уровня предыдущего года в сопоставимых ценах) [3]. В 2017г. снижение аналогичного показателя составляет 3%. Структурный анализ трендов рынка информационных технологий показывает, что «большая часть объема рынка информационных технологий пришлась на рынок аппаратных средств и составила 56,4%. Рынок программных средств составил 19,4%, а рынок услуг - 24,2%» [3]. Важным значением, заложенным в прогноз социально-экономического развития Российской Федерации на 2018 год и на плановый период 2019 и 2020 годов, при развитии экономики по базовому варианту в 2020 г. является то, что «объем рынка информационных технологий достигнет 886,9 млрд. рублей, что составит 98,5% от уровня 2016 г.» [3].

Таким образом, можно говорить о том, что развития информационной среды в РФ в среднесрочной перспективе идет неравномерно, с нестабильной динамикой, а факторами, ограничивающими его развитие, являются «уровень платежеспособного спроса населения и предпринимательской активности, дефицит кадров, недостаточный уровень подготовки специалистов, недостаточное количество исследований мирового уровня, ведущихся в стране в области информационных технологий, недостаточный спрос со стороны государства, слабое использование возможностей государственно-частного партнерства в области обучения и исследований» [3].

В долгосрочной перспективе определяется решение серьезных социально-экономических и инфраструктурных барьеров, мешающих активному распространения информационных технологий в повседневную отечественную практику. Так, прогноз долгосрочного социально-экономического развития Российской Федерации на период до 2030 года, разработанный Минэкономразвития России, определяет следующие ориентиры для развития информационных технологий [4]:

- формирование стойкой потребности отечественной экономики в разработках в области информационных технологий;
- повышение уровня внедрения информационных технологий в отечественной экономике;
- стимулирование заинтересованности российских компаний в покупке отечественных разработок в области программного обеспечения;
- преодоление отсталости инновационной инфраструктуры в целом в стране;
- формирование комплексной программы поддержки развития ИТ-кадров.

В данном исследовании рассмотрим, как решают основные трудности на пути

внедрения информационных технологий в российскую действительность в средне- и долгосрочной перспективе.

2. Развитие информационных технологий в области государственного управления: Федеральный проект "Цифровое государственное управление"

Основой функционирования ЭВМ является аппаратные средства (АС), которые принимаем во внимание. Также принимаем во внимание пользователя. Это две крайние точки предлагаемой систематизации. Все объекты, участвующие в этом процессе, делим на слои. АС отнесём к слою S_0.

Несколько слов нужно сказать о распространенной сегодня тенденции использования виртуальных машин. Отдельная виртуальная машина – это самостоятельный объект, в котором существуют те же слои рассматриваемых объектов, что и в реальной, но только в «гостевом» варианте. Однако в расширенном контексте, включающем реальные АС, хост и гипервизор, последний занимает слой S_4 (полагаем, что он разрабатывался с помощью инструментального слоя S_3), а значит слои «гостевой» машины, включая виртуальный вариант слоя S_0, должны нумероваться как S_{4+1}, S_{4+2}, и так далее.

3. Поддержка развития ИТ-кадров: Федеральный проект "Кадры для цифровой экономики"

Внедрение современных электронных технологий в образование, облегчение доступа к качественным обучающим программам в сфере информационных технологий как элементы долгосрочного ориентира в области развития информационных технологий связывается с количеством квалифицированных кадров, работающих в ИТ-отрасли [4]. Действительно, в прогнозе долгосрочного социально-экономического развития Российской Федерации на период до 2030 года говорится об «..отсутствии целенаправленной поддержки развития ИТ-кадров» [4]. А в прогнозе социально-экономического развития Российской Федерации на 2018 год и на плановый период 2019 и 2020 годов среди основных сдерживающих факторов, сдерживающих информатизацию общества указаны дефицит кадров, недостаточный уровень подготовки специалистов, недостаточное количество исследований мирового уровня [3].

Отметим, что решение обозначенных кадровых проблем решаются в среднесрочной перспективе. Например, в Паспорте Национальной программы «Цифровая экономика» [5] заложена поддержка талантливых школьников и студентов в области математики и информатики, которая предполагает выявление и поддержку лучших преподавателей, школьников, выпускников и аспирантов в области математики и информационных технологий, а также разработку и апробацию учебных симуляторов, тренажеров, виртуальных лабораторий для изучения математики, информатики, создание и функционирование сети международных научно-методических центров.

Вопросы подготовки кадров по направлениям, связанным с внедрением технологий искусственного интеллекта в повседневную практику промышленного производства, экономики, а также в сфере государственного управления, раскрываются в федеральном проекте "Кадры для цифровой экономики", который направлен на достижение цели, определенной Указом Президента Российской Федерации от 7 мая 2018 г. N 204 [7] в части решения задачи по обеспечению подготовки высококвалифицированных кадров для цифровой экономики,7в соответствии со "Стратегией научно-технологического развития Российской Федерации" [1].

В области подготовки и переподготовки управленческих региональных кадров в области ИИ федеральный проект "Кадры для цифровой экономики" отвечает целям и задачам "Стратегии развития информационного общества в Российской Федерации на 2017 - 2030" [2], утвержденного указом Президента Российской Федерации от 9 мая 2017 г. N 203 [2], в том числе это использование и развитие различных образовательных технологий (в том

числе дистанционного, электронного обучения, при реализации образовательных программ); развитие технологий электронного взаимодействия граждан, организаций, государственных органов, органов местного самоуправления, а также создание основанных на информационных и коммуникационных технологиях систем управления и мониторинга во всех сферах общественной жизни.

Федеральный проект "Кадры для цифровой экономики" позволит создать условия по реализации персональных траекторий развития и профилей компетенций граждан, развить систему образования в интересах подготовки компетентных специалистов в сфере цифровой экономики, реализовать программы переподготовки по востребованным профессиям в условиях цифровой экономики. По итогам реализации комплекса мероприятий федерального проекта в области подготовки государственных служащих предполагается достигнуть следующие показатели за 2019-2024гг. [5]:

- 270,0 тыс. работающих специалистов, включая руководителей организаций и представителей органов исполнительной власти пройдут обучение по компетенциям цифровой экономики;

- 1000 тыс. человек пройдут обучение по развитию компетенций цифровой экономики в рамках государственной системы персональных цифровых сертификатов.

Таким образом, освоение таких информационных технологий позволит оптимизировать управленческую деятельность и сократить негативное влияние факторов, связанных с недостаточным уровнем знаний лиц, принимающих решения, и ограничивающих внедрение цифровых технологий в государственное управление РФ.

Выводы

Актуальность и практическая необходимость дальнейшего развития информационных технологий в долгосрочной перспективе определяется успехом их применения в среднесрочном периоде.

Список литературы:

1. Указ Президента РФ от 01.12.2016 N 642 "О Стратегии научно-технологического развития Российской Федерации" URL: http:http://www.consultant.ru/document/cons_doc_LAW_207967/ (дата обращения: 06.06.2019).

2 Указ Президента РФ от 09.05.2017 N 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы" URL: http://www.consultant.ru/document/cons_doc_LAW_216363/ (дата обращения: 06.06.2019).

3. Прогноз социально-экономического развития Российской Федерации на 2018 год и на плановый период 2019 и 2020 годов URL: http://www.consultant.ru/document/cons_doc_LAW_282738/ (дата обращения: 06.06.2019).

4. Прогноз долгосрочного социально-экономического развития Российской Федерации на период до 2030 года" URL: http://www.consultant.ru/document/cons_doc_LAW_144190/ (дата обращения: 06.06.2019).

5. Распоряжение Правительства РФ от 28.07.2017 N 1632-р “Об утверждении программы "Цифровая экономика Российской Федерации" URL: http://www.consultant.ru/document/cons_doc_LAW_221756/ (дата обращения: 06.06.2019).

References:

1. Decree of the President of the Russian Federation dated 01.12.2016 N 642 "On the Strategy for the Scientific and Technological Development of the Russian Federation" URL: http: http: //www.consultant.ru/document/cons_doc_LAW_207967/ (date of access: 06.06.2019).

2. Decree of the President of the Russian Federation of 05.09.2017 N 203 "On the Strategy for the Development of the Information Society in the Russian Federation for 2017 - 2030" URL: http://www.consultant.ru/document/cons_doc_LAW_216363/ (date of treatment: 06.06.2019).

3. Forecast of the socio-economic development of the Russian Federation for 2018 and for the planning period of 2019 and 2020 URL: http://www.consultant.ru/document/cons_doc_LAW_282738/ (accessed: 06.06.2019).

4. Forecast of the long-term socio-economic development of the Russian Federation for the period until 2030 "URL: http://www.consultant.ru/document/cons_doc_LAW_144190/ (accessed: 06.06.2019).

5. Order of the Government of the Russian Federation of July 28, 2017 N 1632-r <On approval of the program "Digital Economy of the Russian Federation" URL: http://www.consultant.ru/document/cons_doc_LAW_221756/ (date of access: 06.06.2019).

6. Стенограмма совещания по вопросам развития технологий в области искусственного интеллекта 30 мая 2019 г URL: http://kremlin.ru/events/president/news/60630 (дата обращения: 06.06.2019).
7. Указ Президента РФ от 07.05.2018 N 204 (ред. от 19.07.2018) "О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года" URL: http://www.consultant.ru/document/cons_doc_LAW_297432/(дата обращения: 06.06.2019).

6. Transcript of the meeting on the development of technologies in the field of artificial intelligence May 30, 2019 URL: http://kremlin.ru/events/president/news/60630 (appeal date: 06.06.2019).

7. Decree of the President of the Russian Federation of 05.05.2018 N 204 (as amended on 07/19/2018) "On national goals and strategic objectives of the development of the Russian Federation for the period until 2024" URL: http://www.consultant.ru/document/cons_doc_LAW_297432 / (appeal date: 06/06/2019).

Статья поступила в редколлегию 18.03.19.
Рецензент: к.т.н., доцент,
Брянский государственный технический университет
Терехов М.В
Статья принята к публикации 30.04.19.

