

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

**ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ:
ТЕОРИЯ, ИНСТРУМЕНТЫ, ПРАКТИКА**

Материалы XIII Международной
интернет-конференции молодых ученых,
аспирантов, студентов
(16 ноября – 31 декабря 2021 г.)

Издательство
Пермского национального исследовательского
политехнического университета
2022

Конференция посвящена вопросам системных исследований и моделирования информационно-измерительных и управляющих систем, систем телекоммуникации и связи, энергетики и энергоресурсосбережения, информационных технологий и средств автоматизации, аппаратно-программного обеспечения информационно-управляющих систем.

Представлены работы молодых ученых, аспирантов, а также лучшие работы студентов.

Публикуемые результаты исследований могут быть интересны молодым исследователям, преподавателям и специалистам, интересующимся теоретическими и прикладными разработками в данной предметной области.

Редакционная коллегия:

В.В. Черняев, доцент, канд. техн. наук;

Б.В. Кавалеров, доцент, д-р техн. наук;

Д.К. Елтышев, доцент, канд. техн. наук (отв. редактор);

А.Б. Петроченков, доцент, канд. техн. наук;

Н.М. Труфанова, профессор, д-р техн. наук;

Р.А. Файзрахманов, профессор, д-р экон. наук;

А.Г. Щербинин, профессор, д-р техн. наук;

А.А. Южаков, профессор, д-р техн. наук

Рецензент: заслуженный деятель науки РФ, заслуженный машиностроитель Республики Башкортостан, доктор технических наук, профессор кафедры автоматизированных систем управления Уфимского государственного авиационного технического университета *Г.Г. Куликов*

Секция 1

НОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ

А.Н. Аношкин, Р.Т. Мурзакаев, О.А. Кашин

Пермский национальный исследовательский
политехнический университет, Пермь

ПОСТРОЕНИЕ РАЗВЕРТКИ СРЕДИННЫХ ПОВЕРХНОСТЕЙ СЛОЁВ АРМИРУЮЩЕГО МАТЕРИАЛА

В статье представлен разработанный алгоритм построения развертки срединных поверхностей слоёв армирующего материала в композитных конструкциях. С помощью разработанного алгоритма и программного комплекса построены развертки слоёв модельной конструкции. Разработанный алгоритм может использоваться при определении разверток слоёв для выкройки их из материала на плоттере.

Ключевые слова: математическое моделирование, композиционный материал, многослойная конструкция, развертка поверхности, выкройка слоя.

A.N. Anoshkin, R.T. Murzakaev, O.A. Kashin

Perm National Research Polytechnic University, Perm

CONSTRUCT OF THE DEVELOPING ON THE MIDDLE SURFACES OF THE REINFORCING MATERIAL LAYERS

In this article presents a developed algorithm for constructing a unfold of the middle surfaces of reinforcing material layers in composite structures. Using the developed algorithm and software package, we have built unfolding of the layers in the typical structure. The developed algorithm can be used to determine the unfolding of layers for cutting them out of the material on a plotter.

Keywords: mathematical modeling, composite material, multilayer construction, developing of surface, layer pattern.

В настоящее время при создании конструкций авиационной техники из композиционных материалов широкое применение получила технология ручной выкладки армирующих слоёв. Такая технология используется при изготовлении как плоских деталей, так и деталей сложной геометрии, например, обшивок, лонжеронов, панелей, люков и т.д. [1].

Одной из основных задач при разработке технологии создания конструкций из композиционных материалов методом ручной вы-

кладки является определение геометрии или геометрических моделей выкроек армирующих слоев, соответствующих заданной схеме армирования. Геометрически выкройки являются развертками на плоскость срединных поверхностей армирующих слоев, формирующих конструкцию. Эти поверхности могут описываться поверхностями второго порядка или аппроксимироваться сплайнами. Алгоритм создания набора слоев для формования конструкций рассмотрен в работах [2–3]. Геометрические модели выкроек направляются для раскроя заданного армирующего материала на плоттер, после чего полученные выкройки армирующих слоев используются в технологическом процессе выкладки на оснастку с использованием лазерных проекторов для контроля точности геометрии укладки слоев. Следует отметить, что погрешности при построении моделей выкроек могут привести к погрешностям схемы армирования и геометрии конструкции. Таким образом, задача точного определения развертки армирующих слоев конструкции сложной формы является актуальной.

В настоящей работе рассматривается модельная конструкция с заданными габаритами: шириной 200 мм, длиной 400 мм, высотой 80 мм, толщиной стенки 3,8 мм, изготовленная из полимерного композиционного материала (рис. 1).

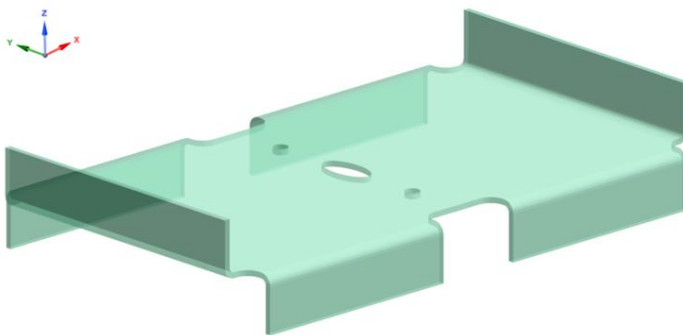


Рис. 1. Общий вид конструкции

Размеры нижней поверхности, на которой задана данная конструкция, указаны на рис. 2. Конструкции подобной геометрической формы применяются при изготовлении композитных лонжеронов и нервюр кессона крыла самолета [4].

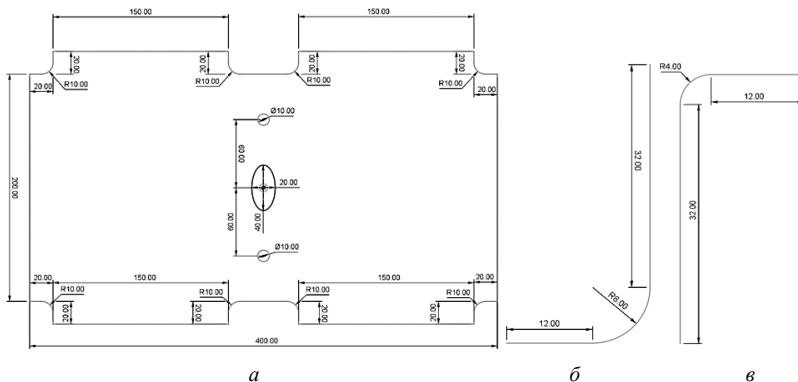


Рис. 2. Чертеж нижней поверхности конструкции с центральным (а), верхним (б) и нижним (в) фрагментами

Рассматриваемая конструкция изготавливается по ручной препреговой технологии – выкладкой в формообразующую оснастку армирующих слоев волокнистого наполнителя, пропитанных полимерным связующим, (препрегов) с последующим отверждением под давлением. Считая толщину каждого слоя препрега равной 0,19 мм, для формования конструкции необходимо подготовить 20 выкроек слоев препрега (рис. 3).

Каждая выкройка представляет собой развертку армирующего слоя на плоскость. Набор выкроек, последовательно уложенных в оснастку, должен обеспечить получение конструкции заданных геометрических размеров.

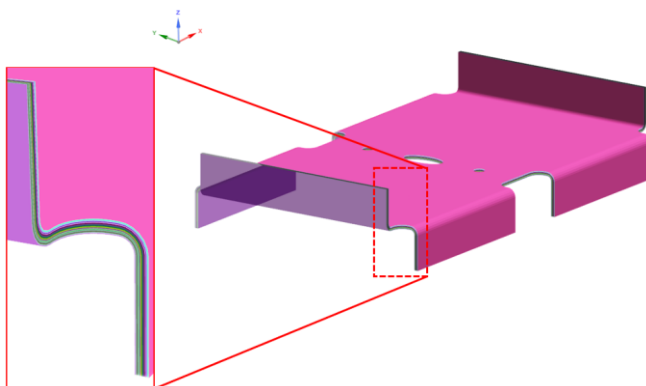


Рис. 3. Конструкция из композита с 20 слоями армирующего материала

Ставится задача – разработать алгоритм построения разверток армирующих слоёв, позволяющий получить требуемый набор выкроек для рассматриваемой типовой конструкции. Следует отметить, что развертка каждого слоя является уникальной из-за различной величины радиуса скругления каждого слоя в области изгиба конструкции.

Геометрия армирующих слоев для заданной конструкции рассматривалась в специально разработанном программном комплексе [5]. При этом каждый слой описывался его толщиной и срединной поверхностью Σ . Цилиндрические подобласти поверхности конструкции были аппроксимированы плоскими с заданной точностью. Таким образом, общая срединная поверхность слоя Σ состоит из n -го количества плоских подобластей $\Sigma_1 \dots \Sigma_n$. Каждая подобласть задана параметрическим уравнением плоскости:

$$\bar{r} = \bar{r}(u, v), u_0 \leq u \leq u_1, v_0 \leq v \leq v_1 \quad (1)$$

и имеет четыре граничные вершины $\bar{r}(u_0, v_0)$, $\bar{r}(u_0, v_1)$, $\bar{r}(u_1, v_0)$, $\bar{r}(u_1, v_1)$, ограничивающие участок плоскости (сегмент), соответствующий фрагменту рассматриваемой конструкции.

Для определения развертки каждой срединной поверхности слоя Σ рассматриваемой конструкции необходимо определить соответствующую наложимую поверхность Σ' , полученную из Σ в результате изгибания, для которой можно установить между их точками M и M' такую биекцию Φ :

$$\Phi: \Sigma \rightarrow \Sigma', \Phi M = M', \quad (2)$$

при которой длины всех соответствующих дуг линий, расположенных на этих поверхностях, равны между собой:

$$s(M_1 M_2) = s'(\Phi(M_1) \Phi(M_2)). \quad (3)$$

Кроме того, будем считать, что слой всегда разворачивается на плоскость OXY , поэтому:

$$z'(u_M, v_M) = 0; \forall M' \in \Sigma'. \quad (4)$$

Из определения наложимости двух поверхностей друг на друга [6] срединную поверхность слоя можно получить изгибанием развертки, аналогично изгибанию гибкой нерастяжимой ткани. Опишем разработанный алгоритм построения развертки срединной поверхности типового слоя.

Шаг 1. Определение исходных данных: массивы криволинейных координат (u, v) , задающих точки поверхности Σ ; массив взаимосвя-

зей точек поверхности Σ , не изменяющихся в процессе преобразования Φ ; параметрические функции $x(u, v), y(u, v), z(u, v)$ для вычисления декартовых координат точек поверхности Σ по заданным криволинейным координатам.

Шаг 2. Определение подобласти начала разворачивания. Составную поверхность Σ будем разворачивать последовательно по подобластям. Первой разворачиваемой подобластью Σ_1 выбирается та, у которой отклонение единичного вектора нормали $N_1 (N_{1x}; N_{1y}; N_{1z})$ от оси OZ минимально.

Шаг 3. Определение координат точек первой подобласти развертки Σ'_1 . Декартовы координаты точек первой подобласти развертки Σ'_1 вычисляются по исходным декартовым координатам точек подобласти Σ_1 с помощью операции поворота на угол α_x вокруг оси OX и на угол $\alpha_y OY$:

$$\alpha_x = \arccos(N_{1x}), \alpha_y = \arccos(N_{1y}). \quad (5)$$

Шаг 4. Определение следующей разворачиваемой подобласти Σ_2 , граничащей с Σ_1 , и подмножества точек G' – общего ребра подобластей Σ'_1 и Σ_2 . Определим на полученном подмножестве G' связанные точки поверхности Σ' , образующие ребро $A'C'$, которому соответствует ребро AC поверхности Σ (рис. 4, а).

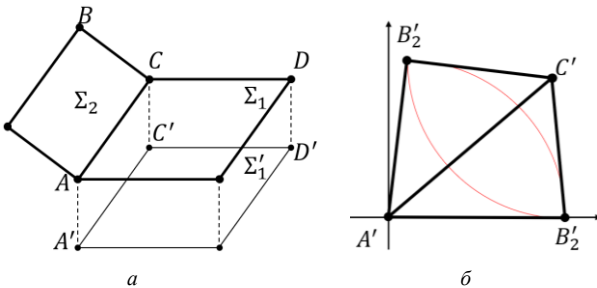


Рис. 4. Определение общего ребра AC подобласти Σ_2 и Σ_1 , разворачиваемой вершины B и дополнительной точки D (а); Отображение точки B на поверхность Σ' с правой и с левой стороны от ребра $A'C'$ (б)

Шаг 5. Определение граничной вершины разворачиваемой подобласти Σ_2 . Определим граничную вершину B , связанную с ребром AC на поверхности Σ , которая не имеет соответствующей ей точки B' на поверхности Σ' (см. рис. 4, а).

Шаг 6. Определение длин отрезков $[BA]$ и $[BC]$ на поверхности Σ по значениям декартовых координат соответствующих точек:

$$s(BA) = |BA|, s(BC) = |BC|. \quad (6)$$

Шаг 7. Определение декартовых координат точек A' и C' на поверхности Σ' :

$$x'_A = x'(u_A, v_A); y'_A = y'(u_A, v_A); x'_C = x'(u_C, v_C); y'_C = y'(u_C, v_C). \quad (7)$$

Шаг 8. Определение декартовых координат точки B' ($x'_B; y'_B; 0$) на поверхности Σ' в результате решения системы квадратных уравнений:

$$\begin{cases} (x'_B - x'_A)^2 + (y'_B - y'_A)^2 = |AB|^2, \\ (x'_B - x'_C)^2 + (y'_B - y'_C)^2 = |BC|^2. \end{cases} \quad (8)$$

Шаг 9. Вырожденным случаем является, если система (8) имеет единственное решение. Геометрически это означает что выбранная точка находится на ребре $A'C'$, и необходимо перейти к шагу 13 алгоритма. Если система (8) имеет два решения, геометрически это означает что выбранная точка может отобразиться как с правой, так и с левой стороны от ребра $A'C'$ (рис. 4, б).

Шаг 10. Определение дополнительной точки D' на поверхности Σ' для соблюдения однозначности отображения точки B . Определим точку D' , связанную с ребром $A'C'$, на поверхности Σ' , не принадлежащую подмножеству G' и имеющую соответствующую ей точку D на поверхности Σ .

Шаг 11. Определение длины отрезка $[BD]$ на поверхности Σ по значениям координат соответствующих точек $s(BD) = |BD|$.

Шаг 12. В качестве точки, соответствующей B , выбирается одна из точек B'_1 или B'_2 , которая удовлетворяет следующему условию:

$$s'(B'_1 D') = |BD| \text{ или } s'(B'_2 D') = |BD|. \quad (9)$$

Таким образом, точке B будет соответствовать точка на поверхности Σ'_2 с координатами $(x'_{B_1}; y'_{B_1}; 0)$ или $(x'_{B_2}; y'_{B_2}; 0)$ соответственно.

Шаг 13. Для определения декартовых координат второй граничной вершины развертываемой подобласти Σ_2 , не имеющей точки на Σ'_2 , перейти на шаг 6.

Шаг 14. Перейти к шагу 4, пока все подобласти поверхности Σ не будут иметь соответствующие развертки на поверхности Σ' .

В результате работы данного алгоритма будет получено множество точек наложимой поверхности Σ' , определяющих развертку срединной поверхности Σ некоторого слоя конструкции на плоскость OXY (рис. 5).

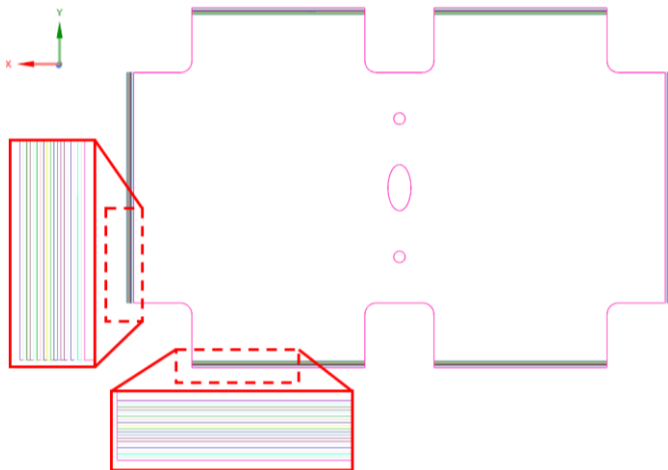


Рис. 5. Развертки срединных поверхностей слоев конструкции из композиционного материала

Габаритные размеры полученных разверток срединных поверхностей 20 слоев композитной конструкции приведены ниже. Следует отметить, что полученные развертки симметричные, а площади разверток равны площади соответствующих срединных поверхностей слоев.

Габаритные размеры разверток слоёв

Слой	1	2	3	4	5	6	7	8	9	10
Длина	473,06	472,06	471,79	471,17	470,54	469,92	469,29	468,66	468,03	467,40
Ширина	300,53	301,15	301,78	302,40	303,03	303,66	304,28	304,91	305,54	306,16
Слой	11	12	13	14	15	16	17	18	19	20
Длина	466,78	466,15	465,52	464,89	464,26	463,63	463,01	462,37	461,74	461,12
Ширина	306,79	307,42	308,05	308,67	309,30	309,92	310,54	311,18	311,80	312,43

Таким образом, разработан алгоритм построения развертки срединных поверхностей слоёв армирующего материала в композитных конструкциях, описываемых совокупностью плоскостей (поверхности нулевой гауссовой кривизны). Применение этого алгоритма позволяет получить развертки слоев без образования областей деформирования и соответственно складкообразования материала.

Библиографический список

1. Савин С.П. Применение современных полимерных композиционных материалов в конструкции планера самолетов семейства МС-21 // Известия Самар. науч. центра Рос. акад. наук. – 2012. – Т. 14, № 4. – С. 686–693.
2. Попов Б.Г. Расчет многослойных конструкций вариационно-матричными методами: учеб. пособие. – М.: Изд-во МГТУ, 1993. – 294 с.
3. Грищенко С.В. Расчет и проектирование изделий конструкции самолёта из слоистых композитов с учетом межслоевых эффектов // Труды МАИ. – 2015. – № 84. – С. 1–19.
4. Михайловский К.В., Барановски С.В. Методика проектирования крыла из полимерных композиционных материалов на основе параметрического моделирования. Ч. 2: Проектирование силовой конструкции // Известия вузов. Машиностроение. – 2016. – № 12 (681). – С. 106–116.
5. Аношкин А.Н., Мурзакаев Р.Т., Кашин О.А. Программный комплекс построения послойной геометрии изделий из тканых препрегов для термостамповки: св-во о регистр. программы для ЭВМ RU 2019663875.
6. Игнатъев Ю.Г. Дифференциальная геометрия кривых и поверхностей в евклидовом пространстве: учеб. пособие. – Казань: Изд-во Казан. ун-та, 2013. – 204 с.

Сведения об авторах

Аношкин Александр Николаевич – доктор технических наук, профессор кафедры «Механика композиционных материалов и конструкций» Пермского национального исследовательского политехнического университета, Пермь, e-mail: anoshkin@pstu.ru

Мурзакаев Рустам Талгатович – кандидат технических наук, доцент кафедры «Механика композиционных материалов и конструкций» Пермского национального исследовательского политехнического университета, Пермь, e-mail: rustmur@gmail.com

Кашин Олег Андреевич – младший научный сотрудник кафедры «Механика композиционных материалов и конструкций» Пермского национального исследовательского политехнического университета, Пермь, e-mail: kashin.oleg@list.ru

П.С. Баранов, А.В. Тарутин, В.А. Щапов

Пермский национальный исследовательский
политехнический университет, Пермь

ИССЛЕДОВАНИЕ ПРОЦЕССОВ ПОИСКА МЕРОПРИЯТИЙ

В статье проведён анализ существующих систем, рассмотрены процессы поиска мероприятий, а также предложено решение.

Ключевые слова: информационные технологии, информационная система мероприятия, агрегаторы мероприятий, система поиска.

P.S. Baranov, A.V. Tarutin, V.A. Shchapov

Perm National Research Polytechnic University, Perm

EVENT SEARCH PROCESS RESEARCH

In this article, an analysis of existing systems will be carried out, the processes of searching for events will be considered, and a solution will be proposed.

Keywords: information technology, information system of the event, event aggregators, search system.

Сегодня люди ищут информацию о различных мероприятиях при помощи информационных технологий, различных сервисов, доступных в Интернете, например, это социальные сети, сайты по продаже билетов, рекламные и другие источники. С каждым днем различные агрегаторы событий набирают популярность среди всевозможных информационных источников. Очень удобно получать много информации при помощи одной площадки, нежели держать в голове, где и что нужно искать. Одним из ключевых недостатков подобных агрегаторов является система поиска информации в них.

Для решения этой проблемы необходимо рассмотреть процесс поиска мероприятия с точки зрения пользователя агрегатора. Контекстная диаграмма процесса реализована с помощью методологии IDEF0 [1] и представлена на рис. 1.

Непосредственно перед поиском мероприятия пользователь узнает о существовании этого мероприятия из различных источников, но в основном из рекламы. После этого он формирует поисковый запрос, при помощи которого рассчитывает найти требуемое мероприятие. Однако у пользователя также есть личные, временные

и дислокационные предпочтения, которые он тоже стремится удовлетворить при поиске мероприятия. Но зачастую пользователь отбирает интересующие его мероприятия, основываясь на уже предварительно составленном, согласно его поисковому запросу, результате поиска. Это занимает множество сил и времени.



Рис. 1. Контекстная диаграмма описания процесса поиска мероприятия

Декомпозиция контекстной диаграммы описания процесса поиска мероприятия представлена на рис. 2.



Рис. 2. Декомпозиция контекстной диаграммы описания процесса поиска мероприятия

На рис. 2 проиллюстрирована распространенная последовательность поиска мероприятий на распространенных агрегаторах. Даже несмотря на то, что зачастую там можно настраивать поисковый запрос в соответствии с предпочтениями пользователя, эти настройки являются друг от друга обособленными, либо же имеют иерархическую структуру,

где выбор по временным предпочтениям зависит от тематики или же тематики зависят друг от друга, и для поиска нужного мероприятия требуется сначала найти иерархического предка нужной тематики.

Распространенными агрегаторами мероприятий являются «Яндекс афиша» [2], «Касса ру» [3] и «Афиша» [4], каждый из которых имеет свою систему поиска. Каждая из этих систем имеет определенные недостатки. Сравнение данных систем представлено в таблице.

Сравнение существующих систем

Недостатки	Яндекс.Афиша	Афиша	Кассы
Фильтр по дате	+	+	+
Количество видимых тематик, характеризующих событие	11	6	8
Принадлежность платформы к конкретной сфере	-	-	-
Присутствие тематик без актуальных мероприятий	+	+	+
Поиск по местам проведения	+	-	-
Поиск тематик	-	-	-

Учитывая недостатки существующих систем, выдвигается измененная концепция декомпозиции диаграммы процесса поиска, представленная на рис. 3.

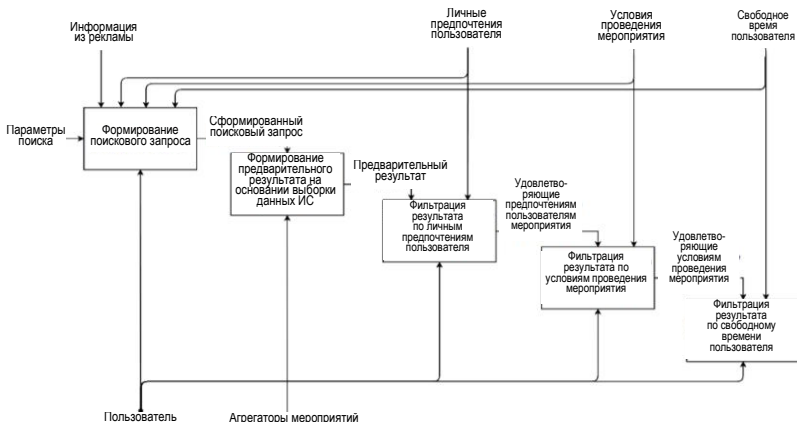


Рис. 3. Измененная декомпозиция контекстной диаграммы описания процесса поиска мероприятия

Изменение алгоритма поиска подобным образом приведет к тому, что пользователь будет тратить меньше времени на фильтрацию предварительного результата, так как результат уже будет отвечать мини-

мальным его требованиям. Иными словами, каждый управляющий элемент должен участвовать в составлении поискового запроса. Таким образом, будет экономиться время пользователя, а также улучшается опыт работы пользователя с системой. Также для реализации подобного алгоритма требуется отказаться от иерархии среди управляющих элементов. Каждый из них должен находиться в открытом для пользователя доступе на этапе построения запроса. Важно предоставить пользователю фильтрацию результата по всем значимым свойствам мероприятия, и, что еще важнее, пользователь должен иметь возможность найти требуемое значение свойства, такого как тематика, среди множества его значений, существующих в системе.

В данной работе были продемонстрированы недостатки существующих информационных систем, проанализированы процессы поиска и выдвинута концепция измененного алгоритма, которая может оптимизировать использование ресурсов.

Библиографический список

1. Методология IDEF0 [Электронный ресурс]. – URL: <https://itteach.ru/bpwin/metodologiya-idef0> (дата обращения: 12.12.2021).

2. Кассы.ру [Электронный ресурс]. – URL: <https://kassy.ru> (дата обращения: 12.12.2021).

3. Афиша [Электронный ресурс]. – URL: <https://www.afisha.ru> (дата обращения: 12.12.2021).

4. Яндекс афиша [Электронный ресурс]. – URL: <https://afisha.yandex.ru> (дата обращения: 12.12.2021).

Сведения об авторах

Баранов Павел Сергеевич – студент Пермского национального исследовательского политехнического университета, Пермь, e-mail: barash.11999@gmail.ru

Тарутин Анатолий Владимирович – кандидат технических наук, доцент кафедры «Информационные технологии и автоматизированные системы» Пермского национального исследовательского политехнического университета, Пермь, e-mail: itas-pnpu@yandex.ru

Щапов Владислав Алексеевич – кандидат технических наук, доцент кафедры «Информационные технологии и автоматизированные системы» Пермского национального исследовательского политехнического университета, Пермь, e-mail: phprus@gmail.com

В.Н. Жуланов

Пермский национальный исследовательский
политехнический университет, Пермь

ПРИМЕНЕНИЕ ГРАДИЕНТНОГО СПУСКА ДЛЯ ОБУЧЕНИЯ МОДЕЛИ МАШИННОГО ОБУЧЕНИЯ

Исследуется способ применения градиентного спуска для обучения модели машинного обучения. Градиентный спуск – это алгоритм оптимизации параметров функции. Он итеративно корректирует параметры функции, чтобы минимизировать функцию ошибок. В этой статье рассматривается решение задачи линейной регрессии. Показан способ реализации алгоритма градиентного спуска на языке Python. Описан общий ход построения модели машинного обучения.

Ключевые слова: градиентный спуск, линейная регрессия, минимизация, машинное обучение.

V.N. Zhulanov

Perm National Research Polytechnic University, Perm

APPLICATION OF GRADIENT DESCENT FOR MACHINE LEARNING MODEL TRAINING

This article explores a way to apply gradient descent to machine learning model training. Gradient descent is an algorithm for optimizing the parameters of a function. It iteratively adjusts the function parameters to minimize the error function. This article discusses the solution of the linear regression problem. The method of implementing the gradient descent algorithm in Python is shown. The general course of building a machine learning model is described.

Keywords: gradient descent, linear regression, minimization, machine learning.

Градиентный спуск – метод нахождения локального минимума функции. Суть метода заключается в том, чтобы осуществлять изменение параметров функции в направлении наискорейшего спуска, т.е. антиградиента*.

* Gradient Descent is the most used learning algorithm in Machine Learning and this post will show you almost everything you need to know about it. – URL: <https://hackernoon.com/gradient-descent-aynk-7cbe95a778da>

Каждое такое изменение параметров называется «итерация». Коэффициенты изменяются при помощи минимизации функции средне-квадратических ошибок:

$$L(y, w) = \sum_{i=1}^N (y_i - \hat{y}_i)^2. \quad (1)$$

Эта функция квадратичная, а значит, имеет форму параболы. Минимум функции соответствует минимуму ошибки. Модель будет изменять параметры функции, чтобы пошагово спуститься в минимум параболы, где ошибка будет минимальной. В минимуме параболы и находятся параметры w , которые мы ищем. Это видно на рис. 1.

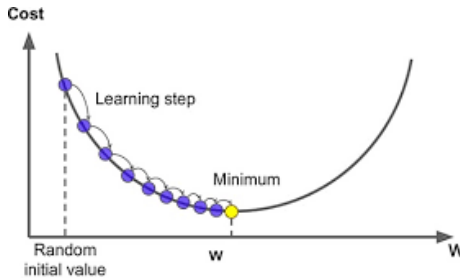


Рис. 1. Поиск минимума параболы

В трёхмерном случае картинка более наглядная. Модель движется по ландшафту и ищет самую нижнюю точку на этом ландшафте [2]. Это видно на рис. 2.

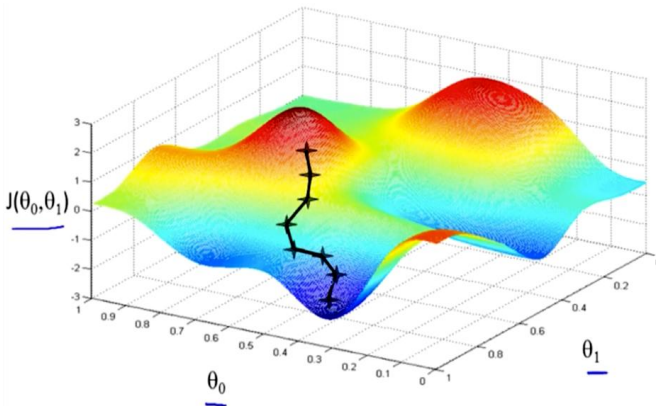


Рис. 2. 3D-визуализация поиска минимума

Средства разработки

№ п/п	Средство разработки	Назначение
1	Python 3.7	Написание алгоритма
2	Numpy	Библиотека математических вычислений
3	Pandas	Библиотека работы с таблицей данных
4	Matplotlib	Библиотека визуализации данных
4	Scikit-learn	Библиотека машинного обучения
5	Jupyter Notebook	Среда разработки
6	CSV	Формат данных

Импорт библиотек, данных и разбиение данных на тренировочную и валидационную выборку представлены в листинге 1.

Листинг 1

```
import numpy as np
import pandas as pd
import matplotlib.pyplot as plt
%matplotlib inline
```

Импорт библиотек линейной регрессии представлен в листинге 2.

Листинг 2

```
from sklearn.model_selection import
train_test_split
from sklearn.linear_model import SGDRegressor
from sklearn.metrics import mean_squared_error
from scipy.spatial import distance
```

Работа с массивом данных, разбиение данных на тренировочную и валидационную выборку представлена в листинге 3.

Листинг 3

```
data = pd.read_csv('non_linear.csv', sep=',')
data = data[(data.x_train > 1) & (data.x_train
< 5)].copy()
```

```
X = data['x_train'].values.reshape(-1, 1)
y = data['y_train'].values
```

```
X_train, X_valid, y_train, y_valid =
train_test_split(X, y, test_size=0.2, ran-
dom_state=10)
```

Первые значения тренировочных данных

№ п/п	x_train	y_train
1	1,182421	1,860341
2	1,251605	1,878928
3	1,270474	2,430015
4	1,402553	2,327856
5	1,427711	2,203649

Запустим обучение модели градиентного спуска. Для градиентного спуска мы используем готовый класс `SGDRegressor`.

Класс принимает следующие параметры:

- `learning_rate='constant'` – используем самую простую модификацию спуска из нескольких возможных;
- `eta0` – шаг градиентного спуска, в формуле мы его обозначали буквой α ;
- `fit_intercept` – параметр нужен, чтобы обучить коэффициент при «свободном члене» линейной регрессии;
- `random_state` – этот параметр нужен для воспроизводимости вычислений.

Функция `partial_fit()`, которую мы вызываем в коде, делает одну итерацию градиентного спуска.

По оси X отложим количество итераций, а по оси Y – значение метрики качества *MSE*, которое получили на валидации.

Обучение модели и визуализация результатов обучения представлены в листинге 4.

Листинг 4

```
sgd_regressor =
SGDRegressor(learning_rate='constant', eta0=0.01,
fit_intercept=True, random_state=42)
```

```
w_current = np.random.random(2)
epsilon = 0.0001
```

```
weight_evolution = []
mse_evolution = []
```

```
for step in list(range(800)):
```

```

sgd_regressor =
sgd_regressor.partial_fit(X_train, y_train)

weight_evolution.append(distance.euclidean(w_current,
sgd_regressor.coef_))
    if weight_evolution[-1]<epsilon:
        print("Итерации остановлены на шаге
%d" % step); break

mse_evolution.append(mean_squared_error(y_valid,
sgd_regressor.predict(X_valid)))
    w_current = sgd_regressor.coef_.copy()
    plt.plot(range(step), mse_evolution)

```

Зависимость значения метрики качества модели MSE (среднеквадратическая ошибка) от количества итераций представлена на рис. 3.

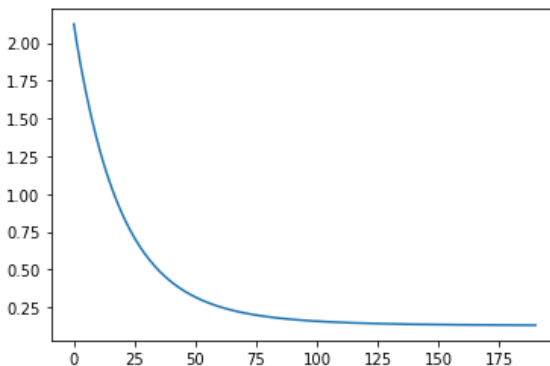


Рис. 3. Зависимость MSE от количества итераций

Визуализация решения задачи линейной регрессии представлена в листинге 5.

```

Листинг 5
In [5]:
x_linspace =
np.linspace(data['x_train'].min(), da-
ta['x_train'].max(), num=100)
y_linspace=
sgd_regressor.predict(x_linspace.reshape(-1,1))
plt.plot(x_linspace, y_linspace)

```

```
plt.scatter(data.x_train, data.y_train, 40,  
'g', 'o', alpha=0.8, label='data')
```

```
plt.show()
```

Результат обучения модели на валидационных данных представлен на рис. 4.

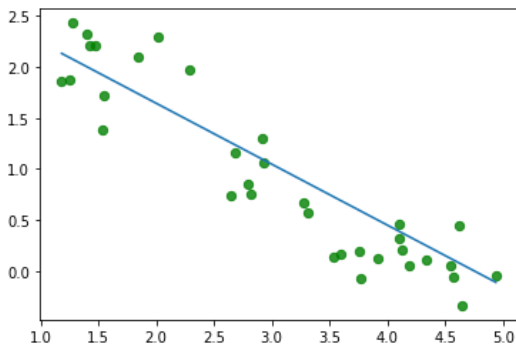


Рис. 4. Результат обучения модели

Мы получили решение задачи линейной регрессии, обучив параметры линейной регрессии небольшими итерациями.

Сведения об авторе

Жуланов Вячеслав Николаевич – студент Пермского национального исследовательского политехнического университета, гр. КОБ-18-1с, Пермь, e-mail: 590slavv@gmail.com

Р.Ф. Закиров¹, А.В. Тарутин²

¹Пермский военный институт войск национальной гвардии
Российской Федерации, Пермь

²Пермский национальный исследовательский
политехнический университет, Пермь

ИСПОЛЬЗОВАНИЕ СИСТЕМ УЧЕТА И АНАЛИЗА УСПЕВАЕМОСТИ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ

Исследуются возможность и необходимость использования визуализации с целью учета и анализа процесса обучения. Проведено исследование наиболее популярных в Российской Федерации систем учета успеваемости. Отмечены их основные достоинства и недостатки. В итоге сделан вывод о необходимости разработки собственной системы учета и анализа успеваемости.

Ключевые слова: успеваемость, наглядность, учет успеваемости, системы учета успеваемости.

R.F. Zakirov¹, A.V. Tarutin²

¹Perm Military Institute of the National Guard
of the Russian Federation, Perm

²Perm National Research Polytechnic University, Perm

THE USE OF SYSTEMS OF ACCOUNTING AND ANALYSIS OF ACADEMIC PERFORMANCE IN THE EDUCATIONAL PROCESS

In this article explores the possibility and necessity of using visualization in order to account for and analyze the learning process. A study of the most popular academic performance accounting systems in the Russian Federation has been conducted. Their main advantages and disadvantages are noted. As a result, it is concluded that it is necessary to develop its own system of accounting and analysis of academic performance.

Keywords: academic performance, visibility, accounting of academic performance, systems of accounting of academic performance.

Развитие информационных технологий в XXI веке играет важную роль в образовательном процессе. Из курса истории мы знаем, что многие люди во времена царской России не умели ни читать, ни писать. После революции В.И. Ленин призывал советский народ:

«Учиться, учиться и ещё раз учиться», и действительно, многие люди пристрастились к саморазвитию, образование стало доступным, ликвидация безграмотности привела к тому, что Советский Союз стал самой читающей державой. В наши дни, в частности, в так называемую эпоху карантина, не все могут посещать образовательные учреждения ввиду карантинных мероприятий [1]. Преподаватели и обучающиеся вынуждены уходить на дистанционный метод обучения, используя мобильные приложения для ведения видеосвязи, школьники и студенты получают домашнее задание по электронной почте.

Контроль успеваемости ведётся в специальных информационных системах, где каждый обучаемый может просмотреть свои оценки, домашнее задание, тему следующего занятия и т.п. Родители обучаемых получают возможность контроля успеваемости и запланированных учебных мероприятий.

Переход к использованию электронных ресурсов в качестве дневников и журналов регулируется соответствующими нормативно-правовыми актами Министерства образования и науки РФ [2]. Там же перечислены основные задачи, которые ставятся при переходе к использованию электронных систем:

- фиксации хода образовательного процесса;
- отражение результатов освоения образовательной программы;
- возможности использования данных, формируемых в ходе образовательного процесса;
- взаимодействие с органами, осуществляющими управление в сфере образования.

Рассмотрим пользующиеся наибольшим спросом в России системы учета успеваемости.

Дневник.ру (рис. 1). Наверняка каждый слышал об этой системе. Сервис широко распространен не только среди детей и родителей, но и в органах государственной власти. Основная цель создания сервиса – разработка единой электронной образовательной среды. На официальном сайте данного сервиса утверждается, что большинство школ России подключено именно к их системе, ею пользуются 800 тыс. преподавателей, 7 млн учащихся и 3,6 млн родителей.

Плюсом данной системы является наглядный просмотр успеваемости обучаемого по четвертям, нет необходимости каждый раз спрашивать у преподавателя «Какую оценку Иванов получил по математике за четверть?» и т.п. Минусом данной системы является

Электронный классный журнал для школы (ЭлЖур) (рис. 2).

	По болезни			12 апреля												Б	У	Н
	Уволенная	Уволенная	Неуволенная	13	14	15	16	17	19	20	21	22	23	24				
1. Белокит Кирилл	6				1					5	6				11	1	6	
2. Величиона Елена	7										6				0	0	13	
3. Колобаев Олег	2			6	6	5	7	6				6			30	0	8	
4. Лаврентьева Маргарита	2	2	1				7	6	5						20	2	1	
5. Левкина Татьяна	1	2	6				7								0	8	8	
6. Май Сергей		2		2					1			6			0	2	9	

Урок	Всего	на «5»	на «4»	на «3»	на «2»	н/а	Усп. %	Кач. %	СОУ. %	Ср
Алгебра	14	4 29%	5 36%	5 35%	0	0	100	64	64	3.93
Англ. яз.	14	4 29%	5 36%	5 35%	0	0	100	64	64	3.93
Биология	14	1 7%	9 64%	4 29%	0	0	100	71	59	3.79
География	14	3 21%	8 57%	3 22%	0	0	100	79	66	4
Геометрия	14	2 14%	3 21%	9 65%	0	0	100	36	51	3.5
Информатика	14	12 86%	2 14%	0	0	0	100	100	95	4.86
Испан. яз.	8	3 38%	5 62%	0	0	0	100	100	78	4.38
История	14	5 36%	5 36%	4 28%	0	0	100	71	69	4.07
Литература	14	4 29%	5 36%	5 35%	0	0	100	64	64	3.93
МХК	14	4 29%	7 50%	3 21%	0	0	100	79	68	4.07

Рис. 2. Страница сервиса «ЭлЖур»

По словам разработчиков, сервис является современной системой учета успеваемости. Целевая аудитория – школы и другие учебные заведения. Отмечается, что «ЭлЖур» – это инструмент для облегчения труда преподавателей, учителей и администрации. Использование данного сервиса значительно облегчает каждодневную бухгалтерскую рутину. Для родителей встроенный электронный журнал – важный помощник в вопросе контроля успеваемости, анализа успехов, а также связи родителей с учителем и администрацией.

Согласно отзывам, родители считают одним из недостатков тот факт, что средняя оценка считается по всем проставленным оценкам. Например, если за выполнение контрольной работы, которая включает в себя теоретическую и практическую часть, подразумевается выставление оценки 3/4 (теория – 3, практика – 4), выставляются обе оценки, в то время как преподаватель подразумевает 3,5, что округляется в большую сторону и должна быть одна оценка – 4, т.е., если

ученик старается, идет на оценку «отлично», то ему придется приложить значительное количество усилий, чтобы средний балл был больше 4,5. Также родители считают недопустимым разбросанный текст по странице, из-за которого остается много свободного пространства и родителям приходится листать незаполненные поля.

Система электронных журналов Ballov.net (рис. 3) – это удобный, мощный, а главное – совершенно бесплатный инструмент для создания единого информационно-образовательного пространства учебного заведения и взаимодействия образовательного учреждения с родителями учащихся.

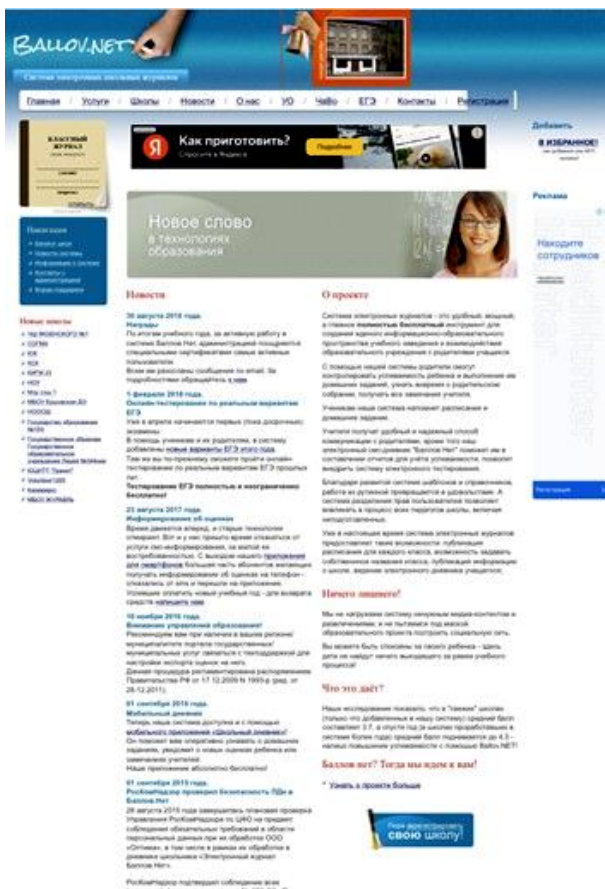


Рис. 3. Официальная страница сервиса «Ballov.net»

Благодаря развитой системе шаблонов и справочников с «Ballov.net» работа из рутинной превращается в удовольствие. А система разделения прав пользователей позволяет вовлекать в процесс всех педагогов школы, включая неподготовленных.

Плюсом данной системы является то, что подключение к сервису и дальнейшее обслуживание являются бесплатными, кроме необязательных sms-оповещений.

К минусам можно отнести тот факт, что на сайте есть реклама, ведь система является бесплатной, и разработчикам необходимо ее как-то окупать, но если пользователи не хотят видеть никакой рекламы вообще, то 30 рублей в месяц могут решить данную проблему, а необязательные sms-оповещения станут бесплатными.

Результатом исследований стала таблица, в которой представлены основные положительные и отрицательные стороны рассмотренных сервисов анализа и учета успеваемости.

Основные достоинства и недостатки сервисов

Название	Плюсы	Минусы
Дневник.ру	Бесплатно, наглядно видны оценки и домашнее задание, есть связь с учителями	Для отключения рекламы нужно приобрести pro-версию
ЭлЖур	Наглядность, легкость доступа, своевременное информирование, оперативная связь с родителями и ученикам. Простые и доступные интерфейсы и система навигации	Низкая производительность и вероятность возникновения ошибок
Ballov.net	Бесплатный сервис для создания единого информационно-образовательного пространства учебного взаимодействия образовательного учреждения с родителями обучающихся	Интерфейс электронного журнала не является интуитивно понятным

В ходе проведения анализа стало ясно, что данные информационные системы, в общем и целом выполняют свои функции, к недостаткам же можно отнести наличие рекламы на сайте, возникновение ошибок во время работы и сложный интерфейс. В этих целях необходимо разработать собственное веб-приложение по учету и анализу успеваемости, исключив недостатки анализируемых информационных систем.

Библиографический список

1. Тарутин А.В. Дистанционное обучение – проблемы роста // Современные инновационные образовательные технологии в информационном обществе: материалы XII Междунар. науч.-метод. конф.;

Пермь, 25 мая 2020 г./ под ред. Е.В. Гордеевой; Перм. ин-т (филиал) Федер. гос. бюджет. образоват. учрежд. высш. образ. «Рос. экон. ун-т им. Г.В. Плеханова». – Пермь, 2020. – С. 85–89.

2. Письмо Министерства образования и науки РФ от 15.02.2012 № АП-147/07 «О методических рекомендациях по внедрению систем ведения журналов успеваемости в электронном виде» // Доступ из справ.-правовой системы КонсультантПлюс

Сведения об авторах

Закиров Радис Фанаесович – курсант Пермского военного института войск национальной гвардии Российской Федерации, Пермь, e-mail: povtas-pvi@yandex.ru

Таругин Анатолий Владимирович – кандидат технических наук, доцент кафедры «Программное обеспечение вычислительной техники и автоматизированных систем» Пермского военного института войск национальной гвардии Российской Федерации, Пермь, e-mail: povtas-pvi@yandex.ru

А.Н. Кильдебаев, А.В. Архипов, А.В. Тарутин

Пермский национальный исследовательский
политехнический университет, Пермь

ВИЗУАЛИЗАЦИЯ ВСТРОЕННЫХ ТИПОВ ОБЪЕКТОВ ПЛАТФОРМЫ «GREENDATA»

В статье рассмотрен процесс построения диаграмм встроенных типов объектов «GreenData». Проанализированы аналогичные распространенные сервисы. Предложена модель взаимодействия сторон.

Ключевые слова: диаграмма, объекты, модели, визуализация, платформа, сервис.

A.N. Kildebaev, A.V. Arkhipov, A.V. Tarutin

Perm National Research Polytechnic University, Perm

VISUALIZATION OF BUILT-IN TYPES OF OBJECTS OF THE «GREENDATA» PLATFORM

This article describes the process of building diagrams of built-in types of objects «GreenData». Similar common services are analyzed. A model of interaction between the parties is proposed.

Keywords: diagram, objects, models, visualization, platform, service.

Компания «GreenData» имеет собственную платформу, которая позволяет создавать сложные приложения без программирования. Основу платформы составляет объектная модель, которая позволяет описывать предметную область понятным языком, и интеллектуальное ядро, которое преобразует объектную модель в реляционную модель для использования под управлением любой из популярных РСУБД (Oracle, MS SQL Server, PostgreSQL и др.) [1].

В настоящий момент большинство средств быстрой разработки приложений имеют классическую парадигму проектирования модели данных, которая предполагает создание пользователем классической реляционной ER-модели. Для создания визуализации подобных моделей существует большее количество компонентов для встраивания в средство разработки приложений. Современные системы предполагают описание предметной области в виде объектной диаграммы.

Рассматриваемая платформа также предоставляет описание модели данных в виде объектной модели, которая гораздо проще к восприятию бизнес-пользователями. Описание объектной модели в платформе «GreenData» строится с помощью табличного интерфейса, что существенно затрудняет восприятие ключевых аспектов объектно-ориентированного подхода. Для того чтобы показать получившуюся модель в понятном виде, согласовать ее с клиентом, приходится ее вручную перерисовывать в виде UML-диаграммы объектов в таких инструментах, как Visio, Draw.io и т.п.

В связи с этим возникла потребность разработать сервис, который бы позволил настраивать объектную модель с помощью диаграмм UML. Данный сервис существенно упростит настройку модели и позволит использовать ее визуальное представление в технических и эксплуатационных документах (техническое задание, руководства пользователя и администратора).

Как указывалось ранее, объектная модель платформы «GreenData» обширна и затрагивает много сфер одновременно, и на данный момент нет никакого разбиения их на отдельные классы, т.е. объекты существуют сами по себе и не соотносятся друг с другом. При анализе объектов и соединении их в группы приходится пользоваться поиском и сортировать их вручную, тем самым увеличивая время работы, и этот процесс продлевается каждый раз. Сервис позволил бы создавать некие абстрактные классы объектов или предметные области, к которым бы относились те или иные объекты платформы. Например, предметная область «Клиенты», куда бы относились такие отношения, как: «Объект», «Физическое лицо», «Юридическое лицо» и т.д. Пользователь мог бы просматривать отношение объектов к конкретной предметной области и выбирать, изменять предметную область по своему усмотрению, что очень удобно в обширной сети объектов.

Объект платформы имеет собственные характеристики, которые могут меняться со временем. При ручном рисовании объектов, приходится каждый раз менять отображение данных характеристик каждого объекта отдельно, что также влияет на время работы. Например, нарисовать или убрать атрибуты (свойства) объекта, а если будет много атрибутов, то каждый раз придется либо добавлять, либо удалять атрибуты из диаграммы. Сервис же позволит менять режимы отображения всех объектов одновременно. Возможны следующие настройки отображения объектов:

- 1) скрыть / показать названия / идентификатор объекта;
- 2) скрыть / показать названия / идентификаторы атрибутов;
- 3) скрыть / показать тип атрибутов;
- 4) скрыть / показать обязательность атрибутов.

Настройки позволяют быстро и просто менять вид диаграммы, при этом выполняя минимум действий, что удобно.

Объекты платформы связаны между собой подобно тому, как связываются объекты в нотации UML, с помощью встроенных инструментов настройки атрибутов, а именно типов данных и ссылок на другие объекты. Для простоты чтения диаграммы нотация позволяет отображать следующие виды связей:

1) агрегация – атрибут объекта является ссылкой на другой дочерний объект, который зависит от данного объекта и будет изменяться вместе с данным;

2) ассоциация – атрибут объекта является ссылкой на другой объект (внешний ключ), который уже существует в системе. При изменении данного объекта ссылаемый объект изменяться не будет;

3) наследование – данный тип объекта будет дочерним по отношению к другому типу объекта и будет иметь доступ к атрибутам и свойствам родителя, тем самым переопределяя его возможности.

Данные связи ясно показывают отношения между объектами, что удобно при чтении объектной модели и объяснении его сторонним пользователям. Сервис позволит отображать данные связи между объектами платформы для наглядности отношений между ними и удобства введения и администрирования объектной модели.

Для реализации сервиса будет использована 2-уровневая архитектура или «клиент-сервер», а именно:

1) сервер или платформа «GreenData», которая позволяет получать данные объектной модели, изменить её с помощью запросов клиента;

2) клиентская часть, в которой будут отображаться объекты платформы, полученные из сервера в виде диаграммы со связями [2].

Модель взаимодействия сторон представлена на рис. 1. Модель была построена на основе нотаций BPMN 2.0 в связи с её актуальностью. Для реализации данной модели был выбран веб-интерфейс, который предоставляет удобные инструменты разработки и позволит пользоваться сервисом многим клиентам одновременно для получения быстрого результата работы.

Таким образом, в связи с проблемой рутинного представления объектной модели платформы «GreenData» и постоянного повтора действий было решено разработать сервис, который позволит решить данную проблему, а именно: представление объектов в удобном и читаемом виде (диаграмма UML), удобное разделение объектов на предметные области, представление отношений (связей) между ними в стандартной нотации, гибкое изменение режимов отображения. Сервис благотворно повлияет на производительность платформы и позволит пользователям системы упростить свою деятельность.

Библиографический список

1. О компании [Электронный ресурс]. – URL: <https://greendatasoft.ru/o-nac-2/> (дата обращения: 01.12.2021).

2. Вигерс Карл, Битти Джой. Разработка требований к программному обеспечению: пер. с англ. – 3-е изд., доп. – М.: Русская редакция; СПб.: БХВ-Петербург, 2014. – 736 с.

Сведения об авторах

Кильдебаев Айнур Назимович – студент Пермского национального исследовательского политехнического университета, гр. АСУ-17-16, Пермь, e-mail: ainur_kildebaev@mail.ru

Архипов Андрей Валерьевич – кандидат технических наук, доцент кафедры «Информационные технологии и автоматизированные системы» Пермского национального исследовательского политехнического университета, Пермь, e-mail: arhipov@greendatasoft.ru

Таругин Анатолий Владимирович – кандидат технических наук, доцент кафедры «Информационные технологии и автоматизированные системы» Пермского национального исследовательского политехнического университета, Пермь, e-mail: itas-pnpu@yandex.ru

В.С. Максимцов, А.А. Широков

Пермский национальный исследовательский
политехнический университет, Пермь

РАЗРАБОТКА МЕТОДОЛОГИИ ТЕСТИРОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В статье рассмотрены методологии разработки и тестирования программного обеспечения, исследованы основные особенности приведенных методологий, на основе которых выбрана оптимальная методология для тестирования ПО.

Ключевые слова: программное обеспечение, компания, тестирование, метод, модель, система, процесс, жизненный цикл.

V.S. Maksimtsov, A.A. Shirokov

Perm National Research Polytechnic University, Perm

DEVELOPMENT OF A SOFTWARE TESTING METHODOLOGY

The article discusses the methodologies for developing and testing software, investigates the main features of the methodologies presented, on the basis of which the optimal methodology for software testing is selected.

Keywords: software, company, testing, method, model, system, process, life cycle.

Процесс тестирования ПО из года в год следует какой-нибудь определенной методологии. Существует множество различных методологий разработки со своими этапами и методами, используемых на каждом этапе. Рассмотрим некоторые модели разработки и тестирования сложных систем.

1. Модель Waterfall, она же каскадная модель, устаревшая модель, которая была крайне популярна в свое время. Данную модель до сих пор практикуют в разработке ПО и его тестировании. У данной модели базовый принцип, четкий порядок выполнения всех этапов разработки. Это означает, что если предыдущий этап завершен без каких-либо критических ошибок, то можно переходить к следующему этапу [1].

Модель Waterfall подходит для малых проектов, в которых известны и определены все требования. Достоинства и недостатки данной модели представлены в табл. 1.



Рис. 1. Модель водопада

Таблица 1

Достоинства и недостатки каскадной модели

Достоинства	Недостатки
Экономическая эффективность	Если произойдет критическая ошибка, то придется начинать все с начального этапа
Простота использования	Если произойдет критическая ошибка, то придется начинать все с начального этапа
Управление документацией	Большая вероятность нахождения критической ошибки в процессе тестирования

2. V-образная модель. Данная модель представляет собой жизненный цикл разработки программного обеспечения, в котором подчеркивается идея «Верификации и валидации». На каждом этапе разработки в V-модели имеется соответствующая фаза тестирования, которая проверяет соответствующий ей процесс. Этапы тестирования планируются параллельно с этапом разработки, на котором они должны быть протестированы и объединены фактическим процессом кодирования, отсюда и название V-модель (рис. 2). Данная модель также считается расширенной формой модели водопада, поскольку один шаг не может быть выполнен без предварительного завершения предыдущего процесса [2].

Ключевые этапы V-модели:

1. Этап определения требований;
2. Высокоуровневое проектирование;
3. Фаза детального дизайна;
4. Юнит-тестирование.

Основной недостаток данной модели – это отсутствие готовых решений.



Рис. 2. V-модель

3. Спиральная модель. Спиральная модель аналогична модели водопада, в которой больше внимания уделяется анализу рисков.

Спиральная модель включает в себя четыре основных этапа:

- планирование;
- анализ рисков;
- проектирование;
- оценка [3].

Программный проект большое количество раз проходит через данные этапы в итерациях (в этой модели они называются спиралями) (рис. 3).

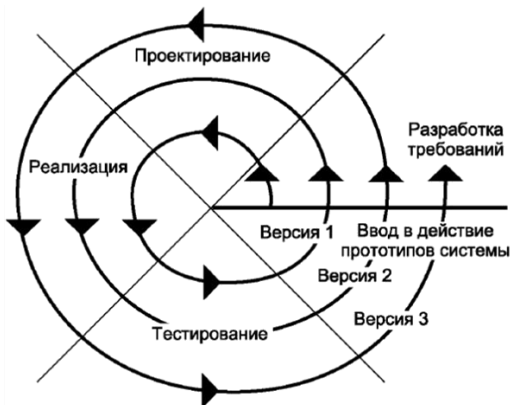


Рис. 3. Спираль

Достоинства и недостатки данной модели представлены в табл. 2.

Таблица 2

Достоинства и недостатки спиральной модели

Достоинства	Недостатки
Мониторинг рисков	Ресурсозатратна
Просмотр клиентом работающей версии ПО на начальных этапах разработки	Начинается тестирование ПО с этапа планирования и длится до стадии оценки качества
Внесение изменений на поздних этапах разработки	
Программный проект может быть разделен на несколько частей или этапов	
Строгий контроль над документацией	

Первые результаты испытаний появляются сразу после результатов испытаний на третьем шаге каждого цикла, что помогает обеспечить правильную оценку качества, и это является основным преимуществом данной модели.

4. Agile – это подход к разработке и тестированию ПО, при котором ключевыми темами являются командное взаимодействие, сотрудничество с клиентами и быстрое реагирование на изменения. В дополнение к этому гибкая методология предоставляет основу, благодаря которой постоянные улучшения происходят на различных этапах разработки ПО [4] (рис. 4).



Рис. 4. Модель Agile

Итерация выглядит следующим образом:

- планирование;
- анализ требований;

- проектирование;
- программирование;
- тестирование;
- документирование.

Программный продукт, выполненный по методологии Agile, готов к выпуску после каждого спринта, хотя, как правило, она недостаточна для выпуска новой версии ПО.

Из всех методологий можно выделить две самых популярных для разработки ПО модели – это спиральная модель и Agile.

Для сравнения Agile и спиральной модели были определены следующие критерии, которые представлены в табл. 3.

Таблица 3

Критерии для сравнения

Критерий	Пояснение	Варианты
Развитие	Отвечает за протекание процесса на любом этапе разработки ПО	Спираль / гибкое
Процесс	Описывает подход разработки ПО	Спиральная / итеративный
Первоначальный план	Отвечает за последовательность действий команды.	Точное / приблизительное
Документация	Отвечает за ведение документации	Строгое/нестрогое
Возможность внесения изменений	Возможность внесения правок на любом этапе разработки.	Возможны / невозможны
Тестирование	Проверка функционала ПО на конкретном этапе	В конце разработки / после каждой итерации
Команды	Тип команды	Отдельные/многофункциональные
Клиент	Участие клиента в разработке	Участвует / не участвует
Софт	Периодичные поставки рабочего продукта (части продукта)	Каждая версия бета-теста / после каждого спринта

Сравнение критериев спиральной и гибкой моделей (Agile) представлено в табл. 4.

Сравнение методологий тестирования

Критерии	Спиральная	Agile
Развитие	Спираль	Гибкий
Процесс	Каждая итерация спираль	Итеративный
Первоначальный план	Точный	Приблизительный
Документация	Строгое	Нестрогое
Отношение к изменениям	Возможны	Невозможны
Тестирование	По версиям	После каждой итерации
Команды	Отдельный	Многофункциональные
Клиент	Не участвует	Участвует
Рабочий софт	Каждая версия для бета-теста	После каждого спринта

Сегодня модели разработки ПО многовариантны. Нет единых правил для всех проектов, стартовых условий и моделей оплаты. Даже гибкую методологию (Agile) не всегда можно применить из-за неподготовленности некоторых клиентов или невозможности гибкого финансирования.

Методологии частично пересекаются с точки зрения средств и в чем-то похожи друг на друга. И Agile, и спиральная модель помогут в создании практически любого программного продукта, но выбирается лишь та методология, которая позволяет наиболее эффективно и результативно реализовать проект.

Если продукт универсальный, необходимо опираться на такие параметры, как:

- затраты времени;
- экономическая составляющая;
- квалификация сотрудников.

Гибкая модель требует от исполнителя высокой квалификации и отлично показывает себя в начинающих проектах.

Спиральная модель может быть полезна, когда вы работаете над проектом со средним или высоким потенциалом риска, или когда клиент не предоставил достаточно точный перечень требований к конечному продукту, или эти требования очень сложны, а также когда речь идет о значительных изменениях в процессе разработки.

Библиографический список

1. Методологии тестирования ПО [Электронный ресурс] // XB Software. Блог. – URL: <https://xbsoftware.ru/blog/metodologii-testirovaniya-po-kakuyu-vybrat/> (дата обращения: 04.12.2021).

2. Технология разработки программ // Знанию [Электронный ресурс]. – URL: https://znanio.ru/media/tehnologiya_razrabotki_programm-369325 (дата обращения: 08.12.2021).

3. Методы тестирования программного обеспечения [Электронный ресурс] // Блог Web-программиста. – URL: <http://juice-health.ru/program/software-testing/495-software-testing-methods> (дата обращения: 06.12.2021).

4. AGILE методология разработки [Электронный ресурс] // QA evolution. – URL: <https://qaevolution.ru/metodologiya-menedzhment/agile/> (дата обращения: 07.12.2021).

Сведения об авторах

Максимцов Владислав Сергеевич – магистрант кафедры «Микропроцессорные средства автоматизации» Пермского национального исследовательского политехнического университета, Пермь, e-mail: riaedes@mail.ru

Широков Александр Аркадьевич – кандидат технических наук, доцент кафедры «Микропроцессорные средства автоматизации» Пермского национального исследовательского политехнического университета, Пермь, e-mail: shirokov@pstu.ru

Г.И. Борзунов, П.А. Новикова

Российский государственный университет
им. А.Н. Косыгина, Москва

ВИЗУАЛЬНОЕ МОДЕЛИРОВАНИЕ ПРИ ПОДГОТОВКЕ И РЕАЛИЗАЦИИ ДИЗАЙН-ПРОЕКТОВ С ИСПОЛЬЗОВАНИЕМ СТЕКЛЯРУСООБРАЗНЫХ ЭЛЕМЕНТОВ

В данной статье предлагается визуальное моделирование как метод реализации системного подхода к разработке и реализации современных дизайн-проектов. На примере подготовки дизайнерского решения применения стеклярусообразных объектов показана эффективность использования унифицированного языка моделирования UML. Создаваемая при этом наглядная информационная система исполнения дизайнерского решения позволяет применять в реализации проекта системный подход. Предлагаемый подход сокращает временные затраты при подготовке и реализации дизайн-проектов, четко разграничивая действия участников и описывая все этапы воплощения идей.

Ключевые слова: системный подход, унифицированный язык моделирования (UML), информационная система, дизайн-проект, визуальное моделирование.

G.I. Borzunov, P.A. Novikova

Russian State University named after A.N. Kosygin, Moscow

VISUAL MODELING DURING PREPARATION AND IMPLEMENTATION OF DESIGN PROJECTS USING GLASS-SHAPED ELEMENTS

This article proposes visual modeling as a method of implementing a systematic approach to the development and implementation of modern design projects. On the example of preparing a design solution for the use of glass-bead objects, the effectiveness of using the unified modeling language UML is shown. The visual information system for the execution of the design solution created in this case allows a systematic approach to be applied in the implementation of the project. The proposed approach reduces the time spent in the preparation and implementation of design projects, clearly delineating the actions of the participants and describing all stages of the implementation of ideas.

Keywords: systems approach, unified modeling language (UML), information system, design project, visual modeling.

Разработка и реализация дизайн-проектов – трудоемкий и длительный процесс, который затрагивает разные предметные области и требует взаимодействия специалистов в разных сферах деятельности.

Создание дизайн-проекта – результат деятельности довольно большого коллектива, где за каждым специалистом закреплена своя часть работы, своя задача. Дизайн-проекты включают в себя множество шагов, направленных на конечный результат. Руководители и авторы проекта, программисты, промышленные дизайнеры и специалисты в области дизайна среды, психологи, технологи и материаледы, колористы – каждый делает свое дело: постановка задачи, поиск материала, создание схем и прототипов, визуализация и размещение макета в конкретной среде или интерьере, подбор цветовых сочетаний и колористических решений, влияющих на эмоциональное состояние человека. Экономисты готовят экономическое обоснование проекта: подсчет количества необходимых материалов в зависимости от масштаба и расчет себестоимости. Как завершающий шаг, только объединив усилия всех этих людей, можно насладиться готовым результатом – реализацией проекта в материале.

Большое количество шагов создания дизайн-проектов свидетельствует о сложности воплощения проектов и требует постоянного контроля каждого действия. При реализации дизайнерского решения может возникнуть семантический разрыв между исполнителями и менеджерами. Вопросы недопонимания в творческом коллективе можно решить с помощью системно-объектного подхода, который прекрасно описывается унифицированным языком моделирования UML.

Информационная система, описывающая этапы разработки проекта, позволит отслеживать каждый шаг выполнения цепочки дизайн-решения, что значительно упростит создание проекта и позволит сэкономить временной ресурс.

UML является стандартным инструментом для моделирования программного обеспечения, позволяющим разрабатывать сложные системы различного назначения. Как показал опыт разработки информационной системы подготовки схем для вышивки стеклярусом [1], UML обеспечивает эффективное проектирование и сопровождение реализации дизайн-проектов.

Была создана модель подготовки вышивок из стекляруса «как есть», т.е. без использования информационной системы.

При анализе предметной области дизайна с использованием стекляруса были выделены следующие задачи:

1. Создание графической базы данных цветных и черно-белых изображений исходных эскизов для подготовки дизайн-проектов из стеклярусных элементов.

2. Пополнение, редактирование, сортировка и поиск изображений базы данных для проектирования дизайн-проектов.

3. Подготовка схемы-текстуры – автоматизированная компьютерная обработка изображения.

4. Расчет спецификации по количеству элементов (цвет, длина).

5. Расчет оптимального раскроя заготовок в зависимости от масштаба предполагаемой схемы или от интерьера, куда схему планируется поместить, посредством программ для автоматического раскроя трубчатых элементов.

6. Визуализация результата посредством создания 3D-моделей.

7. Реализация дизайн-проекта в материале.

Все эти задачи требуют системного подхода. Прототип системы выполнен в виде диаграммы вариантов использования под названием «Информационное обеспечение дизайн-проектов с использованием стеклярусоподобных элементов» на языке UML.

При использовании системного подхода на первом этапе были определены задачи, определяющие всё окружение (среду) системы. С целью наглядной демонстрации работы системы, в которой фигурируют несколько участников, их взаимодействия между собой, с системой, подсистемой или классом была создана диаграмма вариантов использования.

Диаграмма является представлением системы в процессе ее проектирования и разработки. Состоит из актеров (участников), вариантов использования и отношений между ними. Каждый вариант использования определяет некоторый набор действий, совершаемых системой при взаимодействии с актером.

В диаграмме вариантов использования фигурируют несколько актеров. Программист, создающий базу данных и отвечающий за пополнение и обновление материалов в ней. Дизайнер-1, производящий цветокоррекцию и кадрирование изображения. Система, автоматически создающая схемы-текстуры из подготовленных дизайнером-1 изображений. Дизайнер-2, занимающийся визуализацией в среде размещения по полученной системой текстуре. Технолог, подсчиты-

вающий количество деталей в зависимости от выбранного размера проекта и места его размещения. Раскройный автомат, производящий нарезку материалов в соответствии с оптимальным раскромом элементов. Инженер и вышивальный автомат, реализующие дизайн-проект в материале.

Использование диаграммы вариантов использования языка UML позволяет изобразить взаимодействие всех участников проекта в системе, описывая зону ответственности каждого из них. Диаграмма вариантов использования «Информационного обеспечения дизайн-проектов с использованием стеклярусоподобных элементов» представлена на рис. 1.

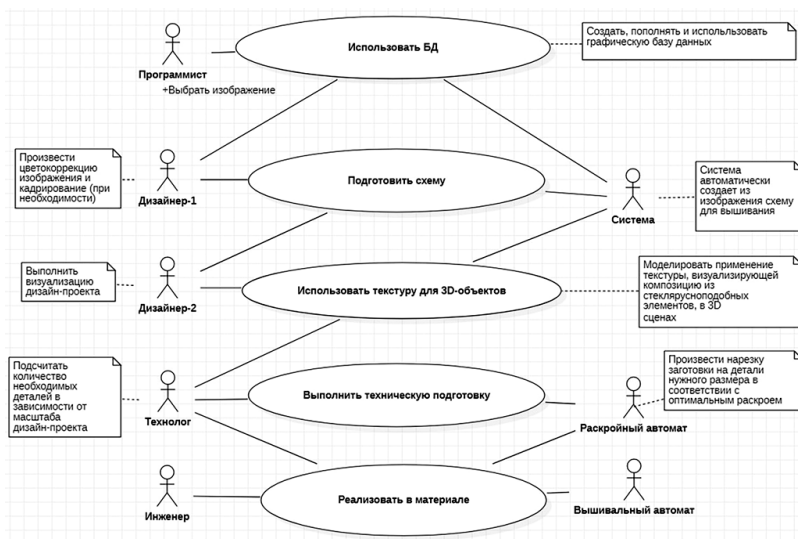


Рис. 1. Диаграмма вариантов использования «Информационного обеспечения дизайн-проектов с использованием стеклярусоподобных элементов»

С целью наглядного представления функционирования программы, автоматически создающей схемы-текстуры из цилиндрических элементов, была создана диаграмма деятельности «Пользователь – система». Она демонстрирует шаг «Подготовить схему», который выполняется системой в диаграмме вариантов использования «Информационного обеспечения дизайн-проектов с использованием стеклярусоподобных элементов».

Диаграмма деятельности UML позволяет более детально визуализировать конкретный случай использования. Это поведенческая диаграмма, которая иллюстрирует поток деятельности через систему. Диаграмма пригодна для демонстрации рабочего процесса некоторой деятельности, основанной на поэтапных действиях.

В рассматриваемом случае диаграмма деятельности отображает взаимодействие между пользователем (человеком) и системой (написанной программой, автоматически создающей схемы-текстуры для вышивки из стекляруса), позволяет визуализировать систему запросов и наглядно отображать все исполняемые процессы, необходимые для получения конечного результата. Предлагаемый подход облегчает процесс восприятия и понимания работы системы в целом. Появляется возможность увидеть весь ход работы.

Первоначально пользователь открывает программу и выбирает количество обрабатываемых изображений.

При необходимости обработать одно изображение пользователь выбирает команду «Выберите изображение»; если же нужно обработать набор изображений, используется команда «Выберите папку». В случае если пользователю не нужно обработать ни одно, ни несколько изображений, данная программа не подходит, и пользователь может ее закрыть.

Определившись с командой, в зависимости от количества обрабатываемых изображений пользователь выбирает в появившемся окне нужный элемент и загружает его в программу. Для корректной работы программы название элемента и адресный путь к нему должны быть на английском языке.

После загрузки элемента в программу пользователь вводит параметры будущей схемы: цвет разделительной сетки, ориентация изображения, количество цветов будущей схемы.

По завершении выбора параметров пользователь использует команду «Обработать изображение» при обработке одного изображения или «Обработать папку» при обработке папки с несколькими изображениями.

После команды «Обработать изображение»/«Обработать папку» система получает сигнал о начале работы и выполняет обработку изображения по методике создания схем, разработанной ранее. По окончании обработки изображения программа завершает процесс и сохраняет результат в папку с оригинальным изображением.

Пользователь может открыть папку с результатом обработки и удостовериться в качестве полученной схемы. Если качество схемы пользователя устраивает, процесс создания схемы-текстуры завершен. Если качество схемы не устраивает, можно повторить обработку изображения с новыми параметрами. Диаграмма деятельности «Пользователь – система» представлена на рис. 2.

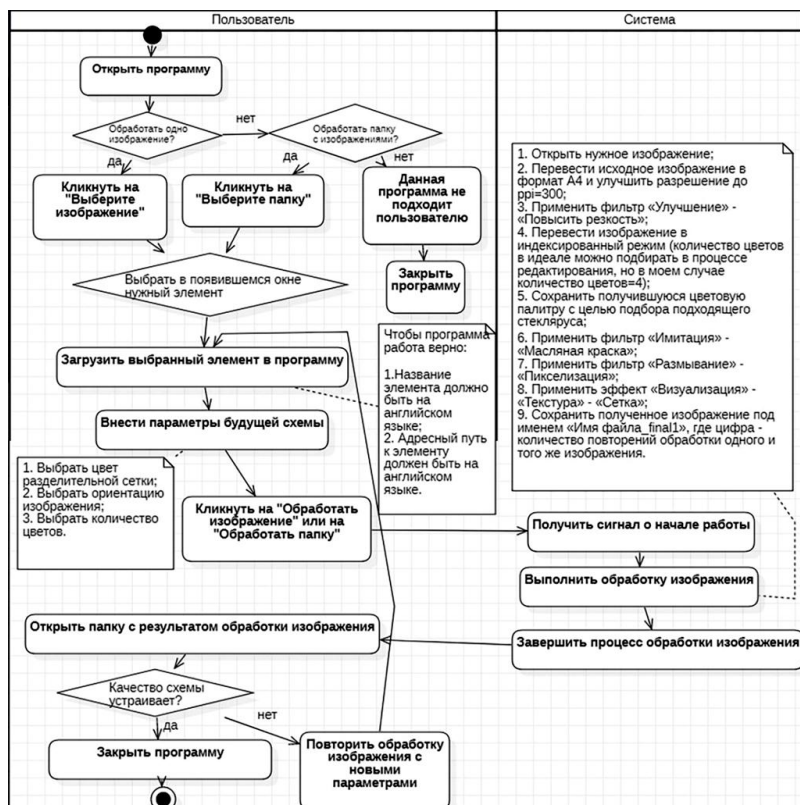


Рис. 2. Диаграмма деятельности «Пользователь – система»

Описанные алгоритмы обработки изображений реализованы программно [2].

Полученная диаграмма деятельности – маленькая шестеренка большого механизма. В рамках дальнейших исследований планируется создать целую систему, состоящую не из одной задачи – задачи разработки схемы-текстуры для дальнейшей визуализации, а из

нескольких задач, описывающих действия от создания базы данных изображений до реализации дизайн-проекта в материале.

Таким образом, унифицированный язык моделирования UML позволил создавать диаграммы деятельности и диаграммы вариантов использования для детальной демонстрации всех этапов реализации дизайн-проекта. А системный подход обеспечивает наглядную визуализацию действия всех участников, контроль процессов шаг за шагом. Данный способ позволил организовать и структурировать работу, сэкономить временной ресурс и более детально следить за созданием дизайн-решений.

Библиографический список

1. Борзунов Г.И., Новикова П.А. Подготовка схем для вышивки стеклярусом с использованием фильтров графического редактора GIMP // Декоративное искусство и предметно-пространственная среда Вестник МГХПА: науч.-аналит. журнал по вопросам искусствоведения. Вестник МГХПА» / Моск. гос. худож.-промыш. акад. им. С.Г. Строганова. – 2020. – № 4, Ч. 1. – С. 294–301.

2. Св-во о гос. регистр. программ для ЭВМ №2021660193. Автоматизированная подготовка схем для вышивания стеклярусом / Г.И. Борзунов, А.В. Фирсов, П.А. Новикова, М.С. Улизко. – Зарег. в Реестре программ для ЭВМ. – Москва, 23 июня 2021 г.

Сведения об авторах

Борзунов Георгий Иванович – доктор технических наук, доцент кафедры «Информационные технологии и компьютерный дизайн» Российского государственного университета им. А.Н. Косыгина, Москва, e-mail: pargroc@gmail.com

Новикова Полина Александровна – магистрант Российского государственного университета им. А.Н. Косыгина, Москва, e-mail: povpol@inbox.ru

Д.С. Хохряков, А.В. Тарутин

Пермский национальный исследовательский
политехнический университет, Пермь

ИССЛЕДОВАНИЕ ПРОТОКОЛОВ WEBRTC

WebRTC – проект, позволяющий создавать p2p – соединения между двумя пользователями через браузер. Чтобы составить модель сервера для коммуникации трех и более участников конференции, в данной статье будет проведён анализ протоколов, используемых в WebRTC. После анализа будет составлен бизнес-процесс функционирования медиасервера.

Ключевые слова: WebRTC, видеоконференции, сетевые протоколы, шифрование.

D.S. Hohryakov, A.V. Tarutin

Perm National Research Polytechnic University, Perm

RESEARCH OF WEBRTC PROTOCOLS

WebRTC is a project that allows you to create p2p connections between two users through a browser. In order to create a server model for communication of three or more conference participants, this article will analyze the protocols used in WebRTC. After the analysis, a business process for the functioning of the media server will be drawn up.

Keywords: WebRTC, video conferencing, network protocols, encryption.

Системы для видеосвязи обладают широкими возможностями для применения. С их помощью можно проводить полноценные конференции, которые по своей эффективности уступают лишь живому общению, при этом собеседники могут находиться в любом месте, где есть доступ к Интернету.

И так как многие приложения в наше время уходят в веб, WebRTC стал проектом, разработанным для того, чтобы люди могли связаться друг с другом, просто используя страницу браузера, без установки какого-либо дополнительного ПО. Однако WebRTC был создан для создания Peer-to-Peer-соединений, а это означает, что конференции с тремя и более пользователями требуют разработки дополнительных решений.

Для решения этой проблемы сразу возникает логичное решение – просто соединить всех пользователей конференции друг с другом. Такая схема действительно существует и приведена на рис. 1.

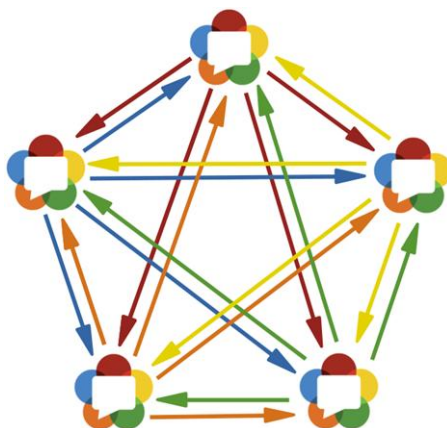


Рис. 1. Схема соединения Mesh

Однако у данной схемы есть один существенный недостаток: чтобы обеспечить соединение, каждому пользователю необходимо иметь высокую пропускную способность сети и высокую производительность устройства, так как ему придется кодировать и шифровать видео для каждого участника в комнате. Поэтому решение с использованием сервера, как на рис. 2, просто необходимо.



Рис. 2. Схема соединения с использованием сервера

При этом для обеспечения соединения достаточными сетевыми ресурсами должен обладать только сервер. А нагрузка на вычислительные возможности сервера будет заключаться лишь в шифровании видео, а не в сжатии.

Для обеспечения данной конфигурации серверу необходимо позиционировать себя как еще одного WebRTC-клиента, чтобы другие браузеры передавали ему медиаданные и получали исходящие от него потоки.

С этой целью проводится данная работа, она предполагает изучение WebRTC-протоколов с целью создания такого сервера, который позволил бы обеспечить соединение трех и более пользователей.

Передача видео- и аудиоданных пользователя является крайне приватной информацией и поэтому обязательно должна быть защищена от третьих лиц. Как следствие этого, все браузеры, поддерживающие WebRTC, предполагают обязательное надежное шифрование медиапотока. Как следствие этого, WebRTC использует протокол SRTP – расширенную версию протокола RTP, предназначенного для шифрования и передачи данных в реальном времени.

Поскольку протокол SRTP не устанавливает соединение самостоятельно, для этой цели используется протокол DTLS, который отвечает за соединение двух устройств, а также за вычисление общего секретного ключа. А чтобы проверить доступность подключения и определить IP-адрес для подключения за пределами NAT, используются протоколы ICE и STUN.

Из-за того, что разные браузеры поддерживают разные кодеки сжатия для описания сеанса, также при инициализации подключения используется протокол SDP, в котором указывается, какие медиатородорожки будут использоваться, с каким битрейтом и с другими параметрами.

Чтобы создать медиа-сервер, который будет рассчитан на конференции из трех и более людей, необходимо описать весь бизнес-процесс, по которому будет работать сам сервер.

Итак, для начала, когда пользователь подключается к конференции, ему необходимо выслать SDP сервера, чтобы пользователь знал, какие параметры ему использовать. Затем клиент генерирует свой SDP и отправляет его серверу. После этого и сервер, и клиент начинают обмениваться STUN-пакетами [1] по протоколу UDP, чтобы проверить, доступно ли подключение между ними.

Когда STUN-проверка успешно прошла, необходимо установить само подключение. Для этого придется пройти процедуру рукопожатия (Handshake) – обменяться SSL-сертификатами, согласовать шифронабор и сгенерировать общий секретный ключ, который впоследствии используется в блочном шифровании потоковых данных. За рукопожатие отвечает протокол DTLS [2]. Он работает точно так же, как и повсеместно используемый протокол TLS, только при этом он учитывает возможную потерю пакетов при использовании UDP.

DTLS позволяет проверить подлинность обеих сторон и составить общий секретный ключ. Когда ключ получен, клиент может начинать отправлять данные, шифруя при этом их этим ключом, используя предварительно согласованный шифронабор.

Для отправки потоковых данных используется протокол RTP [3], который, учитывая особенность UDP, отслеживает правильную последовательность передачи пакетов и следит за состоянием соединения. А для шифрования этих самых данных используется протокол SRTP [4], который шифрует данные и дополняет пакеты RTP дополнительными заголовками, предназначенными для аутентификации данных. Схема итогового бизнес-процесса соединения с WebRTC-сервером показана на рис. 3.

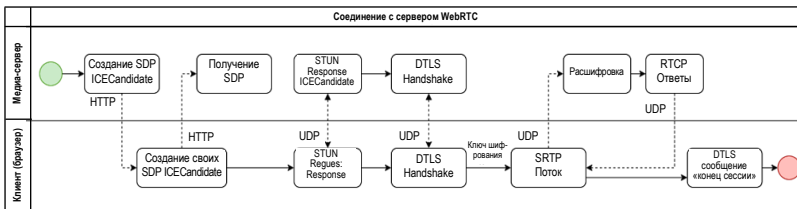


Рис. 3. Модель соединения с сервером WebRTC

Таким образом, при должном изучении протоколов WebRTC появляется возможность разработать приложение с собственным сервером, которое сможет обеспечить коммуникацию группы людей, используя возможности клиентской версии WebRTC в браузере.

С помощью такого приложения люди смогут проводить конференции и онлайн-собрания, используя только свой браузер. WebRTC кроме использования веб-камеры и микрофона позволяет также делиться изображением рабочего стола, что дает возможность приложению обеспечить пользователям удобную работу над обсуждением совместных проектов.

Библиографический список

1. Session Traversal Utilities for NAT (STUN) – IETF [Электронный ресурс]. – URL: <https://tools.ietf.org/html/rfc8489> (дата обращения: 10.12.2021).

2. Datagram Transport Layer Security Version 1.2 – IETF [Электронный ресурс]. – URL: <https://tools.ietf.org/html/rfc6347> (дата обращения: 10.12.2021).

3. RTP: A Transport Protocol for Real-Time Applications – IETF [Электронный ресурс]. – URL: <https://tools.ietf.org/html/rfc3550> (дата обращения: 10.12.2021).

4. The Secure Real-time Transport Protocol (SRTP) – IETF [Электронный ресурс]. – URL: <https://tools.ietf.org/html/rfc3711> (дата обращения: 10.12.2021).

Сведения об авторах

Хохряков Денис Сергеевич – студент Пермского национального исследовательского политехнического университета, гр. АСУ-17-16, Пермь, e-mail: den59k@gmail.com

Тарутин Анатолий Владимирович – кандидат технических наук, доцент кафедры «Информационные технологии и автоматизированные системы» Пермского национального исследовательского политехнического университета, Пермь, e-mail: itas-pnpu@yandex.ru

П.Ю. Шмелев, Л.Ю. Прозорова

Пермский национальный исследовательский
политехнический университет, Пермь

ОСНОВНЫЕ ВОПРОСЫ РАЗРАБОТКИ СИСТЕМ ХРАНЕНИЯ СВЯЗЕЙ МЕЖДУ СЕРВИСАМИ

В статье описана возможность интеграции разрабатываемых IT-проектов при использовании системы хранения связей API. Рассмотрены достоинства и недостатки существующих систем хранения связей. Описан один из вариантов решения поставленной задачи.

Ключевые слова: API, APIManagement, хранение связей, проектирование.

P.Yu. Shmelev, L.Yu. Prozorova

Perm National Research Polytechnic University, Perm

THE MAIN ISSUES OF DEVELOPING STORAGE SYSTEMS FOR LINKS BETWEEN SERVICES

The article describes the possibility of integrating IT projects being developed using the API link storage system. The advantages and disadvantages of existing link storage systems are considered. One of the options for solving the problem is described.

Keywords: API, API Management, link storage, designing.

Современный рынок постоянно наполняется большим количеством IT-проектов. Для корректной работы внедряемых проектов необходимо интегрироваться друг с другом. С целью удобного взаимодействия проектов создан такой инструмент, как API*.

С помощью API сервисы могут обмениваться данными независимо от того, какой язык программирования использует тот или иной сервис. При обмене данные могут состоять из нескольких полей. Кроме того, полученные данные с нескольких сервисов могут передаваться в другой, образуя цепочку, в которой изменение первого элемента повлечет за собой изменение остальных. Порой данная цепочка может оказаться настолько длинной и неодионочной, что проек-

* Что такое системы API Management [Электронный ресурс]. – URL: <https://habr.com/ru/company/X5Group/blog/543324/> (дата обращения: 20.10.2021).

тировщик может упустить звено, что приведет к критическим ошибкам (например, задержка сдачи проекта).

Следующим шагом в развитии использования сервисов является прогнозирование изменений на этапе проектирования при замене того или иного поля. Это во многом ускорит проектирование схемы взаимодействия с сервисами и позволит уменьшить количество ошибок. Практическая значимость заключается во внедрении системы для работы сотрудников компании ООО «Умная логистика» при проектировании разрабатываемых систем, использующих интеграцию с внешними сервисами.

Предпосылками для разработки новой системы хранения связей явились недостатки существующих систем, а именно: системы хранения встраиваются в проект, что ведет к дополнительным затратам и использованию лишних вычислительных мощностей; подключение избыточных функций, которые не используются, но их существование ведет к дополнительным затратам. Перечисленные выше факторы способствовали принятию решения о разработке новой системы. Принцип работы «как должно быть» данной системы описан ниже в нотации IDEF0 на рисунке.

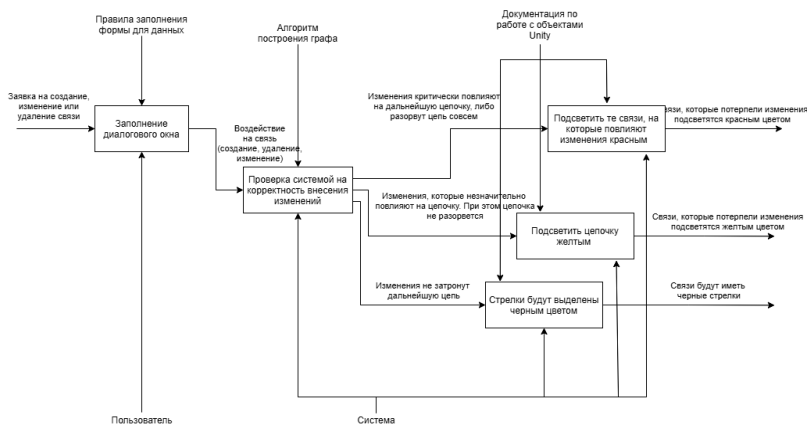


Рис. Контекстная диаграмма работы системы для хранения связей API между сервисами

Перед началом разработки заказчиком были поставлены следующие требования: возможность работы нескольких сотрудников одновременно над одним проектом в облаке; интуитивно понятный

интерфейс; наличие тонкого клиента, т.е. для работы с системой не устанавливается ПО; разработанная система не должна занимать много места.

Исходя из перечисленных требований, для разработки была выбрана платформа Unity с использованием языка программирования C#. Выбранная платформа позволит реализовать такие возможности: скомпилированный проект можно разместить на серверах, куда пользователи смогут подключиться для работы без установки дополнительного ПО; готовое приложение на Unity будет легче по сравнению с Unreal Engine.

Сведения об авторах

Шмелев Павел Юрьевич – магистрант кафедры «Информационные технологии и автоматизированные системы» Пермского национального исследовательского политехнического университета, Пермь, e-mail: schmelev.pacha.kz@yandex.ru

Прозорова Любовь Юрьевна – кандидат экономических наук, доцент кафедры «Информационные технологии и автоматизированные системы» Пермского национального исследовательского политехнического университета, Пермь, e-mail: ljur@mail.ru

Секция 2

**АВТОМАТИЗАЦИЯ И УПРАВЛЕНИЕ ТЕХНОЛОГИЧЕСКИМИ
ПРОЦЕССАМИ И ПРОИЗВОДСТВАМИ**

Н.В. Андриевская, С.Л. Рассада

Пермский национальный исследовательский
политехнический университет, Пермь

ИДЕНТИФИКАЦИЯ НЕСТАЦИОНАРНЫХ ОБЪЕКТОВ УПРАВЛЕНИЯ

При исследовании систем управления важное место отводится задаче идентификации особенно если объект управления является нестационарным. Зависимость параметров модели от времени сильно усложняет задачу идентификации. На сегодняшний день, с одной стороны, наблюдается интерес к задаче идентификации нестационарных объектов, с другой стороны, анализ работ, опубликованных по данной тематике, показывает, что оптимального алгоритма разработки и исследования идентификационных моделей нестационарного объекта не существует. В данной статье предлагаются подходы к решению задачи идентификации нестационарных объектов и представлено исследование алгоритмов идентификации в программной среде управления System Identification Toolbox.

Ключевые слова: идентификация, нестационарная система, динамический объект.

N.V. Andrievskaia. S.L. Rassada

Perm National Research Polytechnic University, Perm

IDENTIFICATION OF NON-STATIONARY CONTROL OBJECTS

In the research of control systems, the identification task occupies an important place, especially if the control object is non-stationary. The dependence of the model parameters on time greatly complicates the identification task. Today, on the one hand, there is an interest in the problem of identifying non-stationary objects. On the other hand, the analysis of the works that have been published on this topic shows that there is no optimal algorithm for the development and research of identification models of a non-stationary object. This article suggests approaches to solving the problem of identification of non-stationary objects and presents the results of a study of identification algorithms in the System Identification Toolbox management software environment.

Keywords: identification, non-stationary system, dynamic object.

Нестационарная линейная система (система с переменными параметрами) – это система, в которой все звенья описаны линейными дифференциальными уравнениями, в которых хотя бы один коэффициент изменяется со временем. Все реальные системы являются в той или иной мере нестационарными, поскольку в реальных системах в процессе эксплуатации параметры меняются.

Основными примерами нестационарных объектов исследования можно назвать следующие системы: электромеханические системы с изменяющимися активными и реактивными сопротивлениями, высокоскоростные летательные аппараты, в которых переменной величиной является масса, уменьшающаяся за счет сгораемого топлива, система управления полетом снаряда, параметры которой могут зависеть от дальности снаряда до цели и изменяться со временем в процессе движения снаряда [1].

В общем случае объект управления может быть описан следующей системой нелинейных дифференциальных уравнений [2]:

$$\frac{dx}{dt} = f(x, u, t) + G(x, t), \quad (1)$$

$$y = H(t)x(t), \quad (2)$$

где u – вектор управляющих воздействий; y – вектор наблюдаемых сигналов; x – расширенный вектор состояния (включая параметры динамического объекта); $G(x, t)$ – матрица коэффициентов.

В качестве объекта исследования рассмотрена модель 2-го порядка, в которой нестационарность обеспечивается изменяющимся по времени коэффициентом усиления. Структурная схема нестационарного объекта представлена на рис. 1.

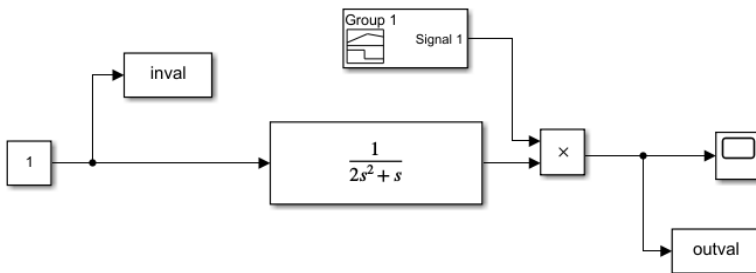


Рис. 1. Структурная схема заданного объекта

С помощью блока Signal Builder задается изменение коэффициента усиления во времени (с 0 по 4 с $K = 1$; с 4 по 6 с $K = 3$; с 6 по 10 с $K = 5$). На рис. 2 представлен график временной характеристики данных.

В качестве методов идентификации нестационарного объекта в данной статье предложены следующие модели и алгоритмы идентификации [3]:

- авторегрессионные модели;
- нелинейные модели.

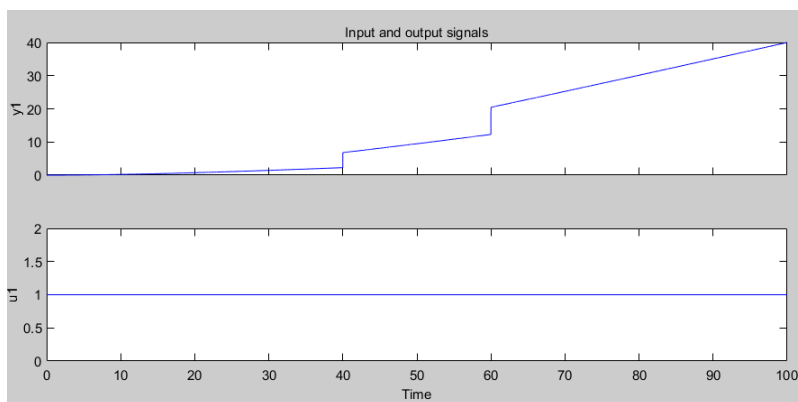


Рис. 2. График временной характеристики данных

Программный пакет System Identification Toolbox (SIT) позволяет осуществить идентификацию на основе следующих авторегрессионных моделей:

- 1) авторегрессионные модели ARX:

$$A(z)y(t) = B(z)u(t) + e(t), \quad (3)$$

где $e(t)$ – ошибка идентификации, вызванная либо помехами, либо неучтенными входными сигналами.

- 2) ARMAX – модель авторегрессии скользящего среднего:

$$A(z)y(t) = B(z)u(t - nk) + C(z)e(t), \quad (4)$$

где nk – величина задержки (запаздывание); $C(z)$ – оценка влияния $e(t)$, $C(z) = 1 + c_1z^{-1} + c_2z^{-2} + \dots + c_{nc}z^{-nc}$.

3) модель ОЕ – модель «вход-выход»:

$$y(t) = \frac{B(z)}{F(z)}u(t - nk) + e(t), \quad (5)$$

где $F(z) = 1 + f_1z^{-1} + f_2z^{-2} + \dots + f_{nf}z^{-nf}$

4) модель Бокса–Дженкинса:

$$y(t) = \frac{B(z)}{F(z)}u(t - nk) + \frac{C(z)}{D(z)}e(t), \quad (6)$$

где $B(z)$, $F(z)$, $C(z)$ определены ранее, а полином $D(z)$ определяется как

$$D(z) = 1 + d_1z^{-1} + d_2z^{-2} + \dots + d_{nd}z^{-nd}.$$

В пакете SIT возможно оценить нелинейные модели следующего вида:

1) нелинейная авторегрессионная модель ARX расширяет линейную ARX модель и имеет структуру:

$$y(t) = f(y(t-1), \dots, y(t-na), u(t-nk), \dots, u(t-nk-nb+1)), \quad (7)$$

где нелинейная функция f зависит от конечного числа предыдущих значений входов u и выходов y ; na – количество предыдущих выходных значений; nb – количество предыдущих входных значений, используемых для прогнозирования текущего выхода; nk – задержка от входа до выхода, указанная как шаг дискретизации.

Нелинейная функция f оценивается как суммированный ряд нелинейных зависимостей в виде вейвлет-сети или сигмоидной функции. При идентификации количество слагаемых нелинейных зависимостей (n) может выбираться произвольно;

2) модель Гаммерштайна–Винера представляет собой модель, состоящую из линейного и нелинейного блоков. Нелинейный блок описывается моделью Винера [3] и представляет (идентифицирует) статическую характеристику нелинейного элемента, а линейный блок представлен дискретной передаточной функцией, т.е. реализует динамические свойства объекта управления.

В данной статье представлены результаты идентификации вышепредложенных моделей. При этом для каждой модели было проведено исследование при разных значениях na , nb , nk и выбрана наилучшая модель. На рис. 3 представлены графики переходных процессов идентификационных моделей и оценка адекватности моделей.

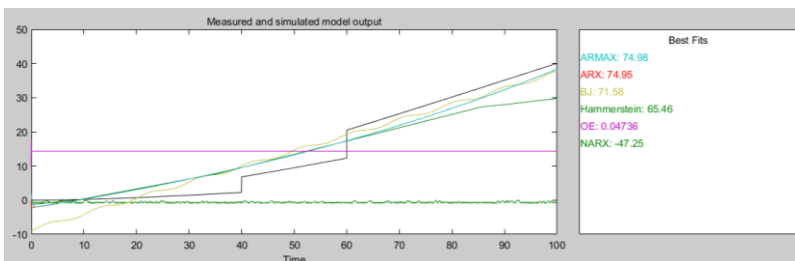


Рис. 3. Проверка моделей на адекватность

Анализ моделей показал, что наилучшими моделями являются модель Гаммерштайна–Винера и модель авторегрессии скользящего среднего, графики переходных процессов представлены на рис. 4.

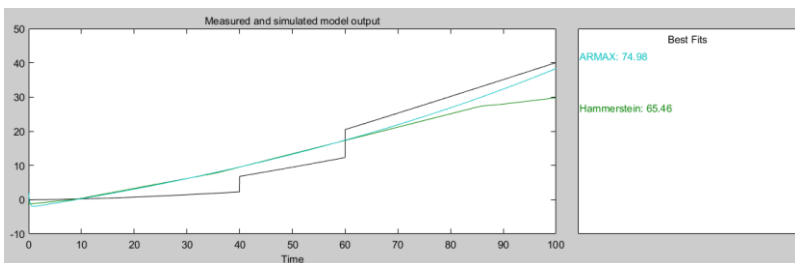


Рис. 4. Проверка адекватности моделей ARMAX и Гаммерштайна–Винера

Адекватность данных моделей оценивается так: модель Гаммерштайна–Винера – 65,48 %; модель ARMAX – 74,90 %.

Разработка и исследование идентификационных моделей нестационарных систем с помощью пакета System Identification Toolbox (MatLab) показали, что использование автоматизированной процедуры идентификации дает средние результаты.