Сведения об авторах

Аверченков Андрей Владимирович
д.т.н., доцент
Заведующий кафедрой «Компьютерные технологии и системы» ФГБОУ ВО «Брянский государственный технический университет»
Тел..: +7 (4832) 58-83-62
E-mail: mahar@mail.ru

Аверченкова Елена Эдуардовна
Кандидат технических наук, доцент,
ФГБОУ ВО «Брянский государственный технический университет»
Тел..: +7 (4832) 56-49-90
E-mail: lena_ki@inbox.ru

Лозбинев Федор Юрьевич
д.т.н., профессор каф. «Компьютерные технологии и системы» ФГБОУ ВО «Брянский государственный технический университет»
Тел..: +7 (4832) 56-49-90
E-mail: kts@tu-bryansk.ru

Information about authors:

Averchenkov Andrey Vladimirovich
Doctor of Technical Sciences, Associate Professor
Head of the department "Computer technology and systems" FSBEI HE «Bryansk State Technical University»,
Tel.: +7 (4832) 58-83-62
E-mail: mahar@mail.ru

Averchenkova Elena Eduardovna
Candidate of Technical Sciences, Associate Professor,
FSBEI HE «Bryansk State Technical University»
Tel.: +7 (4832) 56-49-90
E-mail: lena_ki@inbox.ru

Lozbinev Fedor Yurevich
Doctor of Technical Sciences, Professor of the department «Computer technologies and systems» FSBEI HE «Bryansk State Technical University»,
Tel.: +7 (4832) 56-49-90
E-mail: kts@tu-bryansk.ru

УДК: 658.5.012.7
DOI: 10.30987/article_5d8d113dce2cf3.56127534

О.В. Кондратьева

ОЦЕНКА ЗАКАЗЧИКОМ СЕРВИСА ПОДДЕРЖКИ ИСУП В СФЕРЕ РАДИОЭЛЕКТРОННОЙ ПРОМЫШЛЕННОСТИ В РАМКАХ ЗАПУСКА ЦИКЛА РЕИНЖИНИРИНГА

Представлены результаты исследования, методология оценки сервиса ИСУП. В статье описаны результаты использования метода оценки качествана основе древовидной структуры показателей для запуска цикла реинжиниринга на предприятиях радиоэлектронной промышленности. В статье делается акцент на оценке показателей значимых для Заказчика.

Ключевые слова: *оценка качества услуг, квалиметрия, ключи Кобаяси, функциональность, голос потребителя, древовидная схема показателей качества.*

O.V. Kondratyeva

EVALUATION OF ISUP SUPPORTING SERVICE IN THE RADIO ELECTRONIC INDUSTRY SPHERE WITHIN THE REENGINEERING CYCLE START

The results of the study, the methodology for assessing ISUP service.We have used the method of quality assessment, based on the tree structure of indicators to start the reengineering cycle at the enterprises of the radio-electronic industry and describe the results. The article focuses on the significant for the Customer evaluation of indicators.

Keywords: *service quality, qualimetry, Kobayashi keys, functionality, the user's voice, dendrogram of the indicators of quality.*

Введение

С переходом в постиндустриальную эпоху нарастает глобализация экономики. Доля материальных активов постоянно снижается в пользу нематериальных активов большую часть из которых составляет интеллектуальная собственность, программное обеспечение и услуги.

Сервис поддержки ИСУП стоит на стыке нескольких видов деятельности:

- радиоэлектронной промышленности;
- индустрии программного обеспечения;
- бизнеса услуг.

Можно говорить о устойчивом росте потребности в подобных услугах, объединяющих самые актуальные и быстроразвивающиеся области [2].

Актуальность разработок методик интегрированных систем менеджмента качества определяется недостатком исследований в области услуг и ее связки с нематериальным товаром - программным обеспечением для производств радиоэлектронной промышленности [3].

В данной статье рассматривается методика оценки ствола «Заказчики», для реинжиниринга ИСУП с помощью двух инструментов:

- Оценка текущего состояния качества услуг с помощью древовидной схемы показателей по четырем стволам:
  - Заказчики;
  - Процесс;
  - Владельцы
  - Государство.

Разработки плана мероприятий, на основе методики PROF Кобаяси.

1. Оценка качества сервиса Заказчиком

Оценка ствола «Заказчики» (q_1) ведется по трем ветвям:

P_1 - функциональность;

P_2 - удобство;

P_3 - эмоциональный фон;

Так как нулевой показатель качества по ветви «Функциональность» автоматически приводят к нулевому показателю качеству всего ствола, то:

$$q_1 = P_1\left(\frac{P_2 + P_3}{2}\right) \quad (1)$$

2. Показатель «Функциональность»

По стволу «Заказчики» оценивается в разрезе выполненных за 2016 год заявок по видам работ и достаточным уровнем Надежности, Ответственности, Доступности и Коммуникабельности каждой из них по отношению ко всем заявкам:

$$Y_{vi} = \frac{KD_{vi}}{K}, \quad (2)$$

где Y_{vi}- значение метрик показателя «Функциональность» ствола «Заказчики»;v – вид работ; i – вид оценки, такой что: i = 1 -> Надежность ; i = 2 -> Ответственность; i = 3 -> Доступность; i = 4 -> Коммуникабельность; KD_{vi} - количество заявок, выполненных по виду работ (v) с достаточным уровнем по виду оценки (i); K – количество заявок, выполненных за весь период.

Таблица 1. «Значение метрик показателя «Функциональность» ствола «Заказчики» по заявкам»

Вид работ / Вид оценки	Надежность	Ответственность	Доступность	Коммуникабельность
Администрирование	0,9895632	0,8492649	Нет	Нет
Внутренние изменения	0,8763291	0,8494321	0,98756	0,9307534
Внешние изменения	0,6742187	0,7593218	0,98756	0,8393632
Новые технологии	Нет	0,9430721	0,98756	Нет
Узкие места	0,6309821	0,6937183	0,78530	0,8302735
Стандартные операции	0,9895209	0,9502784	0,98756	0,9960276
Регламентные работы	0,8956108	Нет	0,87301	Нет
Инциденты	0.4328200	0,5710834	0,73028	0,483021

Несколько слов нужно сказать о распространенной сегодня тенденции использования виртуальных машин. Отдельная виртуальная машина – это самостоятельный объект, в котором существуют те же слои рассматриваемых объектов, что и в реальной, но только в «гостевом» варианте. Однако в расширенном контексте, включающем реальные АС, хост и гипервизор, последний занимает слой S_4 (полагаем, что он разрабатывался с помощью инструментального слоя S_3), а значит слои «гостевой» машины, включая виртуальный вариант слоя S_0, должны нумероваться как S_{4+1}, S_{4+2}, и так далее.

Метрика безопасность рассчитывается как процент заявок в службу безопасности по виду заявки «Инцидент» ко все заявкам за год.

$$Y_{\text{безопасность}} = \frac{KD_{\text{безопасность}}}{K}, \quad (3)$$

где $Y_{\text{безопасность}}$ - значение метрики «Безопасность» показателя «Функциональность» ствола «Заказчики»;

$KD_{\text{безопасность}}$ - количество заявок, выполненных подразделением «Служба безопасности» с видом заявки «Инцидент»;

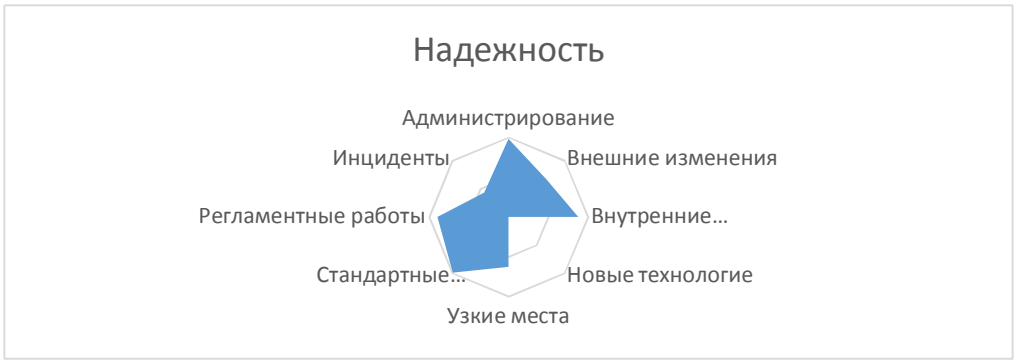
K – количество заявок, выполненных за весь период.

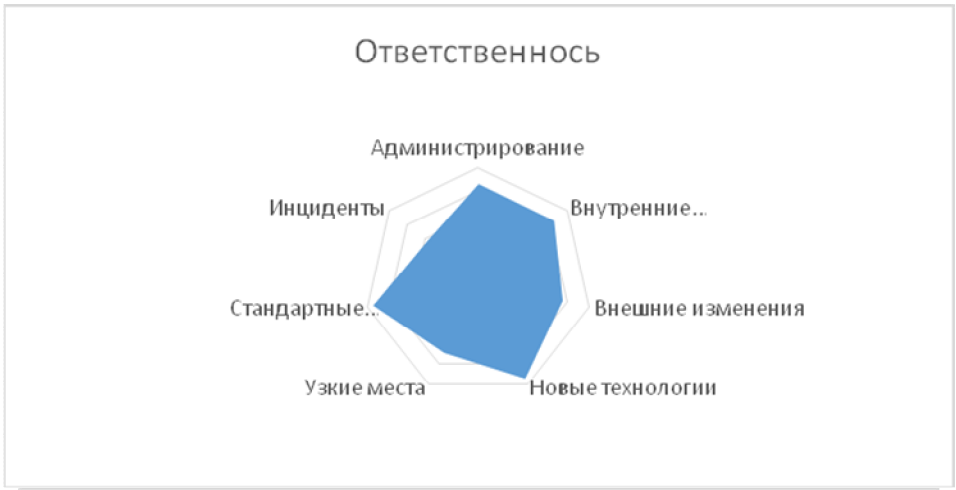
В 2016 году для службы поддержки

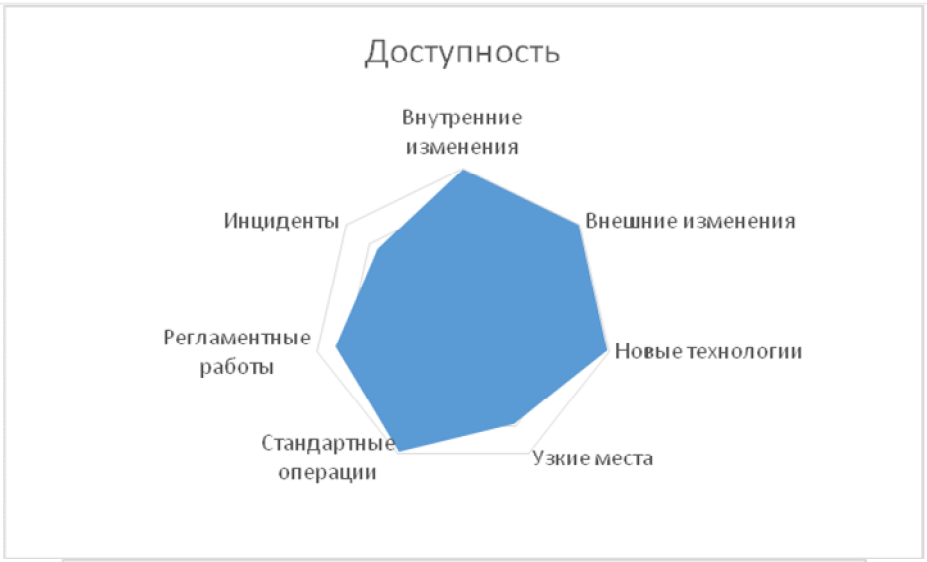
$$Y_{\text{безопасность}} = 0{,}957626$$

Для показателя «функциональность» (P_1) все метрики $Y_1 \in [0,1]$, т.е. нормированы. Также не представляется возможным выделить более/менее важный вид работ или вид оценки, поэтому будем считать все метрики равнозначными. Следовательно, значение интегрального показателя «Функциональность» можно представить в мультипликативной форме:

$$P_1 = \prod_{i=1}^{n} Y_i \quad (4)$$







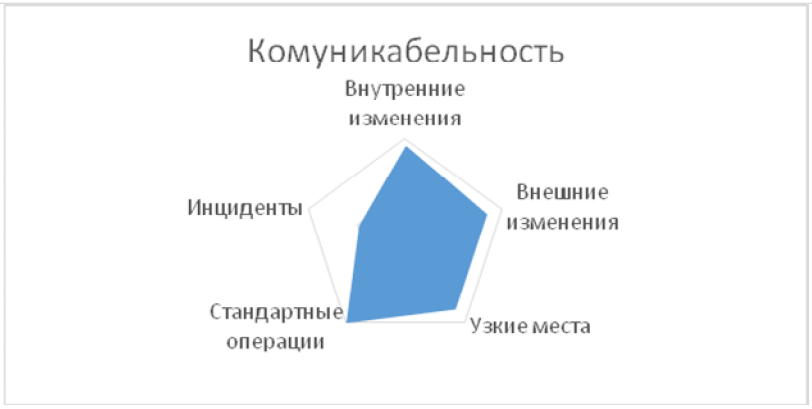


Рис. 1. Оценка функциональности

За 2016 год

$$P_1 = 0.843567.$$

3. Ветка «Удобство»

Ветка «Удобство» оценивается путем опроса заказчиков с помощью анкетирования на сайте по критериям (листьям): комфорт, интерфейс, конфликтные ситуации, обратная реакция, экстренные ситуации и функциональность [5]. Для обработки результата используется кано-модель, т.е. анкетирование происходит в два этапа:

- сначала определяется степень важности показателя для анкетируемого (http://www.kanosurvey.com/?id=p12470259983);
- затем оценивается удовлетворенность существующим уровнем сервиса по каждому показателю.

В результате обработки ответов респондентов первого этапа полученные результаты распределяем в соответствии с представленной ниже таблицей.

Таблица 2 Таблица ответов респондентов по методу Кано

Функциональная характеритика	Дисфункциональная характеристика				
	Доволен	Обязательно должно быть	Безразлично	Относительно не доволен (терпимо)	Не доволен
Мне так нравится	Свойства, вызывающи	Привлекательные свойства	Привлекательные свойства	Привлекательные свойства	Одномерная
Я ожидаю, что это так и есть	Свойства обратного	Незначительные	Незначительные	Незначительные	Обязательные свойства
Я нейтрален	Свойства обратного	Незначительные	Незначительные	Незначительные	Обязательные свойства
Относительно не доволен (терпимо)	Свойства обратного	Незначительные	Незначительные	Незначительные	Обязательные свойства
Не доволен	Свойства обратного действия	Свойства обратного действия	Свойства обратного действия	Свойства обратного действия	Свойства, вызывающие сомнения

Потенциал удовлетворённости клиентов рассчитывается по следующей формуле:

$$ПУ = \frac{k_c + k_o \times 100}{(k_c + k_o + k_н + k_{о.д.} + k_{н.з.})} \quad (5)$$

ПУ. − потенциал для удовлетворённости потребителей, %; k_c − количество ответов респондентов, характеризующие свойства, вызывающие сомнения %; k_o − количество ответов респондентов, характеризующие одномерные свойства, %; $k_н$ − количество ответов респондентов, характеризующие обязательные свойства, %; $k_{о.д.}$ − количество ответов респондентов, характеризующие свойства обратного действия, %; $k_{н.з.}$ − количество ответов респондентов, характеризующие незначительные свойства, %.

Потенциал для неудовлетворённости клиентов рассчитывается по формуле:

$$ПНУ = \frac{(k_o + k_н + k_{о.д.}) \times (-100)}{(k_п + k_o + k_н + k_{о.д.} + k_{н.з.})} \quad (6)$$

После вычисления Потенциала удовлетворенности *(ПУi.)* и неудовлетворенности *(ПНУi.)* для каждого показателя происходит обработка результатов анкетирования пользователей «Качество работы сервиса поддержки ИСУП» по тем же критериям: комфорт, интерфейс, конфликтные ситуации, обратная реакция, экстренные ситуации и функциональность по шкале: Полностью устраивает, Достаточный, Недостаточный, Полностью не устраивает. С помощью такой оценки можно разделить все ответы на две группы (удовлетворительные и неудовлетворительные), при этом следует учесть, что разные ответы дают разную оценку качества критерия и, следовательно, вносят различный вклад в оценку качества.

Таблица 3 Результаты опроса

i	Критерий	Привле-кательная (%)	Одно-мерная (%)	Необхо-димая (%)	Не имеет значения (%)	Обратно-го действия	Сомни-тельная (%)	Удовлетв орённость *ПУi*.	Неудов-летворён ность
1	комфорт	0	3,6585	0	12,195	3,6585	80,4878	84,14634	-37,5
2	интерфейс	8,536585	64,634	13,4146	7,3170	2,4390	3,65853	74,66667	-83,5443
3	Конфликт-ные ситуации	40,2439	3,6585	0	18,292	4,8780	32,9268	61,22449	-12,7273
4	обратная реакция	28,04878	31,707	14,6341	20,731	0	4,87804	50,84746	-48,7179
5	экстренные ситуации	14,63415	63,414	10,9756	4,8780	0	6,09756	81,42857	-79,2208
6	Функцио-нальность	25,60976	40,243	15,8536	10,975	0	7,31707	63,93443	-60,5263

Таблица 4. «Коэффициенты значимости в зависимости от ответа»

i	Оценка критерия	K_i
1	Полностью устраивает	1
2	Достаточный	0,75
3	Недостаточный	0,25
4	Полностью не устраивает	0

После этого, необходимо найти усредненное значение всех положительных оценок «Полностью устраивает» и «Устраивает» с учетом потенциала удовлетворенности данного критерия и всех отрицательных с учетом потенциала неудовлетворенности.

$$P_2 = \frac{\sum_{j=1}^{j} \begin{cases} w_{ij} > 0{,}5 \rightarrow w_{ij} * \text{ПУ}_i \\ w_{ij} < 0{,}5 \rightarrow -w_{ij} * \text{ПНУ}_i \end{cases}}{100 * j} \quad (7)$$

где W_{ii} - вес оценки качества *i*- того критерия (таблица 4.5) *i*- м респондентом.
Делить на 100 нужно для приведения показателя P_2 в нормальную форму от 0 до 1.
По итогам анкетирования

$$P_2 = 0.4956$$

4. Оценка ветки P_3 - эмоциональный фон

Т.к. имеет смысл оценивать только изменение эмоционального фона [6], то :

$$\underline{P_3 = 0.}$$

Тем не менее, чтобы можно было учесть данные по эмоциональному фону для 2017 года за 2016 год проведены следующие исследования: были собраны сообщения от пользователей в 2016 году

Теперь можно посчитать показатель качества ствола «Заказчики» исходя из формулы 1 $q_1 = P_1\left(\frac{P_2 + P_3}{2}\right)$ и вычисленных показателей P_1, P_2, P_3

$$q_1 = 0.843567(0.4956+0)/2 = 0{,}2090$$

Таблица 5. Эмоциональный фон общения

Сфера/Фон	Общий уровень эмоционального фона (Т)	Уровень агрессивности (Та)	Уровень неформальности (Тн)
Имидж предприятия в глазах внешних и новых Клиентов	2.17	0,01	0
Сфера потенциального роста и расширения деятельности	1.03	0	0
Область обычной деятельности	1.48	0, 04	0,03
Область повышенной активности	1,33	0,02	0.05

Заключение

Предложенная древовидная информационная модель построения структуры показателей на основе полезности[4] и методика оценки эмоционального фона общения применительно к сервису поддержки ИСУП дает возможность оценить качество услуг в сфере поддержки ИСУП на предприятиях радиоэлектронной промышленности [1] для того, чтобы опытным путем определить оптимальные ряда качественных показателей, таких как удовлетворенность заказчика с учетом изменений эмоционального фона общения.По результатам оценки сервиса поддержки ИСУП была определена база для сравнения результатов внедрения цикла реинжиниринга и оценки эффективности заявленных к выполнению мероприятий.