Построенные модели могут быть использованы для задач прогнозирования или синтеза систем управления, но для обратной конструкторской задачи данные модели не могут быть применены, так как в них отсутствует физическая интерпретация параметров по отношению к материальным параметрам нестационарных объектов исследования.

Библиографический список

1. Пупков К.А. Статистический расчет нелинейных систем автоматического управления: учеб. пособие. – М.: Машиностроение, 1965. – 404 с.
2. Понятский В.М. Использование метода инвариантного погружения для исследования нестационарного динамического объекта. – СПб.: Изд-во БГТУ, 2007. – С. 85–96.
3. Андриевская Н.В. Проектирование и исследование идентификационных моделей управляющих систем реального времени: учеб. пособие. – Пермь: Изд-во Перм. нац. исслед. политехн. ун-та, 2013. – 201 с.

Сведения об авторах

Андриевская Наталья Владимировна – кандидат технических наук, доцент кафедры «Микропроцессорные средства автоматизации» Пермского национального исследовательского политехнического университета, Пермь, e-mail: nataly-anv@mail.ru

Рассада Софья Леонидовна – магистрант кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, гр. АТ1-20-1м, Пермь, e-mail: Rassada_Sofia@mail.ru

И.А. Белов, А.Д. Дыкий

Пермский национальный исследовательский
политехнический университет, Пермь

АВТОМАТИЗАЦИЯ И УПРАВЛЕНИЕ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ В ЭНЕРГЕТИКЕ

Современная среда экономических преобразований обеспечивается за счёт инновационного прогресса, что объясняется достижением успеха в применении современных технологий. Автоматизация стала совершенством для развития научных идей, а также научной деятельности, что связано, прежде всего, с развитием энергетической промышленности. В данной статье будет рассмотрена автоматизация производственных процессов в сфере энергетической промышленности.

Ключевые слова: автоматизация, энергетика, производство, технологии, оборудование, производственный процесс, инновационные технологии.

I.A. Belov, A.D. Dyky

Perm National Research Polytechnic University, Perm

AUTOMATION AND CONTROL OF TECHNOLOGICAL PROCESSES IN POWER ENGINEERING

The modern environment of economic transformation is provided by innovative progress, which is explained by the achievement of success in the application of modern technologies. Automation has become a perfection for the development of scientific ideas, as well as scientific activities, which is primarily associated with the development of the energy industry. This article will discuss the automation of production processes in the energy industry.

Keywords: automation, power engineering, production, technology, equipment, production process, innovative technologies.

Под автоматизацией подразумевается процесс развития производства, где выполняемые ранее функции человека передаются автоматическими устройствами. Однако управление автоматизацией остаётся за человеком. Данный автоматизированный процесс создаётся при помощи АСУТП, который представляет полноценный автоматизированный комплекс программ, предназначенный для управления оборудованием. Под данным процессом управления, как правило, понимается комплексное решение, обеспечивающее автоматизацию производства.

Научные труды исследователей в данной сфере позволяют выделить следующее направление: использование аппаратуры по управлению и контролю техники с автоматизацией работы, где главной целью, прежде всего, является повышение эффективности и безопасности производственного процесса.

Поставленные цели достигаются решением следующих задач:

- развитием и совершенствованием качества процесса;
- совершенствованием готовности данного автоматизированного процесса и оборудования;
- совершенствованием производственного процесса.

Решение поставленных задач осуществляется в первую очередь при внедрении инновационных методов данного процесса, которое требует четкости в производственной деятельности всех звеньев производственного процесса. В энергетической отрасли, несмотря на существующую неоднородность рынка автоматизации, востребованы решения, направленные на повышение бесперебойности и производительности энергетического комплекса.

В данной отрасли внедряются и совершенствуются традиционные продукты автоматизации, такие как системы электронного документооборота или бизнес-анализа, так и инновационные инструменты: аналитика на базе алгоритмов или искусственный интеллект для оптимизации производства. На данный момент существуют три основных направления деятельности электросетевых компаний по автоматизации передачи и распределения электроэнергии. Это специальные решения АСДУ, условно говоря, это диспетчерский зал с видеостеной. Вторым немаловажным направлением автоматизации стало управление транспортом электроэнергии, где решаются задачи технического учета, расчета отпуска энергии и потерь. Для данных целей используются системы АСТУЭ и АСКУЭ. Среди других трендов можно выделить развитие SmartGrid.

Энергетические предприятия с интересом следят за инновационными ИТ, хотя и осваивают их пока с крайней осторожностью. В ближайшие годы будут востребованы конвергентные решения, например, VI+ГИС или VI + технологические данные. В энергетике большое значение отведено безопасности, в связи с этим облачные технологии оцениваются с большей осторожностью. Основной причиной данной предосторожности является боязнь за сохранность данных. ИТ-инфраструктура является важнейшей составляющей, так, к приме-

ру, биллинговую систему внедрили «Энергетические системы Востока» (РАО ЭС Восток), в основе которой лежит отраслевое решение компании Ferranti для предприятий ЖКХ и энергетики.

Системы PLM используются с меньшей эффективностью в отличие от машиностроения. САПР востребован немного больше, например, имеются продукты трёхмерного проектирования и автоматического формирования в начертательном формате. С применением ГИС-направления можно прогнозировать местоположение новых подстанций. PLM-системы приобретают все большее распространение в электроэнергетике, они позволяют вести паспорта оборудования компаний на протяжении долгого времени. Элементами систем являются также решения, основанные на геоинформации, например, решение на базе GE SmallWorld. Благодаря поддержке со стороны государства широкое распространение получили системы глобального позиционирования (ГЛОНАСС).

Предприятия энергетики продолжают развивать, модернизировать, расширять функциональность, менять «старое на новое», появляются также модифицированные решения, которые адаптированы под отрасль. Однако данные преобразования происходят в отношении автоматизации основной деятельности предприятий, которые требуют более глубокого погружения в специфику данной отрасли. Так, например, энергетической отрасли пришлось разобраться с физикой гидродинамических процессов, происходящих в Волжско-Камском каскаде гидроэлектростанций, прежде чем энергетика смогла применить нейронные сети для автоматизации технологических процессов диспетчерского центра. На основе приобретённых знаний в энергетической отрасли разработали систему, позволяющую рассчитывать плановый режим работы объекта. Другой же задачей стала автоматизация планирования производственных программ для «Рус-Гидро», которая также потребовала от сотрудников полнейшего погружения в производственный процесс организации, а также в работу систем и оборудования.

Проблемой автоматизации является прежде всего «технологическая безработица», представляющая собой потерю рабочих мест, которая обуславливает негативное мнение в отношении введения данного процесса. Также острой проблемой является недостаток «профессионалов» в данной отрасли. Однако автоматизация технологического процесса имеет больше положительных сторон, так как она

позволяет увеличить производительность более чем в три раза. Автоматизация позволяет решить вопрос низкой производительности труда и улучшения качества продукции в отношении данной отрасли. Сегодня предлагается большой выбор программ для осуществления производства, и, конечно же, это вселяет надежду на то, что интеллектуальные АСУ займут пусть не первое, но достойное место в нашей деятельности.

Библиографический список

1. Селевцов Л.И. Автоматизация технологических процессов. – М.: Академия, 2014. – 352 с.
2. Цветаев С.С., Логачев К.И. Актуальные проблемы автоматизации промышленных предприятий // Вестник Белгород. гос. технол. ун-та им. В.Г. Шухова. – 2012.
3. Хлебенских Л.В., Зубкова М.А., Саукова Т.Ю. Автоматизация производства в современном мире // Молодой ученый. – 2017. – № 16 (150).

Сведения об авторах

Белов Илья Анатольевич – студент Пермского национального исследовательского политехнического университета, гр. ЭЭ-20-4Б, Пермь, e-mail: gb.ilya@mail.ru

Дыкий Антон Дмитриевич – студент Пермского национального исследовательского политехнического университета, гр. ЭЭ-20-4Б, Пермь, e-mail: oda.tar.02@mail.ru

И.А. Васенин, О.В. Гончаровский

Пермский национальный исследовательский
политехнический университет, Пермь

ПРИМЕНЕНИЕ ПРОТОКОЛА MODBUS В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ УПРАВЛЕНИЯ НА БАЗЕ РОБОТОТЕХНИЧЕСКИХ СИСТЕМ И КОМПЛЕКТОВ КОМПАНИИ «ПРОМОБОТ»

В работе исследуются принципы управления робототехническими системами и комплектами компании «Промобот». Под робототехническими системами понимаются сервисный робот «Promobot v4», а под комплектами компании – отдельные вынесенные части робота как самостоятельная система для изучения в вузах. Рассматривается подсистема управления робототехнической системы. В работе представлены результаты анализ полевой шины Modbus как базовой для построения распределенной системы управления сервисным роботом.

Ключевые слова: распределенная система управления, робототехническая система, протокол управления, Modbus, робот «Промобот».

I.A. Vasenin, O.V. Goncharovsky

Perm National Research Polytechnic University, Perm

APPLICATION OF THE MODBUS PROTOCOL IN DISTRIBUTED CONTROL SYSTEMS BASED ON ROBOTIC SYSTEMS AND KITS OF THE COMPANY «PROMOBOT»

In this paper, the principles of management of robotic systems and complexes of the company Promobot are investigated. Robotic systems are understood as the service robot Promobot v4 and Si, and the company's kits are separate parts of the robot as an independent system for studying at universities. The control subsystem of the robotic system is considered. The paper presents the results of the analysis of the Modbus fieldbus as a base for building a distributed control system for a service robot. The features of controlling various devices of the robotic system are shown.

Keywords: distributed control system, robotic system, control protocol, Modbus, Promobot robot.

Современные сервисные робототехнические системы состоят из разнообразных подсистем. Взаимодействие происходит между датчиками, контроллерами и исполнительными механизмами и осуществляется через локальную сеть (ту или иную полевую шину) по соответствующим протоколам. Надежность, стоимость и быстрдействие –

основные характеристики полевых шин. Примерами таких шин являются: CAN, Ethernet, Modbus, Profibus.

Сенсорная сеть может представлять свободную топологию и состоять из отдельных сегментов: повторители (П), мосты (Мо), маршрутизаторы (Ма), точки доступа (ТД), программируемые логические контроллеры (ПЛК), шлюзы (ШЛ), преобразователи интерфейсов (ПИ), серверы баз данных (СБД) информации о состоянии объектов управления (Supervisory control and data acquisition, SCADA), промышленные персональные компьютеры (ППК).

Нижний уровень модели робототехнической системы – это уровень сенсоров, общая модель архитектуры представлена на рис. 1.

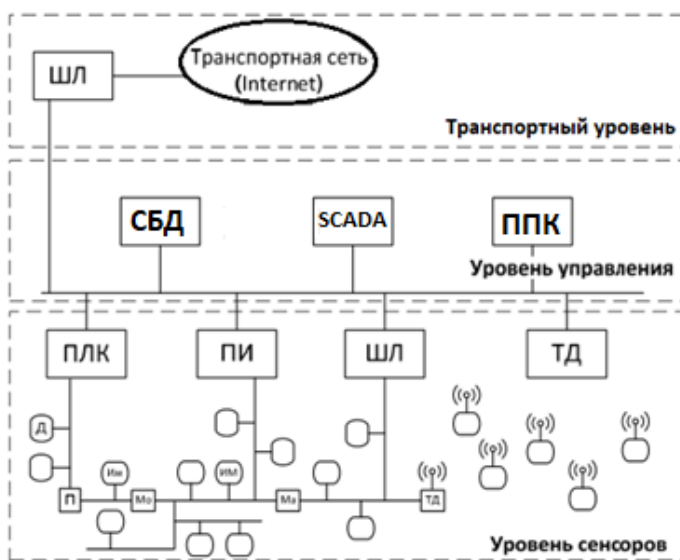


Рис. 1. Общая модель архитектуры информационно-управляющей сети

В него входят следующие элементы: датчики, контроллеры и исполнительные механизмы, объединенные в сенсорную сеть для обмена измерительной и управляющей информацией. Управление в таких системах создано по распределенному принципу. Средний уровень модели – уровень управления. Назначением уровня являются: сбор, обработка и сохранение на сервере баз данных информации о состоянии объектов управления, выработка управляющих воздействий на исполнительные механизмы системы. Третий уровень модели –

транспортный уровень. Назначением уровня является организация доступа и передачи информации от/к территориально удаленным техническим объектам с целью получения данных мониторинга и совершения воздействий управления на удаленные объекты системы посредством глобальных систем (Интернет).

Важным является решение задач измерения и управления множеством параметров технической системы. Робот «Промобот V4», представляет собой многосенсорную систему. При рассмотрении данной робототехнической системы можно отметить, что в ней имеется множество датчиков определения расстояния, элементы управления Led-подсветкой и сервоприводы, которые нужно контролировать и которыми нужно управлять (рис. 2).

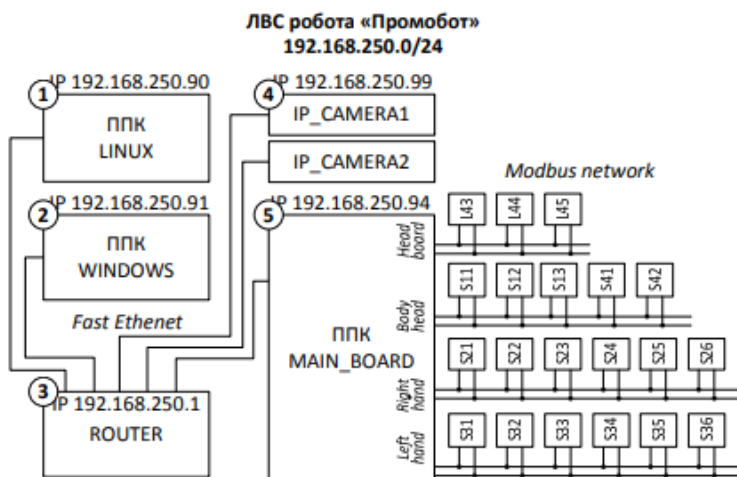


Рис. 2. Упрощенная структурная схема робототехнической системы «Промобот»

В состав робототехнической системы входят:

1. Промышленный персональный компьютер с операционной системой (ОС) Linux Ubuntu. Компьютер является основным управляющим модулем робота.

2. ППК с установленной ОС Windows для реализации задач управления встраиваемыми периферийными устройствами со специальным программным обеспечением: принтеры фото, чеков, диспенсер карт, казначей, медицинское оборудование.

3. Маршрутизатор для объединения промышленных персональных компьютеров в сеть по технологии Fast Ethernet.

4. Две IP-камеры (обычная и широкоугольная) для захвата и передачи видеопотока в ППК Linux для работы системы распознавания лиц.

5. ППК Main_Board представляет собой основной исполняющий модуль робототехнической системы «Промобот» с операционной системой Raspbian (рис. 3). Данный модуль осуществляет преобразование команд в сигналы физических интерфейсов для управления периферией робота. Компьютер для управления использует преобразователь интерфейсов UART-RS-485 для доступа к сенсорной сети Modbus, объединяющей сервоприводы управления движениями робота. Управление осуществляется четырьмя шинами:

- левая «рука» (6 сервоприводов);
- правая «рука» (6 сервоприводов);
- «Торс» (2 сервопривода) и «Голова» (3 сервопривода);
- LED-матрица и «Уши» (3 led устройства).



Рис. 3. Пример исследуемого робота «Промобот», в котором представлена распределенная система

1. Сеть управления сервисного робота на базе протокола Modbus. Modbus – это сетевой протокол прикладного уровня, широко используемый в промышленном производстве для обмена данными между устройствами (Machine-to-Machine, M2M). Modbus использует архитектуру Master-Slave, которая относительно недавно была переименована разработчиком в Client-Server. Данный подход выделяет

следующий принцип работы: клиентское (ведущее) устройство периодически отправляет запросы на серверные (ведомые) устройства с целью чтения или записи их параметров (рис. 4, 5).

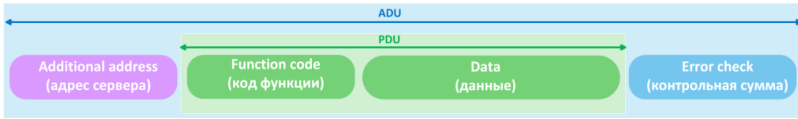


Рис. 4. Структура пакета данных Modbus в общем виде

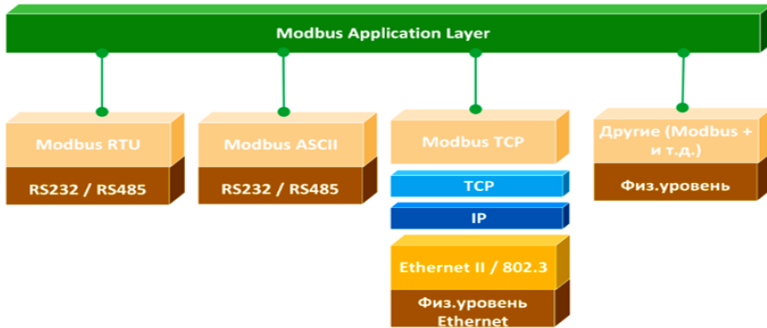


Рис. 5. Разновидности протокола Modbus

– Modbus ASCII – для обмена используются только ASCII-символы. Для проверки целостности используется однобайтовая контрольная сумма. Начало и конец сообщения помечаются специальными символами;

– Modbus RTU – компактный двоичный вариант. Сообщения разделяются по паузе в линии. Сообщение должно начинаться и заканчиваться интервалом тишины длительностью не менее 3,5 символов при данной скорости передачи. Проверка целостности осуществляется с помощью CRC;

– Modbus TCP – для передачи данных через TCP/IP-соединение.

2. Тестирование распределенной системы управления на базе Modbus. На рис. 6, в левой части, представлено ведомое устройство (mod_RSsim), справа – ведущее (TIK Modscan). Симулятор ведомых устройств mod_RSsim предназначен для тестирования modbus-устройств. Симулятор ведущих устройств TIK Modscan предназначен для тестирования ведомых modbus-устройств в сети, отладки взаимодействия с ними осуществляется по сети.

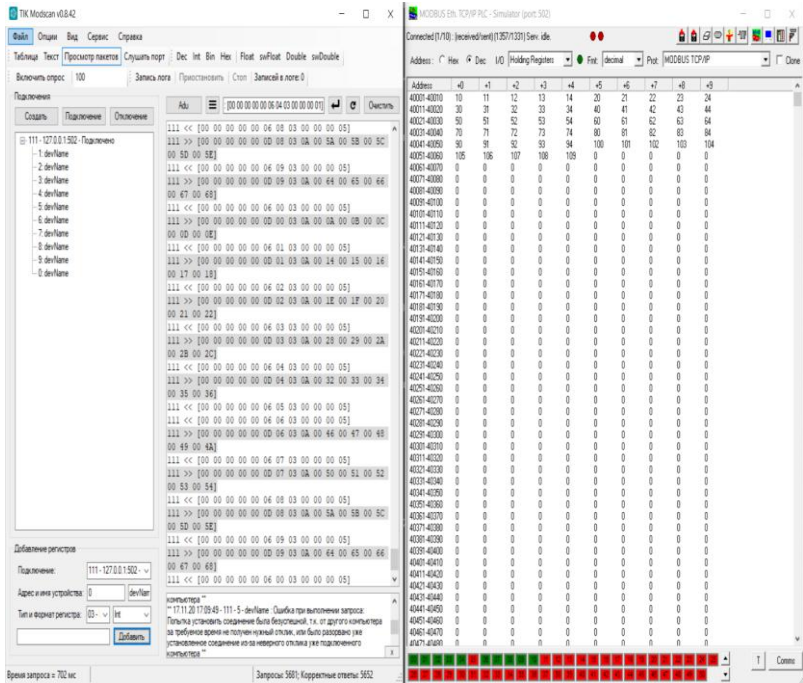


Рис. 6. Окна программ, выполняющих роли ведомого и ведущего устройств

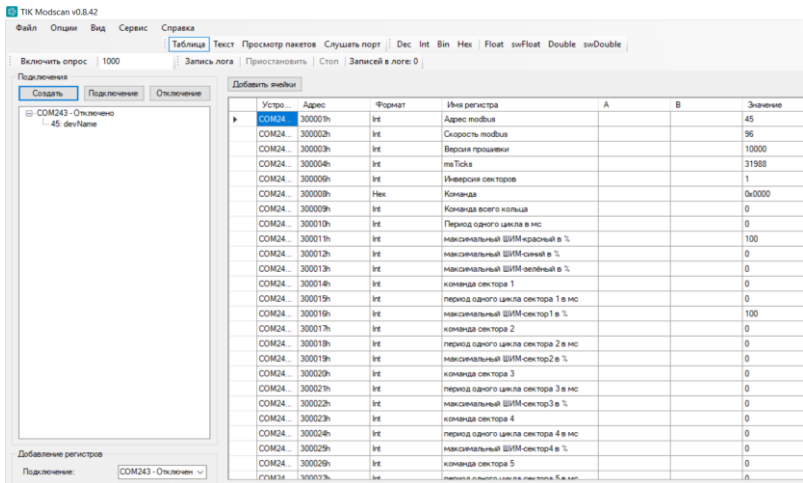


Рис. 7. Карта регистров и задание последовательности для подсветки

2.1. Тестирование устройства «Ухо» робота «Promobot v4». На рис. 7 представлена карта регистров исполнительного механизма – «Ухо». Управление и задание подсветки осуществляются при прямом подключении устройства «Ухо» к компьютеру. С помощью карты регистров и задания определенных значений в них можно управлять цветом, яркостью, продолжительностью горения и типом горения светодиодов (рис. 8).

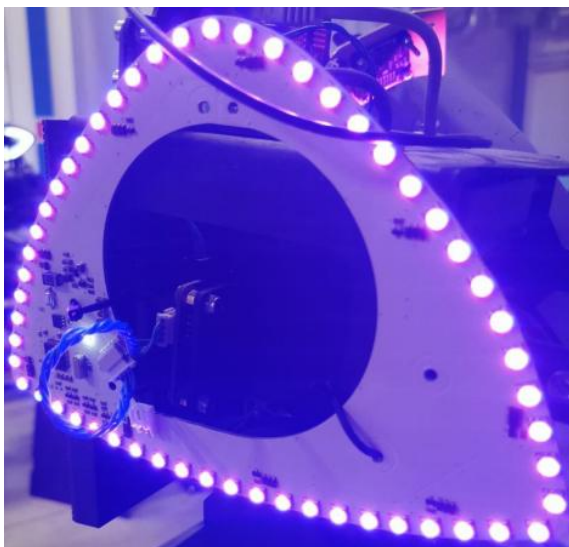


Рис. 8. Картинка горящего «Уха» при заданной последовательности

2.2. Тестирование манипулятора «Рука» робота «Promobot v4». В ходе проведения запусков управления и работы с узлами (сервоприводами) было выявлено, что необходимо на роботе отключить GUI (интерфейс, который запускается при включении робота), иначе выполнить корректно дальнейшие действия будет невозможно. При включении робота GUI первый захватывает права управления и опроса сервоприводов. Данная проблема уже считается решенной, так как это является особенностью работы протокола (ведущий-ведомый) – отсутствие поддержки работы с несколькими ведущими устройствами. На рис. 9 показано управление регистром 35, отвечающим за сгиб руки на заданное значение. Значение послано в формате ASCII в окне программы справа, полученный результат – слева на фото.

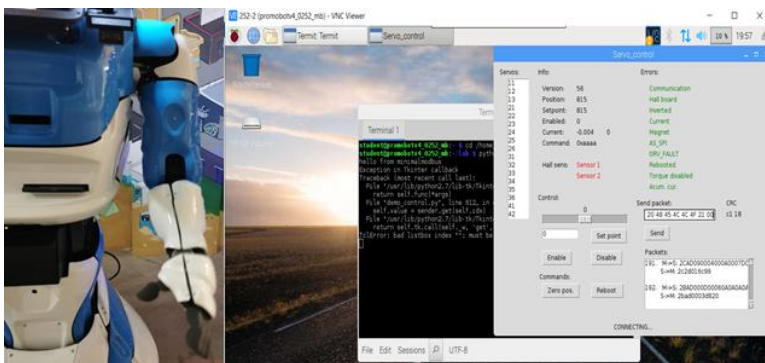


Рис. 9. Управление рукой

Библиографический список

1. Modbus: простыми словами о популярном протоколе [Электронный ресурс]. – URL: <https://mcs.mail.ru/blog/modbus-dlya-m2m-vzaimodejstviya> (дата обращения: 15.12.2021).
2. Modbus [Электронный ресурс]. – URL: <https://ru.wikipedia.org/wiki/Modbus> (дата обращения: 16.12.2021).

Сведения об авторах

Васенин Иван Андреевич – магистрант кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, гр. АСП-20-1м, Пермь, e-mail: Vasenin.Ioann@yandex.ru

Гончаровский Олег Владленович – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: 35911953@mail.ru

Д.А. Даденков, К.С. Белькевич

Пермский национальный исследовательский
политехнический университет, Пермь

**ОБЗОР МЕТОДОВ ДЛЯ РЕАЛИЗАЦИИ СИСТЕМЫ
АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ
АБСОРБЦИЕЙ ФОРМАЛЬДЕГИДА**

В статье рассматривается технологический процесс абсорбции формальдегида для получения формалина заданного качества. Рассматриваются недостатки существующей системы управления, и выполняется анализ методов синтеза систем автоматического управления нестационарными объектами, которые можно использовать непосредственно для реализации системы автоматического управления абсорбцией формальдегида.

Ключевые слова: абсорбция, технологический процесс, нестационарный объект, методы синтеза систем автоматического управления.

D.A. Dadenkov, K.S. Belkevich

Perm National Research Polytechnic University, Perm

**OVERVIEW OF CONTROL METHODS FOR THE DEVELOPMENT
OF AN AUTOMATIC FORMALDEHYDE ABSORPTION
CONTROL SYSTEM**

This article discusses the technological process of formaldehyde absorption to obtain formalin of a given quality. The disadvantages of the existing control system are considered, and the methods of synthesis of automatic control systems for non-stationary objects are analyzed, which can be applied directly to the implementation of an automatic control system for the absorption of formaldehyde

Keywords: absorption, technological process, non-stationary object, methods of synthesis of automatic control systems.

Описание технологического процесса и существующей системы управления процессом абсорбции. Абсорбция – это химический или физический процесс, при котором одно вещество поглощается другим. При этом поглощаемое вещество полностью пропитывается поглощающее [1].

Основным элементом узла абсорбции является абсорбер, который представляет собой аппарат колонного типа, установленный вертикально. Колонна состоит из трех насадочных секций, заполненных

неупорядоченной насадкой (кольца Палля). Между первой и второй насадочными секциями располагаются первая и вторая клапанные тарелки. Между второй и третьей насадочными секциями располагаются третья и четвертая клапанные тарелки. Над третьей насадочной секцией – семнадцать колпачково-барботажных тарелок.

Узел абсорбции формальдегида предназначен для получения формалина с концентрацией формальдегида $55 \pm 0,5$ % и низким остаточным содержанием метанола менее 1,0 % из насыщенного формальдегидом технологического газа.

Насыщенный формальдегидом технологический газ из реактора поступает в нижнюю часть абсорбера и проходит через весь абсорбер. В верхнюю часть абсорбера подается технологическая (деминерализованная) вода в противоток технологическому газу. Расход деминерализованной воды выводится на дисплей оператора с датчика расхода в пределах не более 5000 кг/ч. При отклонении от уставки по расходу в пределах от ± 50 кг/ч срабатывают световая и звуковая сигнализации. В контур регулирования расхода воды входят: датчик расхода, регулирующий клапан. Также ведется учет суммарного расхода деминерализованной воды.

В нижней части абсорбера располагается первая насадочная секция. В контур циркуляции входят: циркуляционный насос, который обеспечивает контакт между технологическим газом и водным раствором формальдегида, увеличивая контактную поверхность и время контакта технологического газа с водным раствором формальдегида. Важным фактором является равномерное распределение жидкости по насадочной секции: любое сухое место в насадочном материале повышает опасность образования параформальдегида.

Уровень формалина в нижней части абсорбера выводится на дисплей оператора с датчика уровня в пределах от 20 до 80 %. При достижении минимального значения (20 %) или максимального (80 %), а также при отклонении показаний от заданной границы в пределах ± 5 % срабатывают звуковая и световая сигнализации. Контур регулирования уровня формалина состоит из следующих элементов: из датчика уровня и регулирующего клапана.

Концентрация формальдегида в выходном продукте выводится на дисплей оператора по данным с массового расходомера в пределах от 54,5 до 55,5 %. При достижении минимального значения (54,5 %) или максимального значения (55,5 %) срабатывают звуковая и световая

сигнализации. Регулирование концентрации формалина осуществляется подачей деминерализованной воды в контур циркуляции в автоматическом режиме. В контур регулирования концентрации входят: массовый расходомер, регулирующий клапан.

Расход деминерализованной воды в контуре циркуляции выводится на дисплей оператора по расходомеру в пределах не более 400 кг/ч. При достижении максимального значения (400 кг/ч) срабатывает световая и звуковая сигнализации.

Формалин с концентрацией формальдегида в пределах от 54,5 до 55,5 % из контура циркуляции откачивается насосом формалина в емкостный наружный склад через холодильник формалина.

Недостатки существующей системы управления. На данный момент используется система, которая представляет собой совокупность несвязанных подсистем автоматического регулирования отдельных технологических параметров. В частности, для контура управления расходом деминерализованной воды, уровнем формалина в нижней части абсорбера и концентрацией используются не связанные между собой локальные регуляторы, которые поддерживают параметры процесса согласно уставке в технологическом регламенте.

Существующая система управления не всегда позволяет эффективно решать задачу обеспечения качества выходного формалина, а именно обеспечить поддержание требуемой концентрации формальдегида в допустимых пределах.

Производство формалина характеризуется нестационарностью параметров процесса синтеза, что влияет на массовую долю формальдегида в продукте. В частности на систему регулирования концентрацией влияют такие параметры, как температура в абсорбере (так как реакция экзотермическая), расход газовой смеси, расход деминерализованной воды, снижение активности катализатора, концентрация формальдегида в газе, количество воды, образующееся после окисления метанола в реакторе.

На систему регулирования уровня влияет расход деминерализованной воды, подаваемой в верхнюю часть абсорбера, а также расход воды в контуре циркуляции.

Если осуществлять настройку каждого контура в отдельности и не принимать во внимание их взаимное влияние друг на друга, то это приводит к снижению качества формалина (требуемой концен-

трации), а также к увеличению риска образования параформальдегида на насадочном материале абсорбера.

Поскольку по ходу технологического процесса формалин используется в качестве сырья для производств смол, пентаэритрита и уротропина, то снижение качества формалина приведет и к снижению качества производных продуктов.

Из вышеизложенного следует, что необходимо провести модернизацию системы автоматического управления для исключения выхода концентрации формальдегида за пределы от 54,5 до 55,5 % и исключения образования параформальдегида на насадочном материале абсорбера.

Анализ методов управления. В теории автоматического управления существует множество разнообразных методов синтеза регуляторов: классические методы синтеза типовых регуляторов класса вход-выход, методы синтеза нейронных и нечетких регуляторов, методы синтеза многосвязных и нестационарных систем, адаптивных систем управления и т.д. Абсорбер как объект управления является нестационарной системой, в которой технологические параметры меняются с течением времени.

В работе [2] для управления нестационарным объектом рассматриваются МРС-регулятор и адаптивный ПИД-регулятор на основе нечеткой логики.

Сущность предложенного в статье [2] способа управления заключается в расчете определенной последовательности значений для управляемой переменной $u(t)$ с целью обеспечения оптимальной траектории движения переменной $y(t)$. При этом длина последовательности управляющего сигнала $u(t)$ принимается постоянной величиной и определяет горизонт управления, а последовательность значений управляющего воздействия предлагается рассчитывать с помощью решения классической задачи оптимизации с использованием целевого функционала А.А. Красовского. Данный функционал формируется с учетом квадрата рассогласования между выходной прогнозируемой переменной $y(t)$ и желаемой траекторией движения $g(t)$. В процессе расчета оптимальных значений для переменной $u(t)$ синтезируемый регулятор осуществляет процедуру минимизации функционала, который можно записать в виде следующего выражения:

$$J = \sum_{i=k}^{k+h_e} (g(i) - y(i))^2 + \sum_{i=k}^{k+h_u} (u(i) - u(k))^2,$$

где $k = 1, 2, \dots, \infty$; h_e – количество шагов для расчета прогноза поведения переменной $y(t)$ (горизонт предсказания); h_u – длина последовательности будущих значений управляющего воздействия $u(t)$ (горизонт управления).

После подачи рассчитанного оптимального управляющего воздействия $u(t)$ на объект на следующем такте управления процедура расчета повторяется циклически с учетом новых измеренных значений переменных. На рис. 1 показана структурная схема MPC-регулятора.

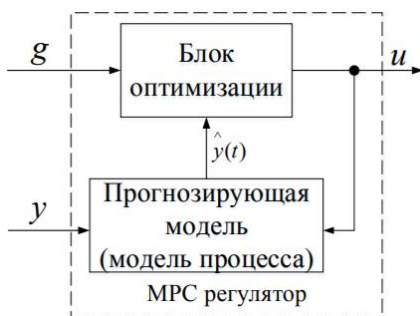


Рис. 1. Структурная схема MPC-регулятора

В системе управления с адаптивным регулятором [2] для расчета параметров регулятора предложено использовать нечеткий контроллер с базой правил, которая получается в результате минимизации функционала. Рассмотренный регулятор настраивается с использованием метода оптимального модуля и частотного метода для объектов управления, которые можно представить в виде передаточных функций первого порядка. Члены оптимизируемого функционала формируются на основании двух групп параметров регулятора.

Параметры первой группы (K_n , T_n , T_d) рассчитываются с помощью метода оптимального модуля, а другая группа параметров вычисляется на основе амплитудно-фазовой частотной характеристики (АФЧХ) разомкнутой системы. Далее выполняется процедура итерационного поиска параметров регулятора с помощью специального адаптера-оптимизатора. Таким образом, используя две группы параметров регулятора, формируется база правил для нечеткого контроллера. Структурная схема адаптивного регулятора представлена на рис. 2.

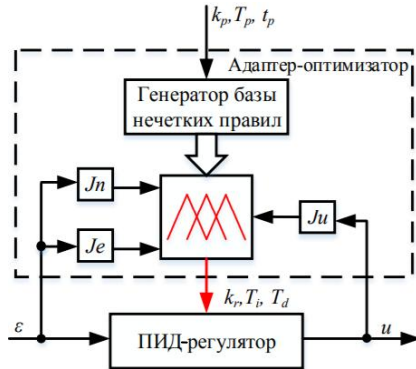


Рис. 2. Структурная схема адаптивного ПИД-регулятора

В книге [3] в качестве нестационарного объекта управления рассматривается колонна синтеза аммиака. Для разработки системы управления рассмотрен метод синтеза, основанный на развязывании внутренних перекрестных связей между выходными переменными и на компенсации возмущающих воздействий с помощью синтеза специальной системы многосвязного управления, содержащей дополнительные внешние компенсирующие связи между отдельными локальными регуляторами. С учётом предложенного в работе [3] подхода реализована структура цифровой системы управления (ЦСУ) температурой в слоях катализатора колонны синтеза аммиака. На рис. 3 представлена структурная схема многосвязной цифровой системы управления температурой в слоях катализатора.

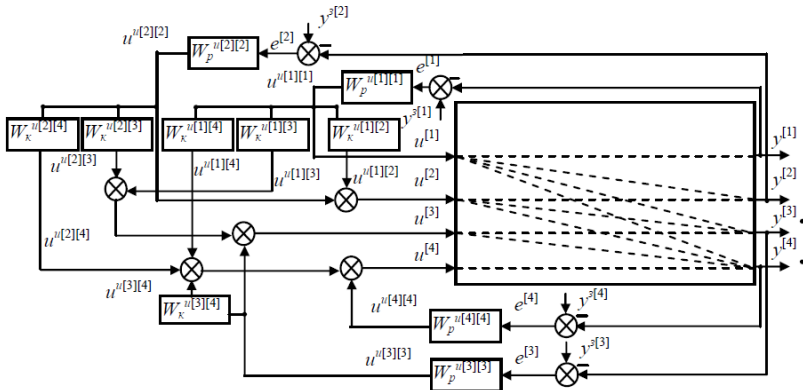


Рис. 3. Структурная схема многосвязной цифровой системы управления температурой в слоях катализатора

В общем случае синтез корректирующей части многосвязной цифровой системы управления с использованием принципов инвариантного и автономного управления предлагается выполнять в следующей последовательности:

1. Синтез корректирующих звеньев для компенсации перекрестных связей с обеспечением автономности каналов управления;
2. Формирование передаточных функций для эквивалентных элементов;
3. Расчет и оптимизация параметров основных локальных регуляторов на основе передаточных функций эквивалентных элементов;
4. Выполнение процедуры синтеза цифровых корректирующих звеньев для компенсации возмущений с учетом обеспечения условия инвариантности.

Заключение. На основании анализа недостатков существующей системы управления абсорбцией формальдегида установлено, что система является многосвязной и имеет несколько контуров управления, которые не связаны между собой. Поэтому для реализации управления целесообразно выбрать метод синтеза, основанный на развязывании перекрестных каналов между входными и выходными параметрами системы. Поэтому наиболее перспективным для реализации системы управления является метод, представленный в работе [3].

На следующем этапе исследования и реализации системы управления планируется разработать математическую модель технологического процесса адсорбции формальдегида с целью выполнения синтеза и настройки многосвязной системы автоматического управления процессом абсорбции формальдегида.

Библиографический список

1. Ларионова Н.И., Елизаров В.В. Автоматизация процессов абсорбции и адсорбции: учеб. пособие. – Нижнекамск: Изд-во Нижнекамск. химико-технолог. ин-та (филиал) КНИТУ, 2013. – 53 с.
2. Надеждин И.С., Горюнов А.Г., Маненти Ф. Системы управления нестационарным объектом на основе прс-регулятора и ПИД-регулятора с нечеткой логикой // Управление большими системами. – 2018. – № 75. – С. 50–75.

З. Кудряшов В.С., Рязанцев С.В., Иванов А.В. Моделирование и синтез цифровой многосвязной системы управления процессом получения аммиака: монография. – Воронеж: Изд-во ВГТА, 2011. – 171 с.

Сведения об авторах

Даденков Дмитрий Александрович – кандидат технических наук, доцент кафедры «Микропроцессорные средства автоматизации» Пермского национального исследовательского политехнического университета, Пермь, e-mail: dadenkov@mail.ru

Белькевич Константин Сергеевич – магистрант кафедры «Микропроцессорные средства автоматизации» Пермского национального исследовательского политехнического университета, гр. ИСУП-20-1м, Пермь, e-mail: belka2h@mail.ru

А.Д. Косачёв, А.А. Широков

Пермский национальный исследовательский
политехнический университет, Пермь

**РАЗРАБОТКА МЕТОДИКИ ПРОГНОЗИРОВАНИЯ
АВАРИЙНЫХ СИТУАЦИЙ ДЛЯ ХИМИЧЕСКИ
ОПАСНЫХ ОБЪЕКТОВ**

В работе рассматривается методика прогнозирования аварийных ситуаций, которые могут возникнуть в лабораториях химических исследований и приводящие к насыщению воздушной среды опасными для здоровья и жизнедеятельности человека веществами. Описывается принцип работы программы прогнозирования системы поддержки принятия решений по профилактике аварийных ситуаций.

Ключевые слова: прогнозирование, система поддержки принятия решений, газоанализатор, нейронная сеть.

A.D. Kosachyov, A.A. Shyrokov

Perm National Research Polytechnic University, Perm

**DEVELOPMENT OF AN EMERGENCY PREDICTION
METHOD FOR CHEMICALLY HAZARDOUS FACILITIES**

The paper considers a method for predicting emergency situations that may arise in chemical research laboratories and lead to the saturation of the air environment with substances hazardous to human health and life. The principle of operation of the forecasting program of the decision support system for the prevention of emergency situations is described.

Keywords: forecasting, decision support system, gas analyzer, neural network.

В сфере эксплуатации систем вентиляции ключевую роль играют качественное регулирование параметров процесса вентиляции и своевременная реакция системы управления и персонала на всевозможные аварии [1]. Причинами загазованности могут быть техногенные внешние факторы, а также нарушения правил выполнения работ с химическими реактивами персоналом лаборатории. И если внешние факторы практически не поддаются прогнозированию, то «человеческий» фактор может иметь определенные закономерности, связанные с усталостью персонала, интенсивностью работы и другими причинами, а зна-

чит, его можно предсказать. Данное направление можно считать особенно актуальным для лабораторий, работающих с опасными химическими и/или биологическими компонентами, такими как лаборатории химической и экологической безопасности [2].

Одним из наиболее современных способов прогнозирования аварий является машинное обучение. Оно включает в себя различные методы: градиентный бустинг, метод случайного леса, нейронные сети и другие. Наиболее перспективным можно считать метод прогнозирования при помощи нейронных сетей. Данный метод позволяет предсказывать события посредством параллельной обработки информации всеми звеньями сети, что значительно ускоряет процесс прогнозирования. При длительном обучении на заранее определённом массиве данных сеть учится обобщать полученную информацию, что значительно уменьшает вероятность ошибки при прогнозировании на других массивах данных [3].

Для рассматриваемого в данной статье объекта – лабораторий химической и экологической безопасности цеха тепловодоснабжения и канализации (ТВСиК) Инженерно-технического центра (ИТЦ) ООО «Газпромтрансгаз “Чайковский”» – важным аспектом по предотвращению аварий является своевременный сбор данных о состоянии загазованности помещения. Для лаборатории химической безопасности это данные о наличии в воздушной среде едких щелочей, серной кислоты, азотной кислоты, синильной кислоты, уксусной кислоты, соляной кислоты, акриловой кислоты. Для лаборатории экологической безопасности это данные о наличии в воздушной среде диоксида углерода и метана. Сбор данных осуществляется вручную аналоговыми газоанализаторами 3 раза в день (начало, середина, конец рабочей смены), а также автоматически – ежедневно, с интервалом в 30 с, дискретными газоанализаторами ГАНК-4С (в лаборатории химической безопасности) и ИГМ-12 (в лаборатории экологической безопасности). Данные собираются промышленным контроллером в каждой лаборатории в течение всего рабочего дня, формируя тем самым 960 сигналов в день, и передаются в базу данных (БД) SCADA системы управления вентиляцией. Каждый из газоанализаторов в случае аварийной ситуации передаёт дискретный сигнал в течение 2 минут либо до ручного отключения сигнала оператором контроллера [4, 5]. Анализ прогноза возможного времени возникновения аварийной ситуации позволяет создать систему помощи принятия решений

(СППР) по проведению превентивной вентиляции лабораторий в временные промежутки, для которых наиболее характерно возникновение аварийной ситуации, а также добавить дополнительное визуальное предупреждение для сотрудников в данные временные промежутки.

Методика прогнозирования реализуется на основе программного обеспечения (ПО) Orange. Данное ПО реализовано на принципах визуального программирования и использует графические объекты – виджеты, каждый из которых отвечает за определённую функцию, будь то загрузка данных, вычисления или визуальное отображение результатов. Для создания прогноза воспользуемся базой данных замеров газоанализаторами за период сентябрь-октябрь 2021 г. как наиболее загруженного периода работы лабораторий в течение календарного года [6]. Создание модели прогнозирования осуществляется на основе данных за сентябрь, данные за октябрь используются для проверки качества прогноза. База данных формируется из сигналов, полученных с интервалом в 30 с. Затем средствами SCADA-системы рассчитываются дата и время каждого замера (с учётом системного времени рабочего места оператора SCADA и исходя из известного интервала снятия замеров). На основе вышеперечисленного формируется таблица, где каждой строке соответствуют замеры газоанализаторов, переданные через контроллер в SCADA. В каждой строке указываются номер, дата, время измерения, дискретные показания газоанализатора лаборатории химической безопасности (Датчик1) и лаборатории экологической безопасности (Датчик2). В итоге формируются 21 120 строк замеров в сентябре и 20 160 строк замеров в октябре. Заголовок таблицы представлен на рис. 1.

Номер измерения	Дата	Время	Датчик1	Датчик2
-----------------	------	-------	---------	---------

Рис. 1. Структура базы данных системы вентиляции офисного здания

Накопленные данные путем преобразования позволяют создать массивы, атрибутами которых будут начало и конец рабочего дня, день недели и день месяца. Далее определяются вероятностные зависимости возникновения аварийных ситуаций, а именно вероятность возникновения загазованности в лаборатории безопасности в зависимости от дня месяца, дня недели и часа рабочего дня. Для наглядно-

сти в данной статье рассматривается только лаборатория химической безопасности. Программа прогнозирования действует следующим образом:

1. База данных загружается с рабочую среду Orange посредством виджета File. Исходная обучающая выборка случайным образом разбивается на 80 % рабочей обучающей выборки и 20 % валидационной выборки при помощи виджета Data Sampler.

2. Производится прогноз целевого поля на основании модели, построенной виджетом Neural Network, и выводится в виджет Predictions (данный процесс повторяется 1000 раз для обучения нейронной сети). График прогноза выводится виджетом Scatter Plot.

3. Результаты прогноза преобразуются в стандартный вид с хронологической нумерацией в виджете Data Table и сохраняются отдельным файлом при помощи виджета Save Data для дальнейшего сравнения с контрольным набором данных за октябрь. Конечный вид программы представлен на рис. 2.

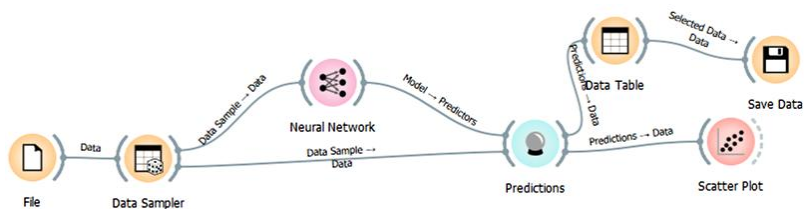


Рис. 2. Структура программы прогнозирования

Результаты прогнозирования аварийных ситуаций в лаборатории химической безопасности для сентября представлены на рис. 3.

На графиках чёрными точками отмечены моменты аварийных ситуаций согласно прогнозу. Серым цветом отмечено нормальное состояние загазованности. По оси абсцисс отмечаются дни месяца. На оси ординат отображаются состояния загазованности в соответствии с порядковым номером измерения. Каждому дню месяца соответствует кластер эллипсоидного вида множества измерений, состоящий из чёрных и серых точек. Всего таких кластеров 23, по количеству рабочих дней в месяце. Данные кластеры формируют группу рабочей недели, состоящую из 5 кластеров (как частный случай, 3 кластера – для первой рабочей недели). Чем выше в кластере расположена чёрная точка, тем ближе предполагаемая авария к концу дня,

чем ниже, тем ближе предполагаемая авария к началу дня. Каждая чёрная точка хранит в себе также информацию о предполагаемом времени аварии с точностью до 30 с.

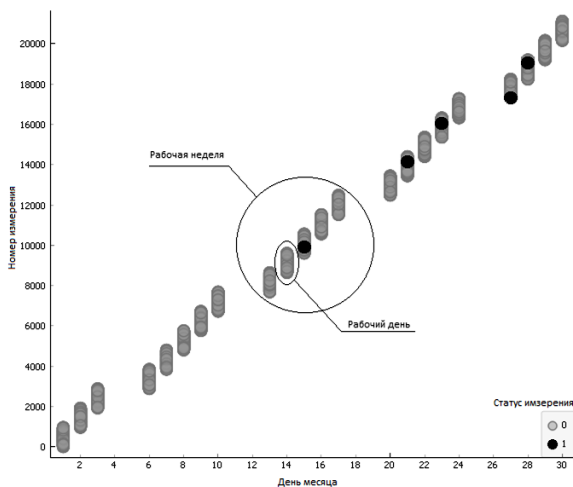


Рис. 3. Диаграмма рассеяния предсказания аварийной ситуации в лаборатории химической безопасности в течение месяца

Согласно полученному прогнозу, аварийная ситуация может произойти в понедельник в 9:12 (последняя рабочая неделя), во вторник может произойти 2 аварийных ситуаций – в 14:36 (4-я рабочая неделя) и в 15:34 (последняя рабочая неделя), в среду – одна, в 11:34 (3-я рабочая неделя), в четверг – одна, в 14:24 (4-я рабочая неделя). С учётом вышеперечисленного можно рекомендовать проводить оповещения для сотрудников лаборатории химической безопасности о возможной аварийной ситуации во второй половине дня. Особое внимание следует уделить первой половине рабочей недели и последней неделе месяца.

Формула точности прогноза аварийной ситуации в октябре для лаборатории химической безопасности примет вид:

$$A_x = (B_x - M \cdot N_o) / N_o \cdot 100 \% = \frac{20152 - 20160 \cdot 0.2}{20160} \cdot 100 \% = 79,96 \%,$$

где A_x – точность прогноза аварийной ситуации в октябре для лаборатории химической безопасности; B_x – количество соответствий прогнозируемых и контрольных измерений для газоанализатора лаборатории химической безопасности; M – доля измерений, сгенерированных случайным образом и создающих погрешность.

Полученную точность прогнозирования можно признать удовлетворительной с учётом количества измерений, используемых для создания тренируемой выборки, и количества итераций, используемых для обучения нейронной сети. Полученная программа как ключевой элемент СППР позволит существенно упростить работу персонала по профилактике аварийных ситуаций в лабораториях экологической и химической безопасности цеха ТВСиК ИТЦ ООО «Газпромтрансгаз «Чайковский»».

Библиографический список

1. Косачёв А.Д., Широков А.А.. Модернизация системы вентиляции офисного здания // Материалы всерос. науч.-техн. конф. АСУИТ-2020. – Пермь, 2020. – С. 417–422.
2. Косачёв А.Д., Широков А.А. Модернизация системы вентиляции офисного здания // Материалы всерос. науч.-техн. конф. АСУИТ-2021. – Пермь, 2021. – С. 407–412.
3. Adewole Adetunji Philip, Akinwale Adio Taofiki, Akintomide Ayo Bidemi, Artificial Neural Network. Model for Forecasting Foreign Exchange Rate // World of Computer Science and Information Technology Journal (WCSIT). – 2011. – Vol. 1, No. 3. – P. 110–118.
4. ПНДФ 12.13.1-03. Техника безопасности при работе в аналитических лабораториях (общие положения) // Доступ из справ.-правовой системы КонсультантПлюс.
5. ГОСТ Р ЕН 13779-2007. Вентиляция в нежилых зданиях. Технические требования к системам вентиляции и кондиционирования // Доступ из справ.-правовой системы КонсультантПлюс.
6. СТО Газпром 1.8-2014 // Доступ из справ.-правовой системы КонсультантПлюс.

Сведения об авторах

Косачёв Андрей Дмитриевич – магистрант Пермского национального исследовательского политехнического университета, гр. ИСУП-20-1м, Пермь, e-mail: crazimakky@gmail.com

Широков Александр Аркадьевич – кандидат технических наук, доцент кафедры «Микропроцессорные системы автоматизации» Пермского национального исследовательского политехнического университета, Пермь, e-mail: shirokov@pstu.ru

Д.Е. Крамер, Е.А. Чабанов

Пермский национальный исследовательский
политехнический университет, Пермь

**ИСПОЛЬЗОВАНИЕ РОБОТОВ-МАНИПУЛЯТОРОВ
В АВТОМАТИЗАЦИИ ПРОЦЕССОВ ПРОИЗВОДСТВА.
ПЕРСПЕКТИВЫ РАЗВИТИЯ**

Исследуется возможность автоматизации процессов производства путем внедрения на предприятии роботов-манипуляторов, описывается устройство классического манипулятора и способы управления им. Приведены статистические данные уровня автоматизации производства в некоторых странах, также рассматриваются основные направления развития робототехники в ближайшие годы.

Ключевые слова: роботы, манипуляторы, автоматизация, промышленные роботы, производство.

D.E. Kramer, E.A. Chabanov

Perm National Research Polytechnic University, Perm

**THE USE OF ROBOTIC MANIPULATORS
IN THE AUTOMATION OF PRODUCTION PROCESSES.
DEVELOPMENT PROSPECTS**

This article explores the possibility of automating production processes by introducing robotic manipulators to the enterprise, describes the device of a classical manipulator and how to control it. Statistical data on the level of production automation in some countries are given. The article also discusses the main directions of robotics development in the coming years.

Keywords: robots, manipulators, automation, industrial robots, production.

Робот – автоматический механизм, предназначенный для выполнения различных механических операций, заложенных в программе.

Робот анализирует окружающий мир посредством сенсоров (микрофонов, камер, датчиков), составляет определенную модель поведения, необходимую для выполнения той или иной команды, различными способами может оказывать воздействие на физический мир.

В настоящее время роботов по всему миру активно внедряют в различные области жизни и деятельности людей. Большинство

современных предприятий автоматизируется, исключая человека из производственного процесса. Роботов внедряют в медицину, некоторые службы спасения используют их для более эффективной работы, также роботов внедряют в обыденную жизнь людей, тем самым избавляя их от рутинной работы, требующей большого количества времени.

Роботы-манипуляторы представляют собой высокопроизводительную автоматизированную систему, которая функционирует за счет электронной платформы управления. Промышленные роботы могут различаться устройством в зависимости от того, для выполнения каких задач они были созданы. На данный момент самыми распространёнными являются роботизированные манипуляторы.

Классический манипулятор может состоять из 7 сегментов, которые соединены между собой с помощью шести суставов (устройство представлено на рисунке). В каждом сегменте присутствуют шаговые двигатели, управляющие суставами. Они обеспечивают высокоточное позиционирование манипулятора. Управление осуществляется контроллерами, которые задают определенные траектории движения отдельных сегментов робота путем управления режимами работы выбранными шаговыми двигателями. Общее управление роботом-манипулятором осуществляется компьютером (сервером).

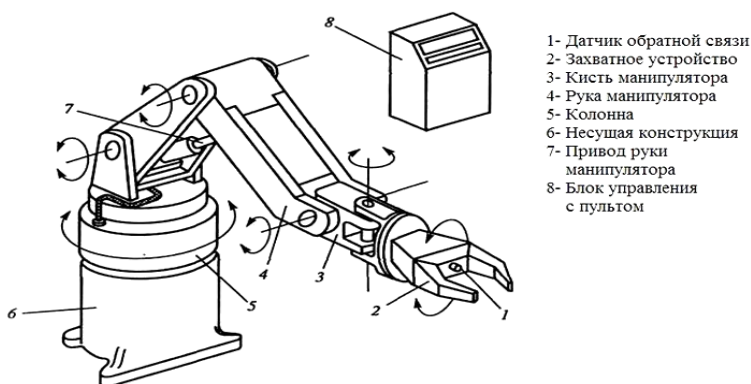


Рис. Устройство классического робота манипулятора

Для контроля точности выполненных команд используются датчики движения. При возникновении незначительных отклонений от заданной траектории движения сегмента программа контроллера

осуществляет его коррекцию. При существенном отклонении работы робота-манипулятора от заданной программы подается соответствующий сигнал главному компьютеру (серверу). Этот компьютер выполняет общую коррекцию работы комплекса или, при аварийных ситуациях или неисправностях, останавливает робота для починки.

Манипулятор имеет устройство захвата, которое внешне напоминает человеческую руку с механическими пальцами. В зависимости от области применения захватывающее устройство может быть заменено на пульверизатор, отвертку или любое другое приспособление, использование которого в данном технологическом процессе является целесообразным. Для питания роботов чаще всего используется промышленная электрическая сеть, а для обеспечения бесперебойности их работы применяют аккумуляторы, которые подключаются автоматически в случае некорректной работы общей электросети.

Как было отмечено, большинство промышленных роботов-манипуляторов имеют 6 суставов (6 степеней свободы), т.е. он может двигаться в 6 направлениях [1].

Степень подвижности можно вычислить по формуле Сомова–Мальшева:

$$W = 6 \cdot n - 5 \cdot P_5 - 4 \cdot P_4 - 3 \cdot P_3 - 2 \cdot P_2 - P_1, \quad (1)$$

где n – число подвижных звеньев; P – число кинематических пар соответствующего класса.

Управление роботами манипуляторами может быть следующих типов:

- 1) программное управление: роботы управляются посредством заложенной в них программы;
- 2) адаптивное управление: роботы оснащены сенсорами, которые анализируют объект и в зависимости от полученных результатов измерений принимают решение о дальнейших действиях;
- 3) управление посредством искусственного интеллекта;
- 4) управление человеком (ручное управление).

В настоящее время самыми распространёнными роботами являются роботы-манипуляторы, которые получили широкое распространение в различных областях деятельности человека, но чаще всего используются в промышленности. По данным Федерации робототехники (IFR), только за 2019 г. в мире было установлено 373 000 промышленных роботов. Основными преимуществами таких роботов

являются: снижение затрат на рабочую силу, ускорение производственных процессов, повышение производительности труда, а также точности и качества изготавливаемого изделия.

Сегодня робототехника становится значительно дешевле. За последнее десятилетие стоимость промышленных роботов снизилась на 30 %. Прогнозируется снижение стоимости еще на 20–22 % за следующие 10 лет.

Теперь роботы-манипуляторы используются не только крупными производствами, но и предприятиями малого бизнеса. Почти все ведущие компании по выпуску робототехники производят манипуляторы, в том числе и робототехнические.

Компании Changying Precision Technology, Mcdonald's, Vanguard Plastics Corp и FANUC Robotics провели практические исследования, по результатам которых сделали следующие выводы:

1. Роботы успешно заменяют человека в производственном процессе, при этом дешевле обходятся на производстве.
2. Каждый робот-манипулятор может заменить десятки работников.
3. За 12–15 лет эксплуатации роботы окупятся и увеличат производство продукции во много раз.

В настоящее время большинство промышленных предприятий автоматизируется. Однако лишь в некоторых развитых странах уровень автоматизации промышленности превышает 20 % от общего числа предприятий.

К 2020 г. уровень автоматизации в главных секторах экономики в развитых странах выглядел так:

- США – 26 %;
- Франция – 21 %;
- Германия – 17 %;
- Великобритания – 16 %;
- Индия – 15 %.

В России около 15 % крупных предприятий уже внедрило автоматизацию в свой производственный процесс. Автоматизация производства не только сокращает затраты на выплаты работникам, но и увеличивает объемы производства, улучшает качество продукции, сокращает расходы сырья, уменьшает объемы производственного брака и отходов.

Можно выделить следующие направления развития робототехники на ближайшие несколько лет [2]:

1. *Новые источники энергии.* Для повышения эффективности работы роботов и уменьшения затрат на их обслуживание необходимо улучшить их энергетические характеристики. Сейчас большинство роботов функционируют, получая электроэнергию от аккумуляторов на основе лития. Улучшить такие аккумуляторы можно за счет новых материалов электродов, совершенствования химического состава аккумулятора, более равномерной толщины покрытия, посредством оптимизации технического прогресса. Возможно сегодня использование альтернативных источников энергии. Ведутся исследования по созданию новых роботов, получающих электроэнергию от альтернативных источников электроэнергии (солнечных батарей, ветроэнергетических установок и др.), и оптимизации работы существующих, а также по созданию сетей беспроводной зарядки. Дистанционная подзарядка роботов может быть реализована с помощью источников энергии, встроенных в конструкции зданий и строений (стены и пол). Данными разработками уже занимается компания WitBotic, которая предлагает заинтересованным лицам приобретать беспроводные устройства зарядки дронов, наземных и подземных роботов.

2. *Взаимодействие групп роботов и людей.* Предполагается создание системы для управления группой роботов, которая, используя различные алгоритмы (например, генетический), сама будет определять траекторию движения во избежание столкновения и аварий. Также в перспективе рассматривается улучшение таких систем с целью передачи информации между роботами. Роботы смогут обмениваться друг с другом данными об окружающей среде, о наличии в непосредственной близости каких-либо факторов или предметов, которые могут оказать влияние на выполняемую ими работу. Такие системы тестируются в Великобритании, США и России.

3. *Навигация в экстремальных условиях.* Роботы используются также для работы в экстремальных условиях, в которых функционирование человека нежелательно или практически невозможно, поэтому важным является создание такой системы, которая сможет проложить маршрут и обеспечить выполнение поставленной задачи без какого-либо вмешательства человека. Примером такой системы является инерциальный измерительный модуль (IMU). Однако он не способен долговременно обеспечивать систему точными данными, так как со временем датчики накапливают ошибки.

Заключение. В настоящее время активно проводятся исследования в области робототехники, поскольку это одна из самых перспективных отраслей деятельности человека. Автоматизация производства требует больших финансовых затрат в связи с высокой стоимостью роботов. Однако интенсивно проводятся исследования по оптимизации процессов автоматизации производства и снижению связанных с этим затрат. Многие крупные предприятия автоматизируют свои производства, поскольку это позволяет снижать затраты, улучшать качество производимого продукта, увеличивать темпы создания продукции, уменьшать себестоимость производимых изделий.

Библиографический список

1. Игнатъев Б. ТОП–6: виды и назначение роботов-манипуляторов, цена и где купить [Электронный ресурс]. – URL: <https://motocarrello.ru/jelektrotehnologii/roboty/1769–robot-manipulja–tor.html>
2. Тимофеев Г.А. Теория механизмов и машин: курс лекций. – М.: ЮРАЙТ, 2010. – 351 с.
3. Ефимов А., Зятегов Д., Цыганков В. Аналитический обзор мирового рынка робототехники 2019 Сбербанк [Электронный ресурс]. – URL: https://www.sberbank.ru/common/img/uploaded/pdf/sberbank_robotics_review_2019_17.07.2019_m.pdf?_ga=2.37929059.1943410483.1608712996–50184831.1608712996

Сведения об авторах

Крамер Дарина Евгеньевна – студентка Пермского национально-исследовательского политехнического университета, гр. ЭЭ-20-46, Пермь, e-mail: darinakramer.2001@yandex.ru

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

Е.С. Трушников, Я.А. Жуков, О.А. Билоус

Пермский национальный исследовательский
политехнический университет, Пермь

МОДЕРНИЗАЦИЯ АСУ ТП ПАРОВОЙ КОТЕЛЬНОЙ

Предлагается проект модернизации АСУ ТП паровой котельной. Предусмотрен переход к единообразной структуре АСУ ТП на базе дублированных контроллеров, дублированного сервера и функционально дублированных клиентских рабочих мест (АРМов). Для организации отказоустойчивой связи контроллеров и серверов системы применяется контроллерная шина на базе Industrial Ethernet с кольцевым резервированием. Связь клиентских рабочих мест (АРМов) с серверами организована по терминальной шине на базе Industrial Ethernet с кольцевым резервированием. Все АРМы проектируются с равным доступом ко всем объектам управления. Также предусмотрена реализация удалённого защищённого управления инженерной (операторской) станцией.

Ключевые слова: АСУ ТП, клиентское рабочее место (АРМ), удалённое защищённое управление.

E.S. Trushnikov, Ya.A. Zhukov, O.A. Bilous

Perm National Research Polytechnic University, Perm

MODERNIZATION OF THE STEAM BOILER ROOM APCS

A project for the modernization of the automated process control system for a steam boiler house is proposed. The transition to a uniform structure of the APCS based on duplicated controllers, a duplicated server and functionally duplicated client workstations (AWPs) is envisaged. To organize fault-tolerant communication between controllers and system servers, a controller bus based on Industrial Ethernet with ring redundancy is used. Communication of client workstations (AWPs) with servers is organized via a terminal bus based on Industrial Ethernet with ring redundancy. All workstations are designed with equal access to all control objects. It also provides for the implementation of secure remote control of the engineering (operator) station.

Keywords: APCS, client workstation (AWP), remote secure management.

Предлагается проект модернизации АСУ ТП паровой котельной. Необходимость модернизации объясняется тем, что оборудование эксплуатируется в непрерывном режиме с 2003 г. Модернизация поможет увеличить срок службы станции за счет уменьшения аварийных остановов и повысит производительность оборудования.

Для решения задачи модернизации необходим переход к единообразной структуре АСУ ТП на базе дублированных контроллеров, дублированного сервера и функционально дублированных клиентских рабочих мест (АРМов). Также предусмотрена реализация удалённого защищённого управления инженерной (операторной) станцией.

Перечень и порядок выполнения работ для модернизации АСУ ТП паровой котельной:

- приобретение оборудования и программного обеспечения;
- монтаж серверного шкафа;
- монтаж интерфейсных кабелей;
- монтаж сетевого оборудования в пультовой секции ГрЩУ (групповой щит управления);
- монтаж АРМов первого этапа на ГрЩУ;
- инсталляция и настройка общего и специального программного обеспечения;
- наладка и пуск в эксплуатацию АСУ ТП в части верхнего уровня (сервера, АРМы);
- демонтаж контроллерного оборудования котлов;
- монтаж сетевого и контроллерного оборудования котлов;
- наладка и пуск в эксплуатацию АСУ ТП в части котлов;
- установка программного обеспечения JumpDesktop на инженерную станцию.

Состав основного оборудования, устанавливаемого в процессе модернизации:

- дублированные контроллеры;
- интерфейсные модули;
- сетевое оборудование;
- шкаф серверный (дублированный сервер, KVM, источник точного времени);
- клиентские рабочие места (АРМы).

Контроллеры и интерфейсные модули предназначены для замены выработавшего ресурс существующего оборудования и выбраны из номенклатуры выпускаемого фирмой SIEMENS оборудования актуальных версий. При выборе резервированного контроллерного оборудования предпочтение отдано аппаратно-резервируемым контроллерам повышенной надежности серии S7 400-Н.

На рисунке показаны аппаратные компоненты, образующие отказоустойчивую систему управления S7 400-Н.

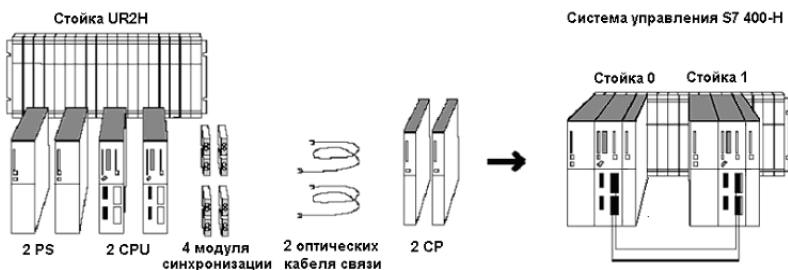


Рис. Аппаратура системы управления S7 400-H

Ядро системы управления образуют два центральных процессора CPU41х-Н. Настройка синхронизационных модулей определяет номера стоек. Используется монтажная шина UR2H. Эта шина делает возможным монтаж двух отдельных подсистем, каждая из которых имеет 9 слотов, на одной 19-дюймовой монтажной стойке. Для каждой подсистемы S7 400-H необходим один источник питания из стандартного ряда SIMATIC S7 400. Синхронизационные модули используются для соединения центральных процессоров. Они устанавливаются в центральных процессорах и соединяются друг с другом посредством волоконно-оптических кабелей. В каждом CPU должно быть установлено два синхронизационных модуля. Волоконно-оптические кабели вставляются в синхронизационные модули и образуют физическое соединение (связь для обеспечения резервирования) между двумя центральными процессорами. Для обеспечения связи системы управления S7 400-H с операторской станцией (системой визуализации) используются коммуникационные процессоры Industrial Ethernet CP443-1. На серверном оборудовании предусмотрено резервирование сетевых интерфейсов на аппаратном уровне. Для этого в каждый сервер устанавливаются по два коммуникационных процессора, обеспечивающих отказоустойчивую связь с дублированными контроллерами. Сетевое оборудование контроллерной и терминальной шин выбирается однотипным для упрощения ввода в эксплуатацию и сокращения номенклатуры ЗИП.

Информационная сеть верхнего уровня АСУ ТП выполняется с использованием современного интерфейса Ethernet. Кольцевое резервирование ЛВС обеспечивает бесперебойность работы сетевого обмена. Построение кольцевых структур ЛВС выполняется на основе вновь прокладываемых оптических кабелей. Оптические линии пере-

даны данных используются в тех случаях, когда особенные требования предъявляются к таким параметрам, как электрическая развязка по току и электромагнитная совместимость (ЕМС) линий передачи. Оптические линии передачи на основе оптико-волоконного кабеля отличаются тем, что являются полностью независимыми от электромагнитных помех. Другим преимуществом кабелей такого рода является обеспечение полной гальванической развязки. Подключение оборудования (контроллеров, серверов) к кольцу выполняется электрическими фрагментами Ethernet.

Для организации перехода на резервированную клиент-серверную архитектуру АСУ ТП предусматривается установка серверного шкафа. В его состав входят два независимо работающих сервера с резервированием. Для доступа к серверам в серверный шкаф устанавливаются KVM-переключатель со складным экраном и контроллер серии S7-1200 для выполнения диагностических функций по оборудованию.

Кроме серверов в шкафу предусматривается источник точного времени, обеспечивающий синхронизацию времени всех устройств АСУ ТП (контроллеров, серверов, АРМов) с использованием GPS/ГЛОНАСС.

В качестве АРМов используются компьютеры, оснащенные программным обеспечением SIEMENS для выполнения функций клиентов в клиент-серверной архитектуре АСУ ТП. Обмен данными с серверами производится по сетевому интерфейсу Ethernet с использованием терминальной шины с кольцевым резервированием.

Для удаленного управления рабочим столом компьютера выбрана программа Jump Desktop.

Особенности программы Jump Desktop:

- поддержка различных протоколов: поддержка протоколов RDP и VNC;

- простая и безопасная установка: автоматическая настройка компьютера для удаленного доступа с использованием Wi-Fi и 3G;

- универсальное применение: работы по iPad, iPhone и iPod Touch, Android. Автоматическая оптимизация интерфейса на основе устройства;

- полная поддержка многозадачности;

- наличие уникального режима презентации на iPad, что позволяет превратить курсор мыши в лазерную указку;

- расширенная поддержка клавиатуры Bluetooth: ярлыки, функциональные клавиши и клавиши со стрелками;
- поддержка очень больших разрешений экрана;
- поддержка нескольких жестов – включает в себя возможность рисовать или писать с помощью пальцев;

Заключение. Модернизация АСУ ТП котельной позволит улучшить показатели качества производства, уменьшить риск травматизма персонала, облегчит работу персонала.

Библиографический список

1. Лыков А.Н. Автоматизация технологических процессов и производств. – Пермь: Изд-во Перм. гос. техн. ун-та, 2008. – 423 с.
2. Рабочая документация существующей АСУ ТП (рабочие проекты ОАО «УРАЛВНИПИЭНЕРГОПРОМ») // Доступ из справ.-правовой системы КонсультантПлюс.
3. СО 34.35.127-2002. Общие технические требования к программно-техническим комплексам для АСУ ТП тепловых электростанций. – М., 2002.
4. СО 34.35.137-00. Технические требования к подсистеме технологических защит, выполненных на базе микропроцессорной техники. – М., 2000.

Сведения об авторах

Трушников Евгений Сергеевич – студент Пермского национального исследовательского политехнического университета гр. АТПП-18-1бзу, Пермь, e-mail: trushnikoves@icloud.com

Жуков Ярослав Александрович – студент Пермского национального исследовательского политехнического университета гр. АТПП-18-1бзу, Пермь, e-mail: yaroslavzhukov.59@gmail.com

Билоус Ольга Анатольевна – старший преподаватель кафедры «Микропроцессорные системы автоматизации» Пермского национального исследовательского политехнического университета, Пермь, e-mail: bilous_oa@pstu.ru

Секция 3

**ИННОВАЦИОННЫЕ НАПРАВЛЕНИЯ В ЭНЕРГЕТИКЕ.
ЭНЕРГОРЕСУРСОСБЕРЕЖЕНИЕ**

С.Н. Быков, П.В. Лыкасов, Д.Ю. Лейзгольд

Пермский национальный исследовательский
политехнический университет, Пермь

ПОВЫШЕНИЕ ЭНЕРГОЭФФЕКТИВНОСТИ И СНИЖЕНИЕ КОЛИЧЕСТВА ВЫБРОСОВ ЗАГРЯЗНЯЮЩИХ ВЕЩЕСТВ

В данной статье рассматривается возможность снижения выбросов в атмосферу парниковых газов, на примере Чульманской ТЭЦ. Основываясь на реализуемое выполнение программы развития Сибирского региона, были предложены мероприятия по повышению энергоэффективности, а также по увеличению экологической безопасности рассматриваемого энергетического объекта, расположенного в Восточно-Сибирском экономическом районе.

Ключевые слова: загрязняющие вещества, электроэнергетика, газотурбинная установка, котёл – утилизатор, расход условного топлива, эмиссия углекислого газа.

S.N. Bykov, P.V. Lykasov, D.Yu. Leyzgold

Perm National Research Polytechnic University, Perm

IMPROVING ENERGY EFFICIENCY AND REDUCING EMISSIONS OF POLLUTANTS

This article discusses the possibility of reducing greenhouse gas emissions into the atmosphere, using the example of the Chulman CHP. Based on the ongoing implementation of the program for the development of the Siberian region, measures were proposed to improve energy efficiency, as well as to increase the environmental safety of the considered energy facility located in the East Siberian economic region.

Keywords: pollutants, electric power industry, gas turbine plant, waste heat boiler, equivalent fuel consumption, carbon dioxide emissions.

Начиная с эпохи индустриализации, антропогенный фактор начал напрямую влиять на содержание парниковых газов в атмосфере нашей планеты. Анализ диаграммы температуры на поверхности Земли (рис. 1) показывает, что с середины XX в. происходит резкий рост температуры, вследствие сжигания ископаемого топлива.

Согласно данным Киотского протокола, существуют следующие виды парниковых газов: углекислый газ, метан, закись азота (N_2O), гидрофторуглероды, перфторуглероды, гексафторид серы (SF_6). Из них определяющую роль занимают такие разновидности газов, как углекислый газ, метан и оксиды азота.

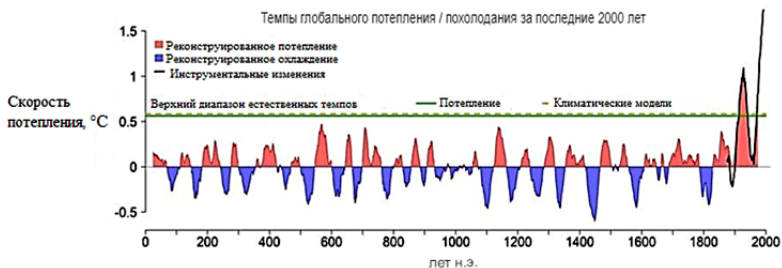


Рис. 1. Диаграмма температуры поверхности Земли

Наибольшую составляющую в выбросах загрязняющих веществ занимает электроэнергетика, а именно генерация. Наиболее «грязным» из всех видов ископаемого топлива, с помощью которого получают тепловую энергию, является уголь, поэтому в данной статье рассматриваются тэпоэлектроцентрали (ТЭЦ), которые работают на сжигании угля.

Учитывая вышеизложенное, а также ссылаясь на выполнение программы развития Сибири, озвученной Сергеем Шойгу [1], важно подготовить электроэнергетическую систему (ЭЭС) Сибирского региона, вывести ее на должный уровень энергоэффективности и экологической чистоты. Поэтому в данной работе рассматривается решение по модернизации существующего объекта генерации.

В качестве объекта модернизации была выбрана Чульманская ТЭЦ с установленной мощностью 48 МВт и тепловой мощностью 165 Гкал/ч, коэффициент использования установленной мощности (КИУМ) которой составляет 26,5 %. В качестве основного топлива на ней используется каменный уголь. Удельный расход условного топлива (УРУТ) значительно превышает целевые показатели по Российской Федерации (табл. 1). Оборудование морально и физически устарело [2, 3].

Таблица 1

Технические показатели Чульманской ТЭЦ в сравнении с мировыми трендами [4, 5]

Параметр	Чульманская ТЭЦ	Среднемировой показатель угольных ТЭЦ	Целевые показатели РФ [6]
УРУТ на отпуск электроэнергии $B_{\text{эл}}$, кг у.т./тыс. кВт·ч	829,99	716,16	285,4
УРУТ на отпуск тепла $B_{\text{тп}}$, кг у.т./Гкал	186,3	174,3	156,4

Исходя из вышеизложенного, следует, что Чульманская ТЭЦ нуждается в серьезной модернизации.



Рис. 2. Расположение газопровода в посёлке Чульман

Оптимальным вариантом является использование установок, работающих на сжигании природного газа. Как видно по карте, в районе Чульманской ТЭЦ уже проведен газопровод, что исключает дополнительные капиталовложения на его прокладку.

В качестве решения предлагается заменить оборудование Чульманской ТЭЦ на три газотурбинные установки ГТЭ-16ПА фирмы ОАО «Авиадвигатель» [7], Россия. В качестве котлов-утилизаторов при разработке «ОБИН» рассмотрены котлы-утилизаторы КУВ производства ООО «Белэнергомаш-БЗЭМ», г. Белгород, Россия [8]. В качестве водогрейных котельных рассмотрены водогрейные котлы типа «Термотехник ТТ300» фирмы ООО «Энтророс», Россия [9].

Исходя из данных, представленных в табл. 2, можно утверждать, что предлагаемый вариант слегка увеличивает установленную электрическую мощность Чульманской ТЭЦ, также незначительно снижает тепловую мощность.

Таблица 2

Технические характеристики предлагаемого оборудования

Наименование показателя	
Тип газотурбинной установки (ГТУ)	ГТЭ-16ПА
Электрическая мощность, МВт	16,3
Количество ГТУ, шт.	3
Полная электрическая мощность, МВт	48,9
Модель котла-утилизатора	КУВ-22-115
Количество котлов-утилизаторов, шт	3
Тепловая мощность КУВ, Гкал/ч	55,8
Модель котлов	Термотехник ТТ300
Тепловая мощность водогрейных котлов, Гкал/ч	103,2
Общая тепловая мощность, Гкал/ч	159,0

Таблица 3

Технические характеристики предлагаемого оборудования

Наименование показателя	ГТЭ-16ПА
Электрическая мощность	16,3
КПД выработки электрической, %	35,5
Расход природного газа, кг/ч	4883,0
Расход газа на выхлопе, кг/с	56,3
Температура газов на выхлопе, град	481
Максимальное давление природного газа перед турбиной, МПа	3,2
Тепловая мощность КУВ, Гкал/ч	18,6
Содержание NO _x , мг/м ³	Менее 50
Содержание CO, мг/м ³	Менее 100
Полный КПД, %	84,7

При переходе на газовое оборудование отпадёт необходимость в утилизации золы, образующейся при сжигании угля, но проблема выброса в атмосферу газообразных загрязняющих веществ остаётся актуальной. Согласно параметрам ГТЭ-16ПА (табл. 3) выбросы оксидов азота не превышают 50 мг/м³, выбросы оксида углерода не превышают 100 мг/м³. Следовательно, сокращается выделение оксидов азота в 6 раз, а оксида углерода в 4 раза [10].

Таблица 4

Технические показатели Чульманской ГЭЦ при установке предлагаемого оборудования

Годовая выработка электроэнергии, млн. кВт·ч	297,3
Годовой отпуск электроэнергии, млн. кВт·ч	270,7
Годовая выработка тепла, тыс. Гкал	503,4
Годовой отпуск тепла, тыс. Гкал	425,3
Число часов использования установленной мощности, ч/год	6080 – Газотурбинных энергоблоков 1590 – Водогрейных котлов
Годовой расход натурального топлива, млн. нм ³	116,4
Годовой расход условного топлива, тыс. т у.т	132,7
УРУТ на отпуск электроэнергии, г/кВт·ч	262,76
УРУТ на отпуск тепла, кг/Гкал	144,94

По прогнозу удельный расход условного топлива (УРУТ) в Российской Федерации на отпуск электроэнергии к 2024 г. будет составлять 285,4 кг у.т./тыс. кВт·ч, а на отпуск тепла – 156,4 кг у.т./Гкал к 2022 г. [6]. Анализируя информацию из табл. 4, можно сделать

выводы о том, что УРУТ на отпуск электроэнергии снижается на 68 %, УРУТ на отпуск тепла снижается на 22,2 %. Полученные показатели свидетельствуют о том, что энергоэффективность превосходит даже целевые показатели: по отпуску электроэнергии на 8 %, по отпуску тепла на 7,3 %.

В заключение стоит отметить, что предложенное решение по модернизации Чульманской ТЭЦ позволит не только повысить энергетическую эффективность посредством увеличения КПД электропроизводящих установок, но и снизить углеродный след в зонах непрерывной и прерывистой вечной мерзлоты, что, несомненно, снизит скорость таяния мерзлых грунтов и возникновения лавинообразного выделения парниковых газов.

Библиографический список

1. Сергей Шойгу – о новых городах в Сибири. Полная версия [Электронный ресурс]. – URL: <https://www.rbc.ru/politics/06/09/2021/6131fab69a79471a71a0b412> (дата обращения: 14.11.2021).

2. Акционерное общество «Дальневосточная генерирующая компания». Годовой отчёт за 2020 год [Электронный ресурс]. – URL: <https://www.dvgk.ru/uploads/attachments/dvgk/AboutCompany/CorpoUpravl/GODGK2020.pdf> (дата обращения: 14.11.2021).

3. Отчёт №447/06. Об оценке рыночной стоимости одной обыкновенной и одной привилегированной акции в составе миноритарного пакета ОАО АК «Якутскэнерго» [Электронный ресурс]. – URL: <https://yakutskenergo.ru/data/files/212ffile.pdf> (дата обращения: 14.11.2021).

4. Техничко-экономические показатели [Электронный ресурс]. – URL: <https://www.dvgk.ru/page/37> (дата обращения: 16.11.2021).

5. Снижение углеродоёмкости электроэнергии [Электронный ресурс]. – URL: https://www.cdu.ru/tek_russia/issue/2019/9/656/ (дата обращения: 16.11.2021).

6. Государственная программа Российской Федерации «Развитие энергетики» [Электронный ресурс]. – URL: <https://minenergo.gov.ru/node/323> (дата обращения: 14.12.2021).

7. Энергетическая газотурбинная установка ГТЭ-16ПА мощностью 16 МВт [Электронный ресурс]. – URL: http://www.pmz.ru/products/gtu_energy/gtu_16p/ (дата обращения: 29.11.2021).

8. Энергомаш – котельное оборудование [Электронный ресурс]. – URL: <http://www.energomash.ru/upload/iblock/bd2/boilers.pdf> (дата обращения: 29.11.2021).

9. Термотехник ТТ300 [Электронный ресурс]. – URL: https://www.entroros.ru/netcat_files/69/124/h_210dad6dc42ffa9c6e3daea490cb33fb (дата обращения: 29.11.2021).

10. Нормативы удельных выбросов загрязняющих веществ в атмосферу от котельных установок [Электронный ресурс]. – URL: https://vti.ru/files/public/uchebno-metod_posobie-k_soglasheniyu_0665.pdf (дата обращения: 11.12.2021).

Сведения об авторах

Быков Сергей Николаевич – студент Пермского национального исследовательского политехнического университета, гр. ЭС-18-16, Пермь, e-mail: bykov-00@mail.ru

Лыкасов Павел Владимирович – студент Пермского национального исследовательского политехнического университета, гр. ЭС-18-16, Пермь, e-mail: lykasov.pavel@mail.ru

Лейзгольд Дмитрий Юрьевич – старший преподаватель кафедры «Микропроцессорные средства автоматизации» Пермского национального исследовательского политехнического университета, Пермь, e-mail: leizgold_du@pstu.ru

Д.А. Ведерников¹, Е.А. Чабанов¹, Е.В. Чабанова²

¹Пермский национальный исследовательский
политехнический университет, Пермь

²Пермский государственный аграрно-технологический
университет имени академика Д.Н. Прянишникова, Пермь

ПЕРСПЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ СВЕТОДИОДНЫХ СВЕТИЛЬНИКОВ ПЕРЕД ЛЮМИНЕСЦЕНТНЫМИ

В статье дано сравнение двух видов светильников. Выполняется проверка норм освещенности при использовании люминесцентных и светодиодных светильников. Рассмотрен вопрос перспективного использования и перехода от люминесцентных светильников к светодиодным. Выполнен сравнительный анализ плюсов и минусов двух типов ламп.

Ключевые слова: люминесцентные светильники, светодиодные светильники, нормы освещенности, энергопотребление светильников.

D.A. Vedernikov¹, E.A. Chabanov¹, E.V. Chabanova²

¹Perm National Research Polytechnic University, Perm

²Perm State Agrarian and Technological University
named after Academician D.N. Pryanishnikova, Perm

THE PROSPECT OF USING LED LAMPS OVER FLUORESCENT

The article discusses a comparison of two types of lamps. Illumination standards are checked when using fluorescent and LED lamps. The issue of perspective use and transition from fluorescent to LED lamps is considered. A comparative analysis of the pros and cons of the two types of lamps has been carried out.

Keywords: Luminescent lamps, LED lamps, lighting standards, energy consumption of lamps.

Сегодня невозможно представить ни одну сферу деятельности общества и производства без осветительных приборов.

Понятие «свет» берет свое начало очень давно. Наши предки преимущественно использовали дневной свет, источником которого является солнце. Позже, с появлением огня, человек понял, что огонь костра, в частности, является не только источником тепла, но и источником света. Вплоть до XIX века, до момента появления электрического источника, население использовало разные источники света, преимущественно это были какие-либо материалы горючего происхождения.

С появлением электричества ситуация стала меняться в лучшую сторону. Первым источником света, работающим от электричества, стала угольно-дуговая лампа. Принцип работы был таким: располагались два угольных электрода, между которыми образовывалась электрическая дуга, которая и давала свечение. Такие источники преимущественно применяли для освещения уличного пространства [1].

Позднее, уже в XX в., разрабатывается новая конструкция ламп, которые получили название «лампы накаливания». В их конструкции присутствовали нити из тугоплавких металлов. Данный тип ламп и на сегодняшний день применяется вследствие своей дешевизны, но перспективы их использования на данный момент нет, поскольку они потребляют большое количество энергии.

Более перспективным вариантом считается использование люминесцентных ламп. Их появление относят еще к середине XIX в., когда начинают проводиться опыты над парами ртути. Люминесцентная лампа, аналог которой можно наблюдать сейчас, появился лишь только в 1927 г. Ученый Эдмунд Джермер ставил перед собой задачу создать источник света, который был бы максимально приближен к естественному свету. На первых порах Джермер и его коллеги использовали ультрафиолетовую лампу, но это не приносило должного результата. Впоследствии же они покрыли ультрафиолетовую лампу люминофором, что позволило получить свет, приближенный к естественному свету [2].

Люминесцентные лампы – лампы газового действия, в основу которого легли электрические процессы, направленные на то, чтобы «взволновать» пары ртути. За счет этого появляется короткая волна ультрафиолетового излучения, которая движется от одной обкладки лампы к другой, за счет этого и появляется видимый свет [3].

Сегодня остро ставится вопрос экономичного использования энергоресурсов. В связи с этим потребовалась разработка таких светильников, которые бы потребляли меньшее количество электроэнергии при максимальной отдаче светового потока. Не стоит также забывать про срок службы светильника, технологию его изготовления и влияние на окружающую среду. Поэтому были разработаны светодиодные светильники.

Начало разработки светодиодных светильников относят еще к началу XX в., когда инженер Г.Д. Раунд случайно увидел свечение, возникшее от точечного контакта вокруг детектора: оранжевого, желтого и зеленого цвета.

Дальнейшие работы ученых привели к тому, что в 1962 г. работнику компании «Дженерал Электрик» Н. Холоньяку удалось создать первые светодиодные светильники [4].

В 2000-х гг. удалось получить «белые» светодиоды, который давали достаточно хорошую степень яркости, что впоследствии позволило начать выпуск их в массовом количестве.

Для доказательства перспективности перехода к светодиодным светильникам от люминесцентных необходимо выполнить их сравнение и рассчитать нормы освещённости [5]. Поэтому целью работы являются проверка и доказательство перспективного использования светодиодных ламп перед люминесцентными лампами. В связи с этим объектами исследования являются люминесцентные и светодиодные лампы.

Для достижения поставленной цели необходимо решить ряд задач:

1) сбор и систематизация информации о люминесцентных светильниках и о светодиодных светильниках;

2) построение 3D-модели помещения объекта с подбором одинаковых параметров светодиодных и люминесцентных светильников;

3) проведение сравнительного анализа получившихся результатов норм освещенности при использовании люминесцентных и светодиодных светильников.

Объект, на котором будет выполняться проверка, – это производное помещение, предварительно предусмотренное под офисное рабочее место с долгим пребыванием людей (рис. 1). Размер помещения $10 \times 5 \times 4$ м. Поскольку помещение офисное, то, как правило, выполняется подвесной потолок типа «Армстронг Байкал» (рис. 2). Такой тип потолка позволяет размещать светильники в зависимости от плит, что дает возможность создавать различные зоны освещенности.

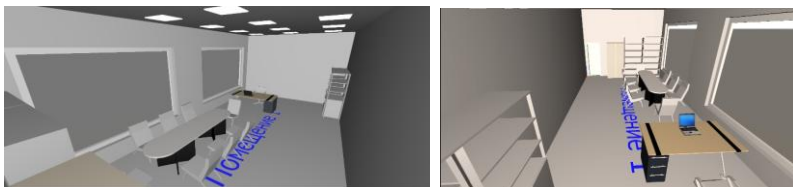


Рис. 1. Офисное помещение, используемое для расчетов норм освещенности (построение модели в DIALux evo)

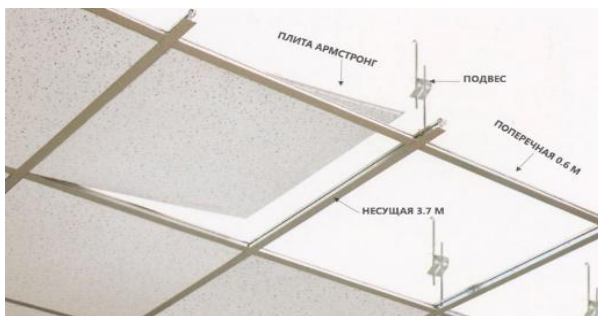


Рис. 2. Подвесной потолок типа «Армстронг»

Для расчета норм освещенности были выбраны светильники компании «Световые технологии». Сравнительная характеристика параметров светильников представлена в табл. 1 [6, 7].

Таблица 1

Сравнительная характеристика параметров применяемых офисных светильников

Марка лампы	OWS/R 418 /595/ IP54/IP54 HF	OWP OPTIMA LED 595 IP54/IP54 EM 4000K
Тип лампы	ЛЛ (Люминесцентная лампа)	LED (Светодиодная лампа)
Мощность светильника	72 Вт	32 Вт
Коэффициент мощности (cos φ)	> 0,96	> 0,95
Переменный/ постоянный ток (AC/DC)	Нет	Да
Напряжение питания	230 В	230 В
Класс защиты от поражения током	I	I
Климатическое исполнение	УХЛ2	УХЛ2
Температурный режим	от -20 до +40 С	от 0 до +40 С
Коэффициент пульсации	< 5%	< 1%
Ударопрочность	IK02/0,2 Дж	IK02/0,2 Дж
Степень защиты (IP)	IP54	IP54

По характеристикам светильники имеют практически одинаковые рабочие параметры и расположены в одном ценовом сегменте. С учетом крепления подвесного потолка монтажная высота светильников составит 3,8 м. Тип светильников – встраиваемый.

Согласно действующим правилам и нормам по своду правил (СП) 52.13330.2016 «Естественное и искусственное освещение», норма освещенности офиса большой площади со свободной планировкой (работа с бумажными носителями и с использованием компьютеров) должна составлять не менее 400 Лк. Также стоит отметить, что рабочая плоскость, согласно СП, должна находиться на высоте 0,8 м от уровня пола.

Для расчета норм освещенности выбран программный комплекс DIALux evo. Данное ПО считается одним из самых первых и известных программ, предназначенных для простого и эффективного моделирования световой среды и расчета систем освещения в интерьере и экстерьере.

При установке цели в 400 Лк количество люминесцентных светильников составило 18 штук. План расположения светильников рассматриваемого объекта выполнен также в программном комплексе DIALux evo и представлен на рис. 3.



Рис. 3. План расположения люминесцентных и светодиодных светильников рассматриваемого офисного помещения

Расчет показал, что при установке данного количества светильников на высоте 3,8 м норма освещенности составила 453 Лк, что удовлетворяет действующему СП. При этом рассчитаем суммарную номинальную потребляемую светильниками мощность по формуле:

$$P_{\Sigma\text{ном}} = P_{\text{ном}} \cdot n, \quad (1)$$

где $P_{\text{ном}}$ – номинальная потребляемая мощность одного светильника, n – количество светильников в помещении.

Мощность, потребляемая одним светильником $P_{\text{ином}}$, выбирается из табл. 1. Рассчитывается номинальная величина потребляемой мощности люминесцентными светильниками:

$$P_{\Sigma\text{ном}} = 72 \cdot 18 = 1296 \text{ Вт, или } P_{\Sigma\text{ном}} = 72 \cdot 18 = 1,296 \text{ кВт.}$$

Выполним проверку светодиодных светильников. Количество светильников остается тем же, что и количество люминесцентных, и устанавливаются они в те же места (план расположения см. рис. 3).

Согласно проведенным расчетам DIALux, норма освещенности светодиодных светильников составила 580 Лк, что также удовлетворяет СП, но уже с превышением. При такой норме сотрудникам будет некомфортно работать.

Рассчитаем потребляемую мощность светодиодными светильниками по формуле (1). Потребляемую мощность одного светильника также берем из табл. 1.

Получаем номинальную величину потребляемой мощности люминесцентными светильниками:

$$P_{\Sigma\text{ном}} = 32 \cdot 18 = 576 \text{ Вт или } P_{\Sigma\text{ном}} = 32 \cdot 18 = 0,576 \text{ кВт.}$$

Как видно из полученных расчетов, величина потребляемой мощности светодиодными светильниками почти в два раза меньше, чем при использовании люминесцентных светильников при одинаковом их количестве. Также стоит отметить, что норма освещенности у светодиодных светильников оказалась выше почти на 100 Лк. Это свидетельствует о том, что появляется возможность убрать ряд светильников.

Выполним проверку при использовании светодиодных светильников в количестве 15 штук. Норма освещенности составила 486 Лк. При такой установке освещенность остается в нормах, требуемых СП. При этом удалось сократить величину потребляемой мощности.

Если выполнить сравнение достоинств и недостатков использования светодиодных и люминесцентных светильников, то преимущество, безусловно, имеют светодиодные светильники [8]. Такой вывод следует из проведенных исследований. Выполним сравнение люминесцентных и светодиодных светильников по ряду критериев. Сравнение выполняем для светильников, чаще всего применяемых для освещения офисных помещений [9]. Сравнение представлено в табл. 2.

Таблица 2

Сравнение люминесцентных и светодиодных светильников

Параметр	Тип светильника	
	Люминесцентный	Светодиодный
Энергопотребление	Низкое энергопотребление 35 Вт/ч	Среднее энергопотребление 72 Вт/ч
Срок службы	Долгий срок службы. Более 50 000 ч	Короткий срок службы. До 10 000 ч
Включение	Мгновенное включение	Длительное включение. Около 1 мин до выхода на заявленные характеристики
Опасность / безопасность	Безопасны. Отсутствует ультрафиолетовое и инфракрасное излучение, мерцание, тяжелые металлы и ртути	Опасны. Содержат ртуть, требуется специальная утилизация
Устойчивость / чувствительность к перепадам напряжения	Устойчивы к перепадам напряжения. Отлично работают в широком диапазоне напряжения (180–260 В)	Чувствительны к перепадам напряжения. Может просто отказать при пониженном напряжении сети

Система питания светодиодных светильников несколько отличается от питания люминесцентных, поскольку люминесцентные светильники имеют свойство появления стробоскопического эффекта с течением долгого срока эксплуатации, поэтому питание необходимо осуществлять от разных линий. Это требует дополнительных затрат на электропроводку. Светодиодные же светильники можно питать последовательно от одной линии, поскольку в них отсутствует стробоскопический эффект. Безусловно, отсутствие такого эффекта положительно влияет на зрение сотрудников.

В настоящее время развиваются тенденции, направленные на сбережение энергоресурсов, поэтому светодиодное освещение является перспективным направлением. Хотя стоимость светодиодных светильников значительно выше, чем люминесцентных, однако окупаемость будет осуществляться за счет меньшего потребления электроэнергии и их длительной эксплуатации.

Стоит также отметить и тот факт, что люминесцентные светильники обладают появлением шума при долгой эксплуатации, диоды же лишены такого недостатка.

Светодиоды имеют возможность разработки различных спектральных характеристик. Помимо этого они также включают разнообразие цветов и оттенков света. За счет таких разработок можно

получать продукцию из светильников и светодиодных лент с различными цветовыми решениями.

На сегодняшний день существует множество производителей, которые занимаются разработкой светодиодов. В связи с этим первоочередной задачей ставится вопрос унификации, что давало бы возможность выпускать модели, которые без проблем могли бы заменять другие типы лампочек как в быту, так и в промышленности.

Таким образом, несмотря на высокую цену качественных лампочек, за 1–1,5 года они окупятся за счет уменьшения платежей за электричество, а также радикально уменьшат эксплуатационные затраты на обслуживание.

В целом же как светодиодное бытовое, так и техническое освещение целиком и полностью соответствует международным требованиям безопасности. Светодиодные элементы не содержат опасных металлов и токсичных веществ, которые испокон веков использовались для производства люминесцентных ламп. Светодиоды оказывают меньшее влияние на зрение человека за счет отсутствия стробоскопического эффекта.

Библиографический список

1. Оболенцев Ю.Б., Гиндин Э.Л. Электрическое освещение общепромышленных помещений. – М.: Энергоатомиздат, 1990. – 111 с.

2. Люминесцентная лампа [Электронный ресурс]. – URL: https://ru.wikipedia.org/wiki/Люминесцентная_лампа (дата обращения: 15.02.2021).

3. Люминесцентная лампа // Большая советская энциклопедия: [в 30 т.] / гл. ред. А.М. Прохоров. – 3-е изд. – М.: Советская энциклопедия, 1969–1978.

4. Светодиодные лампы. История и современность [Электронный ресурс]. – URL: <https://shop220.ru/articles/352.htm> (дата обращения: 15.03.2021).

5. Перспективы использования светодиодных ламп [Электронный ресурс]. – URL: <http://comintour.net/kommercheskaya/item/106-perspektivy-ispolzovaniya-svetodio-dnykh-lamp> (дата обращения: 10.03.2021).

6. Световые технологии. Модель OWS/R 418 /595/ IP54/IP54 HF [Электронный ресурс]. – URL: <https://www.ltcompany.com/ru/products/types/cleanroom-lighting/forcleanro-oms/ows-r/ows-r-418-595-ip54-ip54-hf/> (дата обращения: 25.03.2021).

7. Световые технологии. Модель OWP OPTIMA LED 595 IP54/IP54 EM 4000K [Электронный ресурс]. – URL: <https://www.ltcompany.com/ru/products/types/cleanroom-lighting/for-clean-rooms/owp-optima-led/owp-optima-led-595-ip54-ip54-em-4000k/> (дата обращения: 25.03.2021).

8. Светодиоды – перспективное направление развития технологий освещения [Электронный ресурс]. – URL: http://www.energsovet.ru/bul_stat.php?idd=75 (дата обращения: 03.02.2021).

9. Таблица сравнения светодиодных ламп и энергосберегающих ламп [Электронный ресурс]. – URL: <https://admbaraba.ru/gaznoe/tablicza-sravneniya-svetodiodnyh-lamp-i-energ-osberegaya-yushhih-lamp-kak-vybrat-svetodiodnuyu-lampu-kakie-led-lampy-luchshe.html> (дата обращения: 16.03.2021).