Список литературы:

1. Антохина Ю.А., Варжапетян А.Г., Семенова Е.Г. / Интеграция моделей, методов и инструментов управления проектами. СПб Политехника, 2015, 360 с.
2. Антохина Ю.А., Варжапетян А.Г., Семенова Е.Г / Информационная поддержка процессов улучшения качества технических объектов. СПб, Политехника, 2016 г. - 315 с.
3. Антохина Ю.А. Варжапетян А.Г., Семенова Е.Г. / Управление рисками инновационной деятельности в радиоэлектронной промышленности. СПб. Политехника, 2017 г. 335 с.
4. Реинжиниринг процессов сервиса поддержки исуп в разрезе современных подходов улучшения качества услуг Кондратьева О.В., Кондратьева О.А.Решение. 2018. Т. 1. С. 151-153.
5. Квалиметрический подход к оценке инфраструктуры услуги в сфере информационных технологий. Кондратьева О.В. В сборнике: Инновационные технологии управления сборник статей по материалам IV Всероссийской научно-практической конференции. Нижегородский государственный педагогический университет имени Козьмы Минина. 2017. С. 219-221.
6. Использование автоматизированного контент-анализа для оценки удовлетворенности заказчика Кондратьева О.В. В сборнике: Моделирование и ситуационное управление качеством сложных систем Сборник докладов. 2015. С. 43-46.

References:

1. Antonina Yu. A., Varzhapetyan, A. G., Semenova, E. G. / Models, methods and project management tools integrations. St. Petersburg Polytechnic, 2015, 360 p.
2. Antokhina, Y. A., Varzhapetyan, A. G., Semenova E. G / Quality improvement of technical objects informational support. St. Petersburg, Polytechnic, 2016 315 p.
3. Antokhina, Y. A., Varzhapetyan, A. G., Semenova E. G. / risk Management innovation activities in the electronic industry. SPb. Polytechnic, 2017 335 p.
4. Isupservice processes support reengineering to in the context of improvementof the quality services modern approaches. Kondratieva O. V., Kondrateva O. A. Decision. 2018. Vol.1. P. 151-153.
5. Qualimetric approach to evaluation of the infrastructure services in the field of information technology. Kondratyeva O. V. In the collection: Innovative management technologies collection of articles on the materials of the IV all-Russian scientific and practical conference. Nizhny Novgorod State Pedagogical University named after Kozma Minin. 2017. P. 219-221.
6. Automated content analysis using for assessing customer satisfaction Kondratyeva O. V. In the book: Modeling and situational control of complex systems as a Collection of papers. 2015. P. 43-46.

Статья поступила в редколлегию 06.03.19.
Рецензент: д.т.н., доцент, Брянский государственный технический университет Аверченков А.В.
Статья принята к публикации 15.04.19.

Сведения об авторах

Кондратьева Ольга Васильевна
Аспирант Государственного Университета Аэрокосмического Приборостроения
тел.: +7 (911) 111 32 31
E-mail: Kondratievao@mail.ru

Information about authors:

Kondratyeva Olga Vasilievna
PhD Student Of The State University Of Aerospace Instrumentation,
tel.: +7 (911) 111 32 31
E-mail: Kondratievao@mail.ru

УДК: 33.334.72
DOI: 10.30987/article_5d8d113dea1d58.70434521

А.Ю. Малюкина, Т.М. Геращенкова

НОРМИРОВАНИЕ И ОПРЕДЕЛЕНИЕ УЧЕБНОЙ НАГРУЗКИ ПРЕПОДАВАТЕЛЕЙ КАК СПОСОБ ОПТИМИЗАЦИИ РАСЧЕТА ЗАРАБОТНОЙ ПЛАТЫ ППС

В данной статье рассматриваются проблемы, связанные с эффективностью нормирования и определения всех видов работ профессорско-преподавательского состава. Показано влияние данного фактора на расчет заработной платы ППС, а также оптимизацию указанного процесса.

Ключевые слова: *нормирование, учебная нагрузка преподавателя, расчет заработной платы, профессорско-преподавательский состав (ППС), оптимизация расчета.*

A.Yu. Malyukina, T.M. Gerashchenkova

NORMALIZATION AND DETERMINATION OF THE EDUCATIONAL LOAD OF TEACHERS AS A METHOD FOR OPTIMIZING THE CALCULATION OF PAYMENT OF TS

This article discusses the problems associated with the effectiveness of standardization and determination of all types of work of the teaching staff. The influence of this factor on the payroll calculation of teaching staff, as well as the optimization of this process, is shown.

Keywords: *rationing, teacher's workload, payroll, teaching staff (TS), calculation optimization.*

Введение

Современная политическая и экономическая ситуация в стране актуализирует исследования, направленные на поиск путей эффективного распределения бюджетных средств в условиях, когда ресурсы весьма ограничены. Это в равной степени относится как к системе образования в целом, так и к распределению средств внутри отдельных высших учебных заведений.

Проблема в данном случае заключается не только в определение оптимальной суммы финансирования ВУЗа, но и в поиске подходов к ее обоснованию. Причем, грамотность принятия этих решений напрямую влияет на инновационное развитие высшего учебного заведения и расчет заработной платы профессорско-преподавательского состава.

Безусловно, деятельность ППС, как и любая другая профессиональная деятельность должна нормироваться, и эти нормы должны быть использованы не только для отслеживания трудовой деятельности, но и для расчета денежного вознаграждения преподавателя.

1. Учебная нагрузка

Оплата труда профессорско-преподавательского состава и других работников, задействованных в оказании образовательных услуг, не в полной мере учитывает специфику трудоемкости работ по реализации образовательных программ, и связана, главным образом, с учебной нагрузкой (рис.1). Она складывается из:

1) учебной работы, которая включает аудиторную работу, контроль знаний студентов, консультационные работы, руководство практикой студентов, руководство курсовыми работами и проектами, выпускными квалификационными работами и проектами, магистерскими диссертациями и многим другим;

2) внеаудиторной работы: научно-исследовательская деятельность, учебно-методическая работа, воспитательная работа, время, затраченное на подготовку к занятиям со студентами, проверка курсовых, контрольных и прочее.

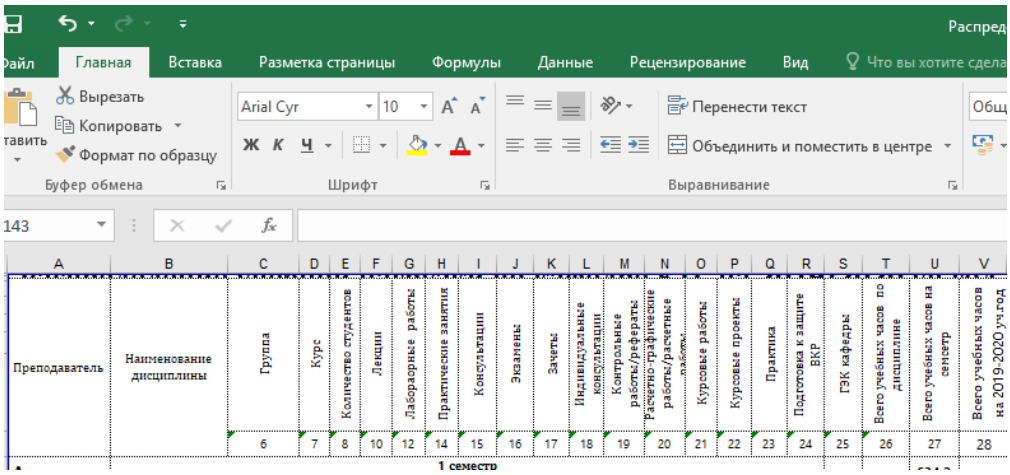


Рис. 1. Виды работ, включенные в расчет учебной нагрузки

Следует учесть, что определенная часть заработной платы (так называемая переменная часть) зависит от количества обучаемых студентов, поскольку обусловливаться нормами времени на прием курсовых проектов (работ), зачетов, экзаменов и прочего, что определяется путем расчета на 1 студента. Однако, как показывает практика, определить, выполнил ли каждый конкретный преподаватель всю годовую нагрузку внеаудиторной работы невозможно.

2. Внеаудиторная работа

Некоторые ВУЗы, чтобы хоть в какой-то степени иметь возможно оценить внеаудиторную работу ППС, вводят в обиход программы оценки рейтинга своих сотрудников. Так, например, в Брянском государственном техническом университете используется программа АС «Мониторинг» (рис.2). Из рисунка видны основные виды работ, учитываемые программой. Программа фиксирует факт выполнения работы, дату выполнения и присваивает определенное количество баллов за проделанный труд, но, к сожалению, не учитывает время затраченное преподавателем для выполнения данной работы.

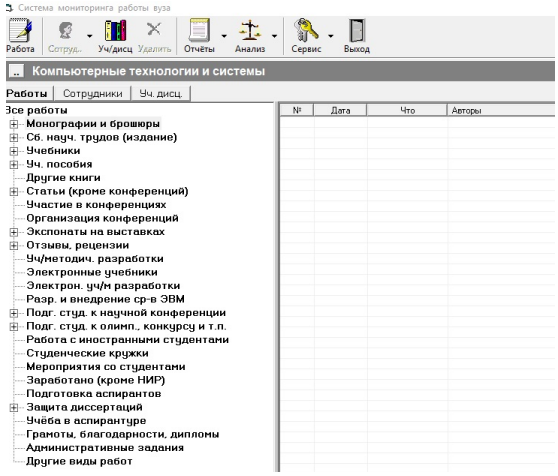


Рис. 2. Скриншот основных вкладок программы АС «Мониторинг»

Для того, чтобы иметь возможность контролировать деятельность преподавателя в рамках вне учебной нагрузки, все виды работы, связанные с ней, должны оцениваться в часах, исходя из продолжительности и степени сложности их реализации. Также должно быть определено соотношение нагрузки аудиторной и внеаудиторной в самой учебной нагрузке преподавателя.

3. Документация

Первичными документами для расчета объема учебной работы ППС университета являются действующие государственные образовательные стандарты высшего

профессионального образования; письмо Министерства образования РФ № 14-55-784 ин/15 от 26.06.2003; учебные планы по специальностям, направлениям и профилямобучения; рабочие учебные планы групп (рис. 3), утвержденные в установленном порядке; заявки на выполнение учебной нагрузки; «Нормы времени для расчета объема учебной работы, планирования основных видов учебно-методической, научно-исследовательской и других работ, выполняемых профессорско-преподавательским составом университета», утвержденные приказом ректора университета № 495/03 от 30.06.2015 г.