Сведения об авторе

Ведерников Дмитрий Андреевич – магистрант кафедры «Электротехника и электромеханика» Пермского национального исследовательского политехнического университета, гр. ЭМ-20-1м, инженер-электрик ООО "Научный проектно-технологический институт «ОПТ-ЭКС»", Пермь, e-mail: vedernikov.d.a98@mail.ru

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

Чабанова Евгения Владимировна – кандидат педагогических наук, доцент кафедры «Иностранные языки» Пермского государственного аграрно-технологического университета им. академика Д.Н. Прянишникова, Пермь, e-mail: jentosina@yandex.ru

К.Г. Зайцев, А.С. Полиехов, Е.А. Чабанов

Пермский национальный исследовательский
политехнический университет, Пермь

ИСКУССТВЕННЫЕ МЫШЦЫ

Статья посвящена искусственным мышцам, которые позволяют улучшить жизнь людей, потерявших конечности из-за несчастных случаев на производстве. Искусственные мышцы – это особый материал, который может сокращаться и расслабляться подобно настоящим мышцам, но при этом они являются искусственными. Материал, из которого производят искусственные мышцы, может отлично подойти для изготовления функциональных протезов, а может быть использован и для производства человекоподобных роботов.

Ключевые слова: искусственные мышцы, ферромагнетик, силикон, электропроводящий материал, эластичный материал.

K.G. Zayzew, A.S. Poliekhov, E.A. Chabanov

Perm National Research Polytechnic University, Perm

ARTIFICIAL MUSCLES

The article is devoted to artificial muscles that will improve the life of people who have lost limbs due to industrial accidents. Artificial muscles are a special material that can contract and relax like real muscles, but they are artificial. The material from which artificial muscles are made can be excellent for the manufacture of functional prostheses, and can also be used for the manufacture of humanoid robots.

Keywords: artificial muscle, ferromagnet, silicone, electrically conductive material, elastic material.

В настоящее время наиболее востребованными для бионики и робототехники являются искусственные мышцы. Это обусловлено отсутствием ряда недостатков, присущих электродвигателям, таких как: низкая энергоэффективность, ограниченность в движении, высокие энергопотери и т.д. Данные недостатки делают классические электромоторы малопригодными для массового производства искусственных конечностей, экзоскелетов, роботов, манипуляторов, поскольку в этих механизмах, построенных по образу и подобию человеческого тела, для электропривода требуется определённая гибкость, да и эквивалент

электромоторов для того количества мышц, задействованных при простом поднимании тяжести рукой, был бы запредельный.

Данная тема весьма актуальна, так как у современных электромоторов существуют недостатки, которые отсутствуют у искусственных мышц. В связи с этим было принято решение найти наиболее оптимальные варианты исполнения этих мышц.

Анализ и систематизация найденной информации позволили выяснить, что на данный момент не существует искусственных мышц, способных целиком и полностью воспроизвести настоящие мышцы. Однако в настоящее время уже существует несколько прототипов, которые можно разделить на 3 группы по их типу активаторов: магнитное поле, электрический ток и теплопередача.

Принцип действия искусственных мышц первой группы основан на сокращении объёма ферромагнитной жидкости в заданном направлении, находящейся в некоторой полости (ограниченном объёме), под действием магнита или электромагнита, в качестве которого выступает катушка индуктивности, подключенная к источнику постоянного напряжения. Использование электромагнита позволяет регулировать в достаточно широком диапазоне степень сжатия ферромагнитной жидкости, а следовательно, получать большие пространственное перемещение и усилие. Мышцы этой группы достаточно подробно описаны в [1–3] и представлены на рис. 1 на основе управляемого магнитоупругого материала [1].

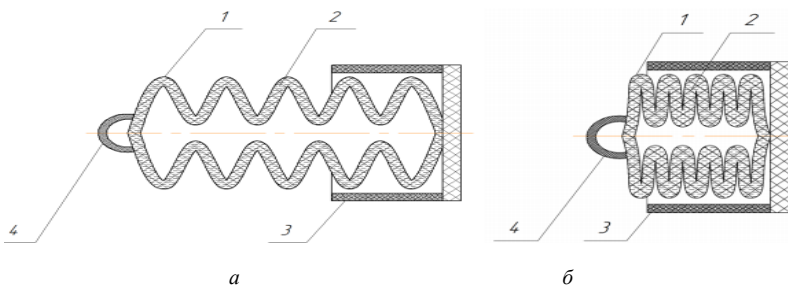


Рис. 1. Искусственная мышца на основе управляемого магнитоупругого материала в расслабленном (а) и сокращенном (б) состояниях: 1 – подвижная гофрированная трубка из эластичного материала двухкомпонентного силикона; 2 – магнитовосприимчивый материал; 3 – катушка индуктивности с источником питания; 4 – точка крепления груза

На рис. 2 представлены искусственные мышцы на основе электромеханических систем, использующих полимерные гидрогели для микроразмерных исполнительных устройств [2].

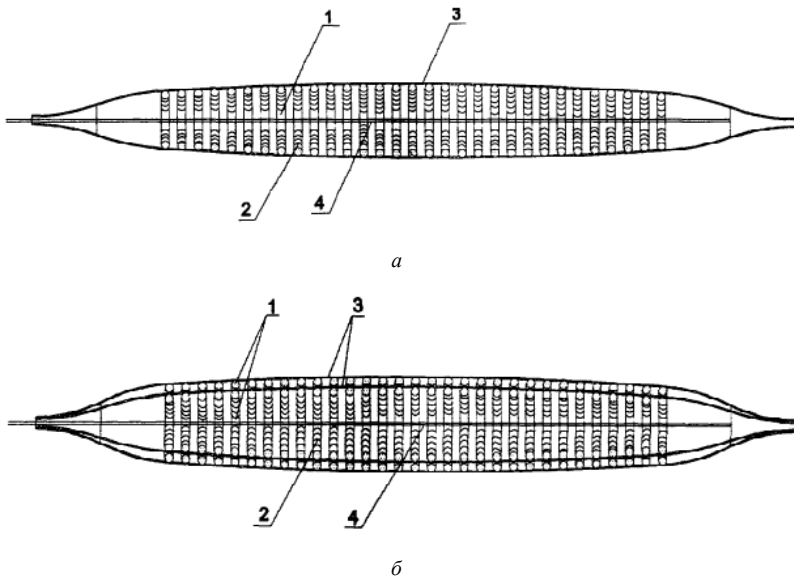


Рис. 2. Искусственные мышцы на основе полимерного гидрогеля в расслабленном (*а*) и сокращенном (*б*) состояниях: 1 – камеры с эластичными стенками, заполненные ферромагнетиком; 2 – электропроводные обмотки; 3 – полная эластичная обмотка; 4 – электрический кабель

Принцип действия искусственных мышц второй группы основан на применении материала с «памятью формы», который деформируется при подаче на него электрического тока. Согласно источникам [4, 5] в качестве таких материалов используют полимерные волокна полиэтилена или нейлона и интерметалида (сплава, который под действием электрического тока способен возвращать исходную форму после деформации), обладающие хорошей степенью сжатия в 20–35 % и высокой скоростью как отклика, так и восстановления после деформации. В соответствии с [6] существует возможность использовать гидрогель или полиэлектродный гель, деформация которых слишком мала и длительна [7–9].

Самым необычным принципом действия обладает третья группа искусственных мышц, в основе которых лежит тепловое расширение веществ. В соответствии с источниками [10, 11] эластомер на основе этилового спирта, находящийся в силиконовой матрице, может осуществлять переход из жидкого состояния к газообразному под действием электрического тока (рис. 3, 4).

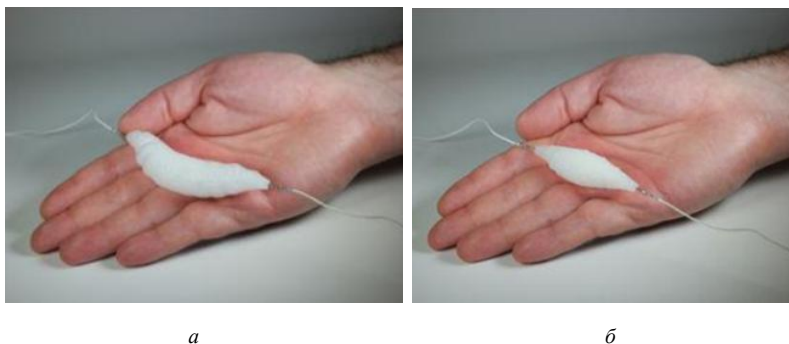


Рис. 3. Мягкие искусственные мышцы: эластомер на основе этилового спирта в расслабленном (*а*) и сокращенном (*б*) состояниях

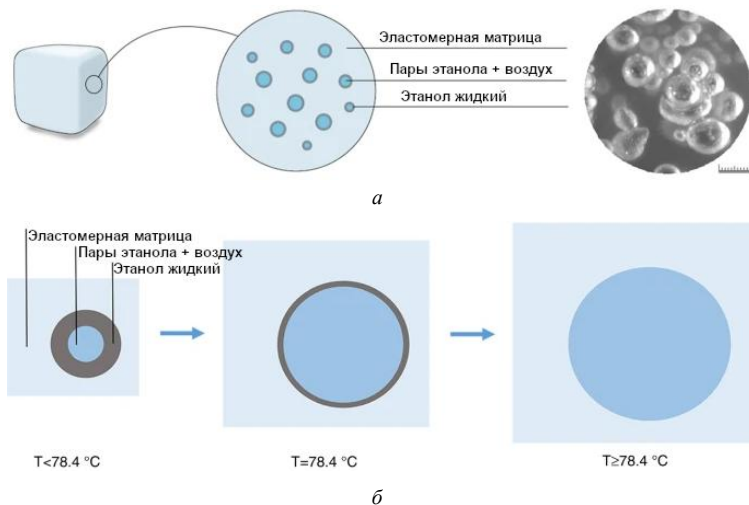


Рис. 4. Мягкие искусственные мышцы: *а* – структура эластомера; *б* – модель эластомера, демонстрирующая изменение его размера; *в* – эластомер с демонстрацией тепловых процессов

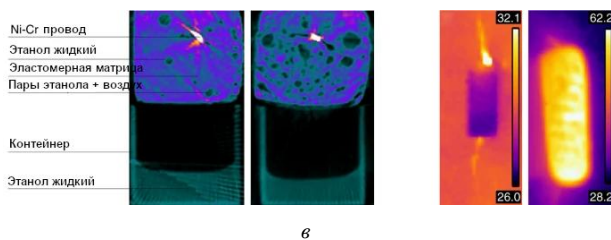


Рис. 4. Окончание

Такой переход способствует увеличению объёма мышцы, хотя эффективность ее, как оказалось, была сравнительно низкой (0,2 %). Схожим образом могут быть использованы нити из наноматериалов [12] (рис. 5).

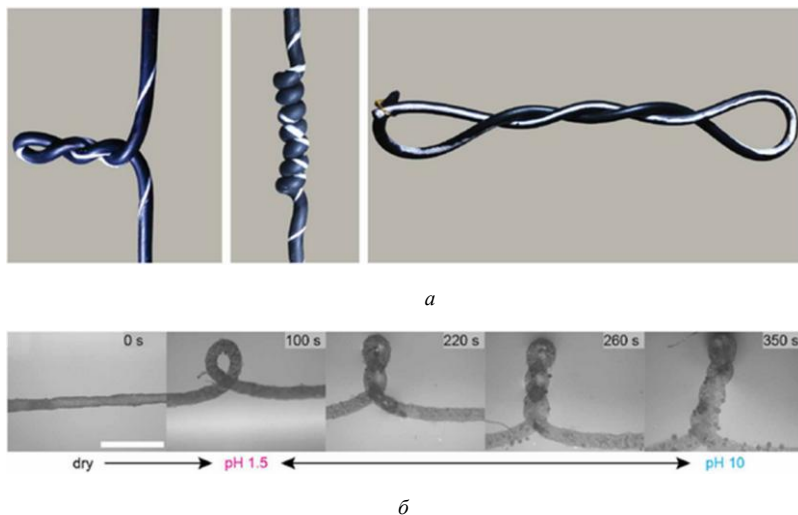


Рис. 5. Искусственная мышца на основе нитей из наноматериалов:
a – различные способы скручивания нити; *б* – процесс скручивания нити

Заключение. Искусственные мышцы, несмотря сегодня на их неконкурентоспособность по сравнению с электромоторами, очень перспективное изобретение, у которого имеется большой потенциал в сфере протезирования, робототехники, создания экзоскелетов и манипуляторов для промышленного и бытового использования. Из рас-

смотренных вариантов наиболее целесообразными и перспективными можно считать мышцы основанные на ферромагнетиках, так как в отличие от других видов мышц этот тип меньше всех подвержен воздействию внешних факторов, обеспечивает достаточное перемещение и усилие, а также быстро восстанавливается после активации.

Библиографический список

1. Буравцов А.С., Григорьев Б.В. Разработка технологии создания магнитоуправляемого упругого материала // *Sciences of Europe*. – 2019. – № 43–1.

2. Искусственная мышца (варианты): пат: RU2372056C1 / В.М. Кузьминых, И.Ф. Юрин.

3. Искусственная мышца: пат. RU2598763C2 / А.И. Алексеев.

4. Искусственная мышца: пат. RU2563815C1 / Д.А. Журавлёв.

5. Shape memory alloy fibers having rapid twitch response: pat. US5092901A / I. Hunter, S.R. Lafontaine.

6. Электромеханические системы на основе полимерных гидрогелей для микроразмерных исполнительных устройств / Г.К. Ельяшев, И.С. Курындин, И.Ю. Дмитриев, П.В. Власов, В.П. Иванов // *Научно-технический вестник информационных технологий, механики и оптики*. – 2018. – № 4.

7. Исследование механизма электромеханических преобразований в полиэлектrolитных гелях – на пути к созданию искусственных мышц / Е.А. Литвинова, Е.А. Толстовская, А.П. Сафронов, Т.Ф. Шкляр // *МНИЖ*. – 2013. – № 6–1.

8. Булатов А.П. Искусственные мышцы в бионике и робототехнике // *Молодёжь и современные информационные технологии*: материалы XIV Междунар. науч.-практ. конф. студ. аспирант. и молодых учёных, г. Томск, 7–11 ноября 2016 г.: в 2 т. – Томск : Изд-во ТПУ, 2016. – Т. 1. – С. 280–282.

9. Беляев А.Ю., Щукин Т.Н., ТРИЗ – Анализ направлений проектирования искусственных мускулов // *Молодежный научно-технический вестник*. – Сентябрь 2015. – № 9.

10. Miriyev, A., Stack, K. & Lipson, H. Soft material for soft actuators // *Nat Commun.* – 2017. – 8. – 596. – URL. <https://doi.org/10.1038/s41467-017-00685-3>

11. Artificial muscles: патю US20100268352A1 / Dennis Majoe.

12. Coiled and non-coiled twisted nanofiber yarn and polymer fiber torsional and tensile actuators: pat. WO2014022667A2 / N. Li, C.S. Haines, M.D. Lima, A.M. Jung De, S. Fang, J. Oh, M.E. Kozlov, F. Goktepe, O. Goktepe, D. Suh, R.H. Baughman (US).

Сведения об авторах

Зайцев Кирилл Германович – студент Пермского национально-исследовательского политехнического университета, гр. ЭЭ-21-46, Пермь, e-mail: zayzewkirill03@gmail.com

Полиехов Андрей Сергеевич – студент Пермского национально-исследовательского политехнического университета, гр. ЭЭ-21-46, Пермь, e-mail: poliekhov.andrey@mail.ru

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

К.А. Конев, А.О. Фурина, Е.А. Чабанов

Пермский национальный исследовательский
политехнический университет, Пермь

ЗАМЕНА ЭЛЕКТРИЧЕСКОГО ДВИГАТЕЛЯ В ОТБОЙНОМ МОЛОТКЕ

Оборудование, создаваемое по новым технологиям, постоянно появляется, эффективно и качественно заменяет старые устройства и агрегаты. В городах с большой и малой численностью населения регулярно ведется строительство жилых домов, развлекательных центров, предприятий и т.д. В связи с этим возникает необходимость улучшения и автоматизации технического оснащения. В статье исследуется возможность использования электродвигателя нетрадиционной конструкции в строительной области. Обзорный анализ показывает, что при использовании нового двигателя в электроинструменте потери энергии будут уменьшаться, срок годности увеличиваться, эффективность использования инструмента вырастет.

Ключевые слова: цилиндрический линейный двигатель, отбойный молоток, электрический двигатель, электроинструмент.

K.A. Konev, A.O. Furina, E.A. Chabanov

Perm National Research Polytechnic University, Perm

REPLACING THE ELECTRIC MOTOR IN THE JACKHAMMER

The equipment created using new technologies, constantly appearing, effectively and efficiently replaces old devices and units. In cities with large and small populations, the construction of residential buildings, entertainment centers, enterprises, etc. is carried out on a regular basis. In connection with this, it becomes necessary to improve and automate technical equipment. The article examines the possibility of using an electric motor of an unconventional design in the construction field. An overview analysis shows that when using a new motor in a power tool, energy loss will decrease, shelf life will increase, and tool use efficiency will increase.

Keywords: cylindrical linear motor, jackhammer, engine replacement.

В настоящее время большинство механизмов совершают свою работу, используя при этом электрическую энергию. При передвижении какого-либо предмета или устройства применяются двигатели, а именно электрические двигатели вращательного движения. Они применяются практически во всех областях деятельности человека: в быту, в автомобилях, в промышленности, в строительстве и т.д. Данные элек-

тродвигатели используются даже там, где можно намного проще, дешевле и лучше применять электрические машины других типов и конструкций, например, цилиндрические линейные двигатели (ЦЛД). Существуют различные типы подобных электрических машин, а именно:

- асинхронные линейные двигатели;
- синхронные линейные двигатели;
- вентильные линейные двигатели.

Цилиндрический асинхронный линейный двигатель (ЦЛАД) может быть получен при сворачивании линейного двигателя в цилиндр (рис. 1, *а*, *б*). Катушки в виде колец образуют обмотку индуктора. Шайбы, изготовленные из стали, в которых сделаны надрезы, стыкуются и образуют магнитопровод индуктора (рис. 2, *а*, *б*). Также прорезы уменьшают токи Фуко и соответственно потери в статоре. Листовая электротехническая сталь, из которой изготавливается магнитопровод, как и в других электродвигателях, используется для того, чтобы уменьшить потери.

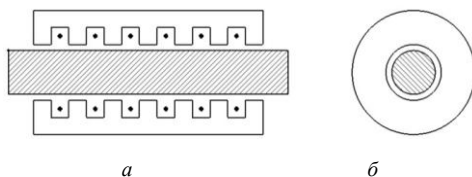


Рис. 1. ЦЛАД: *а* – продольный разрез; *б* – вид сбоку

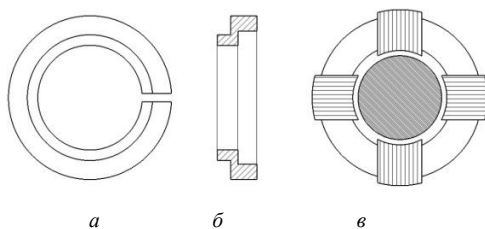


Рис. 2. Элементы конструкции ЦЛАД: *а*, *б* – шайба; *в* – магнитопровод двигателя

В состав цилиндрического линейного вентильного двигателя (ЦЛВД) входят неподвижный цилиндрический индуктор и шток с постоянными магнитами. На рис. 3 представлено продольное сечение индуктора и вторичного элемента ЦЛВД. Цилиндрическая обмотка индуктора двигателя размещается в пазах.

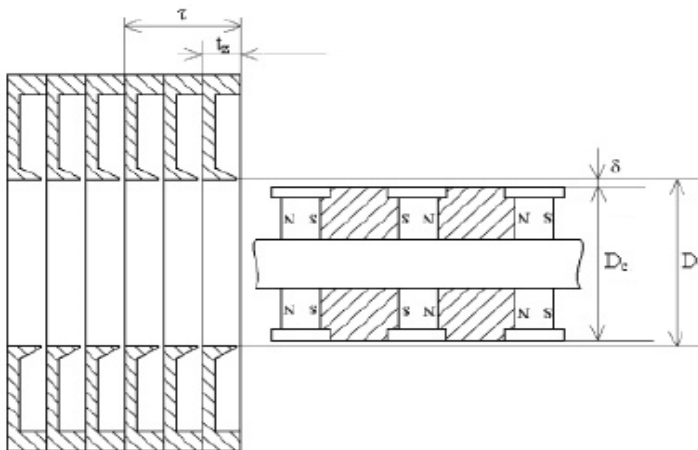


Рис. 3. Продольный разрез индуктора и ротора ЦЛВД

Катушки соединяются последовательно по всей длине индуктора и образуют трехфазную обмотку, которая получает электроэнергию от преобразователя частоты (ПЧ). Обмотка цилиндрического индуктора создает бегущее поступательно магнитное поле, скорость движения которого и направление изменяются с помощью ПЧ. Переключение обмоток статора производится в зависимости от положения магнитов ротора. Ротор (вторичный элемент) имеет симметричное положение, т.е. горизонтальная ось проходит по середине штока. Концы штока вторичного элемента выступают за пределы цилиндрического индуктора обеих сторон и закрепляются в подшипниках скольжения.

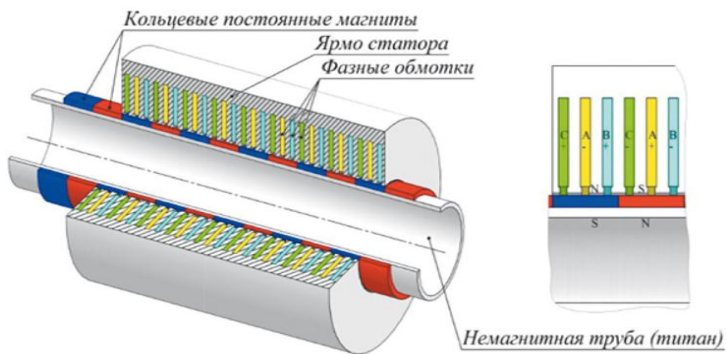


Рис. 4. Разрез ЦЛСД

Цилиндрический линейный синхронный двигатель (ЦЛСД) состоит из подвижной части – якоря и магнитной дороги – статора. Редкоземельные магниты чередующейся полярности, которые наклеены на стальную пластину, образуют статор. Якорь – зубчатый магнитопровод, в пазах которого находится трехфазная обмотка, залитая компаундом (рис. 4).

ЦЛСД развивают равномерное линейное усилие за счёт взаимодействия магнитного поля якоря с постоянными магнитами статора. Отличительная особенность ЦЛСД по сравнению с другими линейными двигателями заключается в отсутствии механической передачи. Как отмечалось ранее, двигатели вращательного движения используются повсеместно, даже там, где было бы целесообразнее применять электрические машины других конструкций. Поэтому рассмотрим возможность замены коллекторного двигателя, применяемого в бытовом электроинструменте (например, отбойном молотке или перфораторе), на ЦЛД. Отбойный молоток (перфоратор) – механическое устройство, предназначенное для демонтажа железобетонных или каменных конструкций (стен) или их раскалывания (рис. 5, 6).

Одной из основных частей перфоратора является электродвигатель, который приводит в движение механизмы перфоратора. Качающийся подшипник приводит в действие поршень, создавая ударное усилие, а патрон обеспечивает зажим насадок. В бытовом электроинструменте обычно используется коллекторный двигатель, обмотки статора которого создают постоянное электромагнитное поле, а внутри вращается ротор. На роторе размещается несколько обмоток, выводы которых подключены к коллекторным пластинам якоря. Питание на обмотки якоря подается через медно-графитовые щетки. Переключением обмоток якоря создается поле скольжения, за счет которого и происходит вращение ротора.

На рис. 5 и 6 видно, что для создания возвратно-поступательного движения с помощью коллекторного двигателя используют множество шестеренок, которые в ходе работы изнашиваются и приходят в негодность, а следовательно, они подлежат замене. Кроме того, коллекторный двигатель требует обслуживания: замена щеток, чистка поверхностей от щеточной (графитовой) пыли. Также механические передачи от электродвигателя к ударному механизму сопровождаются потерями энергии, а следовательно, уменьшается КПД всего устройства.



Рис. 5. Перфоратор с вертикальным расположением двигателя в разрезе

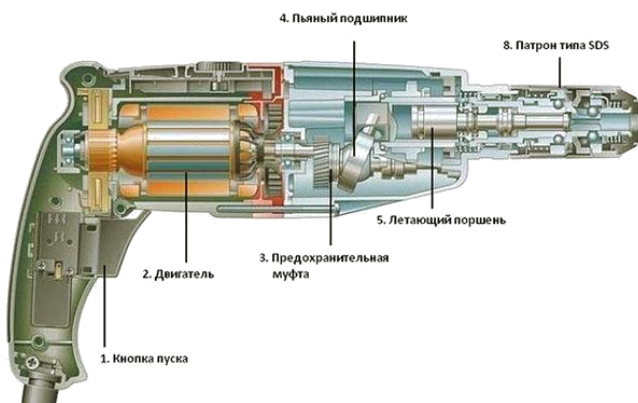


Рис. 6. Перфоратор с горизонтальным расположением двигателя в разрезе

Для решения изложенных выше проблем современного электроинструмента предлагается рассмотреть возможность применения в подобных устройствах линейных двигателей. Таким образом, возвратно-поступательное движение будет создаваться таким типом двигателей без использования различных вспомогательных устройств и приспособлений (шестеренок, подшипников), способствующих преобразованию вращательного движения коллекторного электродвигателя в поступательное (возвратно-поступательное).

На рис. 7 представлена модель отбойного молотка (перфоратора) с линейным двигателем. Вторичный элемент ЦЛД, совершая возвратно-поступательные движения, будет передавать ударные усилия бойку. К ударнику будет неподвижно крепиться патрон с установленным в нем инструментом (пика, лом).

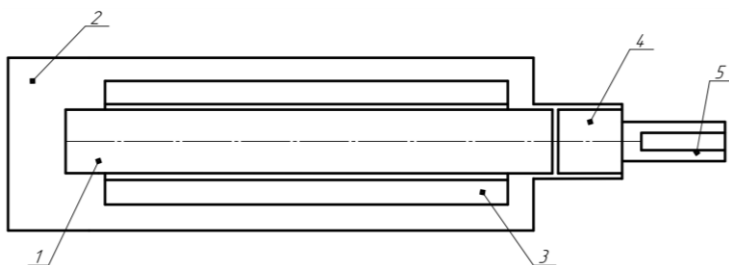


Рис. 7. Продольное сечение корпуса отбойного молотка: 1 – слайдер, 2 – корпус отбойного молотка, 3 – индуктор ЦЛД, 4 – ударник, боек, 5 – атрон

Заклучение. Использование в отбойном молотке ЦЛД позволит повысить КПД устройства в целом за счет уменьшения потерь энергии на механических передачах по причине их отсутствия, поскольку электродвигатель будет сразу создавать возвратно-поступательное движение, передавая при этом ударные усилия от двигателя до бойка (ударника), а от него через патрон к рабочему инструменту. По указанной причине обслуживание устройства также станет менее затратным (в том числе финансово), при этом надежность работы электроинструмента вырастет. В процессе производства данного агрегата потребность в некоторых материалах уменьшится или полностью исчезнет.

Таким образом, ЦЛД является целесообразной и обоснованной заменой коллекторному двигателю вращательного движения при производстве электроинструмента (в частности, отбойного молотка).

Библиографический список

1. Шулаков Н.В. Электрические машины: конспект лекций. – Пермь: Изд-во Перм. гос. техн. ун-та, 2008. – 325 с.
2. Ключников А.Т., Коротаев А.Д., Шутемов С.В. Моделирование цилиндрического линейного асинхронного двигателя // Электротехника. – 2013. – № 11. – С. 14–17.
3. Цилиндрический линейный вентильный двигатель для добычи нефти бесштанговым методом / К.А. Конев, А.О. Фурина, А.Д. Коротаев, Е.А. Чабанов // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2021. – № 39. – С. 150–168.

4. Коротаев А.Д., Шулаков Н.В., Шутемов С.В. Экспериментальные исследования цилиндрического линейного вентильного электродвигателя // Актуальные проблемы энергосберегающих электротехнологий: материалы XIV Междунар. науч.-техн. конф.; 17–20 марта 2014 г. – Екатеринбург, 2014. – С. 198–200.

Сведения об авторах

Конев Константин Андреевич – магистрант Пермского национального исследовательского политехнического университета, гр. ЭМ-21-1м, Пермь, e-mail: looking_99@mail.ru

Фурина Александра Олеговна – студентка Пермского национального исследовательского политехнического университета, гр.ЭС-19-1б, Пермь, e-mail: alexandra.furina@yandex.ru

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

М.А. Константинов, Е.А. Чабанов

Пермский национальный исследовательский
политехнический университет, Пермь

**УЛУЧШЕНИЕ РАБОТЫ И ПРОИЗВОДИТЕЛЬНОСТИ
СТАНКА ПРИ СОВМЕЩЕНИИ ЧПУ ФРЕЗЕРА,
3D-ПРИНТЕРА И ЛАЗЕРНОГО ГРАВЕРА**

В статье рассматривается совмещение трех разных приборов в одном станке для сокращения объемов затрачиваемого сырья, увеличения скорости выполнения работы и улучшения качества изготавливаемой на станке продукции. Предлагается совмещать фрезер с ЧПУ, 3D-принтер и лазерный гравер (резак). В статье исследуется возможность создания универсального станка, обладающего преимуществами всех перечисленных устройств.

Ключевые слова: 3D-принтер, станок с ЧПУ управлением, лазерный резак, автоматизация обработки деталей.

M.A. Konstantinov, E.A. Chabanov

Perm National Research Polytechnic University, Perm

**IMPROVING THE OPERATION AND PRODUCTIVITY
OF THE MACHINE WHEN COMBINING A CNC ROUTER,
3D PRINTER AND LASER ENGRAVER**

The article discusses the combination of 3 different devices in one machine to reduce the amount of raw materials consumed, increase the speed of work and improve the quality of products manufactured on the machine. It is proposed to combine a CNC router, a 3D printer and a laser engraver (cutter). The article examines the possibility of creating a universal machine that has the advantages of all the listed devices.

Keywords: 3D printer, CNC machine, laser cutter, automation of parts processing.

В настоящее время активно используется изготовление деталей в различных сферах деятельности человека (электроника, аэрокосмическая промышленность, медицина, автомобилестроение, мебельное производство и т.д.) с применением автоматизированных станочных комплексов. Применение того или иного станка для получения готового изделия зависит от операции, которую необходимо выполнить для получения необходимого результата. Каждый из

применяемых станков обладает собственными преимуществами и недостатками, которые не позволяют использовать одно и то же устройство для выполнения всего спектра необходимых операций. Следовательно, возникает необходимость создания универсального устройства, представляющего собой совмещение нескольких станков в одном корпусе.

Анализ текущего состояния поставленной проблемы подтверждает необходимость подобных комбинаций. Наиболее перспективными являются комбинации, состоящие из следующих устройств:

- 3D-принтер – станок с числовым программным управлением, добавляющий порции материала к заготовке [1];

- станок с ЧПУ управлением позволяет обрабатывать детали в автоматическом режиме, т.е. практически без какого-либо участия человека. Процесс механической обработки осуществляется под микропроцессорным управлением в соответствии с записанной заблаговременно программой [2];

- лазерный резак – это устройство с компьютерным управлением, которое использует лазерный луч для точной резки или гравировки материала [3].

Каждый из описанных станков обладает рядом преимуществ и недостатков. Однако огромный интерес представляет устройство, включающее в себя все перечисленные станки: фрезер с ЧПУ, 3D-принтер и лазерный гравер/резак. Для оценки свойств и характеристик нового устройства следует произвести сравнительный анализ его составных частей.

3D-принтер и фрезер с ЧПУ:

Преимущества 3D-печати металлом:

- сокращение количества пространственных перемещений инструмента, обрабатывающего деталь;

- эффективность производства значительно повышается;

- функциональные возможности становятся шире;

- большая свобода проектирования как по форме, так и по содержанию обрабатываемых деталей;

- высокая гибкость;

- значительная повторяемость, в том числе при крупносерийном производстве;

- высокая точность обработки поверхностей.

Сравнение 3D-печати с ЧПУ-обработкой выявляет несколько фундаментальных отличий. Станки с ЧПУ обрабатывают деталь путем удаления материала из первоначальной заготовки. Поэтому при высокой стоимости материала его увеличенный расход является серьезным недостатком механической обработки.

Станок с ЧПУ обрабатывает деталь резцом, поэтому в случае невозможности получения необходимой формы поверхности возникает потребность замены оснастки, что влечет за собой дополнительные материальные и временные затраты. При обработке таким способом деталь должна крепиться неподвижно к жесткому основанию, а резец должен иметь несколько степеней свободы. В некоторых случаях даже пятикоординатному станку становится затруднительно обрабатывать некоторые сложные поверхности. Цилиндрическая форма резцов затрудняет получение идеальных углов и кромок, особенно на внутренних поверхностях. Этого недостатка полностью лишена 3D-печать, с помощью которой можно изготавливать детали сложной геометрии. С целью экономии материала 3D-печать позволяет организовывать и обрабатывать в деталях внутренние каналы и полости любой конфигурации. Такой подход обеспечивает сохранение прочности изделия при уменьшении веса и расходуемого материала, что значительно расширяет возможный перечень областей их применения. При этом повышаются сложность и ответственность программного обеспечения, но исчезает необходимость использования разнообразной оснастки. Еще одним фактором, повышающим обоснованность применения 3D-печати, является крайне низкий уровень погрешности – до $\pm 0,005$ мм

При необходимости обеспечения более жестких допусков обработки деталей существует возможность совмещения двух поэтапных процессов, а именно: сначала деталь формируется с небольшим запасом по размерам на устройстве 3D-печати, а затем она обрабатывается на станке с ЧПУ управлением с целью получения конечного результата заданной точности.

Первые 3D-принтеры зачастую были не способны обеспечить надлежащие механические характеристики при обработке твердых материалов. В настоящее время подобные устройства благодаря современным технологиям могут гарантировать требуемую механическую прочность, коррозионную стойкость, теплоизоляционные свойства при обработке практически любых материалов. Использование

при этом станков с ЧПУ управлением позволяет дорабатывать напечатанные изделия до необходимых размеров [4].

Результаты сравнительного анализа работы лазера с фрезером представлены в таблице.

Сравнительный анализа работы лазера с фрезером

Перечень обрабатываемых материалов	Фрезер обладает большим спектром обрабатываемых материалов, а также толщина прорезаемых деталей значительно больше. Лазер (40 Вт) режет в основном неметаллические материалы, и толщина деталей незначительная
Скорость резки материалов	Скорость напрямую зависит от толщины материала. Совсем тонкие материалы быстрее режет лазер, средней толщины – примерно одинаково, толстые – фрезер. Более того, лазер многие толстые материалы вообще не сможет разрезать
Цена резки материалов	Этот критерий больше зависит от хозяина оборудования и политики компании. Однако в общем случае резка дешевле на фрезе
Сложность задачи по резке материала	Лазер имеет огромные преимущества по сравнению с резаком. Ему совсем неважно, насколько сложен рез, внутренние углы или внешние, он не нуждается в месте для захода фрезы. Лазер достаточно хорошо справляется с мелкими узорами. Однако, если изделие крупное, то и фрезер всё вырежет без труда
2D- и 3D-обработка	Фрезер имеет преимущества. Лазер сможет выполнить гравировку только на небольшую глубину. Фрезер же имеет практически безграничные возможности, особенно при достаточно большом и разнообразном наборе различных фрез
Качество реза	Каждый из способов имеет свои преимущества. Если требуется прозрачный край, то следует использовать лазер. Если нужен бесцветный рез, то фрезер. Также необходимо учитывать, что лазер оставляет нагар, а фрезер – стружку, заусенцы [5]

Представленный анализ текущего состояния поставленной проблемы подтверждает целесообразность совмещения 3D-принтера, лазерного гравера и резака с ЧПУ управлением.

В настоящее время на рынке имеется единственный представитель подобного оборудования, который по своим характеристикам близок к поставленной цели, а именно объединяет в себе сразу три аппарата – 3D-принтер, лазерный гравер и резак с ЧПУ, это модульный гибридный станок Sparmaker (рисунок), обладающий следующими характеристиками:

– 3D-принтер обрабатывает предметы размером 125×125×125 мм, обеспечивая достаточно высокие разрешение и скорость движения печатной головки;

– лазер (мощностью 500 мВт и длиной волны 405 нм) применяется на разнообразном материале;

– резак с ЧПУ работает также с различным материалом (скорость вращения шпинделя от 2000 до 7000 об/мин).

Управление станком Snapmaker осуществляется через специализированное программное обеспечение Snap3D. Также принтер совместим с другим ПО для 3D-печати – Cura, Simplify 3D и Slic3r [6, 7].



Рис. Модульный гибридный станок Snapmaker

Заключение. Совмещение 3D-принтера, лазерного гравера и резака с ЧПУ управлением позволяет получить деталь с меньшей затратой материала при помощи 3D-принтера (экономично). Слаженная работа всех компонентов позволяет получить очень высокую точность и качество изделия, улучшая тем самым производительность. Однако стоимость подобного оборудования пока остается достаточно высокой.

Библиографический список

1. 3D-принтер [Электронный ресурс]. – URL: <https://ru.wikipedia.org/wiki/3D-принтер#:~:text=3D-принтер%20-%20станок%20с%20числовым,относится%20к%20технологиям%20быстрого%20прототипирования> (дата обращения: 24.12.2021).

2. Сферы применения станков с ЧПУ [Электронный ресурс]. – URL: <https://vektor.us/blog/oblast-primeneniya-stankov-s-chpu.html#oblast-ispolzovaniya> (дата обращения: 24.12.2021).

3. Лазерная резка и гравировка – подробное руководство для начинающих [Электронный ресурс]. – URL: <https://www.foroffice.ru/articles/173119/> (дата обращения: 24.12.2021).

4. 3D-принтер vs станок с ЧПУ: конкуренты или союзники? [Электронный ресурс]. – URL: <https://blog.iqb.ru/metal-3d-printing-vs-cnc> (дата обращения: 24.12.2021).

5. Лазер VS Фрезер. Фрезерная и лазерная резка и обработка. Сравнение [Электронный ресурс]. – URL: <https://всягравировка.рф/lazer-vs-frezer-sravnenie-vozmozhnostej.html> (дата обращения: 24.12.2021).

6. SNAPMAKER – 3D принтер, лазерный гравер и фрезер с ЧПУ в одном станке» [Электронный ресурс]. – URL: <https://www.stankoff.ru/blog/post/146> (дата обращения: 24.12.2021).

Сведения об авторах

Константинов Михаил Андреевич – студент Пермского национального исследовательского политехнического университета, гр. ЭЭ-21-4б, Пермь, e-mail: darinakramer.2001@yandex.ru

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

Секция 4

**ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ И СЕТИ.
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

Ю.М. Букирева

Пермский национальный исследовательский
политехнический университет, Пермь

СТРАТЕГИЯ ДОСТУПА К КОРПОРАТИВНЫМ СЕТЯМ С ПРИМЕНЕНИЕМ МОДЕЛИ НУЛЕВОГО ДОВЕРИЯ

В статье исследуется возможность получения доступа к корпоративным сетям с помощью внедрения в систему модели нулевого доверия (ZTNA). В отличие от виртуальных частных сетей (VPN), которые имеют целый ряд ограничений, включая масштабируемость и простое отсутствие информационной безопасности, ZTNA включает в себя создание концепций защиты на основе полного отсутствия доверия ко всем пользователям, подключающимся к корпоративной сети. Пользователи и устройства должны проходить аутентификацию каждый раз, когда они подключаются к ресурсам.

Ключевые слова: модель нулевого доверия, авторизация, Интернет вещей, политика доступа на основе атрибутов, облачный сервис.

I.M. Bukireva

Perm National Research Polytechnic University, Perm

STRATEGY OF ACCESS TO CORPORATE NETWORKS USING THE ZERO TRUST MODEL

This article explores the possibility of gaining access to corporate networks by implementing a zero-trust model (ZTNA) into the system. Unlike virtual private networks (VPNs), which have a number of limitations, including scalability and a simple lack of information security, ZTNA involves the creation of security concepts based on a complete lack of trust in all users connecting to the corporate network. Users and devices must authenticate each time they connect to resources.

Keywords: zero trust model, authorization, Internet of Things, attribute-based access policy, cloud service.

Концепция безопасности с нулевым доверием стала модным словом в последние годы, когда с появлением COVID-19 большинство компаний и организаций в основном или полностью перешли на удаленную работу. Многие компании используют виртуальные частные сети (VPN) для поддержки своего рабочего процесса. Тем не менее VPN имеет целый ряд ограничений, включая масштабируемость и простое отсутствие информационной безопасности.

В отличие от сетевых решений, таких как VPN, ZTNA предлагает совершенно иной подход к обеспечению доступа к внутренним приложениям, основанный на нескольких основных принципах:

- полная изоляция процесса предоставления доступа к сетевым приложениям;

- ZTNA строит только исходящие соединения и делает невидимой для неавторизованных пользователей как сетевую инфраструктуру, так и инфраструктуру приложений. IP-адреса никогда не выходят в Интернет;

- фрагментация приложений. ZTNA дает гарантию, что доступ к приложениям предоставляется индивидуально после авторизации. Авторизованные пользователи имеют доступ только к определенным приложениям, а не полный доступ к корпоративной сети.

Перейдем к концептуальной модели ZTNA (рис. 1) [1]. Аутентификация и авторизация объектов должны выполняться с помощью многофакторной проверки подлинности (MFA). Также важно отделить точку физического предоставления доступа от контроллера или механизма, в котором принимается решение о предоставлении доступа, чтобы избежать единой точки отказа. Каждое соединение должно быть авторизовано, при этом не должно быть наследуемых разрешений, основанных на принципах местоположения.

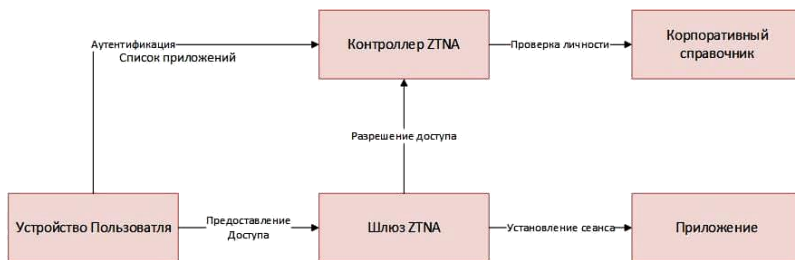


Рис. 1. Концептуальная модель ZTNA

Зоны доверия и деление на сегменты генерируются динамически на основе входящих подключений после авторизации, аутентификации и проверки прав доступа с помощью контроллера ZTNA. По умолчанию нет зон доверия, и трафик не может передаваться по сети. Основными парами взаимодействия являются «Пользователь – приложения», которые формируются на основе введенных учетных данных и определенных правил доступа.

Ценность модели нулевого доступа становится понятной, когда рассматриваются проблемы, с которыми сталкивается эта система.

Одной из самых больших угроз при внедрении ZTNA является растущая площадь атаки на IoT.

Интернет вещей – это относительно новая технология, соединяющая множество «умных» устройств в сеть, которая позволяет им собирать, анализировать, обрабатывать и отправлять данные друг другу. Сегодня основной проблемой Интернета вещей является его уязвимость к кибератакам. По мере роста числа таких подключенных устройств риски несанкционированного доступа к системе IoT растут. Рассмотрим поэтапно, как происходит атака на Интернет вещей (рис. 2):

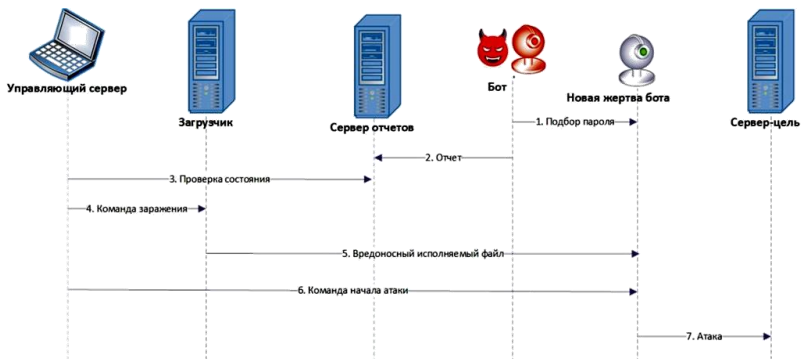


Рис. 2. Атака на Интернет вещей

Шаг 1. Бот выполняет атаку методом подбора и обнаруживает информацию о неизменных заводских паролях устройств IoT.

Шаг 2. После того как бот найдет такие фабричные данные и получит доступ к командной строке или графическому интерфейсу устройства, бот передаст его свойства на сервер отчетов через другой порт.

Шаг 3. Ботмастер постоянно проверяет потенциальные цели и текущее состояние ботнета, связываясь с сервером отчетов через Tor.

Шаг 4. После выбора уязвимых устройств для заражения ботмастер дает соответствующие команды загрузчику со всеми необходимыми деталями, включая IP-адреса и информацию об аппаратной архитектуре.

Шаг 5. Загрузчик проникает в уязвимое устройство и заставляет его загрузить и запустить соответствующий вредоносный файл. Сто-

ит отметить, что после запуска этот файл сразу пытается защититься от конкурентов, блокируя порты, через которые часто происходит заражение, включая Telnet и SSH. На этом этапе вновь созданный дубликат бота уже может взаимодействовать с управляющим сервером и получать от него команды для начала атаки. Это делается путем разрешения доменного имени, которое жестко закодировано в исполняемом файле. Этот метод, используемый вместо прямого доступа к IP-адресу, позволяет ботмастеру изменять IP-адреса сервера управления без изменения двоичных файлов и выполнения дополнительного обмена информацией.

Шаг 6. Ботмастер дает всем дублям бота команду начать атаку на целевой сервер, передавая соответствующие параметры, включая тип и продолжительность атаки, а также IP-адреса самого сервера.

Шаг 7. Боты начинают атаковать цель. Взломанные устройства Интернета вещей используются для организации DDoS-атак. Фактически ZTA уязвима для атак типа «отказ в обслуживании» (DOS) [2]. Цель таких действий, как правило, состоит в том, чтобы нанести экономический ущерб атакуемому и оставаться в тени.

Чтобы свести к минимуму подобные риски, модель нулевого доверия предлагает несколько решений. Следующие примеры типичны для данной модели доступа:

1. Хакер использует атаку цепочки поставок для добавления вредоносного кода в часто используемые сетевые приложения или устройства. Однако в модели нулевого доверия сеть не будет автоматически доверять устройству до тех пор, пока не будет предоставлена соответствующая авторизация

2. Злоумышленник уже получил доступ к сети, используя учетные данные одного из пользователей. Если бы в системе были использованы стандартные средства защиты информации, хакер легко проник бы глубоко в сеть, но с политикой ABAC, используемой при ZTNA, он не сможет выйти за рамки существующих прав пользователей. Пока он пытается проникнуть дальше, у оператора безопасности будет время, чтобы выследить киберпреступника и остановить его действия.

Рассмотрим второй пункт более подробно. В отличие от контроля доступа на основе ролей подход ABAC основан на том, что каждая ситуация оценивается не по роли пользователя и действия, которое он хочет выполнить, а по соответствующим атрибутам.

Ниже представлена схема функционирования модели АВАС (рис. 3). Для выполнения авторизации значения всех атрибутов берутся в момент проверки прав и сравниваются с ожидаемыми значениями. Выполнение всех условий позволяет получить доступ к ресурсу.

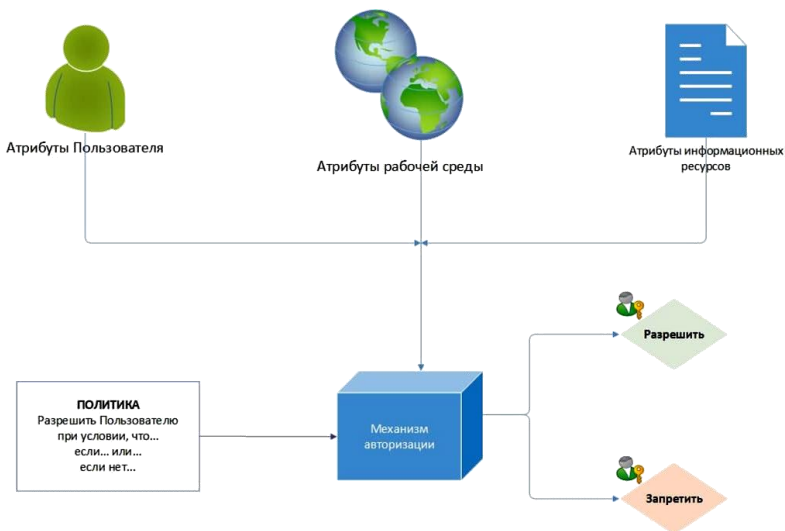


Рис. 3. Схема функционирования модели АВАС

Существует множество логических компонентов, которые формируют архитектуру нулевого доверия в компании. Эти компоненты могут работать как локальная служба или через облако.

Блок «Механизм авторизации», представленный на рис. 3, разделен на несколько уровней трафика: компоненты безопасности, например, такие как система непрерывной диагностики и мониторинга (CDM) и уровень управления.

На уровне управления существует точка принятия решений доступа (PDP), состоящая из двух логических компонентов: механизма политики (PE), который отвечает за принятие решения о том, предоставляется ли конкретному субъекту доступ к ресурсу, и администратора политики (PA), который отвечает за установление или закрытие канала связи между субъектом и ресурсом.

Самый распространенный сценарий развертывания ZTA относится к организации, имеющей штаб-квартиру и несколько географически распределенных мест, соединенных между собой сторонними внешними сетевыми подключениями.