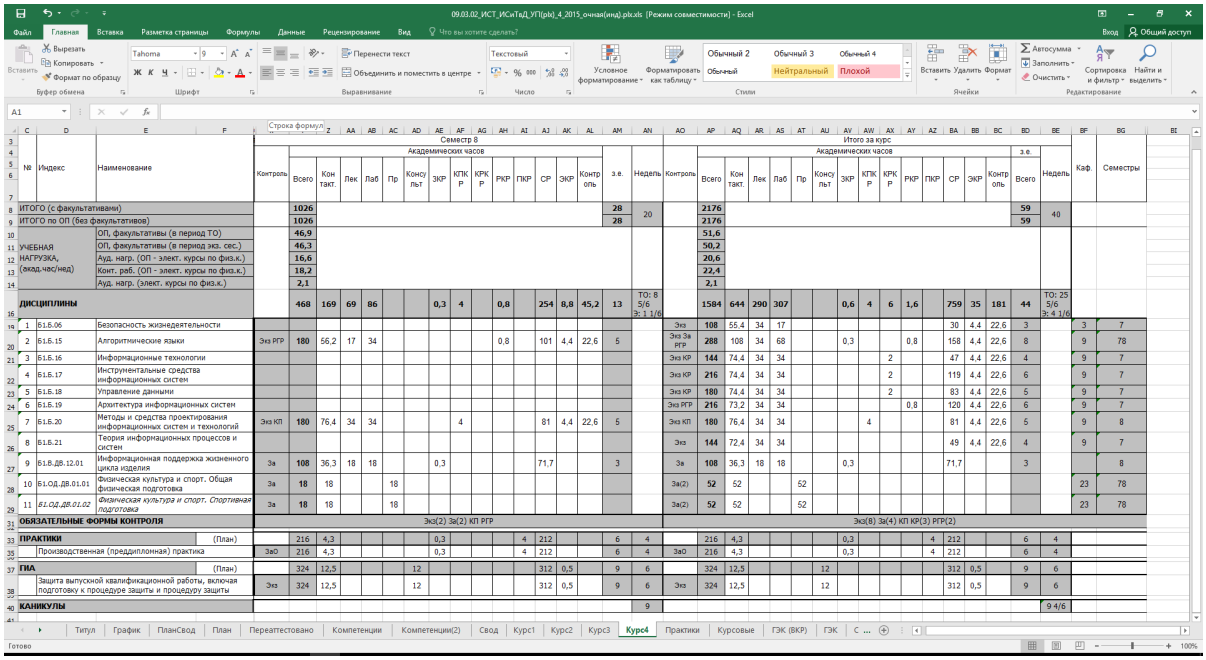


Рис. 3. Скриншот учебного плана в программе MS Excel

Основными документами, определяющими объем и виды работы каждого преподавателя, являются учебное задание и индивидуальный учебный план. Составляется индивидуальный учебный план на каждый текущий учебный год, и включает в себя: плановую учебную, учебно-методическую, научно-исследовательскую и организационно-воспитательную работу, повышение квалификации и другие виды работ составляемых в соответствии с «Нормами времени для расчета объема учебной работы, планирования основных видов учебно-методической, научно-исследовательской и других работ, выполняемых профессорско-преподавательским составом университета» (письмо Министерства образования РФ № 14-55-784 ин/15 от 26.06.2003).

Заключение

У каждого высшего учебного заведения имеется своя база данных учета студенческого контингента, которая помогает отслеживать количество вновь прибывших, отчисленных и переведенных студентов из разных групп. В Брянском государственном техническом университете такую БД называют подсистему «Деканат» (рис.4.).

Изменение соотношения численности учащихся на единицу ставки преподавательского состава позволяет сохранить соотношение аудиторной и внеаудиторной работы преподавателя, но, в то же время, это приводит к увеличению численности персонала преподавательского состава. Как следствие, данное изменение, приводит к увеличению расходов на оплату труда преподавательского состава.

Так, исходя из всего выше сказанного, можно сделать вывод о том, что на расчет заработной платы влияет очень много факторов, которые необходимо учитывать. Разумеется, работа по совершенствованию системы нормирования учебной нагрузки преподавателя должна продолжаться и развиваться. Идеальным вариантом может стать такая система, которая обеспечила бы, с одной стороны, справедливое с точки зрения норм времени, распределение всех видов учебных и внеаудиторных работ, с другой стороны, высокий уровень мотивации преподавателя к стремлению улучшить свои профессиональные навыки и, конечно же, получить адекватное вознаграждение за свой творческий труд.

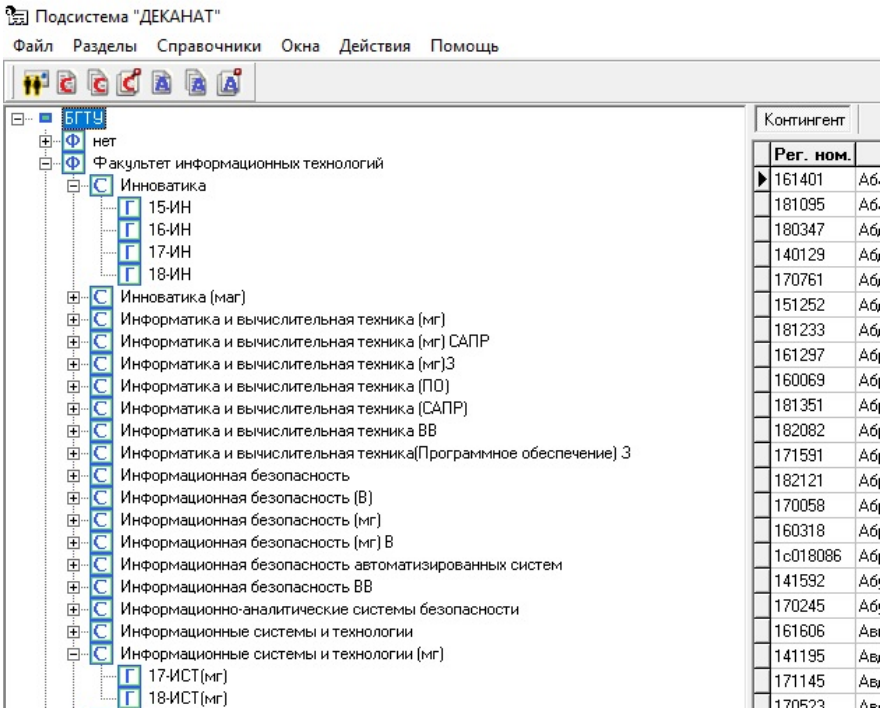


Рис.4. Меню подсистемы «Деканат»

Список литературы:

1. Приказ Министерства образования и науки Российской Федерации от 22 декабря 2014 г. № 1601 г. Москва «О продолжительности рабочего времени (нормах часов педагогической работы за ставку заработной платы) педагогических работников и о порядке определения учебной нагрузки педагогических работников, оговариваемой в трудовом договоре», дата подписания: 22.12.2014 г., дата публикации: 11.03.2015 г., зарегистрирован в Минюсте РФ 25 февраля 2015 г., регистрационный N 36204 [электронный ресурс]. URL: http://www.rg.ru/2015/03/11/chasy-dok.html.

2. Письмо Министерства образования и науки Российской Федерации от 26 июня 2003 г. № 4-55-784 ин/15 и приложение к нему: «Примерные нормы времени для расчета объема учебной работы и основные виды учебно-методической, научно-исследовательской и других работ, выполняемых профессорско-преподавательским составом в образовательных учреждениях высшего и дополнительного профессионального образования» [электронный ресурс]. URL: http://минобрнауки.рф.

3. Постановление Правительства РФ от 17 марта 2015 г. N 234 Москва, «О соотношениях численности работников профессорско-преподавательского состава и обучающихся образовательных организаций высшего образования (В редакции Постановления Правительства Российской Федерации от 29.06.2015 г. N 649)

4. Романов Е. В. Финансирование вузов в целях стимулирования инновационного развития: подходы и механизмы // Университетское управление: практика и анализ. 2015. № 4 (98). С. 87–105.

References:

1. Order of the Ministry of Education and Science of the Russian Federation dated December 22, 2014 No. 1601 Moscow “On the duration of working hours (standards of hours of pedagogical work for the wage rate) of pedagogical workers and on the procedure for determining the teaching load of pedagogical workers, stipulated in the labor contract ", Date of signing: December 22, 2014, date of publication: March 11, 2015, registered with the Ministry of Justice of the Russian Federation on February 25, 2015, registration N 36204 [electronic resource]. URL: http://www.rg.ru/2015/03/11/chasy-dok.html.

2. Letter of the Ministry of Education and Science of the Russian Federation dated June 26, 2003 No. 4-55-784 in / 15 and its annex: “Approximate time standards for calculating the volume of academic work and the main types of teaching, research and other works carried out by the teaching staff in educational institutions of higher and additional professional education ”[electronic resource]. URL: http: //minobrnauki.rf.

3. Decree of the Government of the Russian Federation of March 17, 2015 N 234 Moscow, “On the ratios of the number of employees of faculty and students of educational institutions of higher education (As amended by the Decree of the Government of the Russian Federation of June 29, 2015 N 649)

4. Romanov E. Century. Financing universities in order to stimulate innovative development: approaches and mechanisms // University Management: practice and analysis. 2015. No. 4 (98). S. 87–105.

Статья поступила в редколлегию 03.06.19.
Рецензент: д.т.н., профессор,
Брянский государственный технический университет
Лозбинев Ф.Ю.
Статья принята к публикации 21.06.19.

Сведения об авторах:

Малюкина Ангелина Юрьевна
Аспирант кафедры «Компьютерные технологии и системы» ФГБОУ ВО «Брянский государственный технический университет»
Тел..: +7 (4832) 56-49-90
E-mail: m_eva25@mail.ru

Геращенкова Татьяна Михайловна
д.э.н., профессор кафедры «Компьютерные технологии и системы» ФГБОУ ВО «Брянский государственный технический университет»
Тел..: +7 (4832) 56-49-90
E-mail: gerash-tatyana@yandex.ru

Information about authors:

Malyukina Angelina Yurievna
Postgraduate of the department «Computer technologies and systems»
FSBEI HE «Bryansk State Technical University»,
Tel.: (4832) 56-49-90
E-mail: m_eva25@mail.ru

Gerashchenkova Tatyana Mikhailovna
Doctor of Economic Sciences,Professor of the department «Computer technologies and systems»
FSBEI HE «Bryansk State Technical University»,
Tel.: (4832) 56-49-90
E-mail: gerash-tatyana@yandex.ru

УДК: 66.011:681.51
DOI: 10.30987/article_5d8d113e130732.69448232

А.Н. Лабутин, В.Ю. Невиницын, Г.В. Волкова, А.В. Панасенкова

НЕЛИНЕЙНАЯ СИСТЕМА КАСКАДНО-СВЯЗАННОГО УПРАВЛЕНИЯ ТЕПЛОВЫМ РЕЖИМОМ ХИМИЧЕСКОГО РЕАКТОРА

Используя метод аналитического конструирования агрегированных регуляторов, решена задача синтеза каскадной системы управления тепловым режимом в жидкофазном химическом реакторе, обеспечивающей инвариантность к возмущениям, ковариантность с задающими воздействиями по температуре и асимптотическую устойчивость замкнутой системы. Алгоритмический синтез закона управления проведен с использованием нелинейной математической модели объекта без применения процедуры линеаризации.