Сотрудникам, которые работают дистанционно, по-прежнему требуется полный доступ к корпоративным ресурсам, а компоненты РЕ/РА часто развертывается как облачный сервис.

Когда компания увеличивает количество облачных приложений и сервисов при своей работе, подход с нулевым доверием требует, чтобы РЕР размещались в точках доступа каждого приложения и источника данных. РЕ и РА могут быть размещены в облаке или даже у стороннего облачного провайдера.

Исходя из вышеизложенного, можно сделать вывод, что внедрение архитектуры с нулевым доверием значительно снижает риск для бизнеса в отношении безопасности информационных ресурсов. Предоставляя только некоторым пользователям доступ к действиям, которые необходимы для выполнения их рабочих обязанностей, компания уменьшает ущерб, который может быть нанесен злоумышленником.

Внедрение ZTNA в сетевую экосистему организации считается одной из наиболее успешных практик в области кибербезопасности и не требует существенных изменений сетевой структуры.

Библиографический список

1. Принципы сетевого доступа с нулевым доверием // FORTIS.RU: компания по предоставлению современных высокотехнологичных продуктов, комплексных систем и сервисов в области информационной безопасности, сетевых и облачных технологий. – URL: <https://fortis.ru/safe-t3/#b6692> (дата обращения: 15.11.2021).

2. Наливайко А. Модель Zero Trust: привычная защита сетевого периметра уже недостаточна // ANTI-MALWARE.RU: независимый российский информационно-аналитический центр. – 2020. – URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Reviving-zero-trust-model#part5 (дата обращения: 20.11.2021).

Сведения об авторе

Букирева Юлия Михайловна – студентка Пермского национального исследовательского политехнического университета, гр. КЗИ-19-1б, Пермь, e-mail: yulia.bukireva@yandex.ru

И.В. Головнин, А.В. Гаврилов

Пермский национальный исследовательский
политехнический университет, Пермь

**ПРИМЕНЕНИЕ АВТОНОМНЫХ ДАТЧИКОВ
ПРИ РАБОТЕ В СТАНДАРТЕ NB-IoT НА ПРИМЕРЕ
НЕФТЕДОБЫВАЮЩЕГО ПРЕДПРИЯТИЯ**

Описано испытание модулей передачи данных при работе в стандарте NB-IoT. Разработано 11 модемов стандарта сотовой связи NB-IoT. Произведено тестирование модемов NB-IoT на базовой станции мобильного оператора. В результате доказано, что стандарт сотовой связи NB-IoT позволяет осуществлять передачу данных с МПД ИВЭ-50 с сохранением работоспособности функционала системы ASCiWell. Также определено максимально допустимое расстояние 13,4 км для передачи данных с объекта в условиях сложного рельефа местности.

Ключевые слова: NB-IoT, МПД, APN, сеть передачи данных, стандарт связи, телеметрия.

I.V. Golovnin, A.V. Gavrilov

Perm National Research Polytechnic University, Perm

**THE USE OF AUTONOMOUS SENSORS WHEN WORKING
IN THE NB-IoT STANDARD ON THE EXAMPLE
OF AN OIL-PRODUCING ENTERPRISE**

This article presents a test of data transmission modules when working in the NB-IoT standard. 11 modems of the NB-IoT cellular communication standard have been developed. NB-IoT modems were tested at the base station of the mobile operator. As a result, it is proved that the NB-IoT cellular communication standard allows data transmission from the IVE-50 MPD while maintaining the functionality of the ASCiWell system. The maximum permissible distance of 13.4 km for transmitting data from an object in conditions of difficult terrain has also been determined.

Keywords: NB-IoT, MPD, APN, data transmission network, communication standard, telemetry.

В настоящее время развитие сетей связи дает большие возможности для всех предприятий и сегментов бизнеса осуществлять сбор, контроль, управление данными. Особенно это актуально для крупных предприятий добычи нефти и газа.

В данной статье мы рассмотрим решение задачи по организации телеметрии и мониторинга работы нефтедобывающих скважин на объектах ООО «Лукойл–Пермь». Задача усложнялась тем, что месторождения сильно рассредоточены и большое количество объектов добычи находятся вдали от инфраструктуры связи.

Для решения данной задачи оператором связи предложено использование нового узкополосного стандарта связи Narrow Band Internet of Things (далее – NB-IoT). Данный стандарт был разработан специально для реализации различных проектов Интернета вещей.

Целью проведения данной работы было опробирование разработанного АО «Предприятие В-1336» модема для передачи данных по закрытому протоколу в стандарте сотовой связи NB-IoT, в составе автономного модуля передачи данных ИВЭ-50 (далее – МПД ИВЭ-50), а именно:

- тестирование и оценка стабильности передачи данных в стандарте NB-IoT на скважинах с различной удаленностью от базовой станции;

- оценка функционала системы ASC iWell в стандарте NB-IoT;

- оценка максимально допустимого расстояния от МПД до базовой станции (далее – БС) для работы в стандарте NB-IoT.

Технология NB-IoT – это одно из эволюционных продолжений стандарта LTE. Предполагает интеграцию с LTE, но при его использовании меняется аппаратная составляющая и соответственно программное обеспечение. Необходимо отметить, что аппаратное обеспечение требует изменений только в случае отсутствия поддержки необходимого функционала SDR на БС. При этом NB-IoT не является отдельным стандартом, а является дополнением стандарта LTE. Это связано с целесообразностью унификации инфраструктуры сетей радиодоступа LTE для предоставления всего спектра услуг IoT [2].

Он удовлетворяет двум основным требованиям:

1. Простота, легкость и преимущества применения:

- стандарт можно использовать на существующей физической инфраструктуре;

- эффективное использование существующего LTE спектра – до 50 000 устройств на сектор;

- глубокий индор и большое покрытие (до 20 dB лучше, чем в GSM);

- NB-IoT – одна из наиболее энергоэффективных технологий;

– рекомендован для сбора данных на промышленных объектах и опасных объектах производства, Приказ №113 от 29.03.2019 г. Министерства цифрового развития, связи и массовых коммуникаций РФ «Об утверждении концепции построения и развития узкополосных беспроводных сетей связи Интернета вещей на территории РФ» [1].

2. Безопасность и защищенность передачи данных:

- использование защищенных каналов и средств шифрования;
- выполнение требований к стандартизации, типизации и лицензионной частоте;
- выполнение требований к каналам и протоколам передачи технологических данных;
- сеть АСУТП изолирована от корпоративной сети предприятия;
- передача информации в APN изолирована от любых других пакетных сетей;
- организационные меры исключают НСД (несанкционированный доступ);
- радиointерфейс мобильных сетей зашифрован [2].

Лабораторные испытания модема NB-IoT проводились силами АО «Предприятие В-1336» с привлечением специалистов ПАО «МегаФон». Сначала тестирование проводилось над территорией научно-производственной базы В-1336, а позднее в одном из цехов добычи нефти и газа ООО «Лукойл–Пермь» (далее – ЦДНГ).

Аппаратурно-программные средства:

- МПД ИВЭ-50 со встроенным модемом NB-IoT – далее оборудование;
- система ASC iWell по сбору, передаче данных и визуализации производства АО «Предприятие В-1336»;
- базовые станции оператора связи.

Для достижения поставленной цели оборудование было модернизировано:

- в МПД был заменен модем, который поддерживает NB-iot, и проведены соответствующие настройки;
- на базовых станциях произведена замена плат и радиопередатчиков на те, которые поддерживают NB-iot, и также проведены настройки на сети.

Всего для исследования и дальнейшего использования изготовлено 11 МПД и модернизировано 2 БС – одна на территории размещения предприятия В-1336, другая – в ЦДНГ.

Основными требованиями были обеспечение пропускной способности и корректность передаваемых данных, которую проверяли путем сличения с фактическими данными со станции управления. Считывали на флэш-накопитель архив и сверяли с iWell.

The image shows a configuration interface for the MPPD IVE-50 device. It is divided into three sections:

- Информация (Information):**
 - Наименование изделия: "NB-IoT 4G GPS(1529B025)"
 - Версия загрузчика: 0.0
 - Версия приложения: 1.0
 - Дата последнего обновления: 15.02.2021
 - Дата последнего конфигурирования: 16.02.2021
- Передача данных (Data Transmission):**
 - Таймаут: 120 [сек]
 - Скорость передачи: 115200 [бит/сек]
 - Включить NB-IoT:
 - Включить GPS приемник:
 - Включить SCAN:
 - 2G: 3G: 4G:
- Диапазон NB-IoT (NB-IoT Frequency Band):**
 - DCS 1800: EGSM 900: PGSM 900:
 - BAND 1: BAND 3: BAND 5: BAND 8: BAND 20: BAND 28:

Рис. 1. Настройки МПД ИВЭ-50

Для обеспечения пропускной способности были определены следующие параметры:

- скорость передачи данных не менее 115 000 Бит/с;
- оптимальное время таймаута 120 с – это время, после которого модем перезагружается, если не видит БС, а также интервал, достаточный для контроля оборудования;

– объема данных с одной скважины – это примерно 600 Мб в месяц.

Основные настройки МПД отражены на ри. 1.

С представителями ООО «Лукойл–Пермь» был согласован список объектов для проведения испытаний (таблица). Организована передача данных с МПД ИВЭ-50 в корпоративную сеть ООО «Лукойл–Пермь». Организован ежедневный мониторинг работы МПД ИВЭ-50 в стандарте сети NB-IoT. Произведено тестирование управляющих функций, и организован контроль подкачки архивных данных.

Объекты испытания стандарта NB-iot

№ п/п	Наименование объекта	Расстояние от БС (км)	Тип антенны/коэффициент усиления	Примечание
1	Скважина №1	9,8	"Антей 906"/13,5 dB	Сложный рельеф
2	Скважина №2	10,6	"АКЛ-900 (В) "/18dB	Сложный рельеф
3	Скважина №3	6,94	"Антей 906"/13,5 dB	Сложный рельеф
4	Скважина №4	8,6	"Триада-ВА 994 SOTA"/10dB	
5	Скважина №5	8,6	"Триада-ВА 994 SOTA"/10dB	
6	Скважина №6	0,3	"Триада-ВА 994 SOTA"/10dB	
7	Скважина №7	8,6	"Триада-ВА 994 SOTA"/10dB	
8	Скважина №8	6,94	"Антей 906"/13,5 dB	Сложный рельеф
9	Скважина №9	13,4	"Триада-ВА 994 SOTA"/10dB	
10	Скважина №10	7,6	"Антей 906"/13,5 dB	
11	Скважина №11	0,9	"Триада-ВА 994 SOTA"/10dB	

В процессе работ были выявлены и устранены следующие проблемы: сложный рельеф (большой перепад высот) и интерференция оборудования в ЦДНГ. Для устранения проблемы сложного рельефа проведены дополнительные мероприятия. Организованы работы по улучшению качества связи, произведены замена и подъем антенн на скважинах № 1, 2, 3, 8 с более высоким коэффициентом усиления сигнала.

На примере скважины № 3 представлен профиль высот. Высота отметки базовой станции – 158 м над уровнем моря относительно поверхности земли. Высота установки антенны на базовой станции – 25 м.

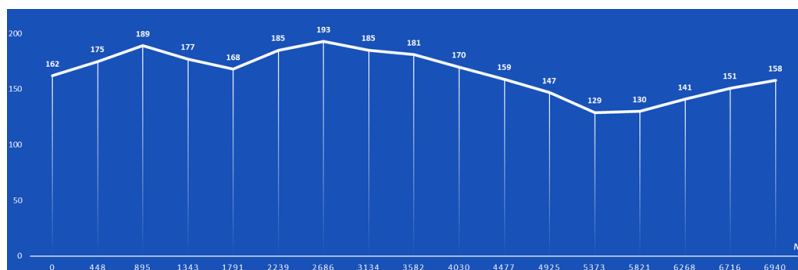


Рис. 2. Профиль высот скважины №3

Причиной интерференции оборудования оказались сверхмощные радиомодули, которые использовались в МПД. Они приводили к внутрисетевой интерференции в uplink. После ограничения максимальной мощности модемов со стороны сети интерференция исчезла.

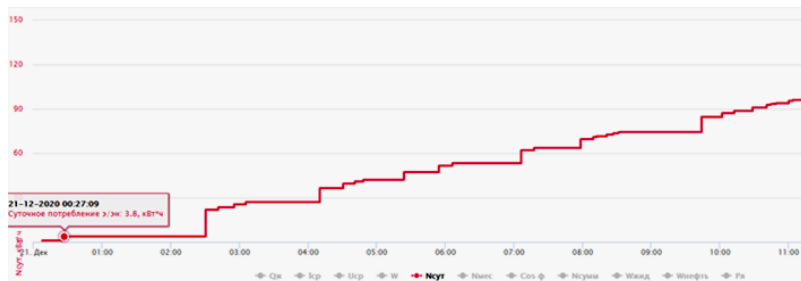


Рис. 3. Суточное потребление эл/эн. скважины № 4

На примере графика потребления электроэнергии видим, что после снижения мощности сигнала МПД в 10:30 часов график пошел более частый и ровный без прерываний.

Заключение:

- критерием успешности практического внедрения стандарта NB-IoT являются отсутствие сбоев и оперативность поступления данных с МПД в систему ASC iWell за весь период проведения испытаний;
- дальность сигнала стандарта NB-iot 19,2 км в городских условиях и с ровным рельефом, что в 3 раза больше стандарта 3G;
- дальность сигнала стандарта NB-iot 13,4 км в условиях со сложным рельефом, что в 2 раза больше стандарта 3G;
- достигнута дискретность онлайн-данных, команды дистанционного управления выполнялись своевременно.

Таким образом, стандарт сотовой связи NB-IoT позволяет осуществлять передачу данных с МПД ИВЭ-50 с сохранением работоспособности функционала системы ASCiWell.

Библиографический список

1. Иванов О.А. Приказ №113 от 29.03.2019 г. Министерства цифрового развития, связи и массовых коммуникаций РФ «Об утверждении концепции построения и развития узкополосных беспроводных сетей связи Интернета вещей на территории РФ» [Электрон-

ный ресурс] // Официальный сайт Министерство цифрового развития, связи и массовых коммуникаций РФ. – URL: <https://digital.gov.ru/>

2. Головнин И.В, Тюрин С.А., Применение NB-iot в промышленности на примере нефтедобывающего предприятия // Автоматизированные системы управления и информационные технологии: материалы всерос. науч.-техн. конф. – Пермь, 2021. – С. 227–231.

Сведения об авторах

Головнин Илья Владимирович – магистрант кафедры «Автоматики и телемеханики» Пермского национального исследовательского политехнического университета, гр. ТК5-20-1м, Пермь, e-mail: Golovnin-ilya@yandex.ru

Гаврилов Алексей Викторович – старший преподаватель кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: gaval@at.pstu.ru

М.А. Дубовикова, А.В. Гаврилов

Пермский национальный исследовательский
политехнический университет, Пермь

ИССЛЕДОВАНИЕ MESH-СЕТЕЙ В СИМУЛЯТОРЕ OMNET++

Рассматривается влияние параметров протокола маршрутизации AODV на характеристики mesh-сети при моделировании в симуляторе OMNeT++ (с использованием INET Framework). Получены зависимости процента потерянных пакетов от размера mesh-сети, времени жизни маршрута и скорости движения узлов сети.

Ключевые слова: mesh-сеть, процент потерянных пакетов, OMNeT++, AODV.

M.A. Dubovikova, A.V. Gavrilov

Perm National Research Polytechnic University, Perm

STUDY OF MESH NETWORKS IN THE OMNET ++ SIMULATOR

The influence of the parameters of the AODV routing protocol on the characteristics of the mesh network when simulating in the OMNeT++ simulator (using the INET Framework) is considered. The dependences of the percentage of lost packets on the size of the mesh network, route lifetime and speed of movement of network nodes are obtained.

Keywords: mesh network, packet loss rate, OMNeT ++, AODV.

Использование распределенных сетевых технологий позволяет реализовать сбор информации с различных устройств (датчиков). В зависимости от характера контролируемого объекта датчики могут быть распределены по большой территории и быть подвижными или неподвижными. Для реализации распределенной сети сбора информации часто используют беспроводные mesh-сети. При этом встает задача надежного получения информации о состоянии объекта. Так как каналы беспроводных mesh-сетей образуют нестабильные соединения, то исследование параметров протоколов, при которых возможно реализовать надежную доставку информации, является актуальным.

Моделирование mesh-сетей будем производить в среде моделирования OMNeT++ с использованием фреймворка INET Framework.

OMNeT++ – это расширяемая, модульная, компонентная библиотека моделирования C++ и фреймворк, в первую очередь для

построения сетевых симуляторов. «Сеть» понимается в более широком смысле, который включает проводные и беспроводные сети связи, сети на кристалле, сети массового обслуживания и т.д. [1].

INET Framework – это библиотека моделей с открытым исходным кодом для среды моделирования OMNeT++. INET Framework содержит модели для интернет-стека (TCP, UDP, IPv4, IPv6, OSPF, BGP и др.), проводные и беспроводные протоколы уровня связи (Ethernet, PPP, IEEE 802.11 и т.д.), поддержку мобильности, протоколы MANET, DiffServ, MPLS с сигнализацией LDP и RSVP-TE, несколько моделей приложений и многие другие протоколы и компоненты [2].

Для моделирования были созданы 3 сети – «решетки», которые состояли в первом случае из 25 узлов (5×5), во втором случае 36 узлов (6×6) и 49 узлов (7×7) в третьем случае. Использовался протокол маршрутизации AODV.

Алгоритм Ad hoc On-Demand Distance Vector (AODV) обеспечивает динамическую, самозапускающуюся, многозвенную маршрутизацию между участвующими мобильными узлами, желающими установить и поддерживать специальную сеть. Он предлагает быструю адаптацию к условиям динамического соединения, низкую нагрузку на обработку и память, низкое использование сети и определяет одноадресные маршруты к пунктам назначения в специальной сети. AODV использует порядковые номера пунктов назначения, чтобы гарантировать свободу цикла в любое время, избегая проблем, связанных с классическими протоколами вектора расстояния [3].

Среди параметров AODV есть «activeRouteTimeout» – значение таймаута для кэшированных маршрутов. От него напрямую зависит параметр «myRouteTimeout» – теоретическое значение жизни маршрута, которое передается от целевого узла в RREP. Поэтому «activeRouteTimeout» был выбран в качестве изменяемого параметра, зависимость от которого будем наблюдать.

За время жизни маршрута берется то время, в течение которого узлы, получающие RREP (Route Reply – ответ маршрута), считают маршрут действительным.

Вторым параметром моделирования была выбрана скорость движения узлов в сети. От нее тоже будем изучать зависимость.

Изучать будем процент потерянных пакетов, чтобы оценить целостность принимаемых данных.

Исходные данные для моделирования сетей: время моделирования – 200 секунд; изначальное расстояние между узлами – 100 метров; расстояние, на которое узел может передать пакет, – 176 метров, т.е. каждый узел может общаться только с ближайшими соседними узлами. В результате исследований были получены результаты, которые отражены на последующих графиках.

Для статической сети (скорость движения узлов отсутствует) график зависимости процента потерянных пакетов от количества узлов в сети и «activeRouteTimeout» (art) представлен на рис. 1.

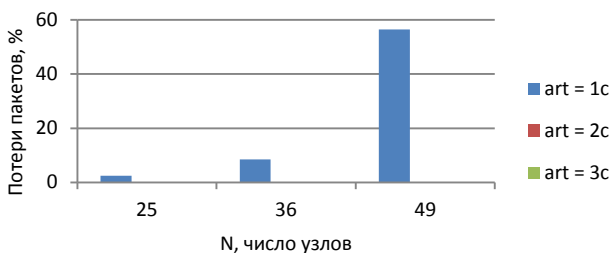


Рис. 1. График зависимости процента потерянных пакетов от количества узлов в сети и «activeRouteTimeout»

Для динамических сетей (присутствует мобильность) графики зависимостей процентов потерянных пакетов представлены от скорости движения узлов сети и «activeRouteTimeout».

Так, для mesh-сети в 25 узлов этот график представлен на рис. 2.

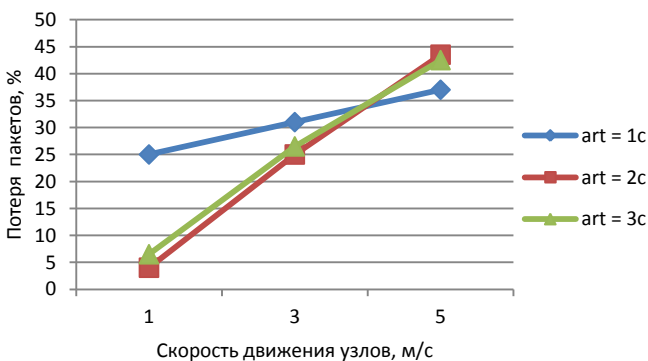


Рис. 2. График зависимости процента потерянных пакетов от скорости движения узлов в сети и «activeRouteTimeout» (25 узлов)

Для mesh-сети в 36 узлов график зависимости процента потерянных пакетов от скорости движения узлов в сети и «activeRouteTimeout» (art) представлен на рис. 3.

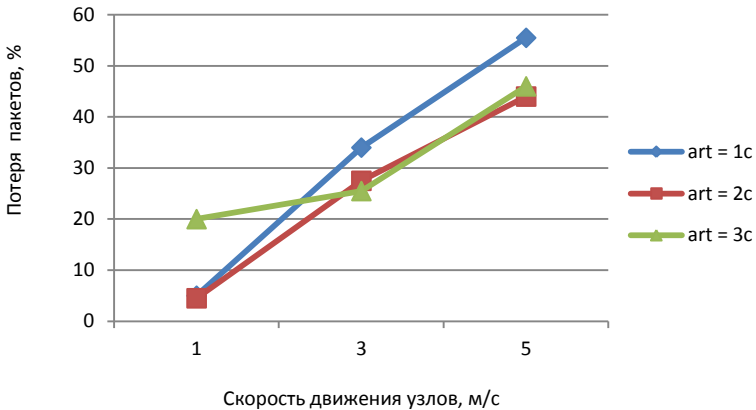


Рис. 3. График зависимости процента потерянных пакетов от скорости движения узлов в сети и «activeRouteTimeout» (36 узлов)

Для mesh-сети в 49 узлов график зависимости процента потерянных пакетов от скорости движения узлов в сети и «activeRouteTimeout» (art) представлен на рис. 4.

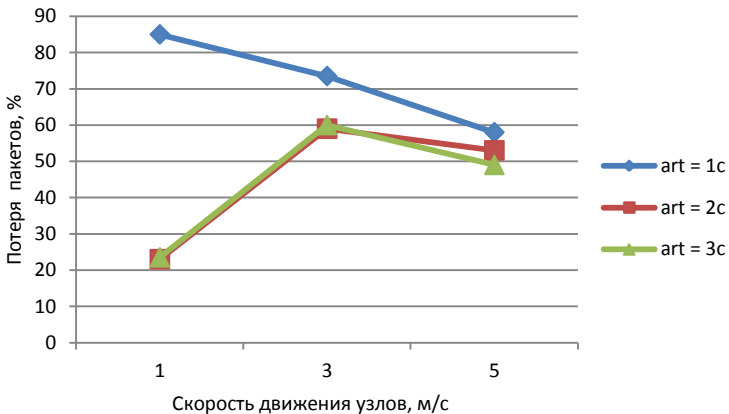


Рис. 4. График зависимости процента потерянных пакетов от скорости движения узлов в сети и «activeRouteTimeout» (49 узлов)

Анализ полученных результатов позволяет сделать следующие выводы:

1. При увеличении количества узлов в сети увеличивается процент потерянных пакетов.
2. При уменьшении времени жизни маршрута в среднем по всем исследованиям также увеличивается процент потерянных пакетов.
3. В большинстве случаев процент потерянных пакетов возрастает при увеличении скорости движения узлов сети, исключение составляет динамическая сеть в 49 узлов. Это можно объяснить тем, что количества узлов хватает на то, чтобы при достаточно высокой скорости их движения между узлом-отправителем и узлом-получателем дольше сохранялся маршрут передачи.

Библиографический список

1. OMNeT++ Discrete Event Simulator [Электронный ресурс] // Официальный сайт «OMNeT++». – URL: <http://omnetpp.org> (дата обращения: 23.12.2021).
2. INET Framework [Электронный ресурс] // Официальный сайт INET Framework. – URL: <https://inet.omnetpp.org> (дата обращения: 23.12.2021).
3. Ad hoc On-Demand Vector (AODV) Routing [Электронный ресурс] // Документация на протокол AODV. – URL: <https://datatracker.ietf.org/doc/html/rfc3561#section-5.2> (дата обращения: 23.12.2021).

Сведения об авторах

Дубовикова Мария Александровна – магистрант кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, гр. ТК5-20-1м, Пермь, e-mail: dma0712@mail.ru

Гаврилов Алексей Викторович – старший преподаватель кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: gaval74@mail.ru

Д.А. Еленкин, И.Ф. Еленкина

Пермский национальный исследовательский
политехнический университет, Пермь

ИСПОЛЬЗОВАНИЕ БИНАРНОЙ СВЁРТОЧНОЙ НЕЙРОННОЙ СЕТИ ДЛЯ АНАЛИЗА ТОНАЛЬНОСТИ ТЕКСТА

В этой статье исследуется возможность построения скоринговой системы, позволяющей классифицировать и оценивать информацию (в зависимости от степени угроз), содержащуюся на пользовательских страницах социальных сетей. Выявление социально-психологических характеристик (маркеров поведения) пользователей деструктивного контента социальных сетей, сосредоточенных в текстовой, графической и звуковой формах, требует создания нового подхода в использовании нейросетей. Необходимо выявить достоинства и недостатки уже существующих методов при анализе информации. В статье рассматривается использование свёрточной нейронной сети, позволяющей классифицировать текстовые, графические, звуковые форматы данных. В частности, рассмотрен метод бинарной классификации текста при анализе тональности пользовательского контента с описанием общего хода алгоритма работы метода.

Ключевые слова: свёрточная нейронная сеть, классификация, машинное обучение.

D.A. Elenkin, I.F. Elenkina

Perm National Research Polytechnic University, Perm

USING A BINARY CONVOLUTIONAL NEURAL NETWORK TO ANALYZE THE TONALITY OF A TEXT

This article explores the possibility of building a scoring system that allows classifying and evaluating information (depending on the degree of threats) contained on user pages of social networks. The identification of socio-psychological characteristics (markers of behavior) of users of destructive content of social networks, concentrated in text, graphic and sound forms, requires the creation of a new approach to the use of neural networks. It is necessary to identify the advantages and disadvantages of existing methods in the analysis of information. The article discusses the use of a convolutional neural network that allows classifying text, graphic, and audio data formats. In particular, a method of binary classification of text in the analysis of the tonality of user content with a description of the general course of the algorithm of the method is considered.

Keywords: convolutional neural network, classification, machine learning.

Современные глобальные вызовы в сфере межнациональных и межгосударственных отношений определяют приоритетные для нашей страны задачи по укреплению российской гражданской идентичности, поддержке культурного и образовательного единства нашей страны.

Профилактических мероприятий, проводимых в образовательных организациях, направленных на формирование у подрастающего поколения традиционных для нашей страны духовно-нравственных ценностей, которые изложены в Стратегии национальной безопасности Российской Федерации [1], явно недостаточно. Необходимо повышать адресность принимаемых мер.

Основными направлениями обеспечения информационной безопасности в области науки, технологий и образования является обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности [2]. Общенаучной проблемой обеспечения информационной безопасности Российской Федерации является проблема обеспечения защищенности личности, общества и государства от деструктивных информационных воздействий [3].

Образовательные организации в настоящее время испытывают дефицит методик по выявлению лиц, нуждающихся в адресном воздействии, рекомендаций и требований по организации работы с ними.

Своевременное выявление интернет-профилей учащихся, находящихся в «группе риска», позволит предвосхитить и не допустить распространение потенциальных угроз и вовлечение в них как самого учащегося (реализации суицидальных идей), так и общества в целом (случаи школьного шутинга, буллинга и др.).

Существующие подходы в проведении анализа интернет-профилей пользователей социальных сетей строятся на основе использования алгоритмов NLP (natural language processing).

В нашем случае существует необходимость создать такой способ, который позволял бы комплексно анализировать информацию, содержащуюся в интернет-профилях учащихся, в зависимости от формата размещенных данных: текст, звук, графика, и в дальнейшем позволял бы классифицировать и оценивать информацию в зависимости от степени угроз (для себя или для общества). Для реализации подобного способа хорошо подходят свёрточные нейронные сети, точнее, их двумерный вариант, который широко применяется для

анализа изображений. Одномерные (бинарные) свёрточные нейронные сети корректно использовать для анализа текстов [4].

Для осуществления первичного мониторинга рисков в молодежной образовательной среде, в том числе в интернет-пространстве, был сформирован краткий перечень поведенческих маркеров – вербальных и визуальных поведенческих характеристик учащихся, находящихся в «группе риска» либо солидаризирующихся с деструктивными идеологиями и ценностями. При этом важным остается следующее: каждый маркер рассматривается в совокупности с другими с учетом поведенческого контекста и поведенческой динамики.

В рамках работы над статьёй выявлены социально-психологические характеристики (маркеры поведения) пользователей деструктивного контента социальных сетей следующих молодежных направлений:

- 1) маркеры увлечения учащихся субкультурой «колумбайн»;
- 2) маркеры увлечения учащихся ультраправой идеологией;
- 3) маркеры увлечения учащихся идеологией радикальных религиозных организаций;
- 4) маркеры увлечения учащихся субкультурой «оффников»;
- 5) маркеры увлечения учащимися суицидальными практиками.

Использование в обученной двумерной свёрточной нейронной сети заранее подготовленного набора данных, содержащего изображения, относящиеся к указанным выше направлениям деструктивного контента, позволит классифицировать «цифровой профиль» пользователя.

Отдельно рассмотрим метод анализа тональностей текстовых данных на основе одномерной свёрточной нейронной сети, позволяющий в рамках исследуемой темы выявлять в профилях учащихся увлечения суицидальными практиками.

Текст необходимо анализировать как последовательность токенов, потому что порядок символов, слов и предложений в тексте имеет значение. Если пренебречь этим правилом, то при анализе тональностей будет неправильно интерпретироваться смысл предложения.

Перед тем как обрабатывать текст, его необходимо представить в числовом виде. В настоящей статье мы будем использовать частотное кодирование. Для анализа пользовательского контента интернет-профиля социальной сети этого будет достаточно. В более сложных случаях целесообразно представлять текст не в численном виде, а в векторном.

Особенность сверточных нейронных сетей заключается в том, что ядра свертки определяются автоматически в процессе обучения, заранее их определять не нужно.

Архитектура сверточной нейронной сети для анализа текстов состоит из чередующихся блоков: слоя свертки и слоя подвыборки, а после этого идёт несколько полно связанных слоёв для решения задачи классификации. С точки зрения машинного обучения анализ тональности пользовательского контента – это задача бинарной классификации.

Преимущество свёрточной нейронной сети заключается в том, что нейросеть можно очень быстро реализовать, особенно на современных ускорителях вычислений, таких как GPU или TPU. Это связано с тем, что все свёртки можно просчитывать параллельно, – в этом существенное отличие от рекуррентной нейронной сети, в которой необходимо учитывать данные от предыдущего этапа работы сети.

Недостаток одномерной сверточной нейронной сети для обработки текстов заключается в том, что длина анализируемых данных ограничена окном свёртки. Поэтому если важные слова встречаются на большом удалении друг от друга, много больше, чем длина окна свертки, то одномерная свёрточная нейронная сеть такие данные корректно проанализировать не сможет. В этом случае лучше применять рекуррентную нейронную сеть (таблица).

Средства разработки

№ п/п	Средство разработки	Назначение
1	Python 3.0	Написание алгоритма программы, описание основного функционала
2	Big Data	Технология для обучения реализованного алгоритма на корпусах огромных текстов
3	Google Books	Многоязычный корпус оцифрованных книг для обучения алгоритма
4	Google Colaboratory	Облачный сервис от Google, предназначенный для программистов, которые работают на языке Python. Блокноты Google Colab позволяют объединить в одном документе исполняемый код и форматированный текст. Также можно получить удаленный доступ к машине с подключенной видеокарткой с тензорным процессором

Обучение свёрточной нейросети представлено в листинге 1. Листинг 2 содержит статистику обучения нейросети на 4 эпохах.

Листинг 1 – фрагмент кода обучения нейросети на Python в пространстве Google Colaboratory:

```
history = model.fit(x_train,  
                    y_train,  
                    epochs=4,  
                    batch_size=128,  
                    validation_split=0.1)
```

Листинг 2 – статистические данные этапов обучения нейросети:

```
Epoch 1/4  
3938/3938 - 52s 13ms/step - loss: 0.1862 - accuracy: 0.9240 - val_loss: 0.1226 - val_accuracy: 0.9539  
Epoch 2/4  
3938/3938 - 53s 13ms/step - loss: 0.1232 - accuracy: 0.9538 - val_loss: 0.1133 - val_accuracy: 0.9571  
Epoch 3/4  
3938/3938 - 53s 13ms/step - loss: 0.0875 - accuracy: 0.9685 - val_loss: 0.1189 - val_accuracy: 0.9553  
Epoch 4/4  
3938/3938 - 53s 13ms/step - loss: 0.0586 - accuracy: 0.9795 - val_loss: 0.1383 - val_accuracy: 0.9528
```

Графическое представление долей верных ответов на обучающем и проверочном наборах данных с ростом числа эпох обучения представлено на рисунке.

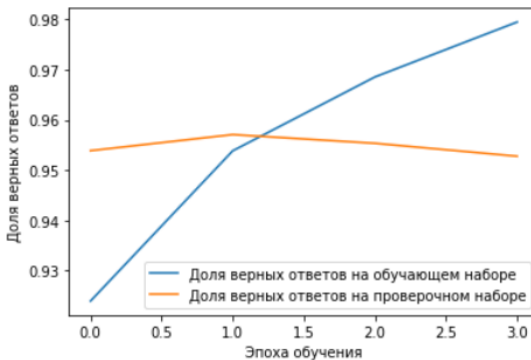


Рис. Доля верных ответов на обучающем и проверочном наборах данных

С задачами, связанными с классификацией текста и определением тональности, одномерные свёрточные нейронные сети справляются очень хорошо и, учитывая то обстоятельство, что свёрточные ней-

росети обучаются быстрее, чем рекуррентные, то для простых задач анализа текстов предпочтительнее использовать одномерные сверточные нейронные сети.

Библиографический список

1. Стратегия национальной безопасности Российской Федерации (утв. Указом Президента РФ № 400 от 2 июля 2021 г.). Раздел II: Россия в современном мире: тенденции и возможности. – Пп. 20, 21. – С. 6.

2. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ № 646 от 5 декабря 2016 г.). Раздел IV: Стратегические цели и основные направления обеспечения информационной безопасности. – С. 8, п. 20; с. 9, п. 23а; с. 11, п. 27д.

3. Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации утв. секретарем Совета безопасности Российской Федерации Н.П. Патрушевым 31 августа 2017 г.). Раздел I: Общенаучные проблемы обеспечения информационной безопасности Российской Федерации. – С. 1, пп. 1.1.3, п. 1.3.1.

4. Григорьева Е.Ю., Мисюра М.А., Палиенко А.Н. Современные глубокие сверточные нейронные сети // Молодой учёный. – Январь 2017. – № 4 (138). –153 с.

Сведения об авторах

Еленкин Дмитрий Александрович – магистрант кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, гр. КЗИ-21-1м, Пермь, e-mail: box_temp@mail.ru

Еленкина Ирина Фёдоровна – магистрант кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, гр. КЗИ-21-1м, Пермь, e-mail: irishka1983.08@mail.ru

А.Н. Еремеев, А.И. Тур

Пермский национальный исследовательский
политехнический университет, Пермь

**ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ
НЕСКОЛЬКИХ АНТИВИРУСОВ НА ОСНОВЕ БАЗЫ
ВИРУСОВ ДЛЯ ТЕСТИРОВАНИЯ АНТИВИРУСОВ**

В данной работе были протестированы различные комбинации бесплатных антивирусных средств на основе готовой базы вирусов. Определена их эффективность и проведено сравнение с платным аналогом.

Ключевые слова: антивирус, оценка эффективности, сравнение, комбинации антивирусов, вирусы.

A.N. Eremeev, A.I. Tur

Perm National Research Polytechnic University, Perm

**RESEARCH OF THE EFFICIENCY OF USING SEVERAL
ANTI-VIRUSES BASED ON THE VIRUS BASE
FOR TESTING ANTI-VIRUSES**

In this work, we tested various combinations of free antivirus tools based on a ready-made virus database. Their effectiveness was determined and compared with a paid analogue.

Keywords: antivirus, efficiency mark, comparison, antivirus combinations, viruses.

В настоящее время для обработки информации, общения и обмена данными повсеместно используются компьютерные сети. Однако благодаря Интернету и большой пропускной способности систем связи распространение вирусов превращается в сетевые эпидемии. Рядовые пользователи зачастую не обращают внимания, когда они попадают на их компьютеры, и даже не имеют установленных антивирусных программ. Поэтому остро встает вопрос о защите компьютерных сетей и информации, и в связи с развитием электроники появляются все новые и новые угрозы.

Цель работы заключается в исследовании эффективности борьбы с вирусами различных комбинаций бесплатных антивирусов.

Все последующие эксперименты проводятся на виртуальной Windows 10 Pro, с отключенным Windows Defender, запущенной через VMware Workstation 16 Player. На ее работу выделено 2 ядра, также 8 Гб оперативной памяти. В качестве базы вирусов использует-

ся база, включающая в себя: Backdoor вирусы, Email-Worm, Trojan, Boot и Dos вирусы и другие.

Для оценки эффективности различных комбинаций антивирусных средств были выбраны следующие критерии:

1. *Требования к ресурсам системы.* Хватает ли аппаратной конфигурации вашего компьютера для работы с данными антивирусами?

2. *Удобство пользования.* Если для повседневной работы антивирусов требуются особые навыки, он может оказаться непрактичным для многих пользователей.

3. *Скорость работы.* Чувствуется ли замедление скорости работы системы при использовании различных антивирусных средств.

4. *Качество защиты.* Антивирусы должны уметь работать в постоянно меняющейся агрессивной среде с новыми вирусами, червями и троянцами, которые становятся все сложнее.

5. *Функциональность.* Есть ли какое-то функциональное преимущество у данной комбинации антивирусов перед другими (табл. 1).

Таблица 1

Комбинация Kaspersky Security Cloud – Free
с другими представителями

Критерии	+ Avast	+ 360 Total Security	+ AVG	+ Avira	+ Comodo
1	8/10	–	9/10	–	–
2	9/10	–	9/10	–	–
3	6/10	–	6/10	–	–
4	7/10	0/10	6/10	0/10	0/10
5	4/10	–	4/10	–	–

Если в критерии «Качество защиты» поставлено 0 баллов, то данные антивирусы не совместимы между собой.

Из всех проведенных тестов наиболее эффективной комбинацией по критерию «Качество защиты» стала Comodo free antivirus + Avira. Данная пара обезвредила 90 % вредоносных файлов. Самая менее требовательная к ресурсам Avast + 360 Total Security, она же и стала лидером в критерии «Скорость работы». Наибольшим функционалом обладает пара Comodo free antivirus + 360 Total Security, данная пара предлагает удобный менеджер рабочего стола, также более безопасный аналог браузера Google Chrome – Comodo Dragon. Но даже самую эффективную комбинацию использовать нецелесообразно, так как во всех тестах Comodo free antivirus самостоятельно обезвреживает 88 %

вредоносных программ. Было принято решение сравнить данный анти-вирус с Dr.Web Security Space (табл. 2).

Таблица 2

Сравнение Comodo free antivirus и Dr.Web Security Space

Критерии	Comodo	Dr.Web
1	9/10	8/10
2	7/10	9/10
3	7/10	9/10
4	9/10	8/10
5	7/10	8/10

На удивление Comodo обезвредил большее количество вредоносных файлов, однако была заметна небольшая просадка в производительности системы, хотя системные требования у него ниже. По скорости обнаружения и обезвреживания Comodo также проигрывает. Несмотря на все недостатки, Comodo free antivirus является отличным аналогом платных антивирусных средств.

Библиографический список

1. Духан Е.И., Синадский Н.И., Хорьков Д.А. Программно-аппаратные средства защиты компьютерной информации. – Екатеринбург: Изд-во УрГУ, 2008. – 240 с.
2. Рудниченко А.К., Шахманова М.В. Актуальные способы внедрения компьютерных вирусов в информационные системы // Молодой ученый. – 2016. – № 11. – С. 221–223.
3. Хруска Ян. Борьба вирусов и антивирусов. – Нью-Джерси, США: Изд-во Саймона и Шустера, 1990.
4. Климентьев К.Е. Компьютерные вирусы и антивирусы: взгляд программиста / под ред. Д.А. Мовчна. – М.: ДМК-Пресс, 2013.

Сведения об авторах

Еремеев Андрей Николаевич – студент Пермского национального исследовательского политехнического университета, гр. КОБ-17-1с, Пермь, e-mail: eremeev.an@yandex.ru

Тур Александр Игоревич – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: tur.aleksandr93@mail.ru

А.В. Зверев

Пермский национальный исследовательский
политехнический университет, Пермь

МЕТОДЫ БАЛАНСИРОВКИ НАГРУЗКИ АГРЕГИРОВАННЫХ ПОРТОВ КОММУТАТОРА

В данной статье рассматриваются общие сведения о технологии агрегирования портов. Внимание уделяется основным требованиям к параметрам порта для включения его в список логического агрегированного канала. Также рассматриваются основные методы балансировки нагрузки агрегированных портов коммутатора и принципы работы этих методов.

Ключевые слова: протокол, агрегирование, канал, балансировка, алгоритмы, основные понятия.

A.V. Zverev

Perm National Research Polytechnic University, Perm

LOAD-BALANCING METHODS OF THE AGGREGATED PORTS OF THE SWITCH

This article provides an overview of the port aggregation technology. Attention is paid to the basic requirements for port parameters to include it in the list of logical aggregated link. Also, the main methods of load balancing of switch aggregated ports are considered, and the principles of these methods.

Keywords: protocol, aggregation, channel, balancing, algorithms, basic concepts.

Информационная сеть часто состоит из нескольких коммутаторов. Соединение коммутаторов обычно происходит по одному магистральному порту, из-за этого существует ряд проблем:

– порт представляет собой единственную точку сбоя. Если порт отключится, то соединение магистрали будет потеряно;

– порт представляет собой узкое место для трафика. Все остальные порты коммутатора будут использовать один порт для связи по магистральному соединению.

Таким образом, очевидным преимуществом добавления избыточности к магистральному соединению являются **отказоустойчивость и увеличение пропускной способности**.

Одним из методов решения данных проблем является технология агрегирования портов. Она позволяет объединить несколько физиче-

ских портов в один логический. Данная технология не имеет какого-то общего названия, каждый вендер придумал этой технологии свое название, например, компания Cisco называет эту технологию Etherchannel, у Huawei – это Link Aggregation, а у D-Link – LAG[1].

Данная технология поддерживает только 8 активных агрегированных портов в одном логическом канале. Реализация данной технологии для магистральных соединений обеспечивает повышенную пропускную способность и резервирование для других коммутаторов. Если один из агрегированных портов выйдет из строя, то трафик будет перераспределен между остальными портами в логическом канале. И для того чтобы этот логический канал стал активным, нужно чтобы все агрегированные порты были настроены одинаково. Настройки порта, которые должны быть идентичными, включают в себя [1]:

- настройки скорости;
- настройки дуплекса;
- настройки STP-протокола;
- членство в VLAN (для портов доступа);
- Native VLAN (для магистральных портов);
- Allowed VLAN (для магистральных портов);
- протокол инкапсуляции (для магистральных портов).

При подключении по магистрали указанные выше параметры должны быть настроены одинаково для всех участвующих портов на обоих коммутаторах. Трафик, передаваемый по логическому каналу, неравномерно распределяется по всем агрегированным портам. Вместо этого используют алгоритмы балансировки нагрузки для определения порта отправки трафика на основе одного из нескольких критериев, указанных в табл. 1.

Таблица 1

Методы балансировки нагрузки в логическом канале

Тип балансировки	Описание	Алгоритм хэширования
src-ip	IP-адрес источника	Bits
dst-ip	IP-адрес назначения	Bits
src-dst-ip	IP-адрес источника и получателя	XOR
src-mac	MAC-адрес источника	Bits
dst-mac	MAC-адрес назначения	Bits
src-dst-mac	Исходный и конечный MAC	XOR
src-port	Номер порта источника	Bits
dst-port	Номер порта назначения	Bits
src-dst-port	Порт источника и назначения	XOR

Использование детерминированного алгоритма предотвращает идеальную балансировку нагрузки. Однако конкретный поток трафика вынужден всегда использовать один и тот же порт. Метод балансировки нагрузки должен быть настроен на коммутаторе глобально [2].

Рассмотрим пример, где порты gi2/23 и gi2/24 на обоих коммутаторах являются элементами рассматриваемой технологии. Пример соединения коммутаторов показан на рисунке.

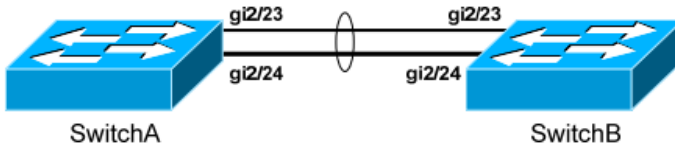


Рис. Пример соединения коммутаторов

Предположим, что методом балансировки нагрузки является src-ip. Порт gi2/23 станет логическим портом ch0, а порт gi2/24 станет логическим портом ch1. Два логических порта в агрегированном канале могут быть представлены в двоичном коде, и алгоритм балансировки нагрузки создаст индекс, который свяжет ch0 двоичным битом 0, а с ch1 с двоичным битом 1. Когда трафик проходит через логический канал, алгоритм преобразует исходные IP-адреса в двоичный хэш для сравнения с индексом.

К примеру, рассмотрим следующие адреса и их двоичные эквиваленты:

192.168.1.10 – 11000000.10101000.00000001.00001010

192.168.2.25 – 11000000.10101000.00000010.00011001

Поскольку в логическом канале всего два порта, в IP-адресе необходимо учитывать только один последний бит. Первый адрес заканчивается битом 0 и таким образом будет отправлен по логическому порту ch0, а второй адрес заканчивается битом 1 и, следовательно, будет отправлен по логическому порту ch1.

Для логического канала, содержащего четыре порта, потребуется двухбитный индекс, требующий учета последних двух битов IP-адреса: ch0 – 00, ch1 – 01, ch2 – 10, ch3 – 11.

Для равномерной балансировки нагрузки лучше использовать четное количество агрегированных портов.

Рассмотрим следующий пример, в соответствии с рисунком только в этом случае будет использоваться метод балансировки нагрузки src-dst-ip. И опять же порт gi2/23 станет логическим портом ch0, а порт gi2/24 станет логическим портом ch1.

При выборе логического порта необходимо учитывать IP-адрес источника и получателя. Для этого требуется выполнить операцию, **исключающую ИЛИ (XOR)**. В табл. 2 показан результат с 1-разрядным индексом.

Таблица 2

Операция XOR с 1-разрядным индексом

Source	0	1	0	1
Destination	0	0	1	1
Result	0	1	1	0

Рассмотрим такую же пару IP-адресов только уже в качестве источника и получателя:

Source: 192.168.1.10 – 11000000.10101000.00000001.00001010

Destination: 192.168.2.25 – 11000000.10101000.00000010.00011001

Результат операции XOR для вышеуказанной пары адресов будет равен 1, таким образом, трафик будет отправлен по логическому каналу ch1.

В табл. 3 показаны все возможные результаты с 2-разрядным индексом. Четыре возможных результата (00, 01, 10, 11) соответствуют четырем логическим портам, как это было изложено ранее.

Таблица 3

Операция XOR с 2-разрядным индексом

Source	00	00	00	00	01	01	01	01	10	10	10	10	11	11	11	11
Destination	00	01	10	11	00	01	10	11	00	01	10	11	00	01	10	11
Result	00	01	10	11	01	00	11	10	10	11	00	01	11	10	01	00

Независимо от используемого метода балансировки нагрузки STP-протокол будет всегда отправлять свои пакеты через первый используемый порт в связке агрегированных портов.

Библиографический список

1. CISCO. Балансировка загрузки канала EtherChannel и избыточность на коммутаторах Catalyst [Электронный ресурс]. – URL: https://www.cisco.com/c/ru_ru/support/docs/lan-switching/etherchannel/12023-4.html (дата обращения: 12.12.2021).

2. Cisco Certified Expert. Configuring Ether Channel Load Balancing [Электронный ресурс]. – URL: <https://www.ccexpert.us/root-bridge/configuring-etherchannel-load-balancing.html> (дата обращения: 11.12.2021).

Сведения об авторе

Зверев Артем Витальевич – магистрант кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, гр. ТК5-20-1М, Пермь, e-mail: zverev.artiom@mail.ru

О.А. Коноваленко, Л.А. Клейман

Пермский национальный исследовательский
политехнический университет, Пермь

МОДЕЛИРОВАНИЕ TCP-СЕРВЕРА И КЛИЕНТА

Целями данного исследования являются моделирование TCP-сервера и клиента и реализация защиты HTTP-сервера от атак в виде HTTP-флуда. Актуальность темы моделирования сервера и клиента – телекоммуникационная отрасль деятельности, которая служит основой телекоммуникационных сетей, жизненно необходимых для существования любой современной сложной общественной структуры. TCP естественным образом интегрируется в среду клиент/сервер. Серверное приложение прочитывает поступающие запросы на соединение. Доступ с терминала – прослушивание запросов, поступающих от клиентов. Связь в TCP запускается соответствующими подпрограммами, которые инициализируют соединение с сервером. Цель защиты от атак заключается в том, чтобы заставить сервер не выделять как можно больше ресурсов для обслуживания атак, тем самым лишая доступ к ресурсам.