Ключевые слова: *аналитическое конструирование агрегированных регуляторов, синергетическая теория управления, химический реактор, каскадная система управления, компьютерное моделирование.*

A.N. Labutin, V.Yu. Nevinitsyn, G.V. Volkova, A.V. Panasenkova

NONLINEAR CASCADE CONTROL SYSTEM OF CHEMICAL REACTOR THERMAL REGIME

Using the analytical design method of aggregated regulators the problem of synthesis of a cascade control system of a thermal regime in a liquid-phase chemical reactor is solved which provides invariance to disturbances, covariance with the giving actions of temperature and asymptotic stability of the closed system. Algorithmic synthesis of the control law was carried out using nonlinear mathematical model of the object without the linearization procedure.

Keywords: *analytical design of aggregated regulators, synergetic control theory, chemical reactor, cascade control system, computer simulation.*

Введение

Реакторная подсистема во многих случаях является центральной в общей схеме превращения исходных реагентов в целевые продукты и в существенной степени определяет ресурсо- и энергосбережение, экономическую эффективность производственного процесса в целом, степень удовлетворения спроса потребителей на те или иные продукты [1]. На стадии проектирования химического производства решается задача оптимального синтеза реакторного узла и задача синтеза алгоритмов управления процессом, а на стадии эксплуатации подзадача организации оптимального функционирования объекта в условиях действия параметрических и сигнальных возмущений [2].

Основной особенностью химических реакторов как объектов управления является их многомерность, нелинейность и многосвязность. В настоящий момент существует ряд различных подходов к синтезу систем управления объектами данного класса, среди которых основными являются: системы адаптивного управления с подстройкой параметров, системы с применением прогнозирующих моделей, регуляторы состояния, робастные системы с использованием ПИД-регуляторов, нечеткие системы управления, нейронные сети. Однако указанные подходы неэффективны при синтезе систем управления существенно нелинейными объектами. На наш взгляд, перспективным в этом плане представляется метод аналитического конструирования агрегированных регуляторов (АКАР), разработанный в рамках синергетической теории управления [3], обеспечивающий асимптотическую

устойчивость системы автоматического управления в целом в широком диапазоне изменения переменных состояния и входных переменных. Эффективность алгоритмов управления, синтезированных методом АКАР, показана в ряде работ [4-9].

Ранее в работе [8] решена задача синтеза нелинейного алгоритма стабилизации температурного режима в жидкофазном химическом реакторе методом АКАР на основе последовательной совокупности инвариантных многообразий (каскадный синтез алгоритма управления температурой). В настоящей работе рассмотрен вариант синтеза нелинейной системы каскадно-связанного управления тепловым режимом методом АКАР.

1. Описание технологического процесса и постановка задачи управления

Жидкофазный химический реактор представляет собой емкостной аппарат непрерывного действия, работающий в политропическом режиме (рис. 1). В аппарате протекает бимолекулярная экзотермическая реакция:

$$A + B \xrightarrow{k_1} P,$$

где A, B – исходные вещества; P – продукт реакции; k_1 – константа скорости. Исходные реагенты A и B подаются в аппарат раздельными потоками. Смесь из реактора забирается насосом. Для отвода тепла и стабилизации температуры в реакторе аппарат снабжен рубашкой, в которую поступает хладагент.

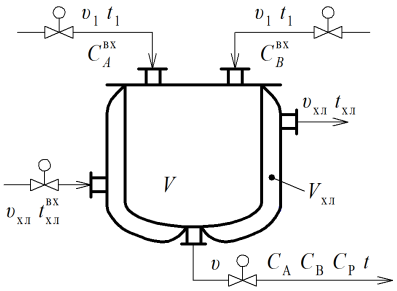


Рис. 1. Принципиальная схема химического реактора

На рис. 1 введены обозначения: $C_A^{\text{вх}}$, $C_B^{\text{вх}}$ – концентрации исходных реагентов; U_1, U_2 – расход исходных реагентов; t_1, t_2 – температуры потоков исходных реагентов; $t_{\text{хл}}^{\text{вх}}$, $t_{\text{хл}}$ – температуры хладоагента на входе и выходе из аппарата; $U_{\text{хл}}$ – расход хладоагента на входе и выходе из аппарата; t – температура реакционной смеси в аппарате; U – расход реакционной смеси на выходе из аппарата; C_{A}, C_{B}, C_{P} – концентрации компонентов A, B, P в реакторе; V – объем реакционной смеси в аппарате; $V_{\text{хл}}$ – объем хладоагента в рубашке.

Математическая модель реактора имеет вид:

$$\begin{aligned}
V\frac{dC_A}{d\tau} &= \upsilon_1 C_A^{вх} - (\upsilon_1+\upsilon_2)C_A - Vk_1C_AC_B,\\
V\frac{dC_B}{d\tau} &= \upsilon_2 C_B^{вх} - (\upsilon_1+\upsilon_2)C_B - Vk_1C_AC_B,\\
V\frac{dC_P}{d\tau} &= Vk_1C_AC_B - (\upsilon_1+\upsilon_2)C_P,\\
V\frac{dt}{d\tau} &= \upsilon_1 t_1 + \upsilon_2 t_2 + \frac{V\Delta Hk_1C_AC_B}{\rho C_T} - (\upsilon_1+\upsilon_2)t - \frac{K_TF_T(t-t_{хл})}{\rho C_T},\\
V_{хл}\frac{dt_{хл}}{d\tau} &= \upsilon_{хл}(t_{хл}^{вх} - t_{хл}) + \frac{K_TF_T(t-t_{хл})}{\rho_{хл}C_{хл}},
\end{aligned} \qquad (1)$$

где $k_1 = k_1^0 \cdot \exp\left(-E_1/R(t+273)\right)$ – константа скорости; k_1^0 – постоянный множитель (предэкспонента) константы скорости; E_1 – энергия активации; R – универсальная газовая постоянная; ΔH – тепловой эффект реакции; ρ, C_T – плотность и теплоемкость реакционной

смеси; $\rho_{хл}$, $C_{хл}$ – плотность и теплоемкость хладоагента; K_T – коэффициент теплопередачи; F_T – поверхность теплообмена.

Общая задача управления химическим реактором заключается в стабилизации температуры смеси в аппарате на заданном уровне $\bar{t}$ в условиях действия возмущений. Управляющим воздействием является расход хладоагента, подаваемый в рубашку.

2. Структурный и алгоритмический синтез каскадной системы управления

Конструктивные и технологические особенности химического реактора, особенности реализации сложного технологического процесса и, соответственно, структурные особенности математической модели (1) позволяют провести декомпозицию системы (1) на две подсистемы. Первая подсистема – это уравнения материального баланса по компонентам и уравнение теплового баланса реакционной смеси. В качестве управления температурным режимом емкости выступает температура хладагента в рубашке. Вторая подсистема – рубашка реактора, функционирование которой описывается уравнением теплового баланса, а состояние характеризуется температурой $t_{хл}$. Управлением для $t_{хл}$ является расход хладагента $U_{хл}$. Структурная схема объекта представлена на рис. 2.

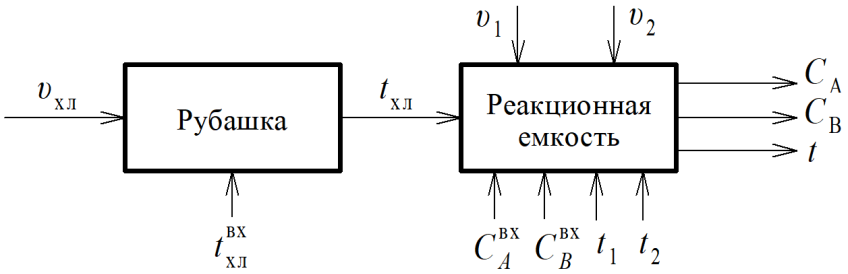


Рис. 2. Структурная схема объекта управления

В линейной теории автоматического управления и в практике автоматизации объектов данной структуры широко используются системы каскадно-связанного регулирования [10]. Решим задачу синтеза системы каскадно-связанного управления температурой в реакторе методами синергетической теории управления. Математическая модель возмущенного движения первой подсистемы (реакционной емкости) примет вид:

$$\begin{aligned} \frac{dC_A}{d\tau} &= f_1, \\ \frac{dC_B}{d\tau} &= f_2, \\ \frac{dt}{d\tau} &= f_4 + \frac{\beta_1}{V}u_1, \end{aligned} \qquad (2)$$

где $f_1 = \dfrac{\upsilon_1 C_A^{вх} - (\upsilon_1 + \upsilon_2)C_A - Vk_1 C_A C_B}{V}$, $f_2 = \dfrac{\upsilon_2 C_B^{вх} - (\upsilon_1 + \upsilon_2)C_B - Vk_1 C_A C_B}{V}$,

$f_4 = \dfrac{\upsilon_1 t_1 + \upsilon_2 t_2 + \alpha k_1 C_A C_B - (\upsilon_1 + \upsilon_2)t - \beta_1 t}{V}$, $\alpha = \dfrac{V\Delta H}{\rho C_T}$, $\beta_1 = \dfrac{K_T F_T}{\rho C_T}$, $u_1 = t_{хл}$.

Задача формулируется следующим образом: необходимо синтезировать закон управления $u_1(C_A, C_B, t)$, переводящий объект из произвольного начального положения в окрестность заданного инвариантного многообразия $\psi_1(C_A, C_B, t) = 0$ и обеспечивающий устойчивое движение вдоль $\psi_1(C_A, C_B, t) = 0$ в конечное состояние.