Ключевые слова: моделирование TCP-сервера и клиента, HTTP-флуд, защита.

O.A. Konovalenko, L.A. Clayman

Perm National Research Polytechnic University, Perm

SIMULATING TCP SERVER AND CLIENT

The subject of this research is the modeling of a TCP server and client, the implementation of the protection of the HTTP server against attacks in the form of HTTP flooding. The relevance of the topic of server and client modeling is a telecommunication branch of activity that serves as the basis for communication networks vital for the existence of any modern complex social structure. TCP integrates naturally into the client / server environment. The server application reads the incoming connection requests. Terminal Access - Listening to requests from clients. Communication in TCP is started by the corresponding subroutines, which initialize the connection to the server. The goal of attack protection is to prevent the server from allocating as many resources as possible to service attacks, thereby denying access to resources.

Keywords: TCP server and client modeling, HTTP flood, protection.

В современных системах автоматизации, в результате постоянной модернизации производства все чаще встречаются задачи построения распределенных промышленных сетей с использованием гибких протоколов передачи данных. Телекоммуникационные сети стали частью нашей жизни. Создание электронных проектов, которые

взаимодействуют с реальным миром, – прекрасное развлечение. Но когда устройства начинают взаимодействовать еще и друг с другом, то это становится не только интересно, но и полезно [1].

Последнее время большую популярность приобрел программно-аппаратный комплекс Arduino, который предназначен для разработки различных интересных электронных конструкций. Конструкции создаются путем соединения основной платы Arduino с дополнительными модулями. На основной плате Arduino находится микроконтроллер, прошивка на которой пишется в специальной среде разработки для Arduino с использованием готовых библиотек для конкретного модуля. Сегодня комплекс Arduino и его конкретные модули можно использовать в разных направлениях. Например, это может быть робот, «умный дом», удаленная активация модулей через веб-браузер и тому подобное [2].

Основы протокола. Протокол передачи данных/гипертекста (HTTP) – протокол передачи данных. Первоначально предназначался для передачи гипертекстовых документов (ссылок), осуществляющих переход к другим документам. Участник обмена – клиентское приложение, которое создает запрос и производит отправку на сервер. После поступления запроса программное обеспечение (ПО) обрабатывает его, формирует ответ и обратную передачу клиенту.

Протоколы связи. С появлением технологий удаленного управления устройствами через Интернет актуальной задачей стала авторизация на серверах. Одной из самых популярных являются веб-серверы, разработанные на основе микроконтроллеров, и наиболее распространенные находятся в составе контроллеров Arduino. В отличие от современных компьютеров Arduino – это скромный вычислительный ресурс, который не способен работать с полноценными сетевыми протоколами. Команды управления устройством отправляются с браузера клиента на веб-сервер Arduino без пароля идентификации [3].

Локальная сеть Ethernet. Модуль ENC28J60 и его подключение к плате. Ethernet – сетевой интерфейс или стандарт, предназначенный для построения локальных сетей. Ethernet взаимодействует с первым и вторым уровнем в терминах семиуровневой модели OSI. На первом уровне модели OSI – физическая передача сигналов, а формирование кадров – второй уровень [9]. В качестве среды передачи данных будут использоваться только две неэкранированные витые пары (4 провода). Одна витая пара предназначена для передачи данных,

другая для приема [4]. Для подключения к портам Ethernet используются 8-контактные разъемы RJ-45. Для подключения платы Arduino к сети Ethernet будет использоваться модуль ENC28J60 (рис. 1) [5].



Рис. 1. Модуль ENC28J60

TCP-сервер. Инициировать обмен данными будет компьютер. Наша задача заключается в отправке данных. Целостность и доставка пакетов данных обеспечиваются протоколом TCP (рис. 2).

```
// TCP сервер, возвращает полученные данные
#include <SPI.h>
#include <UIPEthernet.h>
// определяем конфигурацию сети
byte mac[] = {0xAE, 0xB2, 0x26, 0xE4, 0x4A, 0x5C}; // MAC-адрес
byte ip[] = {192, 168, 1, 10}; // IP-адрес
byte myDns[] = {192, 168, 1, 1}; // адрес DNS-сервера
byte gateway[] = {192, 168, 1, 1}; // адрес сетевого шлюза
byte subnet[] = {255, 255, 255, 0}; // маска подсети
EthernetServer server(2000); // создаем сервер, порт 2000
EthernetClient client; // объект клиент
boolean clientAlreadyConnected= false; // признак клиент уже
подключен
void setup() {
  Ethernet.begin(mac, ip, myDns, gateway, subnet);
  // инициализация контроллера
  server.begin(); // включаем ожидание входящих соединений
  Serial.begin(9600);
  Serial.print("Server address:");
  Serial.println(Ethernet.localIP()); // выводим IP-адрес
  контроллера
}
void loop() {
  client = server.available(); // ожидаем объект клиент
  if (client) {
    // есть данные от клиента
    if (clientAlreadyConnected == false) {
      // сообщение о подключении
      Serial.println("Client connected");
      client.println("Server ready"); // ответ клиенту
      clientAlreadyConnected= true;
    }
    while(client.available() > 0) {
      char chr = client.read(); // чтение символа
      server.write(chr); // передача клиенту
      Serial.write(chr);
    }
  }
}
```

Рис. 2. Скетч сервера

Локальный контроллер в данной работе будет выступать сервером, поскольку используется TCP-протокол, то TCP-сервер. Компьютер в данной задаче будет выступать клиентом. Для создания клиента будет использована программа TCP/IP Buidер. Через нее будут передаваться данные на локальный контроллер (на плату Arduino). Данные, полученные через контроллер, будут выводиться в последовательный порт Arduino IDE, а данные ответа от контроллера будут выводиться на компьютер через TCP/IP Buidер [6].

Программа TCP/IP Buidер позволяет создавать TCP-серверы и клиенты на компьютере и подключать виртуальные COM-порты [8].

Параметры конфигурации сети можно посмотреть с помощью командной строки (cmd).

Для просмотра конфигурации сетевых устройств используется команда ipconfig/all (рис. 3). Она отображает настройки сетевых плат.

```
C:\Users\Ed>ipconfig/all
Настройка протокола IP для Windows

Имя компьютера . . . . . : Ed-PC
Основной DNS-суффикс . . . . . : 
Тип узла . . . . . : Гибридный
IP-вертуализация включена . . . . . : Нет
WINS-прокси включен . . . . . : Нет
Порядок просмотра суффиксов DNS . . . . . : HomeGateway

Ethernet adapter Подключение по локальной сети:

DNS-суффикс подключения . . . . . : HomeGateway
Описание . . . . . : Realtek PCIe FE Family Controller
Физический адрес . . . . . : 00-1A-13-19-26-5D
DHCP включен . . . . . : Да
Автонастройка включена . . . . . : Да
Локальный IPv6-адрес канала . . . . . : fe80::ac22:828a:3219:592d%18<Основной>
IPv4-адрес . . . . . : 192.168.1.2<Основной>
Маска подсети . . . . . : 255.255.255.0
Аренда получена . . . . . : 22 февраля 2018 г. 17:45:36
Срок аренды истекает . . . . . : 26 февраля 2018 г. 10:14:50
Основной шлюз . . . . . : 192.168.1.1
DHCP-сервер . . . . . : 192.168.1.1
IAD DHCPv6 . . . . . : 436214291
DUID клиента DHCPv6 . . . . . : 00-01-00-01-1A-8E-4F-36-00-1A-13-17-DF-15

DNS-серверы . . . . . : 192.168.1.1
NetBios через TCP/IP . . . . . : Включен

Адаптер беспроводной локальной сети Беспроводное сетевое соединение:

Состояние среды . . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . : 
Описание . . . . . : Плата беспроводных сетей 802.11n Wireless LAN
Физический адрес . . . . . : 00-1A-13-17-DF-15
DHCP включен . . . . . : Да
Автонастройка включена . . . . . : Да

Туннельный адаптер isatap.HomeGateway:

Состояние среды . . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . : HomeGateway
Описание . . . . . : Адаптер Microsoft ISATAP
Физический адрес . . . . . : 00-00-00-00-00-00-E0
DHCP включен . . . . . : Нет
Автонастройка включена . . . . . : Да
```

Рис. 3. Использование команды ipconfig

Для просмотра MAC-адреса используется команда getmac (рис. 4).

```
C:\Users\konovalenko>getmac

Физический адрес      Имя транспорта
-----
84-D4-C4-02-6C-4E     \Device\NPF{2F5E3855-7863-4788-8469-E0A56AC9810C}
```

Рис. 4. Использование команды getmac

Для соответствия IP- и MAC-адреса можно посмотреть с помощью команды arp -a (рис. 5) и проверить связь с сетевым устройством с помощью команды ping (рис. 6).

```
C:\Users\konovalenko>arp -a

Интерфейс: 192.168.1.113 --- 0x9
адрес в Интернете      Физический адрес      Тип
192.168.1.1            cc-2d-e0-91-63-34     динамический
192.168.1.2            74-da-88-34-8e-8f     динамический
192.168.1.3            98-da-c4-44-86-69     динамический
192.168.1.5            4a-5a-b4-89-45-a5     динамический
192.168.1.9            a6-e5-69-ea-d4-58     динамический
192.168.1.12           98-0d-67-f7-ba-2e     динамический
192.168.1.14           00-d0-b8-1e-ae-97     динамический
192.168.1.15           88-ac-c0-3e-07-74     динамический
192.168.1.17           3c-ec-ef-29-5a-7e     динамический
192.168.1.25           4a-70-b3-0c-d2-4b     динамический
192.168.1.90           00-bb-c1-77-3e-b8     динамический
192.168.1.91           00-bb-c1-76-1f-3f     динамический
192.168.1.92           00-bb-c1-76-d3-22     динамический
192.168.1.94           00-bb-c1-79-24-4b     динамический
192.168.1.101          04-d9-f5-ad-a3-77     динамический
192.168.1.106          04-d9-f5-ad-a2-ed     динамический
192.168.1.109          d4-5d-64-b5-3a-36     динамический
192.168.1.112          d8-d3-85-c0-d2-7e     динамический
192.168.1.116          d4-3d-7e-4b-f4-c8     динамический
192.168.1.117          74-d0-2b-cb-05-44     динамический
192.168.1.255          ff-ff-ff-ff-ff-ff     статический
224.0.0.2              01-00-5e-00-00-02     статический
224.0.0.22             01-00-5e-00-00-16     статический
224.0.0.251            01-00-5e-00-00-fb     статический
224.0.0.252            01-00-5e-00-00-fc     статический
239.255.102.18         01-00-5e-7f-66-12     статический
239.255.255.250        01-00-5e-7f-ff-fa     статический
255.255.255.255        ff-ff-ff-ff-ff-ff     статический
```

Рис. 5. Использование команды arp -a

```
Обмен пакетами с pwrastic.ru [31.31.196.216] с 32 байтами данных:
Ответ от 31.31.196.216: число байт=32 время=60мс TTL=54
Ответ от 31.31.196.216: число байт=32 время=61мс TTL=54
Ответ от 31.31.196.216: число байт=32 время=61мс TTL=54
Ответ от 31.31.196.216: число байт=32 время=61мс TTL=54

Статистика Ping для 31.31.196.216:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  (0% потерь)
Приблизительное время приема-передачи в мс:
  Минимальное = 60мсек, Максимальное = 61 мсек, Среднее = 60 мсек
```

Рис. 6. Использование команды ping

Проверка работоспособности с TCP/IP Buider. При подключении, когда приходят первые данные без потери, он выдает сообщение «клиент подключен» и передает обратное сообщение клиенту.

Проверка IP-адреса контроллера. В данном окне должно отобразиться следующее (рис. 7).

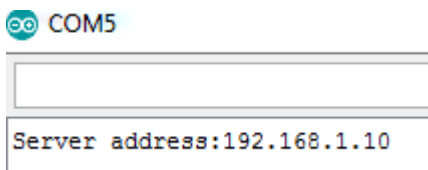


Рис. 7. Проверка IP-адреса контроллера

В окне монитора последовательного порта будут выводиться данные, поступающие на сервер (рис. 8).

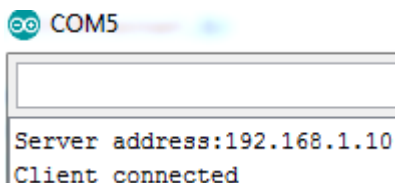


Рис. 8. Поступающие данные

Методы атак и защиты на TCP-сервер. Самым альтернативным способом защиты от небольшого HTTP-флуда является использование утилиты (D)DoS Deflate. Работа данной утилиты заключается в получении количества подключений с одного IP, делается с помощью утилиты netstat.

```
netstat -n -p
```

Данная защита имеет недостаток: нельзя подобрать оптимальное значение количества соединений с одного IP, которое считается атакой, так как провайдеры Интернета используют систему NAT, где пользователи имеют одинаковый статический IP. Сайт может генерировать разное количество запросов с одного IP, как пример – поиск картинок. Поиск может выдать 10 и более результатов, где ресурс – это запрос с IP [7].

Альтернативным решением будет подключение nginx-модуля – ngx_http_limit_req_module. Он позволяет ограничивать количество

одновременных подключений с одного адреса. Отсеять ботов в логах можно с помощью команды:

Листинг 2. Отсеивание ботов:

```
tail -1000 /var/log/nginx-access.log | grep "503" | cut -f1 -d "
" | sort -u
```

После данных манипуляций следует занести их в таблицу фаервола.

Для отслеживания лишних URL-запросов добавляем строки в конфигурационный файл:

Листинг 3. Отслеживание запросов:

```
#vi /etc/sysctl.conf
# Защита
net.ipv4.conf.default.rp_filter = 1
#Проверка TCP-соединения каждые 90 секунд, для ответа на другой
стороне.
net.ipv4.tcp_keepalive_time = 90
#Кол-во проверок перед закрытием соединения
net.ipv4.tcp_keepalive_probes = 5
```

Заключение. В данной статье были рассмотрены моделирование TCP-сервера и клиента на основе платы Arduino, защита от HTTP-флуда. Данная платформа предоставляет широкий функционал для моделирования различных сетей и оборудования.

Сегодня моделирование TCP-сервера и клиента – довольно развивающаяся телекоммуникационная отрасль. И одним из основных и нужных направлений является защита от HTTP-флуда. Реализация защиты проводилась в целях предотвратить поддельный трафик от полезного, посылающий стандартные URL-запросы.

Библиографический список

1. Связь в России [Электронный ресурс] // Mozilla. – URL: <https://developer.mozilla.org/ru/docs/Web/HTTP/Overview> (дата обращения: 11.11.2021).

2. Создание собственной сети самодельных устройств на базе Arduino [Электронный ресурс] // Habr. – URL: <https://habr.com/ru/post/414225/> (дата обращения: 10.12.2021).

3. Протоколы связи в АСУ ТП [Электронный ресурс] // Plcsystems. – URL: <https://plcsystems.by/articles/651> (дата обращения: 8.01.2021).

4. Подключение Ethernet-модуля ENC28J60 к Arduino [Электронный ресурс] // Iarduino. – URL: <https://iarduino.kz/blog/connect-enc28j60-to-arduino.html> (дата обращения: 13.10.2021).

5. Простой протокол с гарантированной доставкой для Arduino [Электронный ресурс] // Habr. – URL: <https://habr.com/ru/post/480110/> (дата обращения: 8.11.2021).

6. Arduino TCP Server [Электронный ресурс] // Arduino. – URL: <http://arduino.ru/forum/programmirovanie/arduino-tcp-server> (дата обращения: 8.11.2021).

7. Модуль ngx_http_limit_req_module [Электронный ресурс] // Coderlessons. – URL: http://nginx.org/ru/docs/http/nginx_http_limit_req_module.html (дата обращения: 13.11.2021).

8. TCP сервер и клиент на Ардуино. Библиотека UIPEthernet [Электронный ресурс] // Coderlessons. – URL: <http://mypractic.ru/urok-64-tcp-server-i-klient-na-arduino-biblioteka-uipethernet.html> (дата обращения: 22.12.2021).

9. ETHERNET НА ПАЛЬЦАХ – ЧТО ЭТО? [Электронный ресурс] // Coderlessons. – URL: <https://wiki.merionet.ru/seti/29/ethernet-na-palцах-что-это/> (дата обращения: 20.12.2021).

Сведения об авторах

Коноваленко Олег Анатольевич – магистрант кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь.

Клейман Лев Александрович – аспирант, младший научный сотрудник кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: smarttty@yandex.ru

Р.А. Мудрый, А.В. Гаврилов

Пермский национальный исследовательский
политехнический университет, Пермь

АНАЛИЗ И СРАВНЕНИЕ ПРОТОКОЛОВ УПРАВЛЕНИЯ В СРЕДЕ ИНТЕРНЕТА ВЕЩЕЙ

Данная статья посвящена описанию основных протоколов, предлагаемых для использования в рамках концепции Интернета вещей. Актуальность данной темы обусловлена многообразием существующих протоколов Интернета вещей и отсутствием устоявшейся терминологии, сравнительных данных протоколов, описывающих концепцию в целом. Цель краткого анализа протоколов управления в среде Интернета вещей состоит в том, чтобы структурировать основные протоколы в целом и рассмотреть их достоинства и недостатки.

Ключевые слова: протокол IoT, Интернет вещей, достоинства и недостатки, стандарты.

R.A. Mudriy, A.V. Gavrilov

Perm National Research Polytechnic University, Perm

ANALYSIS AND COMPARISON OF CONTROL PROTOCOLS IN THE INTERNET OF THINGS ENVIRONMENT

This article is devoted to the description of the main protocols proposed for use in the framework of the concept of the Internet of Things. The relevance of this topic is due to the variety of existing protocols of the Internet of Things and the lack of an established terminology, comparative data of protocols and describing the concept as a whole. The purpose of this brief analysis of control protocols in the Internet of Things environment is to structure the underlying protocols in general and consider their advantages and disadvantages.

Keywords: IoT protocol, Internet of Things, advantages and disadvantages, standards.

Современная тенденция развития общества характеризуется огромным влиянием на него компьютерных технологий, которые углубляются во все сферы человеческой деятельности, обеспечивают распространение информационных потоков в обществе, создавая глобальное информационное пространство.

Самая быстрорастущая система – это система Интернета вещей. Ее концепция заключается в развитии интернет-технологий в области автоматизации и исключения человеческого участия из большинства

процессов работы ИТ-инфраструктуры. Создано огромное количество систем, датчиков, сенсоров, камер и программного софта для автоматизации процессов. Поэтому для каждой системы придумывают и разрабатывают собственные протоколы управления и мониторинга, самые основные протоколы разберем в данной статье.

Протокол MQTT – это сетевой протокол обмена сообщениями между устройствами с низкой пропускной способностью, реализованный по модели «ведущий–ведомый» (рис. 1).

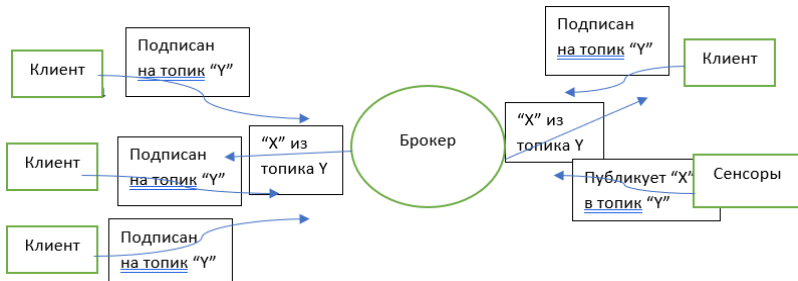


Рис. 1. Архитектура MQTT

Работает поверх протокола TCP/IP, который предоставляет надежный поток данных. Протокол ориентирован на сеть небольших устройств, которыми можно управлять или контролировать удаленно. Также он разрабатывался для «многоадресной передачи» данных на многие приемники. Ключевые особенности протокола: асинхронный протокол, простая интеграция новых устройств, компактность сообщений, работа в нестабильных условиях связи по линии передачи данных и поддержка нескольких уровней качества обслуживания (QoS).

Протокол предоставляет разные уровни услуг для разных типов инфраструктуры Интернета вещей, от выборки данных до управления промышленными машинами: биллинговые системы, информация, поступающая с датчиков окружающей среды, данные о работоспособности машин.

Протокол MQTT наделен некоторыми преимуществами, среди которых стоит выделить:

- нейтралитет по отношению к содержимому сообщений: любая информация может быть передана;
- существование версии Last Will and Testament (LWT), которая объявляет о неожиданном завершении работы издателя или брокера;

- подходит как для распределенных коммуникаций, так и для автономных приложений;
- работает по типовым шаблонам: «ровно один раз», «хотя бы один раз» и «максимум один раз»;
- TCP/IP вполне подходит для решения основных задач связи;
- один и тот же пользователь может одновременно выполнять роль «потребителя» и «издателя».

Система связи на основе MQTT состоит из сервера-публикации, брокерского сервера и одного или нескольких клиентов. Издатель не требует никаких корректировок относительно количества или местоположения подписчиков, получающих сообщения. Кроме того, подписчиков не нужно настраивать для конкретного издателя. В системе может быть несколько брокеров, которые распространяют сообщения [1].

Протокол MQTT-SN (MQTT для сенсорных сетей) был разработан специально для работы в беспроводных сетях и работает так же, как MQTT, однако адаптирован к характеристикам беспроводной среды передачи данных, таким как: высокая вероятность сбоя в соединениях, низкая пропускная способность, короткая длина сообщения и т.п. Перечисленные особенности позволяют применять его в системах M2M и IoT.

Основные отличия MQTT-SN и MQTT заключаются в следующем:

- уменьшен размер сообщений;
- устранена необходимость в постоянном подключении за счет использования UDP в качестве транспортного протокола [2].

Архитектура протокола MQTT-SN. На рис. 2 показаны три компонента: MQTT-SN-клиенты, MQTT-SN-шлюз, MQTT-SN и сервер пересылки.

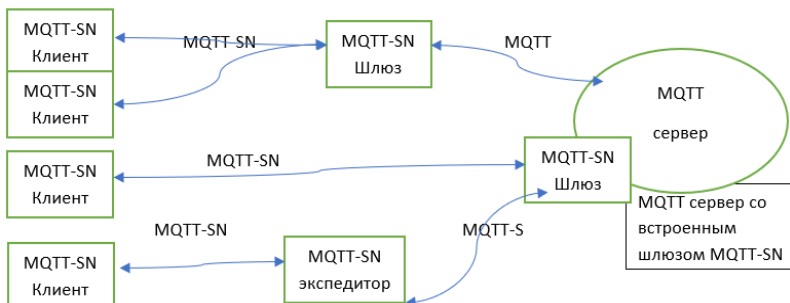


Рис. 2. Архитектура MQTT-SN

Клиенты MQTT-SN подключаются к MQTT серверу через MQTT-SN-шлюзы. В случае автономного шлюза протокол MQTT используется между сервером MQTT и шлюзом MQTT-SN. Шлюз MQTT-SN является основной функцией двусторонней «синтаксической» трансляции MQTT-SN ↔ MQTT. Экспедитор MQTT-SN отвечает за возможность отправки и получения сообщений через него, если шлюз недоступен для клиентов. Сервер MQTT – системное ядро, отвечающее за отправку сообщений [3].

Протокол CoAP – протокол, разработан для взаимодействия простых устройств и описан в документе RFC 7252 (рис. 3).

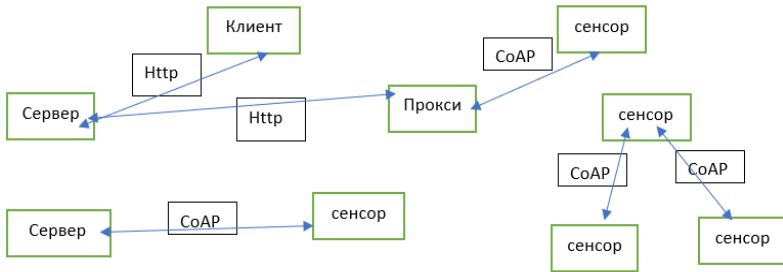


Рис. 3. Архитектура CoAP

Протокол функционирует на прикладном уровне и разработан для передачи данных по линиям с ограниченной полосой пропускания. Модель связи CoAP аналогична модели клиент-сервер HTTP. Однако межмашинные взаимодействия обычно приводят к реализации CoAP, который действует как клиент и как сервер. Обмен CoAP равнозначен обмену HTTP и отправляется клиентом для запроса операции с ресурсом на сервере. Затем отправляется ответ с кодом ответа и, если необходимо, представлением ресурса.

CoAP в отличие от HTTP обрабатывает эти обмены асинхронно через транспорт UDP с поддержкой как одноадресных, так и многоадресных взаимодействий.

Многоадресная передача, низкие накладные расходы и простота важны для связи в IoT и между машиной, которые, как правило, глубоко встроены и имеют гораздо меньше памяти и источника питания, чем у традиционных устройств. CoAP может работать на большинстве устройств, поддерживающих UDP или аналог UDP, также может быть использован поверх других транспортных средств, таких как TCP или SCTP и в безопасности транспортного уровня дейтаграмм (DTLS).

Целью привязки CoAP к UDP является обеспечение минимальной функциональности протокола для работы через UDP без попытки воссоздать полную транспортную функциональность, такую как TCP [4].

Протокол LwM2M. Стандарт LwM2M был разработан организацией по стандартизации OMA SpecWorks на основе стандартов 3GPP. Широко применяется в среде разработки компонентов Интернета вещей. В нем используется как UDP в качестве протокола связи, так и TCP, который может быть полезен при обходе ограничений брандмауэра/NAT и в целом обеспечивает более надежную передачу данных (рис. 4).

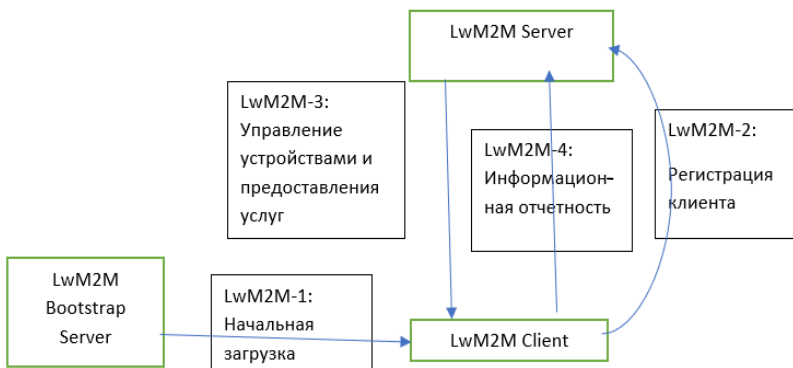


Рис. 4. Архитектура LwM2M

Архитектура LwM2M поддерживает четыре логических интерфейса, которые помогают стандартизировать способ реального управления устройством и телеметрии:

- интерфейс начальной загрузки – этот интерфейс позволяет управлять устройством без подключения к сети;
- интерфейс регистрации клиента – информирует сервер о «существовании» клиента и поддерживаемых функциях;
- интерфейс управления устройством и предоставления услуг – lwm2m позволяет изменять настройки и параметры устройства;
- интерфейс информационных отчетов – позволяет получать отчеты об ошибках с устройств, когда служба больше не работает должным образом, а также отправлять запросы о состоянии устройства.

Стандарт LwM2M, основанный на протоколе CoAP, благодаря встроенному управлению перегрузками, блочной передаче фрагмен-

тов данных, эффективному кодированию заголовков и полезной нагрузки, а также независимый от транспорта может использоваться для всех видов развертывания Интернета вещей (таблица) [5].

Сравнение протоколов CoAP, MQTT, LwM2M

Функции	CoAP	MQTT	LwM2M
Назначение протокола	Протокол для сетей с ограниченными ресурсами	Протокол связи для передачи сообщений между несколькими клиентами	Управления и предоставления сервисов устройствам Интернета вещей
Модель общения	Запрос-ответ, публикация-подписка	Публикация–Подписка	Клиент-сервер
Транспортный уровень	UDP, TCP	Предпочтительно TCP, также можно использовать UDP	UDP, SMS, TCP, NIDD, LoRaWan
Размер заголовка	4 байта	2 байта	4 байта
Количество типов сообщений	4	16	25
Обмен сообщениями	Асинхронный и синхронный	Асинхронный	Асинхронный
Безопасность	IPSEC или DTLS	Не определено в стандарте	TLS, DTLS 1.2+
Посредники	Да	ДА (MQTT-S)	Да
Область применения	Коммунальные полевые сети	Промышленные сети IoT	Разработан для устройств с ограниченными ресурсами во всех областях

Заключение. Концепция Интернета вещей придумана давно. Список задач, которые решают электронные устройства, велик и продолжает расти.

Разрабатываются новые протоколы для общения устройств, и каждый из них хорош в своей среде.

Протоколы приспособляются работать в сетях с низкой работоспособностью и в тех средах, где важна каждая мельчащая деталь.

Библиографический список

1. LwM2M vs MQTT: в чем разница? [Электронный ресурс]. – URL: <https://www.avssystem.com/blog/lwm2m-vs-mqtt-comparison/> (дата обращения: 10.12.2021).

2. Введение в MQTT-SN [Электронный ресурс]. – URL: <http://www.steves-internet-guide.com/mqtt-sn/> (дата обращения: 19.12.2021).

3. Протокол MQTT-SN [Электронный ресурс]. – URL: https://libeldoc.bsuir.by/bitstream/123456789/40038/1/Каптыуг_Protokol.pdf (дата обращения: 24.12.2021).

4. Протокол ограниченного приложения – Constrained Application Protocol [Электронный ресурс]. – URL: https://ru.abcdef.wiki/wiki/Constrained_Application_Protocol (дата обращения: 23.12.2021).

5. LwM2M – облегченный стандарт M2M [Электронный ресурс]. – URL: <https://www.avsystem.com/blog/lightweight-m2m-lwm2m-overview/> (дата обращения: 21.12.2021).

Сведения об авторах

Мудрый Руслан Александрович – магистрант кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, гр. ТК-20-1м, Пермь, e-mail: ruslan38925@yandex.ru

Гаврилов Алексей Викторович – старший преподаватель кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: gaval74@mail.ru

А.К. Обыденнов, А.А. Южаков

Пермский национальный исследовательский
политехнический университет, Пермь

МАШИННЫЙ ПЕНТЕСТ КАК НОВЫЙ ЭТАП VAPT

Сетевая инфраструктура с каждым днем усложняется настолько быстро, что добавляет в систему все новые и новые уязвимости, которыми могут воспользоваться злоумышленники для нанесения вреда целостности и доступности или компрометации конфиденциальной информации, обрабатываемой на предприятиях. Именно поэтому становится критически важно узнавать об этих уязвимостях как можно раньше. Для решения данной проблемы используют тестирование на проникновение, которую очень часто недооценивают для решения вопросов кибербезопасности. В этой статье будут рассмотрены классический жизненный цикл VAPT (Vulnerability Assessment and Penetration Testing) и его обновленная форма с новым этапом машинного пентеста.

Ключевые слова: машинный пентест, VAPT, информационная безопасность.

A.K. Obydenov, A.A. Yuzhakov

Perm National Research Polytechnic University, Perm

MACHINE PENTEST AS A NEW VAPT STAGE

The network infrastructure is becoming more complex every day so quickly that it adds more and more vulnerabilities to the system that attackers can use to harm the integrity and availability or compromise confidential information processed at enterprises. That is why it becomes critically important to learn about these vulnerabilities as early as possible. To solve this problem, penetration testing is used, which is very often underestimated for solving cybersecurity issues. This article will review the classic lifecycle of VAPT (Vulnerability Assessment and Penetration Testing) and its updated form with a new stage of machine pentest.

Keywords: machine penetration test, VAPT, information security.

Классический жизненный цикл VAPT проходит через 9 обязательных шагов (рис. 1). На первом шаге определяются цели, которые планируются достичь в ходе тестирования, также оговаривается, в каком формате будет проходить тестирование на проникновение (белый ящик, черный ящик или же серый) [1].

Вторым обязательным шагом проходит разведка. В ходе разведки определяются структура сети испытываемой организации, используемые ею технологии в производственных процессах и, как следствие, обнаруживаются уязвимости [2].



Рис. 1. Жизненный цикл классического VAPT

Третьим шагом определяются наиболее выгодные, в плане используемых компьютерных ресурсов, и наиболее реализуемые уязвимости, которые можно эксплуатировать для дальнейшего тестирования на проникновения.

Четвертым шагом анализируется вся полученная информация и планируются дальнейшие действия для успешного пентеста. Также на этом шаге прогнозируются возможные результаты.

В пятом шаге на основе полученной информации и составленного плана с помощью специального программного обеспечения и найденных уязвимостей проводится сам пентест.

Шестой шаг представляет из себя задачу любой хакерской атаки – повышение привилегий путем эксплуатация найденных программных уязвимостей.

Седьмым шагом анализируют полученные результаты, даются оценка принятым мерам кибербезопасности и оценка уязвимостей.

На восьмом шаге формируется отчет о проведенном тестировании на проникновение. В этот отчет, как правило, входят:

- цели тестирования;
- объем проведенных работ;
- время, потраченное на тестирование;
- выводы, сделанные в ходе тестирования;
- рекомендации по устранению найденных уязвимостей.

Заключительным девятым шагом является возвращение исходного состояния взломанной информационной системы.

Для проведения оценки уязвимости и тестов на проникновения существует множество инструментов с открытым исходным кодом или платных решений. В таблице приведены 15 самых распространенных инструментов VAPT. [3]

Топ 15 инструментов проведения пентеста

№	Название	Тип	ОС
1	Kali Linux	Сборник инструментов	Linux
2	BlackHat	Сборник инструментов	Linux
3	Metasploit	Сканер уязвимостей	Cross-platform
4	w3af	Сканер web уязвимостей	Cross-platform
5	OpenVAS	Сканер уязвимостей	Cross-platform
6	Paros proxy	Сканер web уязвимостей	Cross-platform
7	Nessus	Сканер уязвимостей	Cross-platform
8	Core Impact	Сканер уязвимостей	Cross-platform
9	Burp Suite	Сканер web уязвимостей	Cross-platform
10	GFI LanGuard	Сканер уязвимостей	Windows
11	Acunetix WVS	Сканер web уязвимостей	Windows
12	MBSA	Сканер уязвимостей	Windows
13	AppScan	Сканер web уязвимостей	Windows
14	Bloodhound	Автоматизированный пентест	Linux
15	PenTera	Автоматизированный пентест	Linux

Отдельно стоит выделить набирающий популярность автоматизированный пентест, так как сам по себе пентест – процесс довольно дорогостоящий, и его необходимо проводить регулярно, чтобы всегда иметь актуальное представление о текущем состоянии защищенности информационной структуры предприятия. Поэтому неудивительно, что данный процесс решили автоматизировать, ведь даже сами злоумышленники уже редко вручную взламывают сети.

Автоматизированный пентест, на примере PenTera, представляет из себя набор указанных в таблице инструментов, куда входят всевозможные сканеры уязвимости и механизмы их эксплуатации, которые действуют практически без участия человека. Это работает следующим образом. Оператор задает начальные настройки программы:

- 1) указывает диапазон IP-адресов;
- 2) задает настройки скрытности;
- 3) в расширенных настройках указывает, какие уязвимости можно использовать, а какие – нет;
- 4) указывает время, когда начинать автоматизированный пентест.

В итоге, спустя какое-то время, как правило, продолжительное, выводятся результаты проведенного пентеста (рис. 2).

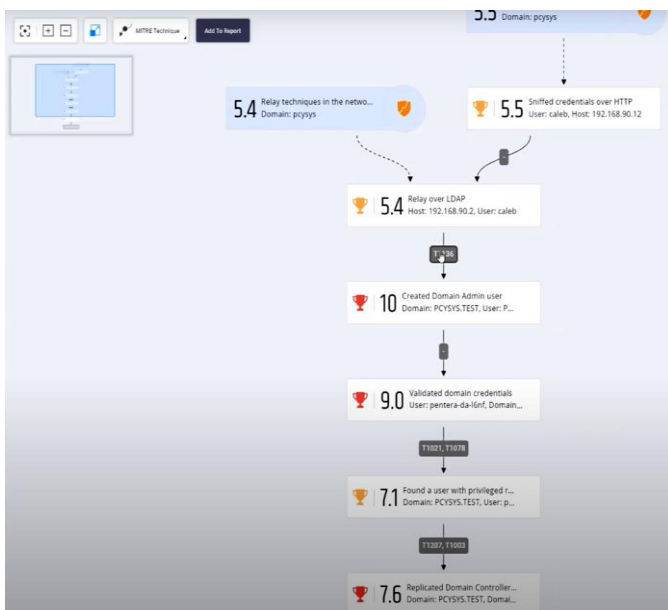


Рис. 2. Attack Map PenTera

Данные результаты чаще всего представляют в виде графа, в случае с PenTega данный граф называется Attack Map, где можно наглядно увидеть цепочку взаимосвязанных уязвимостей, которые позволяют злоумышленникам захватить информационную инфраструктуру предприятия.

Таким образом, предприятие с помощью машинного пентеста может регулярно поддерживать информацию о текущей защищенности информационной структуры в актуальном состоянии и вовремя устранять обнаруженные уязвимости. Современный жизненный цикл VAPT с использованием автоматизированного пентеста преобразился в более сложную блок-схему (рис. 3).

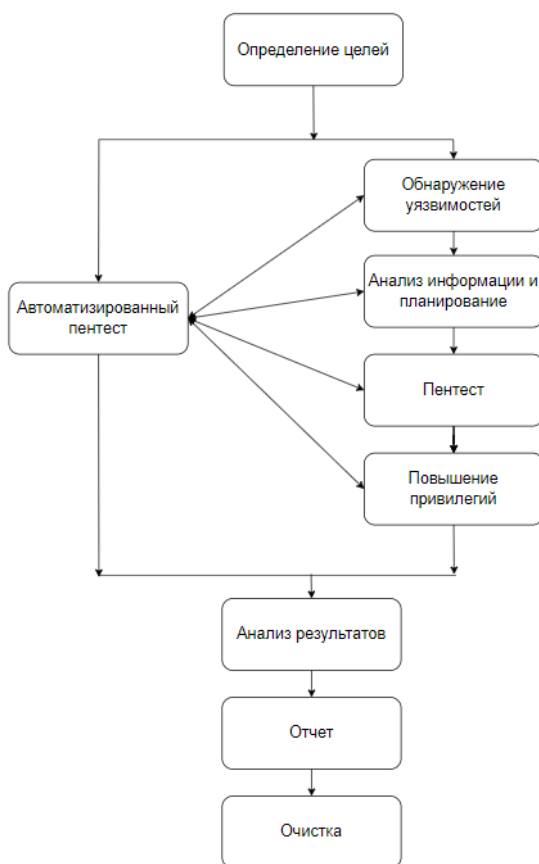


Рис. 3. Современный жизненный цикл VAPT

Теперь автоматизированный пентест без участия человека способен провести обнаружение уязвимостей, проанализировать информацию и построить граф для планирования дальнейших действий, провести сам пентест.

Однако автоматизированный пентест не может полностью заменить человека, так как он использует стандартные сценарии, взятые из сборника общих знаний, и при возникновении нетипичной ситуации машинный пентест остановится на месте. Поэтому наилучшим выбором будет совместное использование автоматизированного пентеста и человека. Таким образом, у предприятия будет более полное представление о всех возможных уязвимостях в ее информационной структуре.

Библиографический список

- 1 Kennedy D. Metasploit: The Penetration Tester's Guide. – 2011. – 118.
- 2 Shah S., Mehtre B.M. An overview of vulnerability assessment and penetration testing techniques // Journal of Computer Virology and Hacking Techniques. – 2014. – 1. – 328.
- 3 Clark B. Rtfm: Red Team Field Manual. – 2014. – 96.
- 4 Скабцовс Н.В. Аудит безопасности информационных систем. – СПб.: Профессия, 2003. – 272 с.

Сведения об авторах

Обыденнов Алексей Константинович – магистрант кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, гр. КЗИ-20-1м, Пермь, e-mail: ktj351@gmail.com

Южаков Александр Александрович – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: a.yuzhakov@mail.ru

А.Н. Кокоулин, Н.Е. Опутин

Пермский национальный исследовательский
политехнический университет, Пермь

АНАЛИЗ ХАРАКТЕРНЫХ ПРИЗНАКОВ ВИРУСОВ МАЙНЕРОВ С ПОМОЩЬЮ ДИНАМИЧЕСКОЙ ОЦЕНКИ

В процессе развития информационных технологий и информационного пространства большие изменения претерпели компьютерные угрозы. Появились новые разновидности компьютерных угроз – сетевые вирусы «майнеры». Для их обнаружения используют антивирусные программы, однако не все они обнаруживают вредоносную активность майнеров. Самостоятельно определить заражение можно по характерным признакам работы майнеров. В данной статье будет проведен анализ 4 образцов майнеров на их характерные признаки с помощью лабораторного стенда, с установленной операционной системой Windows 10.

Ключевые слова: майнинг, криптовалюта, вирусы майнеры, информационная безопасность.

A.N. Kokoulin, N.E. Oputin

Perm National Research Polytechnic University, Perm

ANALYSIS OF CHARACTERISTIC SIGNS OF MINER VIRUSES USING DYNAMICASSESSMENT

In the process of development of information technologies and information space, computer threats have undergone great changes. New types of computer threats have appeared - network viruses - miners. Antivirus programs are used to detect them, but not all of them detect malicious activity of miners. You can independently determine the infection by the characteristic signs of the miners' work. This article will analyze 4 samples of miners for their characteristic features using a laboratory bench with the Windows 10 operating system installed.

Keywords: mining, cryptocurrency, viruses miners, information security.

Динамическое исследование позволяет проанализировать зараженный файл во время его запуска, давая возможность посмотреть, как работает вирус в реальном времени. С помощью данного исследования были выявлены следующие характерные признаки работы майнеров.

Добавление в автозапуск. Образец 1 не добавляет себя в автозапуск, пользователь может запустить его сам, нажав на ярлык файла. Образец 2 добавляется в автозапуск с использованием ветки реестра (рис. 1).

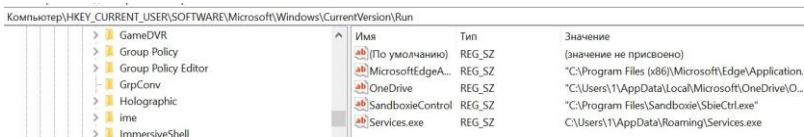


Рис. 1. Добавление в автозапуск. Образец 2

Образцы 3, 4 добавляют себя в автозапуск с помощью папки AppData (рис. 2, 3).

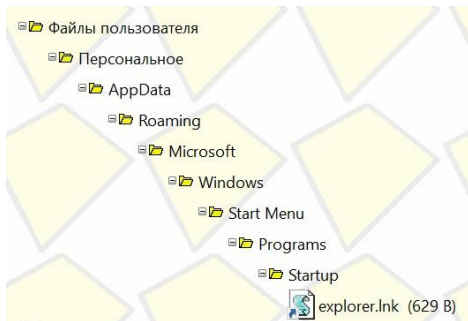


Рис. 2. Добавление в автозапуск. Образец 3

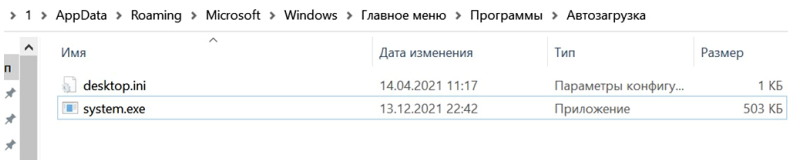


Рис. 3. Добавление в автозапуск. Образец 4

Маскировка под легальный файл. Для просмотра критерия «маскировка под легальный файл» необходимо обратиться к Диспетчеру задач, так как процесс отражается в нём.

Образец 1 маскируется под проводник, используя 26,3 % мощности центрального процессора, при этом ниже в Диспетчере задач есть настоящий процесс Проводник, который использует всего 0,3 % мощности центрального процессора (рис. 4).

Образец 2 маскируется под блокнот, но при запуске Диспетчера задач маскирует свою активность до 0 %, это один из способов скрыть свою активность, тогда активность майнера можно заметить с помощью программы AIDA64.

Имя	Состояние	33% ЦП	59% Память	0% Диск	0% Сеть	2% GPU	Ядро GPU
Проводник		26,3%	8,8 МБ	0 МБ/с	0 Мбит/с	0%	
Microsoft Edge (10)		2,3%	257,0 МБ	0,1 МБ/с	0 Мбит/с	0%	Графический процессор
Диспетчер задач		1,6%	29,1 МБ	1,8 МБ/с	0 Мбит/с	0%	
Диспетчер окон рабочего стола		0,9%	23,7 МБ	0 МБ/с	0 Мбит/с	0,2%	Графический процессор
AIDA64 Extreme (32 бита)		0,6%	71,2 МБ	0 МБ/с	0 Мбит/с	0%	
System		0,3%	0,1 МБ	0,2 МБ/с	0 Мбит/с	1,9%	Графический процессор
Проводник		0,3%	62,5 МБ	0 МБ/с	0 Мбит/с	0%	

Рис. 4. Маскировка под Проводник

Образец 3 пытается маскироваться под службу tasklist.exe.

Образец 4 маскируется под системную программу system.exe, оригинальный файл должен ссылаться на c:\Windows\System32, но данный файл запускается из папки C:\Users\1\AppData\Local\Temp.

Изменения в файловой системе. Образец 1, образец 2 при запуске создают файлы в папках, позволяя работать и использовать мощности компьютера. (рис. 5, 6).

Имя	Дата изменения	Тип	Размер
WR64.sys	13.12.2021 21:48	Системный файл	15 КБ

Рис. 5. Изменения в файловой системе. Образец 1

Имя	Дата изменения	Тип	Размер
ddb64.dll	15.11.2020 1:29	Расширение прилож...	20 143 КБ
nrvtc64_90.dll	15.11.2020 1:29	Расширение прилож...	16 897 КБ
nrvtc-builtins64_90.dll	15.11.2020 1:29	Расширение прилож...	3 108 КБ
WR64.sys	13.12.2021 22:11	Системный файл	15 КБ

Рис. 6. Изменения в файловой системе. Образец 2

Образец 3 создает в корне диска C папку Logs с файлами вируса для использования мощностей компьютера (рис. 7).

В образце 4 кроме файла, добавленного в автозагрузку, изменений не наблюдаются.

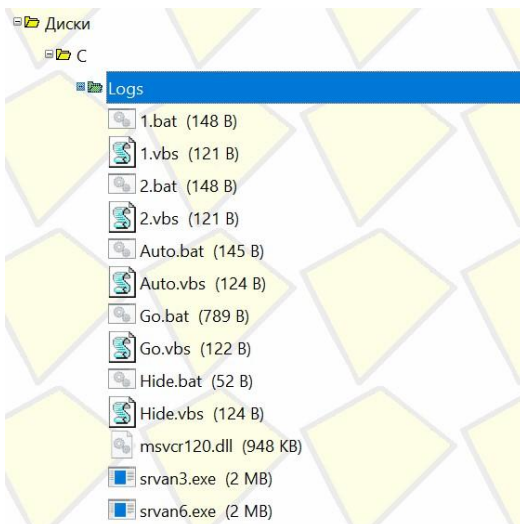


Рис. 7. Изменения в файловой системе. Образец 3

Сетевая активность. Для обнаружения сетевой активности, а именно определения, работают ли данные вирусы в пуле, используем программу Wireshark. Образец 1 при запуске программы показан на рис. 8.

No.	Time	Source	Destination	Protocol	Length	Info
2	0.786182	192.168.0.106	157.90.156.89	TCP	247	49911 → 6084 [PSH, ACK] Seq=1 Min=1025 Len=193 [TCP segment of a reassembled PDU]
3	0.824331	157.90.156.89	192.168.0.106	X11	117	Event: <unknown eventcode 123>
4	0.943780	192.168.0.106	157.90.156.89	TCP	54	49911 → 6084 [ACK] Seq=194 Ack=64 Min=1025 Len=0
10	4.681402	157.90.156.89	192.168.0.106	X11	359	Event: <unknown eventcode 115>Event: MappingNotify, MappingNotify, <unknown eventcode 100>, <unknown eventcode 101>
11	4.845396	192.168.0.106	157.90.156.89	TCP	54	49911 → 6084 [ACK] Seq=194 Ack=369 Min=1025 Len=0
43	16.808475	192.168.0.106	157.90.156.89	TCP	247	49911 → 6084 [PSH, ACK] Seq=194 Ack=369 Min=1023 Len=193 [TCP segment of a reassembled PDU]
44	16.862588	157.90.156.89	192.168.0.106	X11	117	Event: <unknown eventcode 186>Event: <unknown eventcode 110>
45	16.942856	192.168.0.106	157.90.156.89	TCP	54	49911 → 6084 [ACK] Seq=187 Ack=412 Min=1025 Len=0
46	19.681492	157.90.156.89	192.168.0.106	X11	359	Event: <unknown eventcode 115>Event: <unknown eventcode 112>, <unknown eventcode 51>, <unknown eventcode 52>
47	19.843077	192.168.0.106	157.90.156.89	TCP	54	49911 → 6084 [ACK] Seq=387 Ack=737 Min=1025 Len=0
50	21.375618	157.90.156.89	192.168.0.106	X11	859	Event: <unknown eventcode 123>, <unknown eventcode 58>, <unknown eventcode 53>, <unknown eventcode 54>
51	21.454863	192.168.0.106	157.90.156.89	TCP	54	49911 → 6084 [ACK] Seq=187 Ack=1042 Min=1025 Len=0
52	22.673366	192.168.0.106	157.90.156.89	TCP	248	49911 → 6084 [PSH, ACK] Seq=387 Ack=1042 Min=1026 Len=194 [TCP segment of a reassembled PDU]
53	22.731455	157.90.156.89	192.168.0.106	X11	118	Event: MappingNotifyEvent: MappingNotify
54	22.843811	192.168.0.106	157.90.156.89	TCP	54	49911 → 6084 [ACK] Seq=581 Ack=1206 Min=1026 Len=0
67	29.282879	157.90.156.89	192.168.0.106	X11	359	Event: MappingNotifyEvent: <unknown eventcode 44>, <unknown eventcode 46>, <unknown eventcode 47>
68	29.355132	192.168.0.106	157.90.156.89	TCP	54	49911 → 6084 [ACK] Seq=581 Ack=1411 Min=1025 Len=0
70	31.075064	192.168.0.106	157.90.156.89	TCP	248	49911 → 6084 [PSH, ACK] Seq=581 Ack=1411 Min=1025 Len=194 [TCP segment of a reassembled PDU]
71	31.133662	157.90.156.89	192.168.0.106	X11	118	Event: <unknown eventcode 125>, <unknown eventcode 58>
72	31.251963	192.168.0.106	157.90.156.89	TCP	54	49911 → 6084 [ACK] Seq=775 Ack=1475 Min=1025 Len=0
78	44.208021	157.90.156.89	192.168.0.106	X11	359	Event: <unknown eventcode 125>, <unknown eventcode 98>, <unknown eventcode 97>, <unknown eventcode 99>
79	44.244882	192.168.0.106	157.90.156.89	TCP	54	49911 → 6084 [ACK] Seq=775 Ack=1780 Min=1025 Len=0
85	48.561942	192.168.0.106	157.90.156.89	TCP	248	49911 → 6084 [PSH, ACK] Seq=775 Ack=1780 Min=1024 Len=194 [TCP segment of a reassembled PDU]
86	48.641149	157.90.156.89	192.168.0.106	X11	118	Event: <unknown eventcode 125>Event: <unknown eventcode 111>
87	48.756885	192.168.0.106	157.90.156.89	TCP	54	49911 → 6084 [ACK] Seq=969 Ack=1844 Min=1025 Len=0

Рис. 8. Пакеты, полученные с помощью Wireshark

При анализе полученных пакетов можно заметить, что идет постоянная передача информации с получателем под IP-адресом 157.90.156.89. Используя открытую информацию в Интернете, установлено, по данному IP-адресу компьютер подключается к пулу (рис. 9).