Эта задача решается за один шаг, так как управление входит непосредственно в уравнение для температуры реакционной смеси [3].

Введем в рассмотрение макропеременную ψ_1:

$$\psi_1 = t - \bar{t},$$

где $\bar{t}$ – заданное значение температуры. Управляющее воздействие должно быть таким, чтобы изменение макропеременной ψ_1 подчинялось основному функциональному уравнению:

$$T_1\dot{\psi}_1 + \psi_1 = 0.$$

Запишем это уравнение в развернутом виде в силу уравнений модели объекта (2):

$$f_4 + \frac{\beta_1}{V}u_1 = -\frac{1}{T_1}(t - \bar{t}).$$

Отсюда получаем

$$u_1 = -\frac{V}{T_1\beta_1}(t - \bar{t}) - \frac{f_4 V}{\beta_1}. \quad (3)$$

Параметром настройки алгоритма управления является величина T_1. Условие асимптотической устойчивости замкнутой подсистемы управления реакционной емкостью: $T_1 > 0$.

Для доказательства устойчивости движения замкнутой системы в заданное конечное состояние подставим выражение для управления (3) в последнее уравнение модели (2). Получим, что изменение температуры описывается уравнением

$$\frac{dt}{d\tau} = -\frac{1}{T_1}(t - \bar{t})$$

или

$$T_1\frac{dt}{d\tau} + t = \bar{t}.$$

Это уравнение апериодического звена первого порядка, согласно которому при $T_1 > 0$ $t\big|_{\tau\to\infty} = \bar{t}$ – движение асимптотически устойчиво.

Следующий этап синтеза системы управления температурным режимом заключается в синтезе алгоритма управления температурой хладагента – $t_{хл}$. Задача подсистемы управления температурой хладоагента в рубашке заключается в определении такого внешнего управляющего воздействия $-\Delta\upsilon_{хл}$, которое обеспечило бы определенное на первом этапе значение температуры хладоагента $\bar{t}_{хл} = u_1$. Модель подсистемы имеет вид:

$$\frac{dt_{хл}}{d\tau} = f_5 + \frac{(t_{хл}^{вх} - t_{хл})}{V_{хл}}u_2, \quad (4)$$

где $f_5 = \frac{\upsilon_{хл}(t_{хл}^{вх} - t_{хл}) + \beta_2(t - t_{хл})}{V_{хл}}$, $\beta_2 = \frac{K_T F_T}{\rho_{хл} C_{хл}}$, $u_2 = \Delta\upsilon_{хл}$.

В терминах метода АКАР задача синтеза алгоритма управления температурой хладоагента формулируется следующим образом: синтезировать закон управления $u_2(t_{хл})$, переводящий объект из произвольного начального положения в окрестность многообразия $\psi_2(t, t_{хл}) = 0$ и устойчивое движение в заданное конечное состояние.

Притягивающее инвариантное многообразие запишется:

$$\psi_2 = t_{хл} - u_1 = 0.$$

Используя функциональное уравнение $T_2\dot{\psi}_2 + \psi_2 = 0$ и уравнение (4), получим закон управления:

$$f_5 + \frac{(t_{хл}^{вх} - t_{хл})}{V_{хл}}u_2 = -\frac{1}{T_2}(t_{хл} - u_1),$$

$$u_2 = -\frac{V_{хл}}{T_2(t_{хл}^{вх} - t_{хл})}(t_{хл} - u_1) - \frac{f_5 V_{хл}}{(t_{хл}^{вх} - t_{хл})}. \quad (5)$$

Параметром настройки алгоритма управления является величина T_2. Условие

асимптотической устойчивости замкнутой подсистемы управления рубашкой: $T_2 > 0$. Проверка асимптотической устойчивости подсистемы управления температурой хладоагента проводится аналогично, как и на первом этапе.

Исходя из вида выражений (3), (5), структура каскадно-связанной системы управления без учета параметрических возмущений может быть представлена следующим образом (рис. 3).

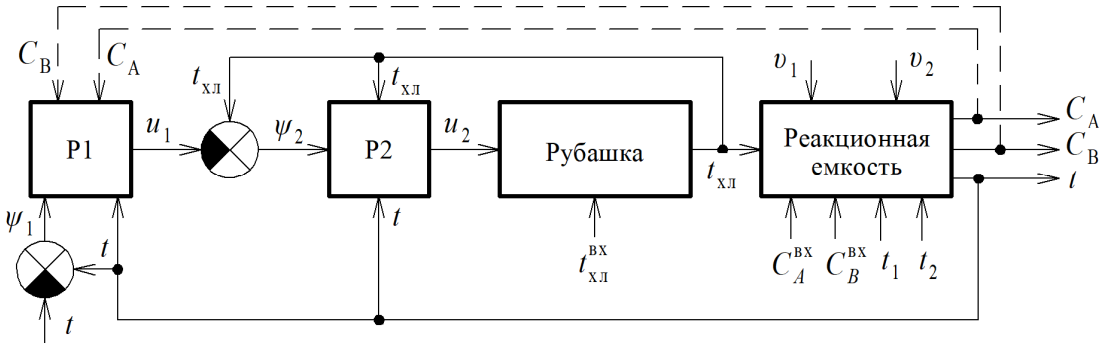


Рис. 3. Структура каскадно-связанной системы управления тепловым режимом реактора: P1 – главный регулятор; P2 – вспомогательный

Подставив u_1 из (3) в (5), получим закон управления для вспомогательного регулятора, определяющий величину внешнего управляющего воздействия:

$$u_2 = -\frac{V_{хл}}{T_2(t_{хл}^{вх} - t_{хл})}\left[t_{хл} + \frac{V}{T_1\beta_1}(t - \bar{t}) + \frac{f_4 V}{\beta_1}\right] - \frac{f_5 V_{хл}}{(t_{хл}^{вх} - t_{хл})}. \quad (6)$$

3. Компьютерное моделирование и результаты

Методами компьютерного моделирования проведено исследование работоспособности каскадно-связанной системы управления тепловым режимом химического реактора с использованием синтезированного нелинейного закона (6). Исследованы свойства инвариантности к возмущениям, ковариантности с задающими воздействиями по температуре и асимптотической устойчивости замкнутой системы.

Моделирование проводилось при технологических и конструктивных параметрах, обеспечивающих оптимальный режим работы химического реактора: V = 500 л; $V_{хл}$ = 290 л; $C_A^{вх} = 19.74$ моль/л; $C_B^{вх} = 10.93$ моль/л; $\upsilon_1 = 1.5$ л/мин, $\upsilon_2 = 3.5$ л/мин, $\upsilon = 5.0$ л/мин, $\upsilon_{хл} = 3.84$ л/мин; t_1 = 20 °C; t_2 = 30 °C; $t_{хл}^{вх}$ = 20 °C; K_T = 12 кДж/(м^2 мин К); F_T = 2.9 м^2; ρ = 0.9 кг/л; C_T = 2 кДж/(кг К); $\rho_{хл}$ = 1 кг/л; $C_{хл}$ = 4.18 кДж/(кг К); ΔH = 80 кДж/моль; E = 48635 Дж/моль; $k_1^0 = 109860$ л/(моль мин). Параметры закона управления (6): значение постоянных времени $T_1 = T_2$ = 20 мин (определялись из требований к времени процесса управления); заданное значение температуры смеси в аппарате $\bar{t} = 140$ °C.

На рис. 4, 5 приведены примеры переходных процессов управления в замкнутой системе при начальном отклонении переменной состояния C_A от статики на -20% ($\Delta C_A = -0.2C_A^0$) и ступенчатом изменении задающего воздействия ($\Delta\bar{t} = -10$ °C). Для наглядности переходные процессы до момента приложения входного воздействия (τ = 50 мин) приводятся в статическом режиме.

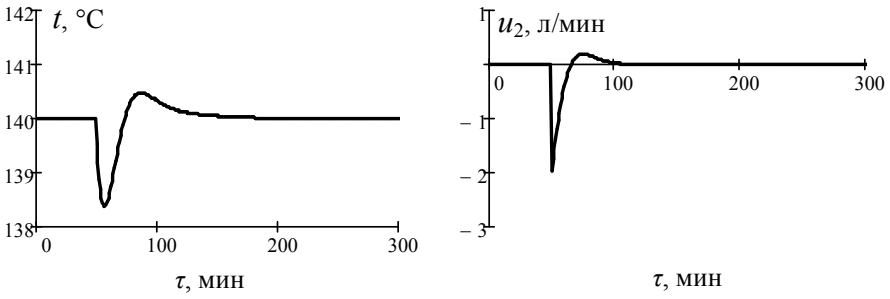


Рис. 4. Переходные процессы в замкнутой системе при начальном отклонении переменной состояния C_A от статики на -20%

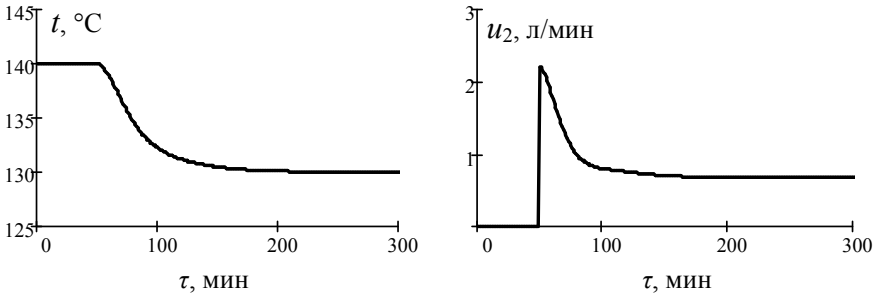


Рис. 5. Переходные процессы в замкнутой системе при ступенчатом изменении заданного значения температуры на -10°С

Скачкообразное изменение управления u_2 в момент приложения возмущений объясняется тем, что не учитывалась инерционность исполнительного механизма на линии подачи хладоагента.

Заключение

В работе предложен вариант синтеза системы управления тепловым режимом химического реактора с применением структуры системы каскадного типа. Методом аналитического конструирования агрегированных регуляторов получены нелинейные алгоритмы управления для главного и вспомогательного регуляторов каскадной системы с применением нелинейной математической модели объекта без применения процедуры линеаризации. Данное обстоятельство является существенным преимуществом при синтезе системы автоматического управления на стадии проектирования при отсутствии физического объекта управления.

Компьютерное моделирование замкнутой системы управления показало ее работоспособность: инвариантность к внутренним и внешним возмущениям, ковариантность с задающими воздействиями и асимптотическую устойчивость при условии полной наблюдаемости объекта управления. Таким образом, показана эффективность метода АКАР при синтезе нелинейных многоконтурных систем управления, в частности систем управления каскадного типа с двумя соподчиненными регуляторами.

Список литературы:

1. Лабутин А.Н., Исаенков А.Е., Волкова Г.В. Оптимальный синтез гибкой реакторной системы // Известия выс-ших учебных заведений. Серия: Химия и химическая технология. 2010. Т. 53. № 12. С. 125-127.

2. Лабутин А.Н., Невиницын В.Ю., Волкова Г.В. Анализ и оптимальный синтез химического реактора как объекта управления // Химическая Промышленность. 2018. Т. 95. № 5. С. 241-248.

3. Колесников А.А. Синергетическая теория управления. М.: Энергоатомиздат, 1994. 344 с.

4. Лабутин А.Н., Невиницын В.Ю., Волкова Г.В. Робастное управление температурным режимом химического реактора // Информатика и системы управления. 2018. № 3. С. 115-123. DOI: 10.22250/isu.2018.57.115-123.

5. Лабутин А.Н., Невиницын В.Ю., Волкова Г.В., Зайцев В.А. Синергетический синтез эффективного

References:

1. Labutin A.N., Isaenkov A.E., Volkova G.V. Optimal'nyj sintez gibkoj reaktornoj sistemy [Optimal synthesis of a flexible reactor system]. Izv. Vyssh. Uchebn. Zaved. Khim. Khim. Tekhnol. 2010. vol. 53. no. 12. pp. 125-127 (in Rus-sian).

2. Labutin A.N., Nevinitsyn V.Yu., Volkova G.V. Analiz i optimal'nyj sintez khimicheskogo reaktora kak ob"ekta up-ravleniya [Analysis and optimal synthesis of the chemical reactor as a control object]. Khimicheskaya Promyshlennost'. 2018. vol. 95. no. 5. pp. 241-248 (in Russian).

3. Kolesnikov A.A. Sinergeticheskaya teoriya upravleniya [Synergetic control theory]. Moscow, Energoatomizdat, 1994. 344 p. (in Russian).

4. Labutin A.N., Nevinitsyn V.Yu., Volkova G.V. Robastnoe upravlenie temperaturnym rezhimom khimicheskogo reaktora [Robust control of a chemical reactor temperature regime]. Informatika i sistemy upravleniya. 2018. no. 3. pp. 115-123. DOI: 10.22250/isu.2018.57.115-123 (in Russian).

5. Labutin A.N., Nevinitsyn V.Yu., Volkova G.V., Zaitsev V.A. Sinergeticheskij sintez ehffektivnogo

комплекса «реактор – управляющая система» //Современные наукоемкие технологии. Региональное приложение. 2018. №4(56). С. 36-43.

6. Лабутин А.Н., Невиницын В.Ю., Зайцев В.А., Волкова Г.В. Робастное управление концентрацией целевого продукта в химическом реакторе // Известия высших учебных заведений. Серия: Химия и химическая технология. 2018. Т. 61. № 12. С. 129-136. DOI: 10.6060/ivkkt.20186112.5914.

7. Лабутин А.Н., Невиницын В.Ю., Волкова Г.В., Сальков В.М. Алгоритм управления концентрацией целевого продукта в химическом реакторе // Автоматизация и моделирование в проектировании и управлении. 2018. №2. С. 34-40.

8. Невиницын В.Ю., Лабутин А.Н., Волкова Г.В. Управление температурным режимом химического реактора // Автоматизация и моделирование в проектировании и управлении. 2018. №2. С. 41-48.

9. Labutin A.N., Nevinitsyn V.Yu. Synthesis of Chemical Reactor Nonlinear Control Algorithm Using Synergetic Ap-proach // Известия высших учебных заведений. Серия: Химия и химическая технология. 2017. Т. 60. № 2. С. 38-44. DOI: 10.6060/tcct.2017602.5479.

10. Ротач В.Я. Теория автоматического управления: Учебник для вузов. 2-е изд. М.: Издательство МЭИ, 2004. 400 с.

kompleksa «reaktor – upravlyayushchaya sistema» [Synergistic synthesis of the effective “reactor – control system” complex]. Sovremennye naukoemkie tekhnologii. Regional'noe prilozhenie. 2018. no. 4 (56). pp. 36-43 (in Russian).

6. Labutin A.N., Nevinitsyn V.Yu., Zaitsev V.A., Volkova G.V. Robastnoe upravlenie koncentraciej celevogo produkta v khimicheskom reaktore [Robust control of target product concentration in a chemical reactor]. Izv. Vyssh. Uchebn. Zaved. Khim. Khim. Tekhnol. 2018. vol. 61. no. 12. pp. 129-136. DOI: 10.6060/ivkkt.20186112.5914 (in Russian).

7. Labutin A.N., Nevinitsyn V.Yu., Volkova G.V., Salkov V.M. Algoritm upravleniya koncentraciej celevogo produkta v khimicheskom reaktore [Algorithm of target product concentration control in a chemical reactor]. Avtomatizaciya i modelirovanie v proektirovanii i upravlenii. 2018. no. 2. pp. 34-40 (in Russian).

8. Nevinitsyn V.Yu., Labutin A.N., Volkova G.V. Upravlenie temperaturnym rezhimom khimicheskogo reaktora [Con-trol of a chemical reactor temperature regime]. Avtomatizaciya i modelirovanie v proektirovanii i upravlenii. 2018. no. 2. pp. 41-48 (in Russian).

9. Labutin A.N., Nevinitsyn V.Yu. Synthesis of chemical reactor nonlinear control algorithm using synergetic approach. Izv. Vyssh. Uchebn. Zaved. Khim. Khim. Tekhnol. 2017. vol. 60. no. 2. pp. 38-44. DOI: 10.6060/tcct.2017602.5479.

10. Rotach V.Ya. Teoriya avtomaticheskogo upravleniya [Theory of automatic control]. Moscow, Izdatel'stvo MEHI, 2004. 400 p. (in Russian).

Статья поступила в редколлегию 19.04.19.
Рецензент: к.т.н., доцент,
Брянский государственный технический университет
Подвесовский А.Г.
Статья принята к публикации 08.05.19.

Сведения об авторах

Лабутин Александр Николаевич
доктор технических наук, профессор кафедры «Техническая кибернетика и автоматика» Ивановского государственного химико-технологического университета. Служебный адрес: 153000, г. Иваново, Шереметевский проспект, 7.
Тел. рабочий: +7 (4932) 32 72 26
Тел. сот: +7 (910) 985 43 05.
E-mail: lan@isuct.ru

Невиницын Владимир Юрьевич
кандидат технических наук, доцент кафедры «Техническая кибернетика и автоматика» Ивановского государственного химико-технологического университета.
Служебный адрес: 153000, г. Иваново, Шереметевский проспект, 7.
Тел. рабочий: +7 (4932) 32 72 26
Тел. сот: +7 (915) 837 94 53
E-mail: nevinitsyn@gmail.com

Information about authors:

Labutin Alexander Nikolaevich
Academic degree and title: Doctor of Technical Sciences, Professor. Position and place of work: Head of Chair, department of «Technical Engineering Cybernetics and Automation», Ivanovo State University of Chemistry and Technology. Location: Sheremetevskiy Avenue, 7, Ivanovo, 153000.
Tel.: +7 (4932) 32 72 26
E-mail: lan@isuct.ru

Nevinitsyn Vladimir Yurievich
Academic degree and title: Candidate of Technical Sciences, Associate Professor. Position and place of work: Associate Professor, department of «Technical Engineering Cybernetics and Auto-mation », Ivanovo State University of Chemistry and Technology. Location: Sheremetevskiy Avenue, 7, Ivanovo, 153000.
Tel.: +7 (4932) 32 72 26
E-mail: nevinitsyn@gmail.com

Волкова Галина Витальевна
кандидат технических наук, доцент кафедры «Техническая кибернетика и автоматика» Ивановского государственного химико-технологического университета.
Служебный адрес: 153000, г. Иваново, Шереметевский проспект, 7.
Тел. рабочий: +7 (4932) 32 72 26
E-mail: konf_gv@mail.ru

Панасенкова Анастасия Валерьевна
магистрант кафедры «Техническая кибернетика и автоматика» Ивановского государственного химико-технологического университета.
Служебный адрес: 153000, г. Иваново, Шереметевский проспект, 7.
Тел. рабочий: +7 (4932) 32 72 26
E-mail: trafalgar322@gmail.com

Volkova Galina Vitalievna
Academic degree and title: Candidate of Technical Sciences, Associate Professor. Position and place of work: Associate Professor, department of «Technical Engineering Cybernetics and Auto-mation », Ivanovo State University of Chemistry and Technology. Location: Sheremetevskiy Avenue, 7, Ivanovo, 153000.
Tel.: +7 (4932) 32 72 26
E-mail: konf_gv@mail.ru

Panasenkova Anastasia Valeryevna
Academic degree and title: – Position and place of work: graduate student, department of «Technical Engineering Cybernetics and Automa-tion », Ivanovo State University of Chemistry and Technology. Location: Sheremetevskiy Avenue, 7, Ivanovo, 153000.
Tel.: +7 (4932) 32 72 26
E-mail: trafalgar322@gmail.com

Учредитель и издатель: Федеральное государственное бюджетное образовательное учреждение высшего образования "Брянский государственный технический университет"
Адрес редакции и издателя: 241035, Брянская область, г. Брянск, бульвар 50 лет Октября, 7
ФГБОУ ВО «Брянский государственный технический университет»
Телефон редакции журнала: (4832) 56-49-90. E-mail: aim-pu@mail.ru
Вёрстка А.А. Алисов. Корректор А.Ю. Малюкина.
Сдано в набор 16.09.2019. Выход в свет 30.09.2019.
Объём 50 Мб. ОЗУ 512 Мб. Internet Explorer, Adobe Reader 5.0 и выше.
12+