Имя	ПРОТОКОЛ IP	Активный	Злобный	Обнаружение вирусов
mine.bmpool.org	157.90.156.89	истинный	истинный	• 0%, Вирусосточка, Обзор

Рис. 9. IP адрес 157.90.156.89

Все рассмотренные вирусы работают через сетевые пулы, образец 1 и 2 майнят в пул mine.bmpool.org:6004, образец 3 и 4 майнят в пул stratum+tcp://xmr.pool.minergate.com:45560.

Нагрузка на CPU. Образец 1 нагружает CPU. Имеются 2 стадии работы: обычный режим и максимальный. При стандартной работе нагрузка на CPU в среднем составляет 50 %, но если на ПК не происходит активных действий, то нагрузка резко возрастает до 100 % (рис. 10).

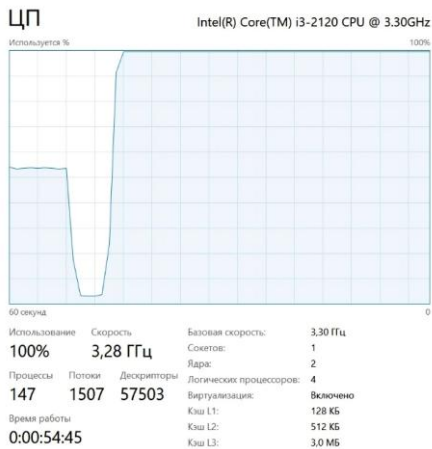


Рис. 10. Нагрузка на CPU. Образец 1

Образец 2 маскируется в Диспетчере задач, стандартный метод отображения нагрузки невозможен, воспользуемся программой AIDA64 для отображения нагрузки (рис. 11).

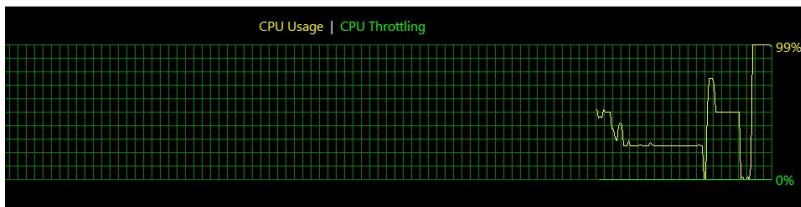


Рис. 11. Нагрузка на CPU. Образец 2

Образец 3 нагружает компьютер не на всю мощность, чтобы пользователь не заметил ухудшения производительности компьютера.

Образец 4 поддерживает нагрузку на Центральный процессор около 40 %, что также является незаметным для обычного пользователя.

Исходя из проведенного динамического исследования, можно сделать следующие выводы:

- половина исследуемых вирусов-майнеров добавляет себя в автозапуск, тем самым запуская вредоносную активность при каждом включении компьютера;
- абсолютно все исследуемые вирусы-майнеры маскируются под легальные программы и процессы;
- вирусы-майнеры могут добавлять себя в автозагрузку, используя ветки реестра и папку AppData;
- все исследуемые вирусы-майнеры подключаются к сетевому пулу для добычи криптовалюты;
- все исследуемые вирус-майнеры нагружают центральный процессор.

Библиографический список

1. Кокоулин А.Н., Опутин Н.Е., Игнатъев П.Н. Анализ характерных признаков вирусов майнеров с помощью статистической оценки базы вирусов DR.WEB // Автоматизированные системы управления и информационные технологии. – 2021. – № 2. – С. 342–348.

2. Слесарев Ю.Н., Трешин Н.И. Недостатки известных антивирусов, способы защиты от вирусов шифровальщиков // XXI век: итоги прошлого и проблемы настоящего плюс – 2019. – № 3. – С. 72–79.

3. Нысанбаева С.Е., Нюсупов А.Т., Манас Ж.Б. Создание инструмента для выявления сетевых вирусов-майнеров на основе криптовалюты монего // Проблемы оптимизации сложных систем. – 2018. – С. 113–119.

4. Тремяскина А.А. Облачные антивирусы как объект дополнительной безопасности // Современные тенденции в науке, технике, образовании. – 2019. – С. 94–97.

5. Малахов М.А., Мельников Ю.С. Защита конечных точек: антивирусы // Информационные технологии в науке, бизнесе и образовании. – 2020. – С. 165–170.

Сведения об авторах

Кокоулин Андрей Николаевич – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: liga_asu@mail.ru

Опутин Никита Егорович – магистрант кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, гр. КЗИ-20-1м, Пермь, e-mail: oputin1906@mail.ru

К.М. Силичев, А.И. Тур

Пермский национальный исследовательский
политехнический университет, Пермь

**ОПРЕДЕЛЕНИЕ БЕЗОПАСНОСТИ РАЗРЕШЕНИЙ
В ПРИЛОЖЕНИЯХ НА ОПЕРАЦИОННОЙ СИСТЕМЕ ANDROID
НА ОСНОВЕ СТАТИЧЕСКОГО
АНАЛИЗА МАНИФЕСТА**

В данной работе были исследованы разрешения Android на основе статического анализа AndroidManifest файла. Определена критичность каждого разрешения и разработана формула коэффициента безопасности приложения.

Ключевые слова: Android, разрешение, оценка безопасности, статический анализ, критичность.

K.M. Silichev, A.I. Tur

Perm National Research Polytechnic University, Perm

**DETERMINATION OF SECURITY PERMISSIONS
IN APPLICATIONS ON THE ANDROID OPERATING SYSTEM,
BASED ON STATIC ANALYSIS OF THE MANIFEST**

In this paper, android permissions were investigated based on the static analysis of the AndroidManifest file. The criticality of each resolution is determined and a formula for the application's security coefficient is developed.

Keywords: Android, permission, security assessment, static analysis, criticality.

Мобильные приложения стали неотъемлемой частью нашей повседневной жизни. Мы общаемся при помощи мессенджеров, переводим деньги через онлайн-банкинг, работаем удаленно через бизнес-приложения, и это лишь малая часть возможностей, которые стали доступны нам благодаря мобильным устройствам. Люди с удовольствием устанавливают мобильные приложения и предоставляют приложениям все запрашиваемые ими разрешения, но редко задумываются о безопасности своих личных данных.

Используя методы статического анализа на AndroidManifest-файлы, были обнаружены самые часто использованные разрешения в android-приложениях, и на основе полученных данных была разработана таблица критериев безопасности.

В качестве критериев безопасности были использованы:

- 1) название разрешения, которое объявлено в элементе «permission» в файле AndroidManifest.xml;
- 2) критичность разрешений, были определены на основе потенциальной угрозы местоположению, настройке устройства, доступа к контактам, SMS-сообщениям, камере и т.д.;
- 3) количество приложений в телефоне с соответствующими разрешениями;
- 4) частота встречаемости разрешения во вредоносных приложениях.

Критерии безопасности

Название разрешения	Критичность	Количество приложений	Частота встречаемости во вредоносных приложениях
INTERNET	Высокая	122	0,9621
READ_PHONE_STATE	Высокая	69	0,9838
ACCESS_NETWORK_STATE	Низкая	121	0,7996
WRITE_EXTERNAL_STORAGE	Высокая	86	0,7466
SEND_SMS	Высокая	10	0,5507
RECEIVE_BOOT_COMPLETED	Низкая	123	0,4961
ACCESS_WIFI_STATE	Низкая	90	0,4616
WAKE_LOCK	Низкая	101	0,3949
RECEIVE_SMS	Низкая	11	0,3874
READ_SMS	Высокая	11	0,3778
ACCESS_COARSE_LOCATION	Низкая	47	0,3458
ACCESS_FINE_LOCATION	Высокая	48	0,3205
VIBRATE	Низкая	82	0,2988
READ_CONTACTS	Средняя	30	0,2402
WRITE_SMS	Средняя	6	0,2244
CHANGE_WIFI_STATE	Низкая	48	0,1803
INSTALL_PACKAGES	Средняя	6	0,1493
GET_TASKS	Низкая	35	0,1478
RESTART_PACKAGES	Низкая	6	0,1361
CALL_PHONE	Средняя	17	0,1336
WRITE_SETTINGS	Высокая	56	0,1235
ACCESS_LOCATION_EXTRA_COMMANDS	Низкая	1	0,1113
WRITE_APN_SETTINGS	Высокая	4	0,1016
WRITE_CONTACTS	Средняя	14	0,0983
SET_WALLPAPER	Низкая	13	0,0954

Используя полученные данные из таблицы, была разработана формула расчёта коэффициента безопасности android-приложения:

M_j – частота встречаемости разрешения во вредоносных приложениях;

$M_i = M_j + 1$ – коэффициент встречаемости во вредоносных приложениях;

C_j – Критичность разрешения:

1) низкая критичность равна 0,2;

2) средняя критичность равна 0,5;

3) высокая критичность равна 1.

j – количество разрешений в android-приложении.

$$K = \frac{(C_1 \cdot M_1) + (C_2 \cdot M_2) + \dots + (C_j \cdot M_i)}{j} \cdot 100 \%$$

Пример использования формулы:

в приложении «FM-радио» используются 3 разрешения:

1) ACCESS_NETWORK_STATE, критичность = 0,2, частота встречаемости во вредоносных приложениях = 0,9838;

2) INTERNET, критичность = 1, частота встречаемости во вредоносных приложениях = 0,9621;

3) WAKE_LOCK, критичность = 0,2, частота встречаемости во вредоносных приложениях = 0,3949.

$$K = \frac{(0,2 \cdot 1,9838) + (1 \cdot 1,9621) + (0,2 \cdot 1,3949)}{3} \cdot 100 \% = 87,9 \%$$

Коэффициент опасности приложения равен 87,9 %, из-за большого полученного коэффициента это приложение является небезопасным.

Используя данную формулу, можно с большей вероятностью определить, является ли приложение безопасным или небезопасным, чем ниже полученный результат, тем приложение считается более безопасным.

Библиографический список

1. Kumar Ajit, Kuppusamy K.S., Aghila G. FAMOUS: Forensic Analysis of MOBILE devices Using Scoring of application permissions. – 2018.

2. Mohd Faizal Ab Razak, Nor Badrul Anuar, Rosli Salleh, Ahmad Firdaus, Muhammad Faiz, Hammoudeh S. Alamri // Less Give More: Evaluate and zoning Android applications. – 2019.

3. Anshul Arora, Sateesh K. Peddoju, Senior Member, Mauro Conti, Senior Member. PermPair: Android Malware Detection Using Permission Pairs. – 2019.

Сведения об авторах

Силичев Кирилл Михайлович – студент Пермского национального исследовательского политехнического университета, гр. КОБ-17-1с, Пермь, e-mail: silichev.72k@mail.ru

Тур Александр Игоревич – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: tur.aleksandr93@mail.ru

Н.Ю. Соболев, Л.А. Клейман

Пермский национальный исследовательский
политехнический университет, Пермь

ИССЛЕДОВАНИЕ АТАК ТИПА «ОТКАЗ» В ОБСЛУЖИВАНИИ

Атаки типа «отказ» в обслуживании (DoS) стали серьезной угрозой для существующих компьютерных сетей. DoS-атаки классифицируются в соответствии с их основными характеристиками. Чтобы лучше понять DoS-атаки, в этой статье представлен обзор существующих DoS-атак по уровням сетевой модели взаимодействия открытых систем (OSI). В частности, методы DoS-атак описываются на основе системы клиент-сервер, чтобы отобразить основные принципы атаки.

Ключевые слова: отказ в обслуживании, распределенный отказ в обслуживании, сети, модель OSI, HTTP-флуд.

N.Y. Sobolev, L.A. Kleiman

Perm National Research Polytechnic University, Perm

DENIAL OF SERVICE ATTACKS RESEARCH

Denial of service (DoS) attacks have become a serious threat to existing computer networks. DoS attacks are classified according to their main characteristics. To better understand DoS attacks, this article provides an overview of existing DoS attacks by layers of the Open Systems Interconnection (OSI) network model. In particular, DoS attack techniques are described on a client-server basis to reflect the underlying principles of an attack.

Keywords: denial of service, distributed denial of service, networks, OSI model, HTTP flood.

Интернет стремительно превращается в рынок услуг с очень большим оборотом денежных средств. Сбой или недоступность информационного сервера влечет огромные финансовые потери для любой организации. В последнее время стала особенно актуальной проблема атак типа «отказ» в обслуживании (DoS).

Поскольку простые в использовании инструменты DoS можно легко загрузить из Интернета, обычные пользователи компьютеров также могут стать атакующими DoS [1]. Однако злоумышленнику сложно перегрузить ресурс, используя лишь один компьютер.

Многие недавние DoS-атаки были запущены через большое количество распределенных атакующих хостов в Интернете. Эти атаки называются распределенными атаками типа «отказ» в обслуживании (DDoS).

Распределенные атаки. В случае DDoS-атаки, поскольку агрегация атакующего трафика может быть огромной по сравнению с ресурсом жертвы, атака может вынудить жертву значительно снизить производительность своего сервиса или даже прекратить предоставление какой-либо услуги.

Например, в феврале 2018 г. официальный сайт оргкомитета зимних Олимпийских игр в Пхенчхане был вынужден приостановить доступ во время зимних Олимпийских игр из-за DDoS-атаки [2]; в марте 2018 г. GitHub подвергся DDoS-атаке с максимальным пиковым трафиком 1,7 TBPS [3]; в октябре 2019 г. сервисы Amazon Web Services подверглись атаке DDoS на несколько часов, что привело к отключению многих веб-сайтов организации [4].

Чтобы понять принцип работы DoS/DDoS-атак, необходимо определить их цели и возможные воздействия, после чего провести классификацию.

Цели и возможные воздействия атак. Хотя большинство DoS/DDoS-атак работает с исчерпанием ресурсов, реальная цель отказа в обслуживании варьируется [5]. Целью может быть серверное приложение, доступ к сети или сетевая инфраструктура, как представлено в табл. 1.

Таблица 1

Возможные цели атак и их реализация

Цель	Реализация атаки
Серверное приложение	Атака нацелена на данное серверное приложение жертвы, таким образом не позволяя легитимным клиентам использовать службу, а также ограничивая ресурсы хост-машины. При атаке может отправляться большой объем запросов аутентификации, чтобы исчерпать ресурсы жертвы и таким образом вывести службу из строя
Доступ к сети	Атака блокирует доступ к компьютеру или сети жертвы, вырабатывается ее сбой или перегрузка механизма связи. Все атакующие пакеты несут адрес назначения целевого хоста без учета содержимого целевой службы. Большой объем пакета потребляет сетевые ресурсы жертвы
Сетевая инфраструктура	Атака на сетевую инфраструктуру нацелена на некоторые критически важные службы, которые имеют решающее значение для работы глобального Интернета. Ключевой особенностью этих атак является не механизм атаки, а цель атаки и влияние атаки

В зависимости от воздействия DoS/DDoS-атаки классифицируются как разрушительные и с понижением качества. Возможные воздействия атак представлены в табл. 2.

Таблица 2

Возможные воздействия атак

Воздействие	Описание
Разрушительные атаки	Главное направление таких атак - полностью остановить работу службы жертвы или вывести ее из строя. Например, сеть жертвы полностью перегружена при атаке или сервер жертвы выходит из строя или останавливается при атаке
Атаки с понижением качества	Главное направление таких атак - использование некоторой части ресурсов жертвы для серьезного снижения производительности службы. Например, атака отправляет большой объем запросов аутентификации, которые могут значительно потреблять вычислительные ресурсы на целевом сервере

Данные разграничения DoS/DDoS-атак позволяют более точно определить вектор направления атаки на потенциальных жертв от возможных злоумышленников.

Классификация атак по уровням OSI. Сегодня существует множество вариантов организации DoS/DDoS-атак. Они различаются характеристиками паразитного трафика. OSI – это семиуровневая эталонная модель, которая описывает схему взаимодействия сетевых устройств.

Если рассматривать DoS/DDoS-атаки в контексте OSI, то можно обнаружить, что данный тип атак возможен на любом из уровней сетевой модели [6]. Виды DoS/DDoS-атак по уровням OSI представлены на рис. 1.

Несмотря на то, что DoS/DDoS-атаки возможны на любом из семи уровней OSI, наиболее часто реализуемые атаки встречаются на сетевом и транспортном уровнях, а также на прикладном уровне. Далее проведем реализацию одной из определенных атак, чтобы отобразить ее основные принципы.

Реализация атаки. В качестве примера рассмотрим DDoS-атаку HTTP-флуд посредством GET- и POST-запросов на прикладном уровне OSI.

Цель атаки – серверное приложение, воздействие разрушительное.

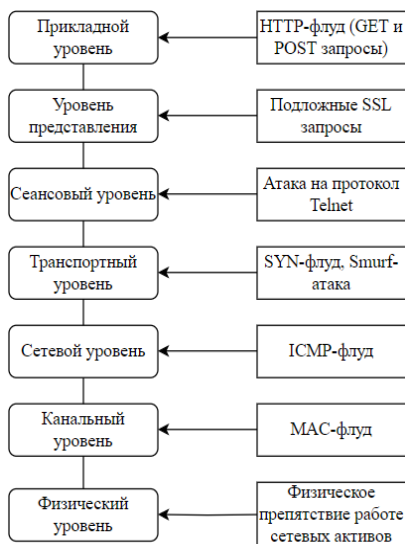


Рис. 1. Виды DoS/DDoS-атак по уровням OSI

HTTP-флуд – атака, направленная на истощение ресурсов приложения, в данном случае веб-сервера. Злоумышленник выполняет HTTP-запросы одновременно с нескольких ботов, имитирующих реальных пользователей, которые обращаются к серверу. Для ответов каждому из ботов необходимо использование большого объема памяти и вычислительной мощности сервера.

Для реализации данной атаки нам потребуется развернуть HTTP-сервер, а также использовать необходимый инструмент для отправки запросов непосредственно на этот сервер.

Необходимые средства для реализации атаки HTTP-флуд представлены в табл. 3.

Таблица 3

Средства для реализации атаки HTTP-флуд

№ п/п	Средство	Описание
1	Web Tours Sample Application	HTTP-сервер с программным кодом из открытых источников разворачивается локально на вычислительной машине
2	Apache JMeter 5.4.1	Инструмент нагрузочного тестирования для генерации виртуальных потоков (пользователей), которые отправляют необходимые запросы на сервер

Технические характеристики локального HTTP-сервера:

– процессор Intel Core i7-4710HQ CPU 2.5 GHz;

– оперативная память Crucial 8 GB 2600 MHz DDR4 Unbuffered DIMM;

– жесткий диск HGST 1 TB 7.2k SATA 6Gbps HDD HS 2.5”.

Проведем два независимых друг от друга эксперимента, цель которых – довести HTTP-сервер до состояния отказа в обслуживании. Также необходимо оценить степень обработки ошибок, которые возникнут на сервере. Исходные данные для экспериментов представлены в табл. 4.

Таблица 4

Исходные данные для экспериментов

№ п/п	Начальное число клиентов	Конечное число клиентов	Интервал добавления новых клиентов	Добавочное время после конечного числа клиентов, с	Время эксперимента, с
1	5	45	10 клиентов каждые 15 с	10 с	70
2	10	150	10 клиентов каждые 5 с	30 с	100

В качестве запросов GET выступают запросы на получение информации о странице сайта, в качестве запросов POST – запросы авторизации на сайте.

В результате первого эксперимента был получен график среднего числа операций в секунду, который представлен на рис. 2.



Рис. 2. График среднего числа операций в секунду во время первого эксперимента

По данному графику видно, что сервер дал ответ на каждый из запросов 45 виртуальных клиентов, ошибок при обработке запросов не произошло.

Также был получен график загрузки процессора сервера в реальном времени, представленный на рис. 3.

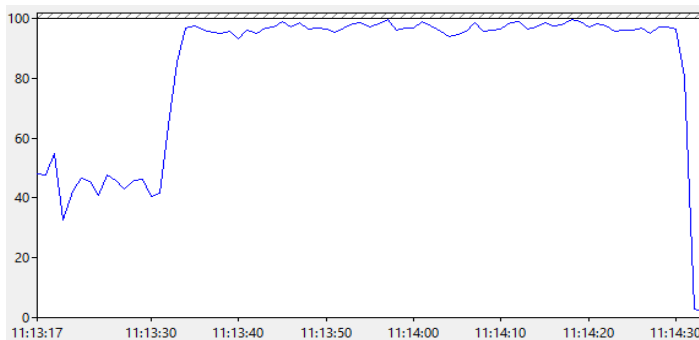


Рис. 3. График загрузки процессора сервера (%) в реальном времени при первом эксперименте

По данному графику видно, что отказа в обслуживании не произошло, сервер функционировал все 70 с, отведенных на проведение эксперимента.

Теперь увеличим число виртуальных пользователей и скорректируем время. В результате второго эксперимента был получен график среднего числа операций в секунду, который представлен на рис. 4.

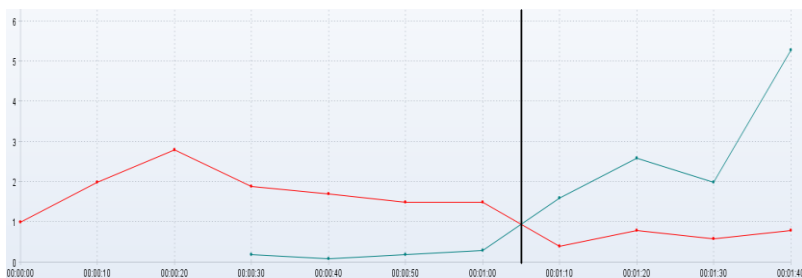


Рис. 4. График среднего числа операций в секунду во время второго эксперимента

По данному графику видно, что ошибки начали появляться после 30 с эксперимента, а после 65 с сервер стал обрабатывать в секунду больше ошибок, чем запросов, поэтому произошел отказ в обслуживании HTTP-сервера.

Также был получен график загрузки процессора сервера в реальном времени, представленный на рис. 5.

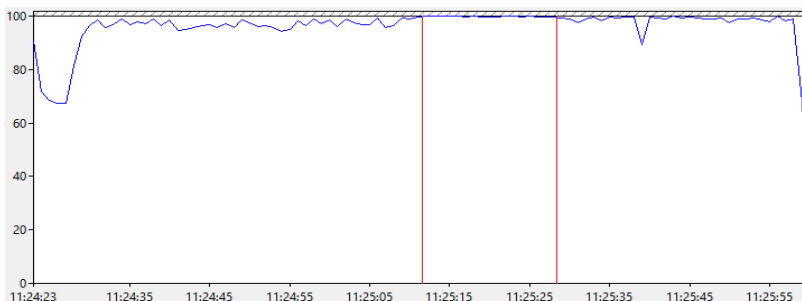


Рис. 5. График загрузки процессора сервера (%) в реальном времени при втором эксперименте

На данном графике видно, что отказ в обслуживании происходил между 49-й и 65-й секундой эксперимента, загрузка процессора сервера была равна 100 %.

Таким образом, цель экспериментов была достигнута.

Заключение. В этой статье были рассмотрены существующие DoS/DDoS-атаки, их цели и возможные воздействия. Была проведена реализация DDoS-атаки HTTP-флуд посредством GET- и POST-запросов, в результате которой веб-сервер полностью отказал в обслуживании на некоторый промежуток времени.

Чтобы защититься от DoS/DDoS-атак, необходимо тестировать сетевые ресурсы на отказоустойчивость, проводить эксперименты с различным количеством потенциальных пользователей, оценивать риски отказа в обслуживании сетевых ресурсов.

Библиографический список

1. DoS и DDoS атаки [Электронный ресурс]. – URL: <https://www.iseo.ru/seo-wiki/dos-ataka/> (дата обращения: 18.12.2021).
2. Sharwood S. Winter olympics website downed by cyber attack. – 2018.
3. Ranger S. GitHub hit with the largest DDoS attack ever seen. – 2018.
2. Arboleda N. AWS hit by DDoS attack dragging half of web down. – 2019.

3. Хлестова Д.Р., Редников Д.В. DDoS-атаки, как средства конкурентной борьбы // Символ науки. – 2017. – № 3. – С. 128–130.

4. DDoS-атаки: типы атак и уровни модели OSI [Электронный ресурс]. – URL: <https://firstvds.ru/technology/types-of-ddos> (дата обращения: 20.12.2021).

Сведения об авторах

Соболев Никита Юрьевич – магистрант кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, гр. ТК5-20-1м, Пермь, e-mail: sobolevn2310@gmail.com

Клейман Лев Александрович – аспирант, младший научный сотрудник кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: smarttty@yandex.ru

В.Д. Симонов, А.И. Тур

Пермский национальный исследовательский
политехнический университет, Пермь

РАЗРАБОТКА МОДЕЛИ ОЦЕНКИ БЕЗОПАСНОСТИ МАРШРУТИЗАТОРА Wi-Fi

В данной статье описывается модель оценки безопасности маршрутизатора Wi-Fi. В ее основе лежат анализ и оценке критериев защиты маршрутизатора Wi-Fi и их влияние на уровень защищенности маршрутизатора.

Ключевые слова: модель, безопасность, критерий, маршрутизатор, коэффициент безопасности.

V.D. Simonov, A.I. Tur

Perm National Research Polytechnic University, Perm

DEVELOPMENT OF A SECURITY ASSESSMENT MODEL FOR A Wi-Fi ROUTER

In this article describes a model for assessing the security of a Wi-Fi router. She is based on the analysis and assessment of the protection criteria of a Wi-Fi router and their impact on the security level of the router.

Keywords: model, safety, criterion, router, safety factor.

Сегодня маршрутизаторы Wi-Fi встречаются повсеместно, но недостаточное внимание уделяется их защищенности. Если маршрутизатор не является безопасным, все устройства, подключенные к сети, станут уязвимыми: смартфон, ноутбук и т.д.

Угрозы, связанные с атаками на роутеры, в настоящее время актуальны для многих. Эксперты Института открытых систем связи им. Фраунгофера [1] проанализировали 127 моделей домашних роутеров 7 разных производителей. Исследование показало, что даже самые лучшие устройства имели, по крайней мере, 21 критическую уязвимость и, по крайней мере, 348 с высокой степенью серьезности. В среднем у маршрутизаторов были 53 критических уязвимости.

Пользователи считают, что их сеть никому не интересна, в том числе злоумышленникам, и поэтому многие пренебрегают рекомендациями настройки безопасности своей сети, а также настройками маршрутизатора.

Правильная настройка безопасности может уберечь как от кражи персональных данных, так и от случайных действий пользователей сети. Злоумышленники могут что-то изменить в настройках, тем самым нарушить ее нормальную работу и оставить пользователя без Интернета.

К основным уязвимостям маршрутизаторов относятся:

- старая версия ОС в маршрутизаторе;
- стандартный пароль для входа в настройки роутера;
- устаревшая прошивка маршрутизатора;
- неправильная настройка маршрутизатора;
- открытые порты.

Действия, которые может совершить злоумышленник в результате нахождения уязвимостей в маршрутизаторе [2]:

- мониторинг сетевого трафика;
- перенаправление сетевого трафика;
- блокирование пользователей;
- использование маршрутизатора в качестве промежуточной точки для осуществления более глубокой атаки.

Исходя из вышеизложенного, становится очевидным, что большинство беспроводных маршрутизаторов Wi-Fi не обеспечивают надлежащую степень защиты. Вопросы безопасности роутера не рассматриваются на должном уровне производителями, а также пользователями.

Описание модели. Предлагаемая модель базируется на последовательной оценке критериев защиты маршрутизатора Wi-Fi (рисунок). Критерии носят разносторонний характер и позволяют оценить как безопасность самого устройства, так и канала передачи информации, реализуемого им.



Рис. Концептуальная модель оценки безопасности маршрутизатора

Коэффициент безопасности (K) – это коэффициент, отражающий состояние защищённости системы, достигнутое с помощью отдельно взятой конфигурации настроек маршрутизатора. В табл. 1 приведены значения коэффициента безопасности (K).

Таблица 1

Значения коэффициента безопасности

Коэффициент безопасности (К)	0-0,3	0,4-0,6	0,7-1
Уровень безопасности	Низкий уровень безопасности	Средний уровень безопасности	Высокий уровень безопасности

Для расчета коэффициента безопасности, рассматривается отдельно взятый критерий маршрутизатора и анализируется его влияние на безопасность. В табл. 2 и 3 приведены значения К для критериев маршрутизатора.

Таблица 2

Значение К для пароля

Номер критерия (i)	Название критерия	Не соответствует требованиям	Соответствует требованиям
1	Пароль для доступа к настройке маршрутизатор	0,3	0,8
2	Пароль для доступа к Wi-Fi сети	0,3	0,8

С требованиями, предъявляемыми к паролю, можно ознакомиться на сайте Microsoft [3].

Таблица 3

Значение К для критериев маршрутизатора

Номер критерия (i)	Название критерия	Не используется	Используется
3	Firewall	0,3	0,8
4	Удаленное подключение к маршрутизатору	0,9	0,2
5	Фильтрация MAC-адреса	0,3	0,6
6	Обновление ПО	0,2	0,8
7	Проверка на наличие сторонних устройств	0,3	0,6
8	Задействованы только необходимые сетевые службы и порты	0,3	0,8
9	Актуальная версия сетевого шифрования	0,2	0,7

Безопасность маршрутизатора (В) определяется суммированием коэффициентов безопасности и делением на количество критериев

(n) маршрутизатора (1). По табл. 4 необходимо сопоставить полученный результат с уровнем безопасности маршрутизатора:

$$B = \frac{\sum_{i=1}^n K_i}{n}.$$

Таблица 4

Оценка безопасности маршрутизатора

Безопасность маршрутизатора (B)	0,0-0,3	0,4-0,6	0,7-1
Уровень безопасности маршрутизатора	Низкий уровень безопасности	Средний уровень безопасности	Высокий уровень безопасности

Предложенная модель ориентирована на пользователей домашней сети. Именно такому сегменту, как домашняя сеть, уделяется недостаточно внимания с точки зрения информационной и сетевой безопасности. Модель позволяет простому пользователю, не обладающему знаниями в области сетевой безопасности, оценить безопасность своего маршрутизатора Wi-Fi, а также повысить уровень его защищенности до необходимого.

Библиографический список

1. Peter Weidenbach, Johannes vom Dorp. Home Router Security Report 2020 // Fraunhofer FKIE. – 2020.

2. Белова Т.С., Ключко О.С. Безопасность данных, передаваемых по сети Wi-Fi // Электронный журнал: наука, техника и образование. – 2016. – № 4(9). – С. 54–61.

3. Справка Windows. Безопасность. Защита от угроз. Пароль должен соответствовать требованиям к сложности [Электронный ресурс]. – URL: <https://docs.microsoft.com/ru-ru/windows/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements> (дата обращения: 10.11.2021).

Сведения об авторах

Симонов Владимир Дмитриевич – студент Пермского национального исследовательского политехнического университета, Пермь, e-mail: simonov_vovchik@mail.ru

Тур Александр Игоревич – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: tur.aleksandr93@mail.ru

А.С. Шабуров, Т.В. Шадрина

Пермский национальный исследовательский
политехнический университет, Пермь

**О РАЗРАБОТКЕ МОДЕЛИ СИСТЕМЫ ЗАЩИТЫ
ИНФОРМАЦИИ АРМ В ОБРАЗОВАТЕЛЬНОМ
УЧРЕЖДЕНИИ В УСЛОВИЯХ ПАНДЕМИИ**

В статье рассматривается обобщенная модель средств защиты информации для обеспечения информационной безопасности информационной системы в образовательном учреждении при дистанционном обучении. Подбираются программные средства защиты информации от наиболее характерной угрозы в условиях удаленной работы в соответствии с техническими требованиями системы, сроком действия сертификата ФСТЭК и стоимостью средства.

Ключевые слова: информационная безопасность, образовательное учреждение, модель средств защиты информации.

A.S. Shaburov, T.V. Shadrina

Perm National Research Polytechnic University, Perm

**ON THE DEVELOPMENT OF A MODEL
OF THE INFORMATION SECURITY SYSTEM AWP
IN AN EDUCATIONAL INSTITUTION IN A PANDEMIC**

This article discusses a generalized model of information security tools to ensure the information security of an information system in an educational institution in the process of distance learning. Software tools are selected to protect information from the most characteristic threat in remote work conditions in accordance with the technical requirements of the system, the validity period of the FSTEC certificate and the cost of the tool.

Keywords: information security, educational institution, model of information security tools.

С развитием информационных технологий проблема обеспечения безопасности информационных систем (ИС) становится все более актуальной. Пандемия, связанная с распространением COVID-19, вынудила большое количество организаций перейти на дистанционную работу. Не являются исключением и образовательные учреждения (ОУ). В связи с переходом ОУ на дистанционную работу появились новые технологии обучения и, как следствие, возникла необхо-

димось внедрения новых средств защиты информации (СрЗИ). Если раньше журналы, отчеты, программы обучения и личные дела учеников общеобразовательных школ хранились под замком в кабинетах, то теперь всю информацию такого рода с бумажных носителей пришлось перенести на электронные.

Актуальность исследования данной проблемы заключается в том, что современное образование невозможно без использования автоматизированных ИС, особенно в условиях пандемии, при этом недостаточно внимания уделяется защите информации (ЗИ), хранящейся и обрабатываемой в таких системах.

В данной статье рассматривается вариант построения обобщенной модели системы защиты информации (СЗИ) для определения рационального состава СрЗИ в рамках конкретной ИС в условиях одной из наиболее актуальных угроз информационной безопасности. Это ограничение обусловлено требованиями к объему работы и необходимостью рассмотрения конкретной угрозы безопасности информации (УБИ) для автоматизированного рабочего места (АРМ).

Целью данной работы является разработка модели СЗИ типовой ИС ОУ от УБИ.190.

Рассматриваемая информационная система, а именно средство электронно-вычислительной техники, такое как рабочий компьютер (ноутбук) педагога, представлена на рисунке.



Рис. Автоматизированное рабочее место педагога

Технические характеристики АРМ:

- модель DELL Inspiron 3567-7879;
- операционная система Windows 10 для ОУ (x64);

- процессор Intel Core i3 6006u;
- количество ядер 2 (2ГГц);
- общий объем жестких дисков (HDD) 1 Тб;
- объем оперативной памяти 4 Гб.

С АРМ выполняется выход в Интернет для работы с такими информационными ресурсами, как ЭПОС.Школа, Траектория, Google Документы и прочие информационные ресурсы, которые хранят и обрабатывают персональные данные (ПДн) учащихся, тайну их личной жизни, ПДн самого педагога и тайну личной переписки.

Состав информации ограниченного доступа, хранящейся или обрабатывающейся на основе АРМ, приведен в табл. 1.

Таблица 1

Состав информации ограниченного доступа

Вид	Пояснения
ПДн самого педагога	Паспортные данные, логины и пароли от информационных ресурсов
Профессиональная тайна (ПДн учеников и тайна их личной жизни)	ПДн учеников: дата и место рождения, адрес проживания, паспортные данные или данные свидетельства о рождении, номера телефонов, e-mail, сведения о доходах семьи и прочие. Тайна личной жизни учеников: сведения о семье, занятиях в кружках, секциях. Сведения о методах и средствах защиты информации
Тайна переписки	Любая информация, содержащаяся в письмах электронной почты и прочих ресурсов, при помощи которых осуществляется общение педагога с директором, завучами, другими педагогами и учениками
Интеллектуальная собственность	Программы обучения, презентации к занятиям, проверочные задания, ответы на них (если таковые имеются) и прочие

К открытой информации, обрабатываемой на АРМ, относятся: ФИО работников ОУ, их должность, квалификация и образование, контактная информация (например, номер рабочего телефона и e-mail), а также ФИО учеников и этапы их обучения.

Для подобных условий обработки информации ограниченного доступа, связанных с доступом к различным открытым информационным ресурсам, наиболее характерна угроза внедрения вредоносного кода за счет посещения зараженных сайтов в Интернете (УБИ. 190).

Угроза заключается в возможности осуществления нарушителем внедрения вредоносного кода в компьютер пользователя при посещении зараженных сайтов. Нарушитель выявляет наиболее посещае-

мые пользователем сайты, затем их взламывает и внедряет в них вредоносный код. Данная угроза обусловлена слабостями мер антивирусной защиты, а также отсутствием правил межсетевое экранирования. Реализация данной угрозы возможна при неограниченном доступе пользователя в Интернет; при наличии у нарушителя сведений о сайтах, посещаемых пользователем [1]. Традиционное описание угрозы на основе БДУ ФСТЭК предполагает последовательное определение источника угрозы, объекта информационного воздействия и негативных последствий. В данном случае источником угрозы является внешний нарушитель со средним потенциалом, объектом воздействия – сетевое программное обеспечение.

Последствиями реализации угрозы являются:

- нарушение конфиденциальности (например, копирование конфиденциальной информации, внедрение шпионских программ);
- нарушение целостности (например, искажение или модификация документов, хранящихся в файловой системе, ошибки в фрагментах программного кода);
- нарушение доступности (например, сбои в работе некоторых компонентов компьютера, внедрение рекламного программного обеспечения, внедрение вируса-шифровальщика, получение удаленного доступа к компьютеру).

К способам реализации угрозы можно отнести:

- переход пользователя по ссылке, ведущей на страницу, на которую помещены вредоносный файл и скриптовая программа, эксплуатирующая браузерную уязвимость (пользователь привлекается на страницу при помощи рассылки спам-сообщений или через поисковые системы);
- скачивание пользователем нелегального программного обеспечения, в которое встроен вредоносный код;
- переход пользователя на фишинговый сайт, ссылка на который может быть получена как путем рассылки, так и через поисковую систему (как правило, нарушитель использует уязвимости самого сайта, например, для подмены форм для заполнения).

Под техническими мерами защиты от УБИ.190 в ОУ подразумевается использование технических средств, препятствующих нанесению ущерба ОУ посредством несанкционированного доступа и блокирующих утечку информации по техническим каналам. Существует множество требований к обеспечению безопасности информации, их

реализация может быть достигнута различными способами. Отсюда следует проблема выбора тех или иных средств на основе определенных критериев.

Применительно к задаче выбора СрЗИ АРМ в ОУ целесообразно учесть принцип разумной достаточности, основанный не только на надежности защиты ИС, но и на технических характеристиках устройства, а также экономическую целесообразность. При этом средства должны быть сертифицированы, а также соответствовать иным требованиям безопасности АРМ, предполагающим применение программных СрЗИ.

Надежность ЗИ оценивается по приращению вероятности ее защиты Δp_i и по приращению времени доступа к ресурсам Δt_i из-за необходимости преодоления рубежей безопасности. Параметром системы также может быть ее стоимостная характеристика c_i . Таким образом, СЗИ, характеризующуюся рядом параметров, можно представить в виде формулы [2]:

$$F_i = (\Delta p_i, \Delta t_i, \Delta c_i), \quad i = \overline{1, m}. \quad (1)$$

Таким образом, поиск оптимального набора СрЗИ осуществляется на основе многокритериальной оптимизации. В случае многокритериальной оптимизации, применение которой имеет смысл тогда, когда ухудшение по одному из параметров, например c_i , приводит к улучшению по другим параметрам, имеет смысл задача целочисленного программирования с несколькими целевыми функциями. В результате решения подобной задачи должен быть определен оптимальный выбор структуры СЗИ.

В качестве критериев оптимизации могут быть выбраны основные характеристики технических средств защиты информации, например, средств антивирусной защиты.

В табл. 2 приведены некоторые программные средства антивирусной защиты информации для АРМ, предназначенного для дистанционной работы. Подбор осуществился на основе технических характеристик (критериев) устройства и сроке действия сертификата ФСТЭК. Для составления данной таблицы использовались государственный реестр сертифицированных СрЗИ, размещенный на сайте ФСТЭК, а также актуальная стоимость каждого средства.

Таблица 2

Средства антивирусной защиты

Наименование	№ сертификата	Срок действия	Стоимость годовой подписки на 2021 год
Dr.Web Enterprise Security Suite	3509	27.01.2024	от 2 000 руб.
Kaspersky Endpoint Security для Windows (версия 11.6.0.394)	4068	22.01.2024	от 1 320 руб.
Kaspersky Web Traffic Security 6.1	2474	24.10.2025	от 1 800 руб.
Secret Net Studio	3745	16.05.2025	от 1 500 руб.
ESET NOD32 Secure Enterprise Pack (версия 6)	4216	04.02.2025	от 2 725 руб.

Так как угроза внедрения вредоносного кода за счет посещения зараженных сайтов в Интернете обусловлена не только слабостями антивирусной защиты, а нарушитель со средним потенциалом способен сам создавать методы и средства реализации угрозы, разумно будет также рассмотреть и межсетевое экранирование.

В табл. 3 приведены некоторые программные межсетевые экраны, подходящие для рассматриваемого АРМ.

Таблица 3

Средства межсетевого экранирования

Наименование	№ сертификата	Срок действия	Стоимость годовой подписки на 2021 год
Symantec Endpoint Protection (версия 14)	3959	13.12.2023	от 3 396 руб.
Kerio Control	4323	10.11.2025	от 2 000 руб.
ViPNet Personal Firewall 4.5	4173	08.10.2024	от 430 руб.

Исходя из табл. 2 и 3, можно выбрать наиболее выгодные средства по защите рабочего компьютера педагога от УБИ.190 – это средство антивирусной защиты Kaspersky Endpoint Security для Windows (версия 11.6.0.394) и средство межсетевого экранирования ViPNet Personal Firewall 4.5.

Таким образом, в данной статье была разработана модели СЗИ типовой ИС ОУ, такой как АРМ педагога, от наиболее характерной в условиях дистанционного обучения угрозы, взятой из банка угроз ФСТЭК, а именно УБИ.190. СрЗИ выбирались из государственного реестра сертифицированных СрЗИ ФСТЭК на основании экономической целесообразности и в соответствии с техническими характеристиками АРМ, а также с учетом действительности сертификата. Стоит отметить, что в связи с неопределенным сроком окончания пандемии и развитием технологий образование все сильнее будет зависеть от информационных систем, их безопасности и надежности, что дает повод для дальнейшей работы в этой области.

Библиографический список

1. Банк данных угроз безопасности информации ФСТЭК [Электронный ресурс] // Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет. – URL: <https://bdu.fstec.ru/threat/ubi.190> (дата обращения: 10.10.2021).
2. Шабуров А.С., Миронова А.А. О повышении эффективности защиты персональных данных в информационных системах открытого типа. – Пермь: Изд-во Перм. нац. исслед. политехн. ун-та, 2015. – 7 с.

Сведения об авторах

Шабуров Андрей Сергеевич – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, e-mail: shans@at.pstu.ru

Шадрина Татьяна Владимировна – студентка Пермского национального исследовательского политехнического университета, гр. КЗИ-19-1б, Пермь, e-mail: shanyat@mail.ru

СОДЕРЖАНИЕ

Секция 1. НОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ	3
Аношкин А.Н., Мурзакаев Р.Т., Кашин О.А. Построение развертки срединных поверхностей слоёв армирующего материала	4
Баранов П.С., Тарутин А.В., Щапов В.А. Исследование процессов поиска мероприятий	12
Жуланов В.Н. Применение градиентного спуска для обучения модели машинного обучения	16
Закиров Р.Ф., Тарутин А.В. Использование систем учета и анализа успеваемости в образовательном процессе	22
Кильдебаяев А.Н., Архипов А.В., Тарутин А.В. Визуализация встроенных типов объектов платформы «GreenData»	29
Максимцов В.С., Широков А.А. Разработка методологии тестирования программного обеспечения	33
Борзунов Г.И., Новикова П.А. Визуальное моделирование при подготовке и реализации дизайн-проектов с использованием стеклярусообразных элементов	40
Хохряков Д.С., Тарутин А.В. Исследование протоколов webRTC	47
Шмелев П.Ю., Прозорова Л.Ю. Основные вопросы разработки систем хранения связей между сервисами	52
Секция 2. АВТОМАТИЗАЦИЯ И УПРАВЛЕНИЕ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ И ПРОИЗВОДСТВАМИ	55
Андриевская Н.В., Рассада С.Л. Идентификация нестационарных объектов управления	56
Белов И.А., Дыкий А.Д. Автоматизация и управление технологическими процессами в энергетике	62
Васенин И.А., Гончаровский О.В. Применение протокола Modbus в распределенных системах управления на базе робототехнических систем и комплектов компании «Промобот»	66
Даденков Д.А., Белькевич К.С. Обзор методов для реализации системы автоматического управления абсорбцией формальдегида	74

Косачёв А.Д., Широков А.А. Разработка методики прогнозирования аварийных ситуаций для химически опасных объектов	82
Крамер Д.Е., Чабанов Е.А. Использование роботов-манипуляторов в автоматизации процессов производства. Перспективы развития	88
Трушников Е.С., Жуков Я.А., Билоус О.А. Модернизация АСУ ТП паровой котельной	94
Секция 3. ИННОВАЦИОННЫЕ НАПРАВЛЕНИЯ В ЭНЕРГЕТИКЕ. ЭНЕРГОРЕСУРСОСБЕРЕЖЕНИЕ	99
Быков С.Н., Лыкасов П.В., Лейзгольд Д.Ю. Повышение энергоэффективности и снижение количества выбросов загрязняющих веществ	100
Ведерников Д.А., Чабанов Е.А., Чабанова Е.В. Перспективность использования светодиодных светильников перед люминесцентными	106
Зайцев К.Г., Полихов А.С., Чабанов Е.А.	
Искусственные мышцы	115
Конев К.А., Фурин А.О., Чабанов Е.А. Замена электрического двигателя в отбойном молотке	122
Константинов М.А., Чабанов Е.А. Улучшение работы и производительности станка при совмещении ЧПУ фрезера, 3D-принтера и лазерного гравера	129
Секция 4. ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ И СЕТИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ	135
Букирева Ю.М. Стратегия доступа к корпоративным сетям с применением модели нулевого доверия	136
Головнин И.В., Гаврилов А.В. Применение автономных датчиков при работе в стандарте NB-IoT на примере нефтедобывающего предприятия	142
Дубовикова М.А., Гаврилов А.В. Исследование mesh-сетей в симуляторе OMNET++	149
Еленкин Д.А., Еленкина И.Ф. Использование бинарной свёрточной нейронной сети для анализа тональности текста	154
Еремеев А.Н., Тур А.И. Исследование эффективности использования нескольких антивирусов на основе базы вирусов для тестирования антивирусов	160

Зверев А.В. Методы балансировки нагрузки агрегированных портов коммутатора	163
Коноваленко О.А., Клейман Л.А. Моделирование ТСП сервера и клиента	168
Мудрый Р.А., Гаврилов А.В. Анализ и сравнение протоколов управления в среде Интернета вещей	176
Обыденнов А.К., Южаков А.А. Машинный пентест как новый этап VAPT	183
Кокоулин А.Н., Опутин Н.Е. Анализ характерных признаков вирусов майнеров с помощью динамической оценки	189
Силичев К.М., Тур А.И. Определение безопасности разрешений в приложениях на операционной системе Android на основе статического анализа манифеста	196
Соболев Н.Ю., Клейман Л.А. Исследование атак типа «отказ» в обслуживании	200
Симонов В.Д., Тур А.И. Разработка модели оценки безопасности маршрутизатора Wi-Fi	208
Шабуров А.С., Шадрин Т.В. О разработке модели системы защиты информации АРМ в образовательном учреждении в условиях пандемии	212

Научное издание

**ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ: ТЕОРИЯ,
ИНСТРУМЕНТЫ, ПРАКТИКА**

Материалы XIII Международной
интернет-конференции молодых ученых,
аспирантов, студентов
(16 ноября – 31 декабря 2021 г.)

Корректор *И.Н. Жеганина*

Подписано в печать 08.06.2022.
Формат 60×90/16. Усл. печ. л. 13,87.
Тираж 100 экз. Заказ 104/2022.

Издательство
Пермского национального исследовательского
политехнического университета.
Адрес: 614990, г. Пермь, Комсомольский пр., 29, к. 113.
Тел. (342) 219-80-33.